

**Министерство образования и науки Республики Казахстан
Евразийский национальный университет им. Л.Н.Гумилева
Институт информационной безопасности и криптологии**



СБОРНИК ТРУДОВ

**III Международной научно-практической конференции
«Информационная безопасность в свете Стратегии Казахстан - 2050»**

15-16 октября 2015 года, г. Астана

УДК 004 (063)

ББК 32.973

С23

Рецензенты:

1. Е.Н. Сейткулов, к.ф.-м.н., директор института информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева
2. Н.Н.Ташатов, к.ф.-м.н., заведующий лабораторией кодирования и защиты информации информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева

С23 Сборник трудов III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан-2050», 2015. – 400 стр.

ISBN 978-9965-31-722-4

Сборник подготовлен по материалам III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан - 2050». Тематика сборника охватывает такие вопросы, как проблемы обеспечения информационной безопасности в государственных и бизнес структурах, информационная безопасность компьютерных систем, математические проблемы защиты информации. Представлены результаты научных исследований, проведенных в вузах и научно-исследовательских организациях Казахстана, России, Белоруссии и др.

УДК 004 (063)

ББК 32.973

Утверждено и рекомендовано к изданию научно-техническим советом института информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева. Протокол № 2 от 19 сентября 2015 года.

ISBN 978-9965-31-722-4

© Институт ИБ и К ЕНУ им. Л.Н.Гумилева, 2015 год

Айжамбаева С.Ж., Бакей Д.К.

**ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
НА АВТОМОБИЛЬНОМ ТРАНСПОРТЕ**

Карагандинский государственный технический университет,
Карагандинский государственный университет им. Е.А.Букетова,
г.Караганда, Республика Казахстан

Сегодня информатизация - одно из важнейших направлений научно-технического прогресса, основанное на широком применении вычислительной техники, средств связи, автоматизированных банков данных, взаимоувязанных между собой в информационно-вычислительные системы. В последние годы стали прочнее входить в различные сферы деятельности информационные технологии и применение этих технологий значительно ускоряет и облегчает те или иные процессы.

Информатизация на транспорте продолжает развиваться, совершенствуются программные продукты и технические средства, внедряются новые технологии, все более активно используется сеть Интернет. Электронная торговля (E-Commerce), интернет-технологии, автоматизированное управление на базе современных технических и программных средств открыли новые возможности повышения эффективности работы транспорта и экономичности логистических систем. Этому в значительной мере способствовали современные системы телекоммуникаций и в первую очередь мобильная система связи на основе стандарта GSM (Global System for Mobile Communication). Большое значение для автоматизации на всех видах транспорта имеет глобальная система определения местоположения транспортных средств (GPS) на основе спутниковой связи.

В значительной мере автоматизации и информатизации на транспорте способствовали успехи в области идентификации грузов и носителей на основе

штрихового кода, а также новые радиочастотные технологии идентификации с применением транспондеров.

В качестве основного направления для оптимизации использования автомобильного транспорта предлагается применение автоматизированных навигационных систем, посредством которых определяется оптимальный маршрут движения транспортных средств. В настоящее время известен целый ряд таких систем с разнообразным программным обеспечением. Большинство этих систем работает на основе глобальной автоматизированной географической системы GIS с топографическими картами в цифровой форме, которая используется не только на автомобильном, но и на других видах транспорта для автоматизации управления [1].

Комплексный подход к автоматизации транспорта – это, прежде всего, автоматизированный учет деятельности предприятий транспорта, а также подразделений в составе организаций.

Новым научным направлением в сфере информатизации систем транспорта является возможность внедрения новых информационных технологий, в частности Географических информационных систем (ГИС), американской системы GPS, европейской системы GALILEO и российской Глобальной Спутниковой радионавигационной системы Глонасс, которые помогут определить потенциальные пути снижения себестоимости автотранспортных услуг. Одновременно с космической группировкой систем спутниковой навигации развиваются абонентские мобильные комплекты спутникового оборудования и связанные с ними технологии: информационные, рекламные, охранные, средства диспетчеризации и управления, всевозможной телематики.

Средства системы позволяют не только решать коммерческие цели управления, но и обеспечат повышение безопасности движения объектов и будут способствовать охране человеческой жизни. Данные о дислокации аварийных объектов могут быть переданы в соответствующие поисково-спасательные службы.

Система GPS мониторинга транспорта является надежным инструментом управления парком предприятий, оказывающих услуги городских, междугородных и международных пассажирских перевозок. Внедрение системы исключает необходимость содержания многочисленного штата диспетчеров, позволяет автоматизировать большинство организационных процессов и сократить количество рабочих ошибок и форс-мажорных ситуаций, связанных с «человеческим фактором».

В данный период в Республике Казахстан ситуация развития средств автоматизации и информатизации вообще и в том числе на транспорте имеет общую проблему - большое разрозненное количество систем, хотя тенденция развития любой технической системы – это прежде всего интеграция [2].

Физическая природа передаваемого сигнала в канале связи

Оптические проводные – световоды (оптоволоконный канал используют в стационарных системах с большим объемом передаваемой информации и повышенными требованиями к скорости передачи, защищенности от возможного подслушивания электромагнитных помех.

Оптические беспроводные – они используют луч лазер для передачи сигнала между приемопередающими устройствами.

Системы беспроводной оптической связи уже установлены в различных компаниях, включая больницы, банки, операторы связи, муниципальные службы и военные ведомства во многих странах мира, предлагая беспроводные решения различного уровня сложности.

Электрические проводные - электрические провода (телефонные), кабели (витая пара (группы скрученных проводов) – высокочастотные, радиочастотные).

Кабели витой пары применяют в локальных вычислительных сетях. Радиочастотные кабели применяют телевизионных сетях, кабельном телевидении, в межблочных соединениях радиотехнических систем.

Электрические беспроводные – радиоканалы (КВ УКВ ВЧ СВЧ)

Форма представления передаваемой информации в канале связи:

Аналоговые - представляют информацию в непрерывной форме в виде непрерывного сигнала какой-либо физической природы.

Сигнал, формируемый мобильным телефоном, имеет переменную амплитуду и меняется по частоте. У такого сигнала спектр будет иметь сложную структуру (рис.3.) и будет состоять из множества частот, группирующихся в районе частоты 800 мгц.

Характеристики аналогового сигнала: – значение амплитуды (A), значение частоты (f), ширина спектра, время существования колебаний (t).

Цифровые сигналы - представляют информацию в цифровой (прерывной — дискретной, импульсной) форме сигналов какой-либо физической природы.

Цифровой сигнал – это набор импульсных сигналов формирующих цифровой код, в котором закодировано текущее значение амплитуды аналогового сигнала. Цифровой код – это двоичный код двоичной системы представления сигналов во времени.

Время существования канала связи

Коммутируемые — временные, создаются только на время передачи информации. По окончании передачи информации они разъединяются.

Некоммутируемые — создаются на длительное время с определенными постоянными характеристиками. Их еще называют выделенными.

Среднескоростные (от 2400—9600 бит/с) используются в телефонных (аналоговых) каналах связи, на новых станциях 14—56 кбит/с. Для передачи информации по среднескоростным каналам используются проводные линии связи (группы параллельных или скрученных проводов витая пара). Скорость передачи дисконтной информации по каналу связи измеряется в бодах. Бод — это скорость, при которой передается 1 бит в секунду (1 бит/с).

Высокоскоростные (свыше 56 кбит/с) называют широкополосными. Для передачи информации используются специальные кабели: экранированные и неэкранированные, оптоволоконные, радиоканалы.

Любое преобразование и передача данных по каналам связи осуществляются в соответствии с принятыми протоколами передачи информации в специальных устройствах преобразования сигнала (модем, точка доступа, устройства сопряжения сигналов).

Протокол передачи данных — это совокупность правил, которые определяют формат данных и процедуры передачи их по каналу связи, в которых, как правило, указываются способ модуляции, соединение с каналом, представление данных и т.д. Все это делается для повышения достоверности передаваемых данных.

Все модемы имеют определенные стандарты передачи данных, которые устанавливаются Международным институтом телекоммуникаций (ITU — International Telecommunication Union). Обычно стандарт включает несколько протоколов передачи данных. Одним из наиболее эффективных стандартов является стандарт V.34. Он выполняет тестирование канала связи, определяя при этом наиболее эффективный режим работы модема.

Рынок услуг передачи данных в Казахстане постоянно развивается. В настоящий момент на рынке присутствуют крупнейшие компании, расположенные в порядке убывания занимаемой доли рынка.

Наиболее распространенными видами современной связи являются:

- Телефонная связь
- Компьютерная телефония
- Радиотелефонная связь
- Системы сотовой радиотелефонной связи
- Системы стандарта Wi-Fi [3].

Литература

1. Информационные технологии и средства связи на автомобильном транспорте: Учеб. пособие / А.Э. Горев I СПб. гос. архит.-строит, ун-т. -СПб., 1999.-162 с.

2. О Транспортной стратегии Республики Казахстан до 2015 года. Указ Президента Республики Казахстан от 11 апреля 2006 года N 86

3. Козырев А.А. Информационные технологии в экономике и управлении: Учебник. - 2-е, изд. - СПб.: Изд-во Михайлова В.А., 2001. - 360 с.

Акашаев Н.А., Сатыбалдина Д.Ж.

ПРОТОКОЛ ОБМЕНА СЕКРЕТНЫМ КЛЮЧОМ, ОСНОВАННЫЙ НА СИНХРОНИЗАЦИИ ДВУХ ДРЕВОВИДНЫХ МАШИН ЧЕТНОСТИ

Евразийский национальный университет, Астана, РК

Защита информации в современных информационных и телекоммуникационных системах обеспечивается использованием комплекса программных, технических и организационных методов и средств [1]. Среди них важное место отводится криптографическим алгоритмам, обеспечивающим защиту конфиденциальности, целостности и аутентичности информации.

В настоящее время разработано достаточно много как национальных алгоритмов криптографических преобразований, так и алгоритмов, имеющих международное признание и применение. При этом открытость этих алгоритмов совершенно не вредит стойкости систем защиты информации с помощью этих криптографических алгоритмов. Это стало возможным благодаря основополагающему принципу построения криптографических систем А. Керкхоффа, согласно криптостойкость криптографической системы базируется на секретности ключа, а не на секретности используемого преобразования [2].

Для обеспечения коммуникаций большого количества абонентов, размещенных в произвольных точках пространства, для распределения ключевой информации приходится использовать открытые электронные каналы доставки. Конфиденциальность ключевой информации в этих каналах необходимо обеспечивать применением криптографических протоколов.

В настоящее время для формирования общих секретных ключей для симметричных систем шифрования с использованием открытых электронных каналов связи наиболее широко применяется протокол Диффи-Хеллмана [3]. Безопасность схемы Диффи-Хеллмана обусловлена трудностью вычисления дискретных логарифмов в конечном поле.

Однако, для всех алгоритмов, в том числе и схема Диффи-Хеллмана, основанных на использовании односторонних функций, несмотря на то, что они обеспечивают достаточно высокое быстродействие, высокую конфиденциальность присущ ряд недостатков: они требуют большой подготовительной работы и сложны в реализации, конфиденциальность ключевой информации, распределяемой методами, базирующимися на односторонних функциях, зависит от уровня развития компьютерной техники и успехов математических методов в области теории чисел.

Как альтернатива способам, основанным на использовании однонаправленных функций, длительное время рассматривался квантовый способ формирования ключевой информации [4]. К настоящему времени предложено и теоретически обосновано достаточно много различных протоколов квантового распределения ключей, например, В84, В92 и протокол Экерта, в качестве квантовых носителей информации в них выступают одиночные фотоны в различных поляризационных состояниях [4].

Однако, несмотря на теоретическую привлекательность, обеспечивающую достаточную конфиденциальность, практического широкого распространения эта технология до сих пор не получила. Причиной этого являются нерешенные проблемы технологического характера: ненадежное генерирование одиночных фотонов; большое количество ложных регистраций в приемных устройствах, малая дальность передачи оптических сигналов, сложность и высокая стоимость используемого оборудования [5]. Кроме того, имеются трудности системного характера – проблемы встраивания квантовых

каналов в компьютерные сети; невозможность использования технологии в условиях прослушивания квантового канала.

Перечисленные обстоятельства стимулируют многочисленные исследования, направленные, в том числе и на поиск новых альтернативных методов формирования общих секретных ключей для симметричных криптосистем.

В 2002 году И. Кантером и В. Кинцелем была предложена общая идея использования синхронизируемых искусственных нейронных сетей (ИНС) для формирования криптографических ключей [6]. Однако до сих пор не решен вопрос сходимости процесса синхронизации в поле дискретных величин, которыми оперируют компьютерные системы.

В связи с этим целью настоящей работы является исследование и программная реализация технологии открытого формирования ключевой информации для симметричного шифрования на основе синхронизируемых искусственных нейронных сетей.

В работе рассмотрен протокол обмена ключами, который основан на синхронизации двух древовидных машин четности (tree parity machines, ТРМ). ТРМ – это особый вид многоуровневой нейронной сети прямого распространения. Она состоит из одного выходного нейрона, K скрытых нейронов и $K \times N$ входных нейронов (см. рисунок 1).

Входные нейроны принимают двоичные значения:

$$x_{ij} \in \{-1, +1\}.$$

Веса между входными и скрытыми нейронами принимают значения

$$w_{ij} \in \{-L, \dots, 0, \dots, +L\}.$$

Значение каждого скрытого нейрона есть сумма произведений входного значения и весового коэффициента:

$$\sigma_i = \text{sgn} \left(\sum_{j=1}^N w_{ij} x_{ij} \right),$$

Где

$$\text{sgn}(x) = \begin{cases} -1 & \text{if } x \leq 0, \\ 1 & \text{if } x > 0. \end{cases}$$

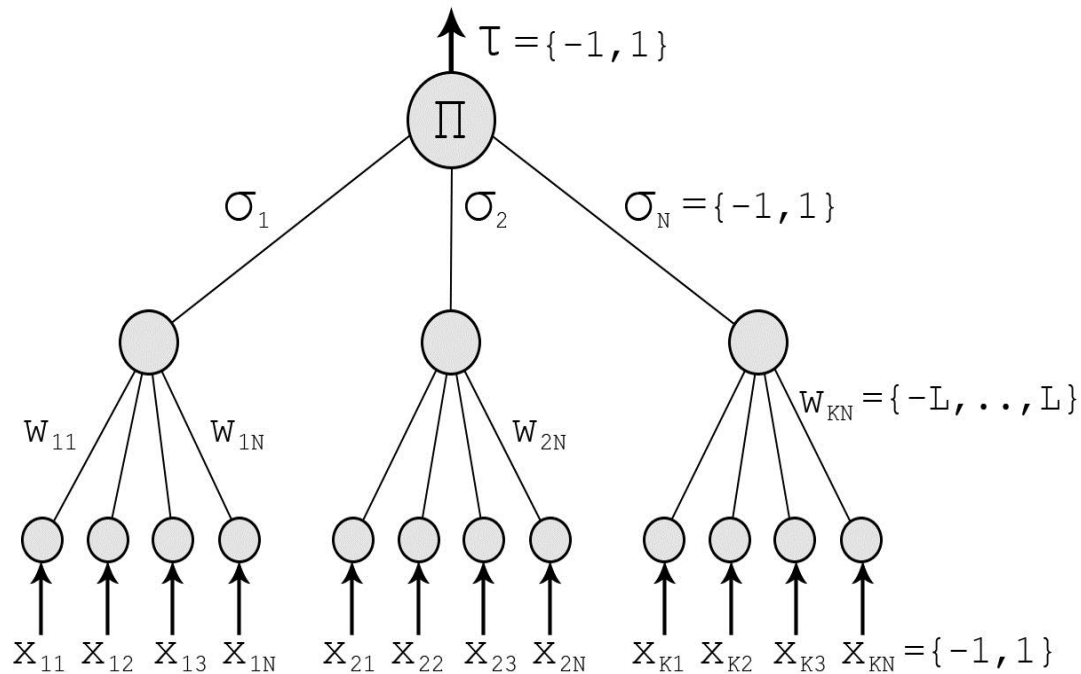


Рисунок 1 – Древоподобная машина четности.

Значение выходного нейрона есть произведение всех скрытых нейронов:

$$\tau = \prod_{i=1}^K \sigma_i.$$

Выходное значение также двоичное.

Протокол обмена ключами, основанный на синхронизации двух древоподобных машин четности, заключается в следующем.

У каждого абонента (А или В) есть своя ТРМ. Их синхронизация происходит следующим образом:

1. Задаём случайные значения весовых коэффициентов
2. Выполняем следующие шаги, пока не наступит синхронизация
3. Генерируем случайный входной вектор X

4. Вычисляем значения скрытых нейронов
5. Вычисляем значение выходного нейрона
6. Сравниваем выходы двух ТРМ:
7. Выходы разные: переход к п. 3
8. Выходы одинаковые: применяем выбранное правило к весовым коэффициентам
9. После полной синхронизации (веса w_{ij} обоих ТРМ одинаковые), А и В могут использовать веса в качестве ключа.

Этот метод известен как двунаправленное обучение.

Для обновления весовых коэффициентов могут использоваться следующие правила.

Правило Хебба:

$$w_i^+ = w_i + \sigma_i x_i \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)$$

Анти-правило Хебба:

$$w_i^+ = w_i - \sigma_i x_i \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)$$

Случайное блуждание:

$$w_i^+ = w_i + x_i \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)$$

К вопросу о стойкости данного протокола.

Крипто аналитик должен проверить все возможные варианты ключей, то есть все возможные веса w_{ij} . Если имеется K скрытых нейронов, $K \times N$ входных нейронов и максимальный вес L , то это даёт $(2L + 1)^{KN}$ вариантов. Например, для $K = 3$, $L = 3$, $N = 100 \approx 3 \cdot 10^{253}$ различных ключей. На сегодняшний день такая лобовая атака является вычислительно трудной.

Пусть у крипто аналитика есть такая же ТРМ, как и у абонентов. Он хочет её синхронизировать с двумя другими ТРМ. На каждом шаге возможны три ситуации:

$\text{Output}(A) \neq \text{Output}(B)$: Абоненты не обновляют веса.

$\text{Output}(A) = \text{Output}(B) = \text{Output}(E)$: Все трое обновляют веса.

$\text{Output}(A) = \text{Output}(B) \neq \text{Output}(E)$: А и В обновляют веса, но Е не может этого сделать. Поэтому он обучается медленнее, чем А и В синхронизируются.

Таким образом, крипто аналитик может определить ключ лишь с очень малой вероятностью.

Для повышения криптостойкости возможно увеличение синаптической длины L . Это увеличивает сложность атаки экспоненциально, в то время как затраты абонентов на расшифрование растут полиномиально. Таким образом, взлом подобной системы является NP-сложной задачей.

Нейронный протокол обмена ключей не основан на теории чисел, он основан на различии между однонаправленной и двунаправленной синхронизацией нейронных сетей. Поэтому, подобные протоколы могут ускорить процесс обмена.

Программная реализация протокола обмена ключами, основанный на синхронизации двух древовидных машин четности, разработана в среде Eclipse на языке Java.

После запуска сервера появляется стартовая страница (см. рисунок 2), на которой можно варьировать количество скрытых и входных нейронов, значения интервала весов, выбрать алгоритмы обучения весовых коэффициентов.

После этого согласно протоколу, абонент А инициирует процесс, запуская процесс создания начальных значений векторов X и весовых коэффициентов своей ТРМ. После вычисления выходного значения, абонент А отправляет абоненту В по открытому каналу связи входной вектор X и значение выходного вектора своей ТРМ.

Реализация распределения ключей методом синхронизации нейронных сетей

Введите количество скрытых нейронов:
Введите количество входных нейронов:
Введите максимальное значение весов:

Для обновления весовых коэффициентов могут использоваться следующие правила:

- Правило Хебба
- Анти-правило Хебба
- Случайное блуждание

Абонент А

Абонент В

Рисунок 2 – Начальная страница.

После выполнения абонентом В вычислений по протоколу, сравниваются выходные значения ТРМ абонентов А и В. Если выходные значения равны, тогда посылаем запрос на проверку синхронности сетей, в противном случае посылаем запрос на обучение сети (см. рис.3). Так же есть вариант посмотреть входной массив сгенерированный на начальной странице.

Выходное значение абонента А = -1

Выходное значение абонента В = -1

[Запрос на проверку синхронности сетей](#)

[Запрос на обучение сети](#)

[Показать входной массив](#)

Рисунок 3 – Шаг №3 протокола.

Решение о наступлении состояния синхронизации принимается после определенного числа неизменных равных выходных значений (см. рисунок 4). На рисунке 4 показаны матрицы весовых коэффициентов синхронизированных сетей абонентов А и В, из которых можно выбрать общий ключ (последовательность чисел или битов) нужной длины.

Ключ

-1	-1	2	-2	-1	-3	2	0	-2	0	-1	-1	2	1	-2	0	-3	-3	-2	-3	-1	-3	2	-2	-1	1	-2	0	1	2	1	0	-3	-3	1	-2	-2	0	-3	-2	2	1	-3	-3	2	-2	0	2	1	2	-3	-1	-2	-1	2	1
-3	0	1	1	0	-1	2	-1	-3	-3	2	-2	0	2	-1	-1	2	2	1	1	1	1	1	-3	-2	2	-3	1	-1	2	1	1	-2	-3	0	2	-2	-1	-1	-2	-2	2	-1	1	2	-2	1	-3	2	0	1	-1	0	2	0	
0	1	-2	-3	1	-2	-1	-3	-1	1	2	-3	-3	-3	0	2	0	2	1	-3	-2	1	-2	-2	-2	-1	-1	2	0	2	2	0	2	0	2	-3	1	-3	2	-1	-1	-2	-1	2	2	-3	-1	-3	0	0	-1	-2	-3			

-1	-1	2	-2	-1	-3	2	0	-2	0	-1	-1	2	1	-2	0	-3	-3	-2	-3	-1	-3	2	-2	-1	1	-2	0	1	2	1	0	-3	-3	1	-2	-2	0	-3	-2	2	1	-3	-3	2	-2	0	2	1	2	-3	-1	-2	-1	2	1
-3	0	1	1	0	-1	2	-1	-3	-3	2	-2	0	2	-1	-1	2	2	1	1	1	1	1	-3	-2	2	-3	1	-1	2	1	1	-2	-3	0	2	-2	-1	-1	-2	-2	2	-1	1	2	-2	1	-3	2	0	1	-1	0	2	0	
0	1	-2	-3	1	-2	-1	-3	-1	1	2	-3	-3	-3	0	2	0	2	1	-3	-2	1	-2	-2	-2	-1	-1	2	0	2	2	0	2	0	2	-3	1	-3	2	-1	-1	-2	-1	2	2	-3	-1	-3	0	0	-1	-2	-3			

Рисунок 4 – Матрицы весовых коэффициентов синхронизированных ТРМ абонентов А и В

Существенным недостатком данного алгоритма является медленная скорость взаимной настройки и значительное число шагов алгоритма, требуемое для настройки одной пары коэффициентов. Так, в эксперименте для настройки одной пары коэффициентов двух нейронных сетей, содержащих по 10 входных нейронов и один скрытый слой, требовалось в среднем до 10 000 эпох. Кроме того, при реализации алгоритма возникает вопрос о том, когда следует прекращать его выполнение. Иными словами, требуется найти критерий синхронизации, удовлетворив который, можно будет остановить алгоритм. Возможны следующие подходы:

1. Полный перебор – обеим ТРМ подаются на входы все возможные входные векторы, а вычисленные выходы ТРМ сравниваются. При достижении синхронизации при всех входных векторах все соответствующие выходы ТРМ будут совпадать.

2. Итеративный подход – заключается в эмпирическом оценивании необходимого числа итераций.

3. Использование дайджестов – сравнение абонентами А и В дайджестов (хеш-значений), вычисленных от набора весов ТРМ.

Литература

- 1 Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М. : Радио и связь, 1999. –328с.
- 2 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ.-М.: Триумф, 2002.-816с.
- 3 Diffie W, Hellman M.E. New Directions in Cryptography // IEEE Transactions on Information Theory-1976.-V.IT -22.№6-Р. 644-654.
- 4 Квантовая криптография: идеи и практика / под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. – Мн., 2008. – 392 с.
- 5 Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / Под ред. Боумейстера Д., Экерта А., Цайлингера А.; Пер. с англ. Кулика С.П., Шапиро Е.А. - М.: Постмаркет, 2002. - 375 с.
- 6 Kinzel, W. Interacting neural networks and cryptography / W. Kinzel, I. Kanter // Advances in Solid State Physics; ed. V. Kramer. – Springer Verlag, 2002. – С 122.

Актаева А., Илипбаева Л., Баймуратов А., Галиева Н
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КВАНТОВЫЕ
ТЕХНОЛОГИИ

Казахская академия транспорта и телекоммуникации им. М.Тынышбаева
Казахский Национальный технический университет им.К.Сатпаева
Алматинский технологический университет

Введение. В последние годы весьма актуальной и востребованной стала проблема применения квантовых технологий в области обеспечения системы информационной безопасности и защиты информации. По данным «Отчёта об угрозах безопасности в Интернете за 2014 год» компании Symantec количество направленных атак на персональные данные возросло за прошлый год на 91%, и более 550 миллионов человек стали их жертвами [2]. Причиной этому стали научные открытия и технологические достижения, сделавшие принципиально возможным решение целых классов сложнейших вычислительных технологий, имеющих стратегическое значение и прямое отношение к критически важным технологиям, таким как криптографические и др.[6].

В настоящее время квантовая информатика представляет собой новую, быстро развивающуюся отрасль науки, связанную с использованием квантовых технологий для реализации принципиально новых методов инфотелекоммуникации и вычислений: *квантовая информатика, квантовые каналы связи, квантовая криптография, квантовый компьютер* [15-21].

Основная часть. Основой квантовых технологий является квантовая информация — это физическая величина, характеризующая изменения, происходящие в системе при взаимодействии информационного потока с внешним окружением. Известно, что основой информации является бит, а классический бит может находиться в одном из двух состояний: $|0\rangle$ или $|1\rangle$. В квантовом рассмотрении информация описывается в кубитах — это те же самые биты, только квантовые, которые, находясь в состоянии суперпозиции и в отличие от первых, могут одновременно принимать оба значения, и при определенных условиях могут быть связаны между собой. В качестве кубитов могут выступать ионы, атомы, электроны, фотоны, спины атомных ядер, структуры из сверхпроводников и многие другие физические системы. Примером такой системы может служить фотон с двумя возможными поляризациями или электрон с двумя возможными направлениями спина. Таким образом, его физическое состояние можно представить как $b = a_1 0 +$

$a_2 I$, которое имеет одну из форм: или $a_1 = 1$ и $a_2 = 0$, тогда $b = 0$, или $a_1 = 0$ и $a_2 = 1$, и тогда $b = 1$. Квантовый бит $|\psi\rangle$ представляется как

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ или в векторном обозначении } |\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \langle\psi| = [\alpha \ \beta]^T.$$

Если $|\psi\rangle = |0\rangle$, то $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ (в обозначениях Дирака в виде кет-вектора).

Состояние квантового бита $|\psi\rangle$ задается вектором в двумерном комплексном векторном пространстве и тогда вектор имеет две компоненты, и его проекции на базисы векторного пространства являются комплексными числами [22].

Амплитуды α и β – комплексные числа, для которых выполнено следующее условие:

$$\alpha\alpha^* + \beta\beta^* = 1, \text{ где «*» – операция комплексного сопряжения;}$$

$\{|0\rangle, |1\rangle\}$ образует пару ортонормальных базисных векторов, называемых состоянием вычислительного базиса [22].

Если α или β принимают нулевые значения, то $|\psi\rangle$ определяет классическое, чистое состояние. В противном случае говорят, что $|\psi\rangle$ находится в состоянии суперпозиции двух классических базисных состояний [22].

Геометрически квантовый бит находится в непрерывном состоянии между $|0\rangle$ и $|1\rangle$, пока не производятся измерения его состояния. Понятие амплитуды вероятностей квантового состояния является комбинацией концепции состояния и фазы. Тогда двухквантовая бит система задается, как (формула Дирака)

$$|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

В случае, когда система состоит из двух квантовых битов, она описывается как тензорное произведение. Число возможных состояний комбинированной системы возрастает экспоненциально при добавлении квантового бита и приводит к проблеме оценки квантовой корреляции, которая присутствует между квантовыми битами в системе [22].

Попыткой поиска ответов на квантовые вызовы в области обеспечения системы информационной безопасности и защиты информации является квантовая криптография. Основные усилия в этой области сосредоточены на задачах синтеза стойких к возможностям квантовых компьютеров *криптографических алгоритмов и протоколов* (см. рис.1) [6].



Рис. 1- Основные направления исследований в СИБ [6]

В Протоколе BB84 носителями информации являются фотоны, поляризованные под углами 0 , 45 , 90 , 135° . В соответствии с законами квантовой физики, с помощью измерения можно различить лишь два ортогональных состояния:

1. если известно, что фотон поляризован либо вертикально, либо горизонтально;
2. поляризация под углами 45 и 135° .

Однако с достоверностью отличить вертикально поляризованный фотон от фотона, поляризованного под углом 45° , невозможно. При попытке измерения фотона, поляризованного под углом 45° , с помощью прямоугольного поляризатора с одинаковой вероятностью могут быть получены результаты 0 и 1 . Эти особенности поведения квантовых объектов легли в основу протокола квантового распространения ключа [3]. Таким образом, квантовая криптография в настоящее время активно расширяется и развивается во взаимодействии со смежными направлениями науки и техники. В соответствии

с данными протокола квантового распространения ключа. Например, реализация шифрования по протоколу BB84 (таблица 1):

1. Прямоугольный анализатор – «+»;
2. Диагональный анализатор – «×»;
3. Вертикальная поляризация – «|» кодирует 0;
4. Горизонтальная поляризация – «—» кодирует 1;
5. Поляризация под углом 45° – «/» кодирует 0;
6. Поляризация под углом 135° – «\» кодирует 1 [3].

Протокол B92 также может использоваться для распределения ключей. В отличие от BB4, где получатель может при получении с вероятностью 0,75 получить состояние каждого фотона, в этом протоколе получатель с вероятностью близкой к 1 может получить состояние 25 % фотонов. Для представления нулей и единиц в протоколе B92 используются фотоны, поляризованные в двух различных направлениях.

Таблица 1. Передача ключа по протоколу BB84

0	0	1	1	1	0	1	0	0	1	1	1	0	1	0	1	0	1	1	0
1		—	\	\		—		/	—	\	\	/	—	/	\		—	\	/
2	+	×	+	×	+	×	+	+	×	×	×	+	×	×	+	×	+	×	×
3	0	?	1	1	0	?	0	1	0	?	1	0	?	0	0	?	1	?	0
4	+		+	×	+		+	+	×		×	+		×	+		+		×
5	√		—	√	√		√	—	—		√	—		√	—		√		√
6				1			0							0					
7				√			√							√					
8	0				0						1						1		0

Квантовая телепортация - передача неизвестного квантового состояния на расстояние при помощи разделенной в пространстве и поделенной между двумя корреспондентами ЭПР-пары и классического канала связи. Явление квантовой телепортации — предмет рассмотрения сравнительно молодой науки квантовой теории информации. Квантовая телепортация, в отличие от плотного кодирования, происходит при отсутствии квантового канала связи, т.е. без передачи кубитов (см.рис.3). Задача квантовой телепортации состоит в следующем: У Отправителя есть кубит, находящийся в произвольном квантовом состоянии

$|\psi\rangle = a|0\rangle + b|1\rangle$, где коэффициенты a и b неизвестны, но выполнено условие

$$(|a|^2 + |b|^2 = 1)$$

При квантовой телепортации кубита предполагается, что генератор перепутанных состояний создал перепутанное двухкубитовое состояние $|\psi\rangle = (|00\rangle + |11\rangle) / \sqrt{2}$ и передал первый кубит Отправителю, а второй кубит Получателю. Состояние трехкубитовой системы в начальный момент имеет вид

$$|\psi_{in}\rangle = |\psi\rangle \otimes |\psi_{00}\rangle = \frac{1}{\sqrt{2}}(a|0\rangle + b|1\rangle) \otimes (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)).$$

Отправитель действует на свои два кубита оператором CNOT, используя первый кубит как контрольный, переводя трехкубитовую систему в состояние $|\psi_1\rangle$:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|10\rangle + |01\rangle)).$$

После этого она применяет к первому кубиту оператор Адамара, в результате чего система переходит в состояние $|\psi_2\rangle$:

$$|\psi_2\rangle = \frac{1}{2}[a(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + b(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle)].$$

Таким образом, телепортация представляет собой идеальный способ передачи любой информации. Так как, здесь отсутствует квантовый канал

связи, ЭПР-пара никакой информации не несет, по каналу связи передается только классическая информация, недостаточная для воспроизведения передаваемого сообщения.

Процесс оптимального извлечения ценной информации из классических состояний, образующих суперпозицию базируется на следующих фактах в квантовой теории информации:

- 1) существует эффективный квантовый алгоритм сжатия данных;
- 2) в квантовом состоянии присутствует «сцепленное» представление классической и квантовой информации;
- 3) полная корреляция в квантовом состоянии представляет собой «смесь» классической и квантовой корреляций;
- 4) присутствует скрытая классическая корреляция в квантовом состоянии [14].

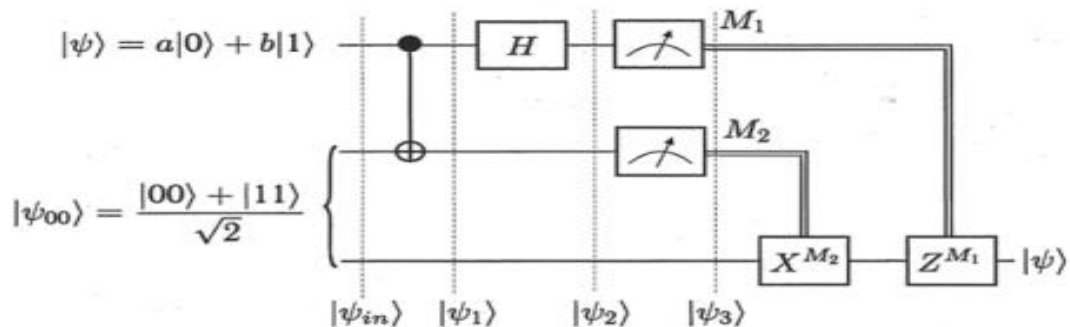


Рис.3 Квантовая схема телепортации неизвестного состояния $|\Psi\rangle$ кубита [4]

Недостаток квантовой телепортации заключается в том, что она не дает возможности передавать информацию быстрее скорости света, т.к. передача информации по классическому каналу связи, а классический канал ограничен скоростью света [4].

Заключение. В связи с интенсивным развитием инновационных технологий особое значение приобретают исследования в электронике, создании интеллектуальных программных и аппаратных продуктов прикладной информатики и квантовых технологий. Применение квантовых

технологий в области обеспечения информационной безопасности — одно из наиболее парадоксальных проявлений квантовой технологии, вызывающее в последние годы огромный интерес специалистов. Этот интерес обусловлен, в первую очередь, передаче зашифрованных сообщений по двум каналам связи — квантовому и традиционному. Проблемы квантовой информационной безопасности будут намного актуальнее многих существующих проблем современности в области информатизации общества.

Учитывая вышесказанное, считаем, что необходимо разработка и внедрение учебных курсов, как «Квантовая информатика», «Квантовые технологии в информационной безопасности и защиты информации», «Квантовые каналы связи», «Основы теории квантовой передачи информации», «Квантовая криптография» в рамках грантовых программ с привлечением государственного финансирования. Внедрение таких специализированных курсов позволяют в Научно-исследовательских университетах использовать в учебном процессе современные тенденции и практические результаты при решении сложных и важных для экономики страны задач подготовки востребованных рынком специалистов и аналитиков в области обеспечения информационной безопасности, а создание инновационных лабораторий кибербезопасности приведет к росту рейтинга ВУзов в мировом сообществе академических Университетов.

Литература

1. Брассар, Ж. Современная криптология. – М.: ПОЛИМЕД, 1999. – 176 с.
2. <http://www.computerra.ru/60709/emerging-tech/>
3. Долгов В.А. и др. Криптографические методы защиты информации. - Хабаровск, 2008
4. Емельянов В.И. Квантовая физика: Биты и Кубиты. - М.: Изд. МГУ, 2012
5. <http://www.gartner.com/newsroom/id/2819918?fnl=search&srcId=1-3478922254>

6. <http://www.itsec.ru>
7. <http://sci-article.ru>
8. Масленников, М. Е. Криптография и свобода. – mikhailmasl.livejournal.com
9. Лапоница О. Р. Криптографические основы безопасности. – www.intuit.ru
10. Шефановский Д. Б. ГОСТ Р 34.11-94. Функция хэширования. – М.: Информзащита, 2001
11. Federal Information Processing Standards Publication 197. Announcing the Advanced encryption standard (AES) [электронный ресурс] / NIST, 2006 – 51 с. – www.csrc.nist.gov
12. Сمارт Н. Криптография. – М.: Техносфера, 2005. – 528 с.
13. Фергюсон Н. Практическая Криптография. – М.: Изд. дом «Вильямс», 2005, 416 с.
14. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S. Quantum information and quantum computational intelligence: Quantum probability, physics of quantum information and information geometry, quantum computational logic and quantum complexity. – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano, 2005. – Vol. 83.
15. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежда и реальность. - Ижевск. РХД. 2001. 352с.
16. Валиев К.А. Квантовые компьютеры и квантовые вычисления// УФН, 2005, том 175, №1, стр.3-39
17. Нильсен М, Чанг И. Квантовые вычисления и квантовая информация. - М.: Мир, 2006, 824 с.
18. Прескилл Дж. Квантовая информация и квантовые вычисления. – Ижевск : РХД, 2008, 464 с.

19. Холево А. Введение в квантовую теорию информации.- М.: МЦНМО,2002,128 с.
20. Физика квантовой информации и др.// Под. ред. Боумейстера Д., и др. - М. Постмаркет, 2002, 376 с.
21. Богданов Ю.И., Валиев К.А и др. Квантовые компьютеры: достижения, трудности реализации и перспективы // Микроэлектроника,2011, Т.40, №4, с.243-255
22. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S., Quantum information and quantum computational intelligence: Quantum optimal control and quantum filtering – Stability, robustness, and self-organization models in nanotechnologies. – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano. – 2005. – Vol. 82; ibid: Applied quantum soft computing in AI, quantum language and programming in computer science, and intelligent wise robust control (4 rd edit.). – 2007. – Vol. 86.

Александров А.В.

**О СЕМЕЙСТВЕ РЮКЗАЧНЫХ БЛОЧНЫХ ШИФРОВ С ОБЩЕЙ
ПАМЯТЮ И РАЗРЕЖЕННОЙ ПЛОТНОСТЬЮ УКЛАДКИ**

Владимирский государственный университет имени Александра Григорьевича
и Николая Григорьевича Столетовых, Владимир, Россия

Хорошо известна задача о ранце в криптографии, на основе которой американские ученые Меркл и Хеллман создали алгоритм шифрования с открытым ключом [1]. Задача о ранце является частным случаем диофантовых уравнений, которые, как установил в 1972 году Ю.В.Матиясевич, алгоритмически неразрешимы. Задача о ранце в самой общей ситуации алгоритмически разрешима, однако NP – сложна. Для построения

ассиметричной рюкзачной криптосистемы в [1] предложено использовать сверхвозрастающие рюкзачные базисы. Однако, подход, основанный на таких базисах, оказался небезопасным. Сначала А.Шамир указал на существование полиномиальной по алгоритмической сложности атаки на пару (открытого ключ, закрытый ключ). Немного позже И.Лагариас, А.Одлыжко опубликовали атаку на саму схему шифрования «накрывающую», как показано в [2], почти все рюкзаки со свойством сверхвозрастания базиса укладки. Авторы назвали ее L^3 - атака в силу своей оценки алгоритмической сложности. В работе [3] представлен новый подход к конструкции рюкзачных криптосистем, позволяющий обойти атаку Шамира и L^3 – атаку. Главная его идея состоит в отказе от асимметрии в пользу симметричного ключа и введении общей памяти D у пары (Sender, Receiver), подмножества которой «параметрически влияют» на построение базиса рюкзачной схемы шифрования. Сами базисы не обладают свойством сверхвозрастания, и не могут подвергаться атакам типа L^3 .

Математические определения и конструкция функции шифрования / дешифрования

Обозначим $D = \{d_1, d_2, \dots, d_n\}$ общую память пары (Sender, Receiver), и для двоичного вектора $e = (e_i)$ длины n определим параметр $d_e = \sum(e_i * d_i)$. Для создания базиса задачи о рюкзаке привлечем линейно рекуррентные последовательности конечного порядка m , где $m \geq 2$, $f_1(d_e)=1, f_2(d_e)=1, \dots, f_m(d_e)=d_e$,

$$f_i(d_e)=f_{i-1}(d_e)+f_{i-2}(d_e)+\dots+f_{i-m}(d_e), \text{ для } i>m. \quad (1)$$

Последовательности такой конструкции достаточно хорошо изучены, называются также возвратными последовательностями (Маркушевич). В частном случае $m=2$, получаем фибоначчиевые последовательности. Относительно свойств введенных базисов справедливо следующее утверждение.

Теорема 1. Утверждение (а). Для любого целого числа S справедливо однозначное представление

$$S = (\sum k_i * f_i(d_e)) + \Delta(S, d_e), \quad i = 1, \dots, l, \quad (2)$$

с двоичными элементами k_i и некоторым остаточным слагаемым $\Delta(S, d_e)$.

Утверждение (b). Существует «жадный алгоритм» получения представления, просматривающий элементы базиса «сверху вниз» с некоторым остаточным после завершения алгоритма слагаемым $\Delta(S, d_e)$. Алгоритмическая сложность получения представления (2) при этом оценивается величиной $O(\log S)$ равномерно по выбору параметров базиса $m \geq 2, d_e$.

Утверждение (с) Асимптотика роста последовательности $\{f(d_e)\}$ при больших индексах не зависит от стартовых значений базиса в (1), и определяется наибольшим вещественным значением, корня соответствующего (1) характеристического алгебраического уравнения $x^m - x^{m-1} - \dots - 1 = 0$. Для любого $m \geq 2$ асимптотика роста обеспечивает плотность укладки задачи о рюкзаке за пределами интервала $(0,1)$.

То, что представление (2) строго говоря не единственно, показывают простые примеры для базиса Фибоначчи. Однако известный жадный алгоритм, просматривающий элементы базиса сверху вниз, всегда дает единственное представление (2) с некоторым остаточным слагаемым Δ . Для базиса Фибоначчи Теорема 1 принадлежит Цекендорфу, и в этом случае $\Delta \equiv 0$ равномерно по всему натуральному ряду. На основе приведенной **теоремы 1(с)** в рамках единого подхода можно строить широкие классы симметричных криптографических систем рюкзачного типа, варьируя параметры m, d_e и стартовые значения рекуррентных базисов, добиваясь того, чтобы плотность укладки задачи о рюкзаке оставалась за пределами интервала $(0,1)$, в котором эффективно работает атака Лагариаса-Одлыжко.

В самом деле, в рамках конструкции (2), основанной на общей памяти D в любом параметризованном базисе $\{f(d_e)\}$ всегда устанавливается однозначное битовое соответствие

$$S \leftrightarrow (e_1, \dots, e_n, k_1, k_2, \dots, k_l, \Delta_2), \quad (3)$$

где Δ_2 – двоичное представление остаточного слагаемого. Набор значений e_1, \dots, e_n определяет выборку элементов общей памяти, и не только соответствующим образом расширяет ключевое пространство в схеме шифрования об укладке рюкзака (2), но и в совокупности со значением S параметрически по d_e образом влияет на последующие значения ключа $k_1, k_2, \dots, k_l, \Delta$.

Наличие общей памяти в приведенных построениях, выходит за рамки шенноновской модели симметричного шифрования, однако, не противоречит более современной криптографической модели безопасности Долев - Яо[4]. Для случая $m=2$ в статье [3] показано, что представленная криптосистема безопасна в модели Долев – Яо при соблюдении двух условий. Во-первых, при условии невозможности компрометации общей памяти. Во-вторых, при условии безопасной процедуры создания и передачи той части ключа (e_1, \dots, e_n) , которая выделяет в общей памяти базовое для алгоритмов шифрования и дешифрования подмножество общей памяти D .

Симметричный блочный шифр и хеш- функция

Зафиксируем достаточно большое натуральное n и l в (1), (2) и обозначим \tilde{S} максимально возможное натуральное число в представлении (1). Пусть S – любой двоичный файл произвольной длины. Зададим конкатенацию блоков $S = S_1 // S_2 // \dots // S_m$, где длина каждого блока, за исключением последнего, фиксирована. Считая выполненным равномерно по всем индексам $S_i \leq \tilde{S}$, для каждого блока применим представление (2). Жадный алгоритм в теореме 1(в), который находит (3) есть функция шифрования блока, которую обозначим

$F_k(d_e, S)$. Обратный алгоритм – функция дешифрования. На основе выделения блоков стандартным образом конструируется блочный шифр в режиме кодовой книги или режиме зацепления блоков. В режиме зацепления блоков каждый блок открытого текста побитово складывается по модулю 2 с предыдущим результатом шифрования. Обозначим B_0 – вектор инициализации режима зацепления блоков, тогда:

$$B_i = F_k^{d_e}(S_i \oplus B_{i-1}), \quad (3)$$

где i – номер текущего блока; $F_k^{d_e}$ – алгоритм шифрования, S_i – блок открытого текста.

Обозначим $F_k^{\pm 1}(S)$ функции блочного шифрования в режиме зацепления блоков для верхнего индекса (+1) и, соответственно дешифрования для (-1). Зафиксируем общую память. Обозначим здесь и ниже $k = (k_1, \dots, k_l, \Delta)$ симметричный ключ шифрования. Свяжем с функцией $F_k^{\pm 1}(S)$ хеш-функцию $H_{d_e}(S)$, для создания которой используем стандартную итеративную процедуру порождения хеш-функций на основе XOR- свертки выходных значений блочного шифра в режиме зацепления блоков $H_0 = const$, $i=1, 2, \dots, r$ $H_i = F_k(S \oplus H_{i-1})$.

Теорема 2. Пусть $e = (e_1, \dots, e_n)$ – набор битов, определяющий выбор подмножества общей памяти для пары (Sender, Receiver). $\{f_{d_e}\}_1^n$ – базис симметричной рюкзачной криптосистемы, $H_{d_e}(S)$ – ей соответствующая хеш-функция, полученная XOR- сверткой из блочного шифра $F_k(S)$, построенного на базисе $\{f_{d_e}\}_1^n$. Тогда: $H_{d_e}(S)$ – односторонняя хеш-функция. Поскольку $H_{d_e}(S)$ – однозначно идентифицирует пару (Sender, Receiver) за счет выбора параметра d_e , то в случае передачи пакета $(S, H_{d_e}(S))$ в открытом канале связи функция $H_{d_e}(S)$ контролирует целостность значения

S, в частности эффективно противостоит атакам подмены текста *S* в канале связи, в том числе атакам типа “Man in the middle».

В самом деле, все построения, в том числе и хеш-функция параметрически зависят от согласованного парой (Sender, Receiver) параметра d_e общей памяти этой и только этой пары (Sender, Receiver), и нескомпрометированной общей памяти по отношению к противнику в открытом канале связи, что, как оговорено выше, предполагается выполненным.

Литература

1. Diffie R. Merkle, M. Hellman. Hiding information and signatures in trapdoor knapsacks // Information Theory, IEEE Transactions, 1978, P. 525-530.
2. Odlyzko A. M. and Lagarias J. C. Solving Low-Density Subset Sum Problems // J. Association Computing Machinery. 1985. V. 32. No.1. P. 229–246.
3. Александров А.В., Метлинов А.Д. Симметричная рюкзачная криптосистема с общей памятью и плотностью укладки больше единицы // Журнал «Проблемы информационной безопасности. Компьютерные системы», №4 2014, с. 58-65.
4. Dolev D., Yao A. On the Security of Public Key Protocols // IEEE Transact. on Inform. Theory. 1983. Vol. 29, N 2. P. 198—208.

Альмухамбетов С.

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Центрально-Азиатский университет

Создание копий программных средств для изучения или несанкционированного использования является одним из наиболее широко распространенных правонарушений в сфере компьютерной информации, что предопределяет необходимость защиты программного обеспечения.

В общем случае под *защитой программного обеспечения* понимается комплекс мер, направленных на защиту программного обеспечения от несанкционированного приобретения, использования, распространения, модифицирования, изучения и воссоздания аналогов.

При организации защиты программного обеспечения используются различные меры: организационные, правовые, технические. Основная идея *организационных мер защиты* заключается в том, что полноценное использование программного продукта невозможно без соответствующей поддержки со стороны производителя: подробной пользовательской документации, «горячей линии», системы обучения пользователей, обновление версий со скидкой и т.п. Организационные меры защиты применяются, как правило, крупными разработчиками к достаточно большим и сложным программным продуктам.

Правовые меры защиты программного обеспечения заключаются в установлении ответственности за использование программного обеспечения с нарушением порядка, установленного действующим законодательством.

Технические методы защиты программного обеспечения можно классифицировать по способу распространения защищаемого программного обеспечения и типу носителя лицензии.

Локальная программная защита

Данный вид защиты подразумевает необходимость ввода серийного номера (ключа) при установке или запуске программы. История этого метода началась тогда, когда приложения распространялись только на физических носителях (к примеру, компакт-дисках). На коробке с диском был напечатан серийный номер, подходящий только к данной копии программы.

С распространением сетей очевидным недостатком стала проблема распространения образов дисков и серийных номеров по сети. Поэтому в настоящий момент данный метод используется только в совокупности одним или более других методов (к примеру, организационных).

Сетевая программная защита

В этом случае осуществляемое программой сканирование сети исключает одновременный запуск двух программ с одним регистрационным ключом на двух компьютерах в пределах одной локальной сети. Недостаток данного метода заключается в том, что брандмауэр можно настроить так, чтобы он не пропускал пакеты, принадлежащие защищённой программе.

Глобальная программная защита

Если программа работает с каким-то централизованным сервером и без него бесполезна (например, сервера обновлений антивирусов), она может передавать серверу свой серийный номер; если номер неправильный, сервер отказывает в услуге. Недостаток в том, что, существует возможность создать сервер, который не делает такой проверки.

Защита при помощи компакт-дисков

Программа может требовать оригинальный компакт-диск. Стойкость таких защит невелика, ввиду широкого набора инструментов снятия образов компакт-дисков. Как правило, этот способ защиты применяется для защиты программ, записанных на этом же компакт-диске, являющимся одновременно ключевым.

Для защиты от копирования используется:

- запись информации в неиспользуемых секторах;
- проверка расположения и содержимого «сбойных» секторов;
- проверка скорости чтения отдельных секторов.

Первые два метода практически бесполезны из-за возможности снятия полного образа с диска с использованием соответствующего прикладного программного обеспечения. Третий метод считается более надёжным (используется, в частности, в защите StarForce). Но существуют программы, которые могут эмулировать диски с учётом геометрии расположения данных, тем самым обходя и эту защиту. В StarForce, в числе прочих проверок, также выполняется проверка возможности записи на вставленный диск. Если она возможна, то

диск считается не лицензионным. Однако, если образ будет записан на диск CD-R, то указанная проверка пройдет. Возможно, также, скрыть тип диска, чтобы CD-R или CD-RW был виден как обычный CD-ROM. Однако, в драйвер защиты может быть встроена проверка на наличие эмуляции.

В настоящее время наибольшую известность в мире имеют системы защиты от копирования SecuROM, StarForce, SafeDisc, CD-RX и TAGES.

Защита при помощи электронных ключей

Электронный ключ, вставленный в один из портов компьютера (с интерфейсом USB, LPT или COM), содержит ключевые данные, называемые также лицензией, записанные в него разработчиком защищенной программы. Защита программы основывается на том, что только ему (разработчику) известен полный алгоритм работы ключа.

Ключ распространяется с защищаемой программой. Программа в начале и в ходе выполнения считывает контрольную информацию из ключа. При отсутствии ключа выполнение программы блокируется.

Одним из основных достоинств защиты программных средств с использованием электронных ключей является то, что ключ можно вставлять в любой компьютер, на котором необходимо запустить программу.

Привязка к параметрам компьютера и активация

Привязка программного обеспечения к информации о пользователе / конфигурации компьютера и последующая активация программного обеспечения в настоящий момент используется достаточно широко (пример – операционная система Windows).

В процессе установки программа подсчитывает код активации – контрольное значение, однозначно соответствующее установленным комплектующим компьютера и параметрам установленной программы. Это значение передается разработчику программы. На его основе разработчик генерирует ключ активации, подходящий для активации приложения только на указанной

машине (копирование установленных исполняемых файлов на другой компьютер приведет к неработоспособности программы).

Достоинство данного метода защиты заключается в том, что не требуется никакого специфического аппаратного обеспечения, и программу можно распространять посредством цифровой дистрибуции (по сети Интернет).

Основной недостаток заключается в том, что программное обеспечение становится неработоспособным в случае, если пользователь производит модернизацию компьютера (если привязка осуществляется к аппаратной конфигурации компьютера).

В качестве привязки используются, в основном, серийный номер BIOS материнской платы, серийный номер винчестера. В целях сокрытия от пользователя данные о защите могут располагаться в неразмеченной области жесткого диска.

Защита программ от копирования путём переноса их в онлайн

Другим направлением защиты программ является использование подхода SaaS, то есть предоставление функционала этих программ (всего или части), как сервиса. При этом код программы расположен и исполняется на сервере, доступном в глобальной сети. Доступ к нему осуществляется по принципу тонкого клиента.

ЗАКЛЮЧЕНИЕ

Защита информации в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств. При этом необходимо помнить, что естественные каналы утечки информации образуются спонтанно, в силу специфических обстоятельств, сложившихся на объекте защиты. Что касается искусственных каналов утечки информации, то они создаются преднамеренно с применением активных методов и способов получения информации. Активные способы предполагают намеренное создание технического канала утечки информации с использованием специальных

технических средств. К ним можно отнести, в том числе, и несанкционированный доступ к информации, обрабатываемой в компьютерных системах и т.д. В этой связи особую роль и место в деятельности по защите информации занимают мероприятия по созданию комплексной защиты, неотъемлемым элементом которой является защита информации в компьютерных системах.

Для более полного уяснения вопросов, рассмотренных в рамках настоящей лекции, необходимо внимательно ознакомиться с основной и дополнительной литературой по теме лекции, а также выполнить задания, вынесенные на самостоятельную подготовку.

Арипов М.М., Курьязов Д.М.

ОБ ОДНОЙ АЛГОРИТМ ЭЦП С УВЕЛИЧЕННОЙ СТОЙКОСТИ

Национальный университет Узбекистана, город Ташкент, Узбекистан

Подпись является юридическим гарантом авторства документа. С широким распространением в современном мире электронных форм документооборота, в том числе и конфиденциальных, в сети телекоммуникации особо актуальной стала проблема установления подлинности и авторства безбумажной электронной документации. Так как, в ситуациях, например в силу изменившихся обстоятельств, отдельные лица могут отказаться от ранее принятых обязательств. В связи с этим необходим некоторый механизм, препятствующий подобным попыткам. Основным механизмом решения таких проблем является электронная цифровая подпись (ЭЦП).

ЭЦП позволяет решить следующие три задачи электронного документооборота в сети телекоммуникации[1-4]:

- осуществить аутентификацию источника сообщения;
- установить целостность сообщения (по значению хеш-функции);

-обеспечить невозможность отказа от факта подписи конкретного сообщения.

ЭЦП включает два алгоритма, один — для вычисления, а второй — для проверки подписи. Вычисление подписи может быть выполнено только автором подписи. Алгоритм проверки должен быть общедоступным, чтобы проверить правильность подписи мог каждый.

В настоящее время предложено несколько принципиально различных подходов к созданию схем ЭЦП. Их можно разделить на три группы:

- 1) схемы на основе систем шифрования с открытыми ключами;
- 2) схемы на основе симметричных систем шифрования;
- 3) схемы со специально разработанными алгоритмами вычисления и проверки подписи.

К примеру, стандарты ЭЦП со специально разработанными алгоритмами являются[2,4]:

1. Российский стандарт ЭЦП: ГОСТ Р 34.10-94 и его модификация на эллиптических кривых ГОСТ Р 34.10-2001.
2. Американский стандарт ЭЦП: DSA и его модификация на эллиптических кривых ECDSA (2000 г.).

Стойкость приведенных стандартов ЭЦП основаны сложности вычисления дискретного логарифма в конечном поле и дискретного логарифма в эллиптических кривых.

Модификация алгоритмов ЭЦП на эллиптических кривых увеличить стойкость сложностью нахождения точку с рациональными координатами на эллиптических кривых высокого порядка (количество точек с таким свойством оказывается не много) относительно введенной операции сложения точек на эллиптических кривых.

На сегодняшний день для повышения безопасности ЭЦП представляет интерес разработка алгоритмов, взлом которых требует одновременного

решения двух независимых (например, задача дискретного логарифмирования в конечной группе большого простого порядка и задача факторизации составного числа) вычислительно трудных задач. Этот подход к повышению уровня безопасности криптосхем были обоснованы и апробирован для случая алгоритмов ЭЦП [5-7], коллективной ЭЦП [10] и протоколов слепой ЭЦП [8].

В данной работе предлагается алгоритм ЭЦП с увеличением стойкости на основе сложности разложения достаточно большого нечетного числа простым множителем.

Приведем основную часть этого алгоритма. В алгоритме используются следующие открытые исходные параметры:

1) Достаточно большое простое число p длиной L , где L принимает значение, кратное 64 бит, в диапазоне от 512 до 1024 бит, т.е. $2^{512} < p < 2^{1024}$.

2) Простое число q длиной L_1 , где L_1 принимает значение, в диапазоне от 159 до 160 бит, т.е.

$$2^{159} \leq q \leq 2^{160}, \text{ делитель числа } p-1.$$

Число $g = h^{(p-1)/q} \bmod p$, где h –любое число, такое $0 < h < p-1$, для которого $g > 1$, т.е. $g = h^{(p-1)/q} \bmod p > 1$.

4) Открытый ключ y , который сформирован по правилу $y = g^x \bmod p$, причем $0 < x < q$, где секретный ключ x , известный только подписавшему лицу.

5) Хеш-функция $H(M)$, которая по исходному сообщению (тексту) M формирует целое число в диапазоне от 1 до q , т.е. $1 < H(M) < q$.

Алгоритм генерация подписи. Входные данные: сообщение M , исходные параметры и секретный ключ подписи. Выходные данные: подпись (r, s) .

Шаги алгоритма генерации подписи:

1. Выбрать случайное число k в интервале $1 \leq k \leq q$, держать его в секрете и уничтожать сразу после получения (сформирования) подписи.
2. Вычислить $r = (g^k \bmod n) \bmod p(\bmod q)$;
3. Вычислить значение хеш-функции $H(M)$ по передаваемому сообщению M .

4. Вычислить $s = k (xr + H(M))^{-1} d \pmod{q}$, где x, d - секретные ключи (причем $0 < x < q$ и $de \equiv 1 \pmod{\varphi(n)}$, достаточно большое число $n = p_1 q_1$, p_1, q_1 - неизвестные простые числа, разумеется $n > p$).

5. Подписью является пара (r, s) .

Алгоритм проверки подписи. Входные данные: сообщение M , исходные параметры, открытый ключ проверки подписи и подпись к M - пара (r, s) .

Выходные данные: утверждение, что подпись действительная или фальшивая.

Шаги алгоритма проверки подписи:

1. Если условия $1 \leq r, s < q$, нарушаются, то вывести «подпись фальшивая» и завершить работу алгоритма.
2. Вычислить $e = H(M)$.
3. Вычислить $w = s^{-1} \pmod{q}$.
4. Вычислить $u_1 = e (H(M) s) \pmod{q}$.
5. Вычислить $u_2 = e (r s) \pmod{q}$.
6. Вычислить $u = ((g^{u_1} y^{u_2}) \pmod{n}) \pmod{p \pmod{q}}$.
7. Если $u = r$, то вывести «подпись действительная», иначе - «подпись фальшивая», и завершить работу алгоритма.

Корректность алгоритма.

Покажем, что значение число r , генерированное по алгоритму ЭЦП, равно значению u , вычисленное в части проверки подписи алгоритма.

Действительно, имеем

$$\begin{aligned}
 ((g^{u_1} y^{u_2}) \pmod{n}) \pmod{p \pmod{q}} &= (g^{H(M) s e} g^{xr s e} \pmod{n}) \pmod{p \pmod{q}} = \\
 &= (g^{(H(M) + x r) s e} \pmod{n}) \pmod{p \pmod{q}} = \\
 &= (g^{k d e (H(M) + x r) (H(M) + x r)^{-1}} \pmod{n}) \pmod{p \pmod{q}} = \\
 &= (g^{k d e} \pmod{n}) \pmod{p \pmod{q}} = \\
 &= (g^{k(t \varphi(n) + 1)} \pmod{n}) \pmod{p \pmod{q}} = \\
 &= (g^{k t \varphi(n)} \pmod{n}) (g^k \pmod{n}) \pmod{p \pmod{q}} = \\
 &= (g^{\varphi(n)} \pmod{n})^{k t} (g^k \pmod{n}) \pmod{p \pmod{q}} = \\
 &= 1^{k t} (g^k \pmod{n}) \pmod{p \pmod{q}} =
 \end{aligned}$$

$$= (g^k \bmod n) \bmod p(\bmod q).$$

Таким образом, $u = r$, и корректность алгоритма доказана.

ЛИТЕРАТУРА

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001-368с.
2. Харин. Ю.С. Математические и компьютерные основы криптологии. – Мн.: Новое знание, 2003.-382с.
3. Шнайер Б. Прикладная криптография. ТРИУМФ. Москва, 2002г. –816 с.
4. Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов.-СПб.: БХВ-Петербург, 2004.-448 с.: ил.
5. Арипов М.М., Курьязов Д.М. Об одном алгоритме ЭЦП с составным модулем. // ДАН Республики Узбекистан. №4. 2012г..
6. Арипов М.М., Курьязов Д.М. ЭЦП основанные на сложности решения двух трудных задач.// Сборник материалах международной научной конференций, Актуальные проблемы прикладной математики и информационных технологий -Аль-Хоразмий 2014. Самарканд 15-17 сентября 2014года, Том 2, стр. 59-63
7. Курьязов Д.М. Алгоритм ЭЦП на эллиптических кривых. // Вестник НУУ №2. 2013г.
8. Молдовян Н.А., Гурьянов Д.Ю. Повышение безопасности протоколов слепой подписи // Вопросы защиты информации. 2012.№4.С.3-6.
9. Дернова Е.С., Молдовян Н.А. Синтез алгоритмов цифровой подписи на основе нескольких вычислительно трудных задач // Вопросы защиты информации.2008.№1.С.22-26.
10. Дернова Е.С., Молдовян Н.А. Протоколы коллективной цифровой подписи, основанные на сложности решения двух трудных задач // Вопросы защиты информации.2008.№2.С.79-85

Aripov M., Tychiev G.

**DEVELOPMENT BLOCK ENCRYPTION ALGORITHM BASED
NETWORKS IDEA16–2 AND RFWKIDEA16–2 USING THE
TRANSFORMATION OF ENCRYPTION ALGORITHM AES**

National University of Uzbekistan, Republic of Uzbekistan, Tashkent

Abstract

A block encryption algorithms AES–IDEA 16–2 and AES–RFWKIDEA16–2 based on a network IDEA16–2 and RFWKIDEA16–2. In the encryption algorithm AES–IDEA16–2 as a round function are chosen transformation SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() and in the encryption algorithm AES–RFWKIDEA16–2 as a round function are chosen transformation SubBytes(), ShiftRows(), MixColumns is developed. The length of the block encryption algorithm is 512 bits, the number of rounds is 10, 12, 14 and key length varies from 256 bits to 1024 bits in steps of 128 bits.

Introduction

In September 1997 the National Institute of Standards and Technology (NIST) issued a public call for proposals for a new block cipher to succeed the Data Encryption Standard (DES). Out of 15 submitted algorithms the Rijndael cipher by Daemen and Rijmen [1] was chosen to become the new Advanced Encryption Standard (AES) in November 2001 [2]. The Advanced Encryption Standard is a block cipher with a fixed block length of 128 bits. It supports three different key lengths: 128 bits, 192 bits, and 256 bits. Encrypting a 128–bit block means transforming it in n rounds into a 128–bit output block. The number of rounds n depends on the key length: $n = 10$ for 128 bit keys, $n = 12$ for 192 bit keys, and $n = 14$ for 256 bit keys. The 16 byte input block $(t_0, t_1, \dots, t_{15})$ which is transformed during encryption is usually written as a 4x4 byte matrix, the called AES *State*.

t_0	t_4	t_8	t_{12}
t_1	t_5	t_9	t_{13}
t_2	t_6	t_{10}	t_{14}
t_3	t_7	t_{11}	t_{15}

The structure of each round of AES can be reduced to four basic transformations occurring to the elements of the *State*. Each round consists in applying successively to the *State* the SubBytes(), ShiftRows(), MixColumns() and AddRoundKey() transformations. The first round does the same with an extra AddRoundKey() at the beginning whereas the last round excludes the MixColumns() transformation.

The SubBytes() transformation is a nonlinear byte substitution that operates independently on each byte of the *State* using a substitution table (S-box). Figure 1 illustrates the SubBytes() transformation on the *State*.

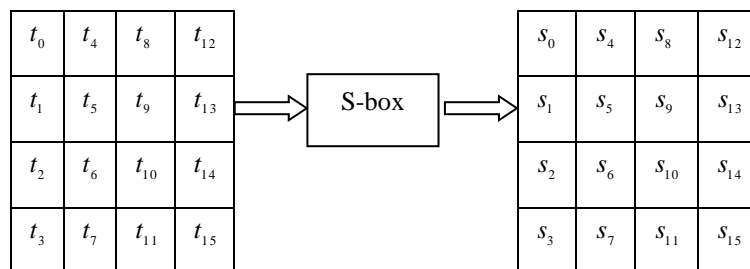


Figure 1. SubBytes() transformation

In the ShiftRows() transformation operates on the rows of the *State*; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. Figure 2 illustrates the ShiftRows() transformation.

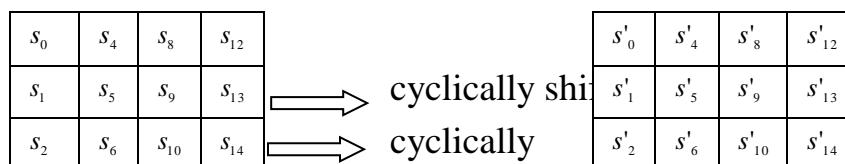




Figure 2. ShiftRows() transformation.

The MixColumns() transformation operates on the *State* column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over $\text{GF}(2^8)$ and multiplied modulo $x^4 + 1$ with a fixed polynomial $a(x)$, given by $a(x) = 3x^2 + x^2 + x + 2$. Let $p = a(x) \otimes s'$:

$$\begin{bmatrix} p_{4i} \\ p_{4i+1} \\ p_{4i+2} \\ p_{4i+3} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s'_{4i} \\ s'_{4i+1} \\ s'_{4i+2} \\ s'_{4i+3} \end{bmatrix}, i = \overline{0..3}$$

As a result of this multiplication, the four bytes in a column are replaced by the following:

$$\begin{aligned} y_{4i} &= (\{02\} \bullet s'_{4i}) \oplus (\{03\} \bullet s'_{4i+1}) \oplus s'_{4i+2} \oplus s'_{4i+3} \\ y_{4i+1} &= s'_{4i} \oplus (\{02\} \bullet s'_{4i+1}) \oplus (\{03\} \bullet s'_{4i+2}) \oplus s'_{4i+3} \\ y_{4i+2} &= s'_{4i} \oplus s'_{4i+1} \oplus (\{02\} \bullet s'_{4i+2}) \oplus (\{03\} \bullet s'_{4i+3}) \\ y_{4i+3} &= (\{03\} \bullet s'_{4i}) \oplus s'_{4i+1} \oplus s'_{4i+2} \oplus (\{02\} \bullet s'_{4i+3}). \end{aligned}$$

Figure 3 illustrates the MixColumns() transformation.

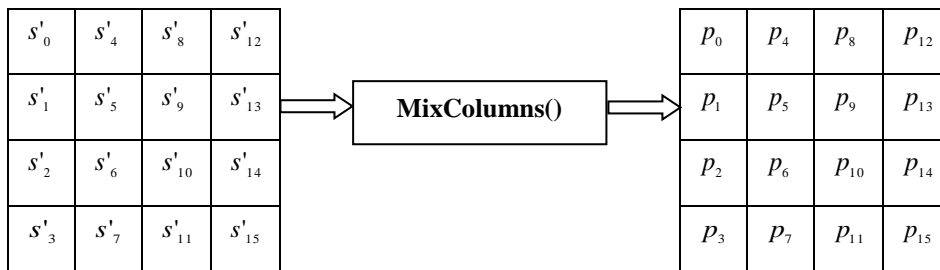
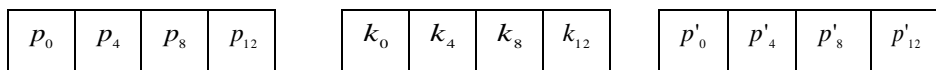


Figure 3. MixColumns() transformation.

In the AddRoundKey() transformation, a round key is added to the *State* by a simple bitwise XOR operation. Figure 4 illustrates the AddRoundKey() transformation.



$$\begin{array}{|c|c|c|c|} \hline p_1 & p_5 & p_9 & p_{13} \\ \hline p_2 & p_6 & p_{10} & p_{14} \\ \hline p_3 & p_7 & p_{11} & p_{15} \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|} \hline k_1 & k_5 & k_9 & k_{13} \\ \hline k_2 & k_6 & k_{10} & k_{14} \\ \hline k_3 & k_7 & k_{11} & k_{15} \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline p'_1 & p'_5 & p'_9 & p'_{13} \\ \hline p'_2 & p'_6 & p'_{10} & p'_{14} \\ \hline p'_3 & p'_7 & p'_{11} & p'_{15} \\ \hline \end{array}$$

Figure 4. AddRoundKey() transformation

Description of networks IDEA16–2 and RFWKIDEA16–2 is given in [7, 10] and similarly as in the Feistel network, while encryption and decryption the same algorithm is used. The network used two round function, having four input and output blocks and as a round function use any transformation.

Using SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() transformation of encryption algorithm AES as a round function networks IDEA8–1 [5], RFWKIDEA8–1 [5], PES8–1 [6], RFWKPES8–1 [7], IDEA16–1 [8], created encryption algorithms AES–IDEA8–1 [9], AES–RFWKIDEA8–1 [10], AES–PES8–1 [11], AES–RFWKPES8–1 [12], AES–IDEA16–1 [13].

In this article, developed a new block encryption algorithms AES–IDEA16–2 and AES–RFWKIDEA16–2 based networks IDEA16–2 and RFWKIDEA16–2 using transformation of the encryption algorithm AES. The block length of encryption algorithm is 1024 bits, the number of rounds is 10, 12, 14 and key length is variable and varies from 256 bits to 1024 bits in steps 128 bits, i.e. key length is 256, 384, 512, 640, 768, 896 and 1024 bits.

The structure of the encryption algorithm AES–IDEA16–2

In the encryption algorithm AES–IDEA16–2 as a round function used SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() transformation of encryption algorithm AES. The scheme of n –rounded encryption algorithm AES–IDEA16–2 shown in Figure 5 and the length of the subblocks x^0, x^1, \dots, x^{15} , the length of the round keys $K_{18(i-1)}, K_{18(i-1)+1}, \dots, K_{18(i-1)+15}, i = \overline{1..n+1}, K_{18n+16}, K_{18n+17}, \dots, K_{18n+47}$ is 32 bits. A length of round keys $K_{18(i-1)+16}, K_{18(i-1)+17}, i = \overline{1..n}$ is 128 bits.

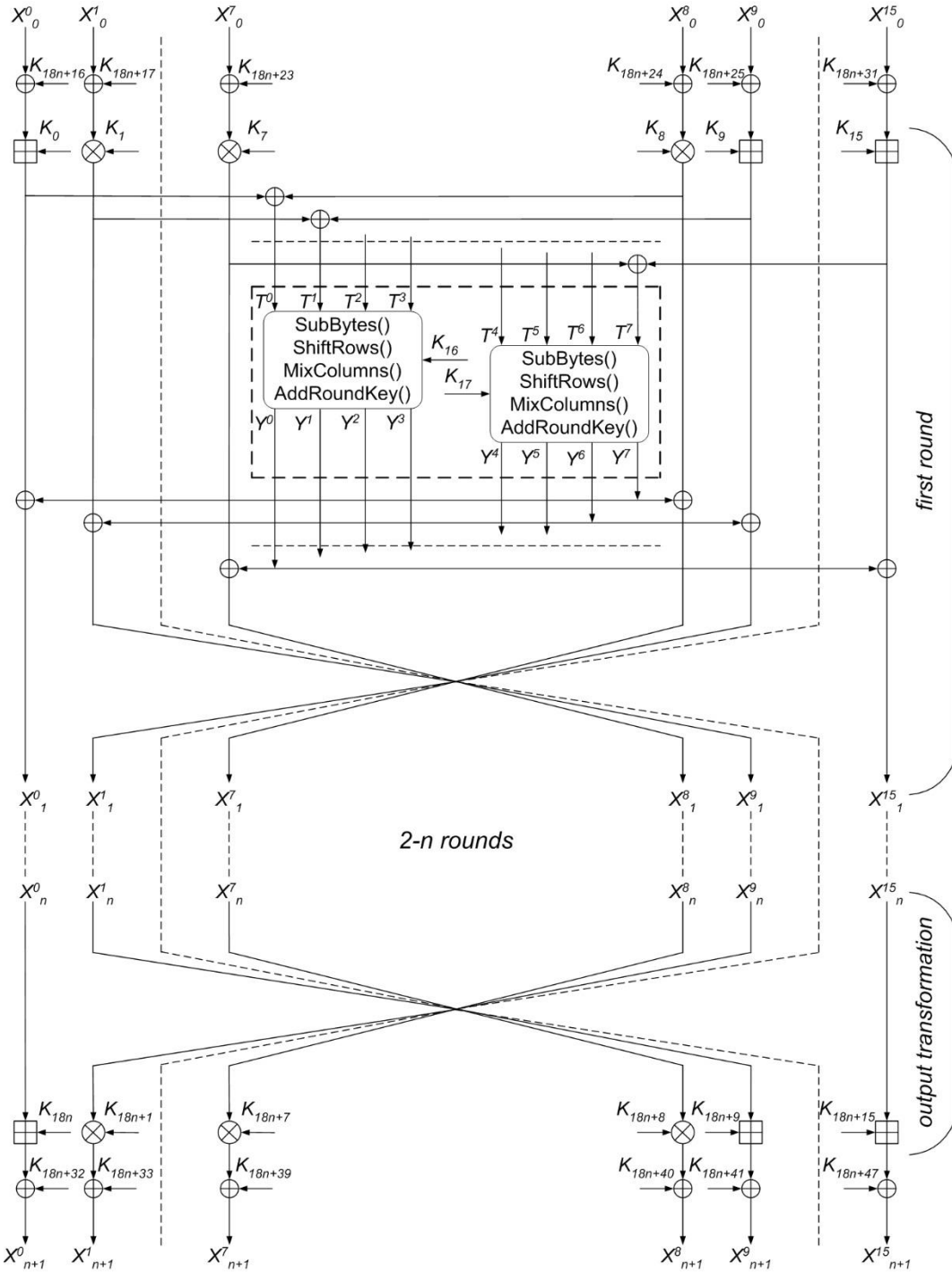


Fig. 5. The structure of the n -rounded encryption algorithm AES-IDEA16-2

Consider the round function of the encryption algorithm AES-IDEA16-2. First, 32-bit subblocks T^0, T^1, \dots, T^7 is divided into 8 bit subblocks $t_0^0, t_1^0, \dots, t_{15}^0$ and $t_0^1, t_1^1, \dots, t_{15}^1$ as follows: $t_i^0 = sb_{i \bmod 4}(T^{i \div 4})$, $t_i^1 = sb_{i \bmod 4}(T^{i \div 4 + 4})$, $i = \overline{0..15}$. Here div -integer part of the division, mod -remainder of the division and $sb_0(X) = x_0 x_1 \dots x_7$, $sb_1(X) = x_8 x_9 \dots x_{15}$, $sb_2(X) = x_{16} x_{17} \dots x_{23}$, $sb_3(X) = x_{24} x_{25} \dots x_{31}$, $X = x_0 x_1 \dots x_{31}$. As elements of the array *State* the first

round function selected $t_0^0, t_1^0, \dots, t_{15}^0$, as well as the second round function selected $t_0^1, t_1^1, \dots, t_{15}^1$. Then performed SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() transformation. In the AddRoundKey() transformation 128 bit keys are divided into 32 bit keys, i.e. $K_{18(i-1)+16}^j, K_{18(i-1)+17}^j, j = \overline{0..3}$. Here $K_{18(i-1)+16} = K_{18(i-1)+16}^0 || K_{18(i-1)+16}^1 || K_{18(i-1)+16}^2 || K_{18(i-1)+16}^3$, $K_{18(i-1)+17} = K_{18(i-1)+17}^0 || K_{18(i-1)+17}^1 || K_{18(i-1)+17}^2 || K_{18(i-1)+17}^3$. The elements of the array of keys the first round function $k_0^0, k_1^0, \dots, k_{15}^0$ and second round function $k_0^1, k_1^1, \dots, k_{15}^1$ is calculated as follows: $k_i^0 = sb_{i \bmod 4}(K_{36(i-1)+32}^{i \bmod 4})$, $k_i^1 = sb_{i \bmod 4}(K_{36(i-1)+33}^{i \bmod 4})$, $i = \overline{0..15}$. After AddRoundKey() transformation 8 bit output values combined and will receive eight 32 bit subblock Y^0, Y^1, \dots, Y^7 . Here Y^0, Y^1, Y^2, Y^3 —output value from the first round function, Y^4, Y^5, Y^6, Y^7 —output value from the second round function and $Y^0 = p_0^0 || p_1^0 || p_2^0 || p_3^0$, $Y^1 = p_4^0 || p_5^0 || p_6^0 || p_7^0$, $Y^2 = p_8^0 || p_9^0 || p_{10}^0 || p_{11}^0$, $Y^3 = p_{12}^0 || p_{13}^0 || p_{14}^0 || p_{15}^0$, $Y^4 = p_0^1 || p_1^1 || p_2^1 || p_3^1$, $Y^5 = p_4^1 || p_5^1 || p_6^1 || p_7^1$, $Y^6 = p_8^1 || p_9^1 || p_{10}^1 || p_{11}^1$, $Y^7 = p_{12}^1 || p_{13}^1 || p_{14}^1 || p_{15}^1$.

The S-boxes of SubBytes() transformation is given in Table 1 and 2 and the only nonlinear transformation. The length of the input and output blocks of S-boxes is equal to eight bits. The first S-box used in the first round function and the second S-box used in the second round function.

Table 1. The first S-box encryption algorithm AES-IDEA16-2

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0x0	0x4	0x0	0xF	0x9	0xA	0xF	0x5	0xA	0x9	0x5	0xB	0x6	0xA	0x3	0x4
0x1	1	B	4	D	A	9	8	2	7	C	0	C	3	4	6	1
0x2	0x4	0xF	0xA	0x0	0x3	0x7	0x7	0x3	0xC	0x4	0xD	0x6	0xF	0x2	0x1	0x4
0x3	C	1	B	E	2	5	A	8	5	3	B	7	E	8	0	6
0x4	0x9	0x8	0xE	0x0	0x5	0xB	0x8	0xB	0xF	0x6	0x7	0x7	0xF	0xB	0xE	0x9
0x5	B	4	0	0	4	9	E	F	6	D	8	D	7	A	2	9
0x6	0x8	0xF	0x1	0xA	0x2	0xF	0xC	0x0	0x6	0x2	0x5	0xC	0x2	0x4	0x8	0xA
0x7	8	0	4	1	5	4	D	D	F	F	3	E	3	5	F	6
0x8	0x3	0xB	0x0	0x8	0xC	0xB	0x9	0x7	0x3	0xE	0xE	0xC	0x1	0x8	0xE	0x0

4	4	4	A	7	2	D	2	9	A	8	1	A	E	B	D	2
0x	0x7	0x5	0xD	0xD	0xF	0xC	0x6	0xD	0xE	0x0	0x7	0x4	0xC	0x3	0x3	0x5
5	F	7	9	0	3	1	8	7	C	9	6	A	6	5	0	8
0x	0x1	0x7	0x7	0x7	0x2	0x7	0x4	0x4	0xD	0xD	0x7	0xA	0x9	0x5	0x1	0xD
6	2	2	3	7	B	0	0	7	8	5	B	C	8	E	9	1
0x	0xD	0x9	0xC	0x4	0xA	0xB	0x0	0x2	0xD	0xD	0x1	0xB	0x8	0x2	0xD	0xB
7	D	E	C	D	5	B	F	C	4	E	8	6	D	6	F	0
0x	0xF	0x2	0x6	0x9	0x8	0xB	0x9	0x3	0x1	0xC	0xE	0x1	0xB	0x2	0x6	0x5
8	A	0	A	5	6	1	D	B	7	F	9	B	7	4	0	5
0x	0xE	0x1	0xD	0xE	0x5	0xF	0x0	0xF	0x3	0x3	0x8	0xD	0x4	0xC	0x9	0x5
9	6	6	2	B	1	9	7	B	F	7	5	C	9	3	6	D
0x	0x6	0x0	0xA	0xD	0x2	0x2	0xA	0x6	0xE	0xF	0x8	0x4	0x4	0x1	0x3	0x5
A	C	5	D	3	1	A	2	1	4	5	0	4	2	3	D	F
0x	0xD	0xE	0x1	0x5	0xE	0x0	0x9	0x9	0x1	0x6	0x6	0x6	0xF	0xB	0x2	0x7
B	A	E	1	A	F	6	7	4	F	B	9	6	2	8	2	1
0x	0x2	0x1	0xE	0xA	0x7	0x8	0x7	0xB	0xC	0xA	0xE	0x9	0x8	0x9	0x1	0x5
C	7	A	7	8	4	A	C	5	4	E	3	3	3	1	C	9
0x	0xB	0xF	0x3	0x1	0x6	0x3	0xC	0x8	0xA	0xB	0x2	0xC	0xA	0x0	0x3	0x5
D	2	C	9	5	4	E	B	2	3	3	E	0	0	3	1	C
0x	0x2	0x9	0xA	0xC	0x0	0xF	0x0	0x5	0x4	0xD	0xE	0x8	0x1	0x8	0x5	0x0
E	9	0	F	8	B	F	8	6	8	6	5	1	D	C	B	C
0x	0xA	0x3	0xB	0x6	0x3	0x9	0x6	0x4	0x8	0xE	0x4	0xC	0x2	0xC	0x6	0x7
F	A	C	E	5	3	F	E	E	9	A	F	7	D	9	2	E

Table 2. The second S–box encryption algorithm AES–IDEA16–2

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x	0xF	0xD	0xE	0x0	0x9	0x5	0x1	0xB	0x6	0x8	0xB	0x0	0x7	0x6	0x2	0xF
0	8	0	3	1	5	7	A	1	B	8	5	E	7	D	3	5
0x	0xC	0x3	0x5	0xC	0x3	0x2	0x1	0x1	0xE	0xF	0x9	0x6	0x0	0x5	0xB	0xE

1	F	9	3	6	A	8	6	F	4	1	A	E	7	D	8	A
0x	0x9	0xE	0x7	0xF	0xA	0x1	0xC	0x0	0x2	0x4	0x1	0x0	0x2	0x1	0x7	0x9
2	7	B	9	A	C	5	E	8	6	B	2	9	4	3	D	3
0x	0xD	0x3	0xA	0x7	0x6	0x2	0xC	0xC	0x4	0x4	0xB	0xC	0x7	0xE	0xC	0x6
3	3	B	1	6	7	2	5	0	F	2	3	3	A	C	C	9
0x	0x2	0x2	0xD	0xE	0xF	0x0	0xB	0x1	0x1	0x5	0x7	0xD	0x8	0xD	0x4	0xF
4	7	F	F	D	B	C	4	0	B	8	B	A	4	5	3	E
0x	0x0	0xA	0x9	0xB	0x3	0xF	0x5	0xA	0x4	0xD	0x2	0xD	0xE	0x2	0x3	0x9
5	D	A	E	D	D	D	0	2	1	9	E	2	2	5	E	4
0x	0xB	0x3	0x3	0x2	0x5	0x3	0xF	0xE	0x9	0xA	0x1	0x4	0x9	0x8	0x9	0xB
6	C	7	5	C	B	3	7	8	C	6	4	C	1	9	B	F
0x	0x8	0x8	0xC	0xC	0x6	0x1	0xC	0x4	0xA	0x8	0x9	0x2	0xC	0x6	0x8	0x3
7	7	C	7	D	F	1	4	4	4	1	9	B	8	1	3	6
0x	0x1	0x7	0x5	0xA	0xE	0x3	0x8	0x1	0xA	0xC	0x5	0x9	0x2	0x6	0x7	0xA
8	E	C	4	B	F	4	A	9	7	1	A	F	9	5	1	E
0x	0x6	0xA	0xB	0x5	0xB	0x1	0xE	0x1	0x0	0x2	0xE	0x8	0xD	0xF	0xA	0x8
9	4	5	9	E	7	8	5	C	0	1	9	5	4	9	D	F
0x	0x4	0xE	0x4	0xB	0x7	0x5	0x7	0x7	0x6	0x2	0xF	0xE	0xF	0xB	0x0	0x8
A	9	1	E	B	E	9	0	3	0	0	2	E	3	E	4	B
0x	0x9	0x4	0xB	0x9	0x4	0xE	0xA	0xA	0x8	0x5	0x5	0x6	0x3	0x1	0x7	0x3
B	8	5	A	0	7	7	F	9	6	6	2	C	F	7	8	1
0x	0x6	0x9	0x6	0x5	0x2	0xD	0x0	0x2	0xE	0x4	0x7	0xB	0xF	0xB	0x8	0x9
C	3	D	6	5	A	7	B	D	6	8	F	6	4	2	0	6
0x	0x3	0x0	0x1	0xA	0x6	0x0	0xD	0xF	0x7	0x3	0x4	0xF	0x7	0xF	0x3	0x8
D	2	3	D	3	8	2	8	6	2	0	0	F	4	C	C	D
0x	0x5	0xB	0x4	0xD	0xD	0x0	0xD	0xA	0xD	0xA	0x6	0xF	0x8	0xC	0x9	0xC
E	F	0	A	E	D	5	B	8	6	0	2	0	2	A	2	2
0x	0x5	0x0	0x0	0x6	0x3	0x8	0x4	0xC	0xD	0x5	0xC	0xE	0x4	0xD	0x7	0x0
F	1	6	A	A	8	E	D	B	1	C	9	0	6	C	5	F

Consider encryption process of encryption algorithm AES–IDEA16–2. First, 512–bit block of plaintext x is partitioned into 32–bit subblocks $X_0^0, X_0^1, \dots, X_0^{15}$ and the following steps are performed:

1. subblocks $X_0^0, X_0^1, \dots, X_0^{15}$ are summed to XOR with the corresponding round keys $K_{18n+16}, K_{18n+17}, \dots, K_{18n+31}$: $X_0^i = X_0^i \oplus K_{18n+16+i}, i = \overline{0..15}$.

2. subblocks $X_0^0, X_0^1, \dots, X_0^{15}$ multiplied and summarized to the same round keys $K_{18(i-1)}, K_{18(i-1)+1}, \dots, K_{18(i-1)+15}$ and calculated T_0, T_1, \dots, T_{15} as follows

$$\begin{aligned} T_0 &= (X_{i-1}^0 + K_{18(i-1)}) \oplus (X_{i-1}^8 \cdot K_{18(i-1)+8}), & T_1 &= (X_{i-1}^1 \cdot K_{18(i-1)+1}) \oplus (X_{i-1}^9 + K_{18(i-1)+9}), \\ T_2 &= (X_{i-1}^2 + K_{18(i-1)+2}) \oplus (X_{i-1}^{10} \cdot K_{18(i-1)+10}), & T_3 &= (X_{i-1}^3 \cdot K_{18(i-1)+3}) \oplus (X_{i-1}^{11} + K_{18(i-1)+11}), \\ T_4 &= (X_{i-1}^4 + K_{18(i-1)+4}) \oplus (X_{i-1}^{12} \cdot K_{18(i-1)+12}), & T_5 &= (X_{i-1}^5 \cdot K_{18(i-1)+5}) \oplus (X_{i-1}^{13} + K_{18(i-1)+13}), \\ T_6 &= (X_{i-1}^6 + K_{18(i-1)+6}) \oplus (X_{i-1}^{14} \cdot K_{18(i-1)+14}), & T_7 &= (X_{i-1}^7 \cdot K_{18(i-1)+7}) \oplus (X_{i-1}^{15} + K_{18(i-1)+15}), \quad i=1. \end{aligned}$$

3. subblocks T_0, T_1, \dots, T_{15} written in two arrays State and performed SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() transformation. After the transformation 32 bit subblocks Y^0, Y^1, \dots, Y^7 is obtained

4. subblocks Y^0, Y^1, \dots, Y^7 are summed to XOR with the corresponding subblocks X_{i-1}^j i.e. $X_{i-1}^j = X_{i-1}^j \oplus Y_{7-j}, X_{i-1}^{j+8} = X_{i-1}^{j+8} \oplus Y_{7-j}, j = \overline{0..7}, i=1$.

5. at the end of round except subblocks X_i^0 and X_{i-1}^{16} all subblocks will be swapped $X_i^j = X_{i-1}^{j-15}, j = \overline{1..14}, i=1$.

6. repeating steps 2–5 n times, i.e., $i = \overline{2..n}$, the 32bit subblocks $X_n^0, X_n^1, \dots, X_n^{31}$ is obtained

7. in the output transformation round keys $K_{18n}, K_{18n+1}, \dots, K_{18n+15}$ are multiplied and summed with the corresponding subblocks $X_{n+1}^0 = X_n^0 + K_{18n}, X_{n+1}^1 = X_n^{14} \cdot K_{18n+1}, X_{n+1}^2 = X_n^{13} + K_{18n+2}, X_{n+1}^3 = X_n^{12} \cdot K_{18n+3}, X_{n+1}^4 = X_n^{11} + K_{18n+4}, X_{n+1}^5 = X_n^{10} \cdot K_{18n+5}, X_{n+1}^6 = X_n^9 + K_{18n+6}, X_{n+1}^7 = X_n^8 \cdot K_{18n+7}, X_{n+1}^8 = X_n^7 \cdot K_{18n+8}, X_{n+1}^9 = X_n^6 + K_{18n+9}, X_{n+1}^{10} = X_n^5 \cdot K_{18n+10}, X_{n+1}^{11} = X_n^4 + K_{18n+11}, X_{n+1}^{12} = X_n^3 \cdot K_{18n+12}, X_{n+1}^{13} = X_n^2 + K_{18n+13}, X_{n+1}^{14} = X_n^1 \cdot K_{18n+14}, X_{n+1}^{15} = X_n^{15} + K_{18n+15}$.

8. subblocks $X_{n+1}^0, X_{n+1}^1, \dots, X_{n+1}^{15}$ are summed to XOR with the corresponding round keys $K_{18n+32}, K_{18n+33}, \dots, K_{18n+47}$: $X_{n+1}^j = X_{n+1}^j \oplus K_{18n+32+j}$, $j = \overline{0..15}$. As ciphertext plaintext x are accepted combining 32bit sub-blocks $X_{n+1}^0 || X_{n+1}^1 || \dots || X_{n+1}^{15}$.

Key generation encryption algorithm AES–IDEA16–2

In the n –round encryption algorithm AES–IDEA16–2 each round are applied 16 round keys length of 32 bits, two key length of 128 bits and in output transformation 16 round keys length of 32 bits. Besides, before the first round and after output transformation applied 16 round keys length of 32 bits. Total number of 32–bit round keys equal to $16n+48$ and 128–bit round key equal to $2n$. If 128–bit round keys convert to four 32–bit key, the total number of 32 bit keys equal to $24n+48$. When encryption in Figure 5 instead k_i used encryption round keys K_i^c , when decryption decryption round keys K_i^d .

When generating round key like encryption algorithm AES are used array Rcon: Rcon=[0x00000001, 0x00000002, 0x00000004, 0x00000008, 0x00000010, 0x00000020, 0x00000040, 0x00000080, 0x00000100, 0x00000200, 0x00000400, 0x00000800, 0x00001000, 0x00002000, 0x00004000, 0x00008000, 0x00010000, 0x00020000, 0x00040000, 0x00080000, 0x00100000, 0x00200000, 0x00400000, 0x00800000, 0x01000000, 0x02000000, 0x04000000, 0x08000000, 0x10000000, 0x20000000, 0x40000000, 0x80000000].

The key of encryption algorithm K length l ($256 \leq l \leq 1024$) bit is divided into 32–bit round keys $K_0^c, K_1^c, \dots, K_{Lenght-1}^c$, $Lenght = l/32$, здесь $K = \{k_0, k_1, \dots, k_{l-1}\}$, $K_0^c = \{k_0, k_1, \dots, k_{31}\}$, $K_1^c = \{k_{32}, k_{33}, \dots, k_{63}\}, \dots, K_{Lenght-1}^c = \{k_{l-32}, k_{l-31}, \dots, k_{l-1}\}$ and $K = K_0^c || K_1^c || \dots || K_{Lenght-1}^c$. Then calculated $K_L = K_0^c \oplus K_1^c \oplus \dots \oplus K_{Lenght-1}^c$. If $K_L = 0$ then as K_L selected 0xC5C31537, i.e. $K_L = 0xC5C31537$.

When generating a round keys K_i^c , $i = \overline{Lenght..24n+47}$ used SubBytes32() and RotWord32() transformation, here SubBytes32()–transformation 32–bit subblock in the S–block, i.e. $SubBytes32(X) = S_0(sb_0(X)) || S_1(sb_1(X)) || S_0(sb_0(X)) || S_1(sb_1(X))$, RotWord32() –

cyclic shift 32-bit subblock left by 1 bit. Here S_0 and S_1 – the S-boxes, given in the table 1 and 2. If the conditions $i \bmod 3 = 1$, then round keys calculated as

$$K_i^c = \text{SubBytes}32(K_{i-\text{Length}}^c) \oplus \text{SubBytes}32(\text{RotWord}32(K_{i-\text{Length}}^c)) \oplus \text{Rcon}[i \bmod 32] \oplus K_L, \quad \text{otherwise}$$

$K_i^c = \text{SubBytes}32(K_{i-\text{Length}}^c) \oplus \text{SubBytes}32(K_{i-\text{Length}+1}^c) \oplus K_L$. After every generation of round keys value K_L rotated to the left by 1 bit.

Decryption round keys are computed based on encryption round keys and decryption keys output transformation associated with encryption keys as follows:

$$\begin{aligned} & (K_{24n}^{d'}, K_{24n+1}^{d'}, K_{24n+2}^{d'}, K_{24n+3}^{d'}, K_{24n+4}^{d'}, K_{24n+5}^{d'}, K_{24n+6}^{d'}, K_{24n+7}^{d'}, K_{24n+8}^{d'}, K_{24n+9}^{d'}, K_{24n+10}^{d'}, K_{24n+11}^{d'}, K_{24n+12}^{d'}, K_{24n+13}^{d'}, K_{24n+14}^{d'}, \\ & K_{24n+15}^{d'}) = (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, (K_8^c)^{-1}, -K_9^c, (K_{10}^c)^{-1}, -K_{11}^c, (K_{12}^c)^{-1}, -K_{13}^c, \\ & (K_{14}^c)^{-1}, -K_{15}^c) \end{aligned}$$

In the same manner, decryption keys second, third, and n-round associated with the encryption keys following:

$$\begin{aligned} & (K_{24(i-1)}^{d'}, K_{24(i-1)+1}^{d'}, K_{24(i-1)+2}^{d'}, K_{24(i-1)+3}^{d'}, K_{24(i-1)+4}^{d'}, K_{24(i-1)+5}^{d'}, K_{24(i-1)+6}^{d'}, K_{24(i-1)+7}^{d'}, K_{24(i-1)+8}^{d'}, K_{24(i-1)+9}^{d'}, K_{24(i-1)+10}^{d'}, K_{24(i-1)+11}^{d'}, \\ & K_{24(i-1)+12}^{d'}, K_{24(i-1)+13}^{d'}, K_{24(i-1)+14}^{d'}, K_{24(i-1)+15}^{d'}) = (-K_{24(n-i+1)}^{c'}, (K_{24(n-i+1)+1}^{c'})^{-1}, -K_{24(n-i+1)+2}^{c'}, (K_{24(n-i+1)+3}^{c'})^{-1}, -K_{24(n-i+1)+4}^{c'}, \\ & (K_{24(n-i+1)+5}^{c'})^{-1}, -K_{24(n-i+1)+6}^{c'}, (K_{24(n-i+1)+7}^{c'})^{-1}, -K_{24(n-i+1)+8}^{c'}, (K_{24(n-i+1)+9}^{c'})^{-1}, -K_{24(n-i+1)+10}^{c'}, (K_{24(n-i+1)+11}^{c'})^{-1}, \\ & -K_{24(n-i+1)+12}^{c'}, (K_{24(n-i+1)+13}^{c'})^{-1}, -K_{24(n-i+1)+14}^{c'}, (K_{24(n-i+1)+15}^{c'})^{-1}), i = \overline{2\dots n} \end{aligned}$$

$$K_{24(i-1)+16+j}^{d'} = K_{24(n-i)+16+j}^{c'}, \quad j = \overline{0\dots 7}, \quad i = \overline{2\dots n}$$

Decryption of round key first round associated a encryption round key as follows:

$$\begin{aligned} & (K_0^{d'}, K_1^{d'}, K_2^{d'}, K_3^{d'}, K_4^{d'}, K_5^{d'}, K_6^{d'}, K_7^{d'}, K_8^{d'}, K_9^{d'}, K_{10}^{d'}, K_{11}^{d'}, K_{12}^{d'}, K_{13}^{d'}, K_{14}^{d'}, K_{15}^{d'}, K_{16}^{d'}, K_{17}^{d'}) = (-K_{24n}^{c'}, (K_{24n+1}^{c'})^{-1}, -K_{24n+2}^{c'}, \\ & (K_{24n+3}^{c'})^{-1}, -K_{24n+4}^{c'}, (K_{24n+5}^{c'})^{-1}, -K_{24n+6}^{c'}, (K_{24n+7}^{c'})^{-1}, (K_{24n+8}^{c'})^{-1}, -K_{24n+9}^{c'}, (K_{24n+10}^{c'})^{-1}, -K_{24n+11}^{c'}, (K_{24n+12}^{c'})^{-1}, -K_{24n+13}^{c'}, \\ & (K_{24n+14}^{c'})^{-1}, -K_{24n+15}^{c'}, K_{24(n-1)+16}^{c'}, K_{24(n-1)+17}^{c'}) \end{aligned}$$

Decryption round key, applied to the first round and after output transformation associated with encryption keys as follows: $K_{24n+16+j}^{d'} = K_{24n+32+j}^{c'}$, $K_{24n+32+j}^{d'} = K_{24n+16+j}^{c'}$, $j = \overline{0\dots 15}$

Encryption round keys K_i^c associated with the keys $K_i^{c'}$ are as follows: $K_{18i+j}^c = K_{24i+j}^{c'}$, $j = \overline{0\dots 15}$, $K_{18i+16}^c = K_{24i+16}^{c'} \parallel K_{24i+17}^{c'} \parallel K_{24i+18}^{c'} \parallel K_{24i+19}^{c'}$, $K_{18i+17}^c = K_{24i+20}^{c'} \parallel K_{24i+21}^{c'} \parallel K_{24i+22}^{c'} \parallel K_{24i+23}^{c'}$. In the same manner, decryption round keys K_i^d associated with the keys $K_i^{d'}$ as follows: $K_{18i+j}^d = K_{24i+j}^{d'}$, $j = \overline{0\dots 15}$, $K_{18i+16}^d = K_{24i+16}^{d'} \parallel K_{24i+17}^{d'} \parallel K_{24i+18}^{d'} \parallel K_{24i+19}^{d'}$, $K_{18i+17}^d = K_{24i+20}^{d'} \parallel K_{24i+21}^{d'} \parallel K_{24i+22}^{d'} \parallel K_{24i+23}^{d'}$.

Structure of an encryption algorithm AES–RFBKIDEA16–2

Scheme n -round encryption algorithm AES–RFWKIDEA16–2 is shown in Figure 6, and the length of the sub-blocks x^0, x^1, \dots, x^{15} , the length of the round keys $K_{16(i-1)}, K_{16(i-1)+1}, \dots, K_{16(i-1)+15}, i = \overline{1..n+1}, K_{16n+16}, K_{16n+17}, \dots, K_{16n+47}$ equal to 32 bits.

In contrast from the encryption algorithm AES–IDEA16–2 in the encryption algorithm AES–RFWKIDEA16–2 as are used in the transformation round function SubBytes(), ShiftRows(), MixColumns() encryption algorithm AES. Like the encryption algorithm AES–IDEA16–2, in algorithm AES–RFWKIDEA16–2 32 bit subblocks T^0, T^1, \dots, T^7 are divided into 8 bit subblocks $t_0^0, t_1^0, \dots, t_{15}^0$ and $t_0^1, t_1^1, \dots, t_{15}^1$. Then performed transformation SubBytes(), ShiftRows(), MixColumns(). After transformation MixColumns() get 32 bit subblocks Y^0, Y^1, \dots, Y^7 , here $Y^0 = p_0^0 \parallel p_1^0 \parallel p_2^0 \parallel p_3^0, Y^1 = p_4^0 \parallel p_5^0 \parallel p_6^0 \parallel p_7^0, Y^2 = p_8^0 \parallel p_9^0 \parallel p_{10}^0 \parallel p_{11}^0, Y^3 = p_{12}^0 \parallel p_{13}^0 \parallel p_{14}^0 \parallel p_{15}^0, Y^4 = p_0^1 \parallel p_1^1 \parallel p_2^1 \parallel p_3^1, Y^5 = p_4^1 \parallel p_5^1 \parallel p_6^1 \parallel p_7^1, Y^6 = p_8^1 \parallel p_9^1 \parallel p_{10}^1 \parallel p_{11}^1, Y^7 = p_{12}^1 \parallel p_{13}^1 \parallel p_{14}^1 \parallel p_{15}^1$.

The S-boxes SubBytes() transformation is given in Table 3 and 4 and the only nonlinear transformation. The length of the input and output blocks of S-boxes is equal to eight bits. The first S-box used in the first round function and the second S-box used in the second round function.

Table 3. The first S-block of an encryption algorithm AES–RFWKIDEA16–2

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x	0x1	0xF	0xF	0xB	0xE	0x2	0x5	0xF	0xD	0x5	0x6	0x4	0xA	0x8	0xF	0x2
0	F	A	4	9	8	4	2	8	0	A	9	3	5	9	0	D
0x	0x8	0xD	0xB	0x2	0xD	0x9	0xA	0x0	0x6	0xB	0x1	0x8	0xE	0x8	0x5	0x5
1	0	C	5	3	3	B	7	4	A	C	2	6	0	8	B	7
0x	0x2	0x9	0x9	0xD	0x4	0xA	0x4	0x1	0xA	0x5	0x3	0xD	0x6	0xF	0x0	0xB
2	0	0	8	7	A	8	7	A	6	1	6	D	E	1	9	1
0x	0xF	0x1	0x7	0x6	0x2	0x3	0x2	0x7	0xC	0xF	0x3	0x7	0x9	0x0	0x8	0x1
3	5	4	8	2	5	7	C	A	0	2	0	5	7	E	F	8
0x	0x6	0x0	0x0	0xC	0x1	0x8	0xA	0xF	0x9	0xD	0x5	0x5	0xA	0xA	0x3	0x4

4	1	5	0	9	0	B	E	E	5	E	0	6	F	C	5	6
0x	0x4	0x1	0x8	0x0	0x4	0x4	0xB	0x7	0xF	0x5	0xC	0x3	0x3	0xA	0x4	0x2
5	C	3	3	D	D	9	A	7	D	9	2	2	3	9	2	F
0x	0xC	0xE	0x2	0x0	0xD	0x7	0xE	0x9	0x4	0xE	0x6	0xC	0x7	0x9	0xD	0xC
6	A	1	9	A	1	0	5	F	B	6	F	F	9	D	5	5
0x	0xA	0xC	0xE	0x4	0x4	0x3	0xE	0xA	0x2	0xF	0x1	0x9	0x1	0x7	0x3	0x2
7	0	B	4	8	1	9	B	B	E	9	D	4	E	C	1	6
0x	0xC	0xC	0x2	0xD	0x0	0xE	0x9	0x5	0x2	0xB	0x1	0x4	0x5	0xE	0xF	0x8
8	3	E	B	4	1	E	2	D	1	D	6	4	C	D	C	2
0x	0x2	0xE	0x9	0x8	0xA	0x9	0xA	0x0	0x7	0x3	0x5	0x6	0x6	0xD	0x8	0xC
9	A	9	C	7	1	A	D	B	E	8	8	8	B	8	D	4
0x	0x9	0x3	0x0	0x5	0x0	0x1	0x3	0x3	0xB	0xF	0xB	0xC	0x7	0x0	0xE	0x5
A	9	C	7	4	6	9	B	4	B	F	3	6	4	2	F	5
0x	0xD	0x6	0x9	0xB	0xA	0x6	0x4	0x1	0x6	0xE	0x7	0x4	0x8	0x6	0x5	0xB
B	A	C	3	E	4	5	5	C	7	3	2	E	5	0	F	8
0x	0xB	0x8	0xE	0xE	0x5	0x6	0x1	0xC	0xA	0x5	0xC	0x6	0xE	0xF	0x3	0xE
C	4	C	2	C	3	4	5	D	2	E	1	6	A	7	E	7
0x	0xB	0x7	0xC	0xB	0xD	0xB	0x9	0x2	0xF	0x7	0x3	0x8	0xA	0x8	0x8	0x0
D	7	1	C	0	F	6	E	2	3	F	A	1	A	E	A	C
0x	0x4	0x3	0x9	0xC	0xC	0x2	0x9	0xD	0xA	0xB	0x7	0x7	0xF	0xD	0x7	0xB
E	0	F	6	7	8	8	1	B	3	F	3	B	6	6	6	2
0x	0x7	0x2	0xD	0x1	0x1	0x0	0x0	0x1	0x3	0x4	0xD	0xF	0x6	0x0	0x6	0x8
F	D	7	2	7	B	3	8	1	D	F	9	B	3	F	D	4

Table 4. The second S–block of an encryption algorithm AES–RFBKIDEA16–2

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x	0x8	0x1	0xB	0x9	0xF	0x9	0xA	0xF	0x7	0x2	0xB	0xD	0xD	0x9	0x7	0x6
0	0	B	9	7	C	A	E	B	6	D	4	9	2	E	8	9
0x	0x6	0x3	0xD	0xC	0xE	0x7	0x3	0x9	0x2	0x2	0xB	0x4	0x7	0xE	0x5	0x1

1	D	4	5	B	6	9	2	4	4	6	2	C	F	E	D	F
0x	0x5	0x6	0xE	0x2	0x2	0xE	0x1	0x3	0x4	0x3	0x7	0x4	0xE	0x0	0xA	0x1
2	B	A	9	7	A	0	8	1	2	E	D	4	5	8	6	4
0x	0xC	0x9	0xC	0xA	0xE	0x0	0x1	0x2	0x7	0x9	0x5	0xF	0x3	0xF	0xB	0xD
3	9	3	3	7	A	D	9	3	1	8	C	1	B	7	F	1
0x	0x3	0xE	0x5	0x8	0x5	0x7	0xC	0xD	0xD	0xD	0x4	0x6	0xB	0x2	0xE	0x6
4	7	4	5	2	2	E	1	A	B	4	E	F	1	1	D	8
0x	0x0	0xC	0xF	0x6	0x7	0xB	0x0	0x1	0x4	0xB	0x9	0xB	0xC	0x9	0xA	0x8
5	B	2	D	7	B	A	7	1	A	D	1	C	C	0	9	9
0x	0x1	0x0	0xA	0x3	0x0	0x4	0xC	0xB	0x5	0x5	0x9	0xA	0xB	0x5	0xC	0xC
6	2	F	8	6	6	0	E	8	A	E	5	3	3	8	7	0
0x	0x6	0x6	0xB	0xC	0x3	0xA	0x6	0x7	0xF	0x8	0x6	0xA	0xF	0x0	0x2	0x7
7	3	2	E	A	9	F	C	0	9	B	0	B	0	2	C	A
0x	0xE	0xD	0x4	0xB	0x2	0xD	0x8	0x7	0x2	0x5	0x7	0x8	0x0	0x4	0x3	0x8
8	1	3	8	7	5	D	A	C	B	6	3	8	C	D	A	D
0x	0x3	0x8	0x2	0x3	0x1	0x0	0x5	0x4	0xE	0xD	0xC	0xC	0x5	0xF	0x5	0xB
9	8	C	8	C	3	9	1	6	2	F	D	4	4	5	F	0
0x	0x9	0x1	0x0	0x8	0x7	0xA	0x4	0x9	0x7	0xA	0xF	0x5	0x8	0xB	0xA	0xF
A	9	E	4	F	4	1	F	D	7	A	4	0	1	5	D	F
0x	0x1	0x0	0xF	0xC	0xA	0xF	0xF	0x1	0x1	0xE	0xA	0xE	0xD	0x4	0x9	0xE
B	5	5	A	6	2	6	8	0	6	F	0	B	C	7	C	7
0x	0xA	0x2	0x9	0x3	0xD	0x8	0xE	0x4	0x8	0xE	0x0	0x6	0x1	0x2	0xF	0x2
C	5	F	F	D	E	6	3	3	3	C	1	6	C	9	E	E
0x	0x3	0x3	0x3	0x6	0xA	0x4	0xC	0xB	0xE	0x9	0x3	0x1	0x0	0xC	0x0	0x1
D	5	0	3	4	4	5	8	B	8	2	F	D	0	F	E	7
0x	0x4	0x8	0x4	0x2	0xF	0xD	0x1	0x6	0xF	0xB	0xD	0x5	0x5	0x5	0x6	0x8
E	9	E	B	0	2	8	A	5	3	6	0	3	9	7	1	4
0x	0x7	0x0	0x9	0x0	0x4	0xC	0xD	0x2	0x6	0x9	0x8	0x6	0xD	0x8	0x7	0xA
F	2	A	6	3	1	5	6	2	E	B	5	B	7	7	5	C

Consider encryption process in the encryption algorithm AES–RFWKIDEA16–2. First 512 bit block of plaintext x is partitioned into 32 bit sub–block $x_0^0, x_0^1, \dots, x_0^{15}$ and the following steps:

1. subblocks $x_0^0, x_0^1, \dots, x_0^{15}$ are summed to XOR with the corresponding round keys $K_{16n+16}, K_{16n+17}, \dots, K_{16n+31}$: $X_0^i = X_0^i \oplus K_{16n+16+i}, i = \overline{0..15}$.

2. subblocks $x_0^0, x_0^1, \dots, x_0^{15}$ multiplied and added to the same round keys $K_{16(i-1)}, K_{16(i-1)+1}, \dots, K_{16(i-1)+15}$ and computed T_0, T_1, \dots, T_{15} as follows $T_0 = (X_{i-1}^0 + K_{16(i-1)}) \oplus (X_{i-1}^8 \cdot K_{16(i-1)+8}),$
 $T_1 = (X_{i-1}^1 \cdot K_{16(i-1)+1}) \oplus (X_{i-1}^9 + K_{16(i-1)+9}),$ $T_2 = (X_{i-1}^2 + K_{16(i-1)+2}) \oplus (X_{i-1}^{10} \cdot K_{16(i-1)+10}),$
 $T_3 = (X_{i-1}^3 \cdot K_{16(i-1)+3}) \oplus (X_{i-1}^{11} + K_{16(i-1)+11}),$ $T_4 = (X_{i-1}^4 + K_{16(i-1)+4}) \oplus (X_{i-1}^{12} \cdot K_{16(i-1)+12}),$
 $T_5 = (X_{i-1}^5 \cdot K_{16(i-1)+5}) \oplus (X_{i-1}^{13} + K_{16(i-1)+13}),$ $T_6 = (X_{i-1}^6 + K_{16(i-1)+6}) \oplus (X_{i-1}^{14} \cdot K_{16(i-1)+14}),$
 $T_7 = (X_{i-1}^7 \cdot K_{16(i-1)+7}) \oplus (X_{i-1}^{15} + K_{16(i-1)+15}), i = 1.$

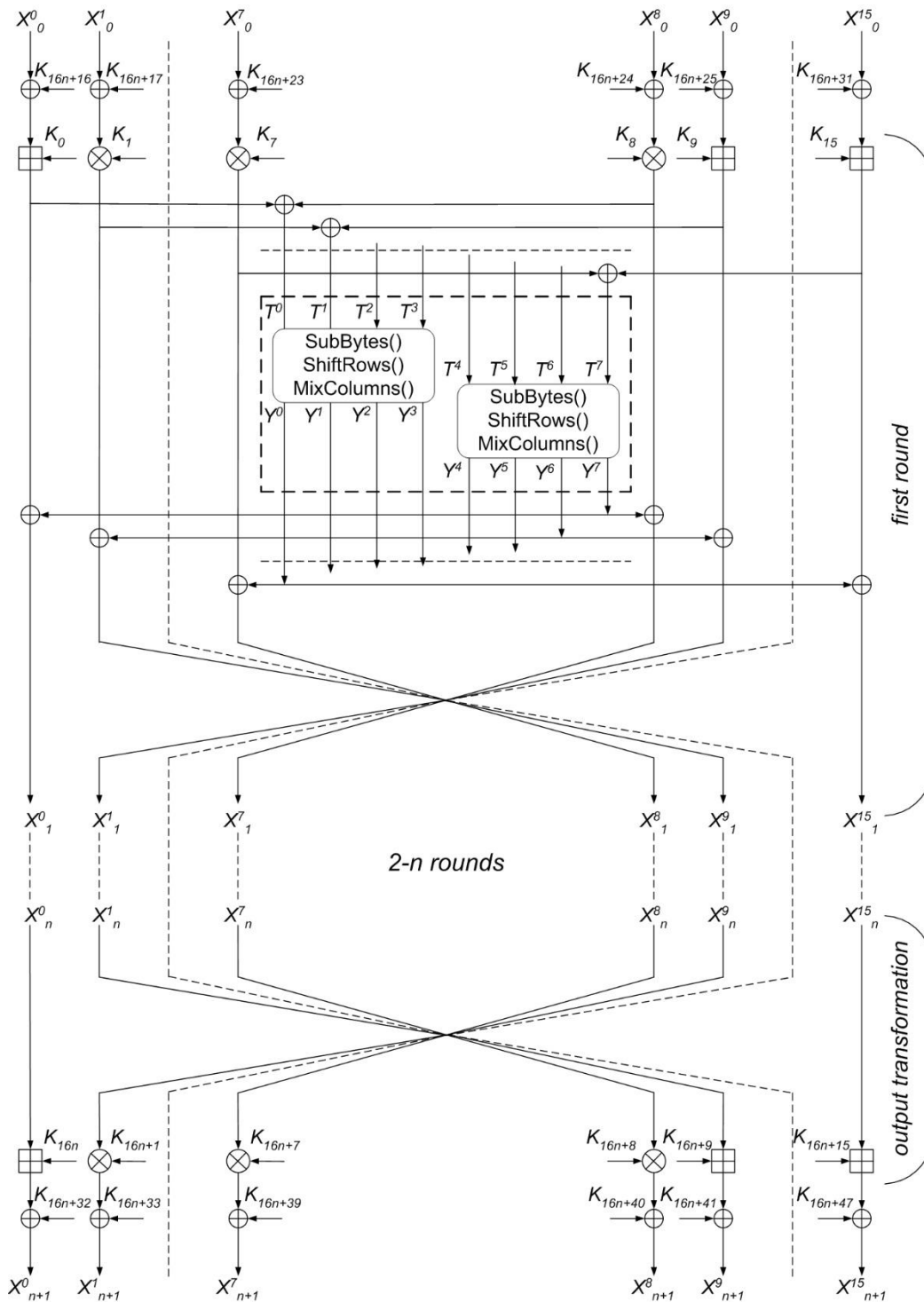


Fig. 6. The structure of n -round encryption algorithm AES-RFWKIDEA16-2

3. subblocks T_0, T_1, \dots, T_{15} written in two arrays State and performed SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() transformation. After the transformation will turn 32 bit subblocks Y^0, Y^1, \dots, Y^7 .

4. subblocks Y^0, Y^1, \dots, Y^7 are summed to XOR with the corresponding subblocks X_{i-1}^j i.e. $X_{i-1}^j = X_{i-1}^j \oplus Y_{7-j}$, $X_{i-1}^{j+8} = X_{i-1}^{j+8} \oplus Y_{7-j}$, $j = \overline{0..7}$, $i = 1$.

5. at the end of round except subblocks X_i^0 and X_{i-1}^{16} all subblocks will be swapped $X_i^j = X_{i-1}^{7+j}$, $X_i^{j+7} = X_{i-1}^j$, $j = \overline{1..7}$, $i = 1$

6. repeating steps 2–5 n times, ie, $i = \overline{2..n}$, the 32 bit subblocks $X_n^0, X_n^1, \dots, X_n^{31}$ is obtained.

7. in the output transformation round keys $K_{16n}, K_{16n+1}, \dots, K_{16n+15}$ are multiplied and summed with the corresponding subblocks $X_{n+1}^0 = X_n^0 + K_{16n}$, $X_{n+1}^1 = X_n^{14} \cdot K_{16n+1}$, $X_{n+1}^2 = X_n^{13} + K_{16n+2}$, $X_{n+1}^3 = X_n^{12} \cdot K_{16n+3}$, $X_{n+1}^4 = X_n^{11} + K_{16n+4}$, $X_{n+1}^5 = X_n^{10} \cdot K_{16n+5}$, $X_{n+1}^6 = X_n^9 + K_{16n+6}$, $X_{n+1}^7 = X_n^8 \cdot K_{16n+7}$, $X_{n+1}^8 = X_n^7 \cdot K_{16n+8}$, $X_{n+1}^9 = X_n^6 + K_{16n+9}$, $X_{n+1}^{10} = X_n^5 \cdot K_{16n+10}$, $X_{n+1}^{11} = X_n^4 + K_{16n+11}$, $X_{n+1}^{12} = X_n^3 \cdot K_{16n+12}$, $X_{n+1}^{13} = X_n^2 + K_{16n+13}$, $X_{n+1}^{14} = X_n^1 \cdot K_{16n+14}$, $X_{n+1}^{15} = X_n^{15} + K_{16n+15}$.

8. subblocks $X_{n+1}^0, X_{n+1}^1, \dots, X_{n+1}^{15}$ are summed to XOR with the corresponding round keys $K_{16n+32}, K_{16n+33}, \dots, K_{16n+47}$: $X_{n+1}^j = X_{n+1}^j \oplus K_{16n+32+j}$, $j = \overline{0..15}$. As ciphertext plaintext x are accepted combining 32 bit subblocks $X_{n+1}^0 || X_{n+1}^1 || \dots || X_{n+1}^{15}$.

The key generation of an encryption algorithm AES–RFWKIDEA16–2

In the n -round encryption algorithm AES–RFWKIDEA16–2 each round applied 16 round keys length of 32 bits and in output transformation 16 round keys length of 32 bits. Besides, before the first round and after output transformation are applied 16 round keys length of 32 bits. Total number 32 bit round key equal to $16n+48$. When encryption in Figure 6 instead K_i used encryption round keys K_i^c , when decryption round keys K_i^d .

The key of an encryption algorithm K length of l ($256 \leq l \leq 1024$) bit is divided into 32 bit round keys $K_0^c, K_1^c, \dots, K_{Lenght-1}^c$, $Lenght = l/32$, here $K = \{k_0, k_1, \dots, k_{l-1}\}$, $K_0^c = \{k_0, k_1, \dots, k_{31}\}$, $K_1^c = \{k_{32}, k_{33}, \dots, k_{63}\}, \dots$, $K_{Lenght-1}^c = \{k_{l-32}, k_{l-31}, \dots, k_{l-1}\}$ and $K = K_0^c || K_1^c || \dots || K_{Lenght-1}^c$. Then calculated $K_L = K_0^c \oplus K_1^c \oplus \dots \oplus K_{Lenght-1}^c$. If $K_L = 0$ then as K_L selected 0xC5C31537, i.e. $K_L = 0xC5C31537$. If the conditions $i \bmod 3 = 1$, then round keys calculated as $K_i^c = SubBytes32(K_{i-Lenght}^c) \oplus SubBytes32(RotWord32(K_{i-Lenght}^c)) \oplus Rcon[i \bmod 32] \oplus K_L$, otherwise

$K_i^c = \text{SubBytes32}(K_{i-\text{Length}}^c) \oplus \text{SubBytes32}(K_{i-\text{Length}+1}^c) \oplus K_L$. After every generation of round keys value K_L rotated to the left by 1 bit.

Decryption round keys are computed based on encryption round keys and decryption keys output transformation associated with encryption keys as follows:

$$\begin{aligned} & (K_{16n}^d, K_{16n+1}^d, K_{16n+2}^d, K_{16n+3}^d, K_{16n+4}^d, K_{16n+5}^d, K_{16n+6}^d, K_{16n+7}^d, K_{16n+8}^d, K_{16n+9}^d, K_{16n+10}^d, K_{16n+11}^d, K_{16n+12}^d, K_{16n+13}^d, \\ & K_{16n+14}^d, K_{16n+15}^d) = (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, (K_8^c)^{-1}, -K_9^c, (K_{10}^c)^{-1}, \\ & -K_{11}^c, (K_{12}^c)^{-1}, -K_{13}^c, (K_{14}^c)^{-1}, -K_{15}^c) \end{aligned}$$

In the same manner, decryption keys second, third, and n–round associated with the encryption keys following:

$$\begin{aligned} & (K_{16(i-1)}^d, K_{16(i-1)+1}^d, K_{16(i-1)+2}^d, K_{16(i-1)+3}^d, K_{16(i-1)+4}^d, K_{16(i-1)+5}^d, K_{16(i-1)+6}^d, K_{16(i-1)+7}^d, K_{16(i-1)+8}^d, K_{16(i-1)+9}^d, K_{16(i-1)+10}^d, \\ & K_{16(i-1)+11}^d, K_{16(i-1)+12}^d, K_{16(i-1)+13}^d, K_{16(i-1)+14}^d, K_{16(i-1)+15}^d) = (-K_{16(n-i+1)}^c, (K_{16(n-i+1)+14}^c)^{-1}, -K_{16(n-i+1)+13}^c, \\ & (K_{16(n-i+1)+12}^c)^{-1}, -K_{16(n-i+1)+11}^c, (K_{16(n-i+1)+10}^c)^{-1}, -K_{16(n-i+1)+9}^c, (K_{16(n-i+1)+8}^c)^{-1}, (K_{16(n-i+1)+7}^c)^{-1}, -K_{16(n-i+1)+6}^c, \\ & (K_{16(n-i+1)+5}^c)^{-1}, -K_{16(n-i+1)+4}^c, (K_{16(n-i+1)+3}^c)^{-1}, -K_{16(n-i+1)+2}^c, (K_{16(n-i+1)+1}^c)^{-1}, -K_{16(n-i+1)+15}^c), i = \overline{2\dots n} \end{aligned}$$

Decryption round key first round associated a encryption round key as follows:

$$\begin{aligned} & (K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d) = (-K_{16n}^c, (K_{16n+1}^c)^{-1}, -K_{16n+2}^c, \\ & (K_{16n+3}^c)^{-1}, -K_{16n+4}^c, (K_{16n+5}^c)^{-1}, -K_{16n+6}^c, (K_{16n+7}^c)^{-1}, (K_{16n+8}^c)^{-1}, -K_{16n+9}^c, (K_{16n+10}^c)^{-1}, -K_{16n+11}^c, (K_{16n+12}^c)^{-1}, \\ & -K_{16n+13}^c, (K_{16n+14}^c)^{-1}, -K_{16n+15}^c) \end{aligned}$$

Decryption round key, applied to the first round and after output transformation associated with encryption keys as follows: $K_{16n+16+j}^d = K_{16n+32+j}^c$, $K_{16n+32+j}^d = K_{16n+16+j}^c$, $j = \overline{0\dots15}$

Results

Using transformation AES encryption algorithm as round transformation network IDEA16–2 and RFWKIDEA16–2 block encryption algorithm AES–IDEA16–2 and AES–RFWKIDEA16–2 is created. The encryption algorithm number of rounds and key length they are variable, and user can select number of rounds and key length in addition the degree of secrecy of information and speed encryption. The greater the number of rounds and length keys the greater the degree of protection of information but the slower encryption.

As encryption algorithms based on the Feistel network, the advantages of encryption algorithms AES–IDEA16–2 and AES–RFWKIDEA16–2 are then that the encryption and decryption using the same algorithm and as round function can be used any transformation, including one–way functions. When deciphering the

encryption algorithms encryption round keys applied in reverse, thus on the basis of the operation must be calculated inversion. For example, if the round key multiplied by the sub-block, when decryption necessary to calculate the multiplicative inverse, If summarized, it is necessary to calculate the additive inverse.

It is known that resistance AES encryption algorithm closely associated with resistance S-box, applied in the algorithm. In S-box AES encryption algorithm algebraic degree of nonlinearity is $\text{deg}=7$, nonlinearity is $NL=112$, resistance to linear cryptanalysis is $\lambda=32/256$, resistance to differential cryptanalysis is $\delta=4/256$, strict avalanche criterion is $\text{SAC} = 8$, bit independence criterion is $\text{BIC} = 8$.

The encryption algorithms AES-IDEA16-2 and AES-RFWKIDEA16-2 resistance S-boxes is equal to resistance of the S-box encryption algorithm AES, i.e. $\text{deg}=7$, $NL=112$, $\lambda=32/256$, $\delta=4/256$, $\text{SAC}=\text{BIC}=8$.

Studies show that, speed of encryption algorithms AES-IDEA16-2 and AES-RFWKIDEA16-2 higher than AES. The encryption algorithm AES-IDEA16-2 1.18 and the encryption algorithm AES-RFWKIDEA16-2 1.25 times faster than encrypts the AES.

Conclusion

It is known that as a algorithms based on the Feistel network, resistance algorithm based on network IDEA16-2 and RFWKIDEA16-2 closely associated with resistance round function. Therefore, choosing conversion resistant AES encryption algorithm on the basis of the round function network IDEA16-2 and RFWKIDEA16-2 relatively developed strong encryption algorithm.

References

1. Daeman J., Rijmen V. AES Proposal: Rijndael // NIST AES Proposal, 1998, <http://csrc.nist.gov/>
2. Daeman J., Rijmen V. The Block Cipher Rijndael // Third Smart Card Research and Advanced Applications Conference Proceedings, 1998.

3. Tuychiev G.N. About networks IDEA16–4, IDEA16–2, IDEA16–1, created on the basis of network IDEA16–8 // Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions» –Tashkent, 2014
4. Tuychiev G.N. About networks RFWKIDEA16–8, RFWKIDEA16–4, RFWKIDEA16–2, RFWKIDEA32–1, created on the basis network IDEA16–8 // Ukrainian Scientific Journal of Information Security, –Kyev, 2014, vol. 20, issue 3, pp. 259–263
5. Tuychiev G.N. About networks IDEA8–2, IDEA8–1 and RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1 developed on the basis of network IDEA8–4 // Uzbek mathematical journal, –Tashkent, 2014, №3, pp. 104–118
6. Tuychiev G.N. About networks PES8–2 and PES8–1, developed on the basis of network PES8–4 // Transactions of the international scientific conference «Modern problems of applied mathematics and information technologies–Al–Khorezmiy 2012», Volume № II, – Samarkand, 2014, pp. 28–32.
7. Tuychiev G.N. About networks RFWKPES8–4, RFWKPES8–2, RFWKPES8–1, developed on the basis of network PES8–4 // Transactions of the international scientific conference «Modern problems of applied mathematics and information technologies–Al–Khorezmiy 2012», Volume № 2, –Samarkand, 2014, pp. 32–36
8. Tuychiev G.N. About networks IDEA16-4, IDEA16-2, IDEA16-1, created on the basis of network IDEA16-8 // Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions» -Tashkent, 2014
9. Tuychiev G. New encryption algorithm based on network IDEA8-1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Computer Science, 2015, Volume 3, Issue 1, pp. 1-6
10. Tuychiev G. New encryption algorithm based on network RFWKIDEA8-1 using transformation of AES encryption algorithm // International Journal of Computer Networks and Communications Security, 2015, Vol. 3, NO. 2, pp. 43-47

11. Tuychiev G. New encryption algorithm based on network PES8-1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security, 2015, vol.4., №1, pp. 1-5
12. Tuychiev G. New encryption algorithm based on network RFWKPES8-1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security, 2014, vol.3., №6, pp. 31-34
13. Tuychiev G. New encryption algorithm based on network IDEA16-1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Information Technology, 2015, Volume 3, Issue 1, pp. 6-12

Ахметов Б.С.¹, Корченко А.Г.², Сейлова Н.А.¹,

Гнатюк С.А.², Алимсеитова Ж.К.¹

**Инфокоммуникациялық жүйелерде қауіпсіздік деңгейін жоғарлату
мақсатында кванттық технологияларды қолдану**

¹Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті,
Алматы, Қазақстан Республикасы

²Ұлттық авиация университеті, Киев, Украина

Микробөлшектер кванттік күйлерінде кодталған, көбісі ақпаратты жіберуде негізделген, ақпаратты қорғаудың кванттық әдістері деректермен қауіпсіз алмасу үшін бірқатар жаңа тәсілдерді ұсынады. Осы аймақтағы қазіргі заманғы көптеген басылымдар [1-3] ең көп қолданатын ақпаратты қорғаудың кванттік әдісіне – кванттік кілтті таратуға (ККТ) арналған. Бұл әдіс қазіргі қаманғы коммерциялық жүйелерде өз қолдануын тапты, және қазіргі уақытта әлемнің көптеген мемлекеттерінде қолданыста. Егер осы әдістің теориялық гипотезадан ақпараттық-коммуникациялық жүйелердің қорғалғандық деңгейін жоғарлату үшін эксперименттік қондығыға (жақында ақпаратты қорғаудың ақиқат жүйелерінде) дейін даму жолын талдаса, онда идеяның (бірінші

көзқараста өте реалды емес) қондырғыға тез айналу фактісін растауға болады. Бұл жоғары технологиялар заманында өзіне қолданысты проблемаларсыз тапты. Осыған қарап, нарықта тағы бір келешегі бар кванттық технологияның – *кванттік қауіпсіз тікелей байланыстың (КҚТБ, quantum secure direct communication)* пайда болуын батыл болжауға болады. КҚТБ тән ерекшелігі қандайда бір криптографиялық түрлендірулердің жоқтығы, осыған сәйкес криптографиялық кілттерді (key distribution problem) тарату проблемасы да жоқ болады [1]. Бұл жұмыстың **мақсаты** бар ақпараттық-коммуникациялық жүйелердің қорғалғандық деңгейін жоғарлату көзқарасынан кванттық қауіпсіз тікелей байланыс мүмкіндіктерін сапалы талдау болып табылады.

Қолданатын кванттық технологияларға (quantum technology) тәуелді, КҚТБ хаттамаларын келесі типтерге бөлуге болады [1]: пинг-понг хаттама (ping-pong protocol) – түпнұсқалық және оның жетілдірілген түрлендірулері; шатысқан кубиттерді (entangled qubits) блоктармен жіберу хаттамалары; бірлік кубиттерді (single qubits) қолданумен хаттамалар; шатысқан кубиттер (entangled qubits) топтарын қолданумен хаттамалар.

Кәзіргі уақытқа бар КҚТБ хаттамаларының көбісі кубиттерді блоктармен жіберуді талап етеді – бұл ақпаратты жіберудің алдында кванттық арнада тыңдауды (eavesdropping) анықтауға мүмкіндік береді. Яғни, егер арнада тыңдау фактісі тіркелсе, онда сеанс заңды пайдаланушылармен үзіледі және қасқой ешқандай ақпаратты алмайды. Кубиттер блоктарын сақтау үшін кванттік жадының (quantum memory) үлкен көлемі қажет. Кванттік жадының технологиясы белсенді құрылуда, бірақ дәстүрлі коммуникациялық жүйелерде көпшілік қолданудан қазірше әлі алыс. Кванттық технологияның дамуының соңғы беталыстарын талдап, жақында ашық жүйелерде кванттық жадының (үлкен көлемді) пайда болуын болжауға болады. Сонымен, техникалық жүзеге асыру көз қарасынан бірлік кубиттерді немесе олардың үлкен емес топтарын (хаттаманың бір циклында) жіберуді қолданатын хаттамалардың артықшылықтары бар. Осындай хаттамалардың бірнешесі бар және олардың

барлығында тек *асимптотикалық қауіпсіздік* бар (яғни шабуылды табу ықтималдығы өте жоғары, бірақ оның алдында қасқой кейбір ақпаратты ала алады). Сонымен, осындай КҚТБ хаттамаларының қауіпсіздігін нығайту проблемасы (problem of privacy amplification) туындайды. Оны шешу үшін, қасқой үшін жолай ұсталған ақпаратты пайдасыз ететін ақпаратты алдын ала өңдеу әдістерін құру талап етіледі. Бұл әдістер квантты болуы міндетті емес, олар классикалық болу мүмкін – жарық мысал болып [4] ұсынылған нығайтудың квантты емес әдісі болу мүмкін. Алдын ала өңдеу үшін Хилл шифрына ұқсас қайтымды матрицалар қолданылады – бірінше абонент өзінің тізбегін қайтымды матрицаға көбейтеді, содан кейін қасқойдың жоқтығын анық білгеннен кейін ашық арнамен оны жібереді. Сонымен қатар, ақпараттық қауіпсіздіктің күтімді деңгейіне тәуелді ол матрицаларды қалай таңдау керек екендігі, көпдеңгейлі кванттік жүйелерді қолдану кезінде матрицаларды қалай есептеу керек екені және т.б. көрсетілген. Жоғары көрсетілген шифрға қарағанда матрицалар кілт деп есептелмейді және ашық түрде жіберіледі (матрицалардың өздерін қасқоймен жолай ұстау оған ешқандай ақпарат бермейді, өйткені олар қасқой болмаған жағдайда мәндік тізбекті жіберген кезде ғана жіберіледі). Осаған ұқсас нығайту үшін нығайтудың басқа классикалық әдістері қолданылу мүмкін [4, 5].

Пинг-понг хаттама [1, 4, 5] үлкен көлемді кванттік жадыны талап етпейтін КҚТБ хаттамаларының бірі. Түпнұсқалық пинг-понг хаттама Эйнштейн-Подольски-Розенның (*ЭПР-жұптар*, *EPR-pairs*) кубиттердың шатысқан жұптарын қолданады және хаттаманың бір циклы ішінде классикалық ақпараттың бір битын жіберуге мүмкіндік береді. **Кванттық жүйелердің шатысқаны** деген олар кейбір **кванттық корреляция** деп аталатын күйде болады. Бұл күйде бір жүйенің кейбір сипаттамаларын өзгерту екінші жүйенің тұра сондай өзгеруіне алып келеді [6, 7]. Квантты асатығыз кодтауды қолдану хаттаманың бір циклында екі битты жіберуге мүмкіндік береді. Ақпараттық көлемін арықарай жоғарлату ЭПР-жұптар орнына

Гринбергер-Хорн-Цайлингер (*ГХЦ, GHZ*) шатысқан күйлеріндегі [5, 6] олардың триплеттерін, квадруплеттерін және т.б. қолдану жолымен мүмкін. ГХЦ-күйлерімен пинг-понг хаттаманың ақпараттық көлемі циклға n битке тең, бұл жерде n - ГХЦ-күйлерінде қолданылатын кубиттер саны. Пинг-понг хаттаманың ақпараттық көлемін көпдеңгейлі кванттық жүйелерді (кудиттерді) қолдану көмегімен жоғарлату мүмкін. Үшдеңгейлі жүйелердің (кутриттердің) Белла (беллдың күйлері) жұп күйлерін және кутриттер үшін кванттық асатығыз кодтауды қолданудың сәйкес хаттамасы [5,7] ұсынылған.

ЭПР-жұптар және ГХЦ-триплеттерден басқа КҚТБ төрт (квадруплеттер) және одан көп ГХЦ немесе кластерлік күйдегі шатысқан кубиттерді қолдануды қарастырады. Сонымен қатар КҚТБ хаттамалары жоғарыда қарастырылған кванттық асатығызды кодтауды, кубит күйлерінің унитарлы түрлендіруді және классикалық аутентификацияланған байланыс арнасын (authenticated communication channel) [1] қолданады.

КҚТБ басты *артықшылығы* – криптографиялық түрлендірулер болмағандықтан, *құпия кілттерді тарату қажеттілігінің болмауы*. Осы факт КҚТБ жүйелері туралы *байланыстың классикалық криптографиялық жүйелердің* альтернативасы деп айтуға мүмкіндік береді. Осыған қоса олардың *артықшылықтарына* келесілерді жатқызуға болады [1]: орталық (бродкастинг) және екіден көп пайдаланушылар арасында ақпаратпен алмасу мүмкіндігі; қасқойдың шабуылын табу (классикалық байланыс жүйелерінде мүмкін емес); кубиттерді блоктармен жіберуді қолданатын КҚТБ хаттамалары үшін қауіпсіздіктің жоғары деңгейін (теориялық-ақпараттық қауіпсіздікке дейін) қамтамасыз ету мүмкіндігі.

КҚТБ *кемшіліктері* туралы айту керек [1]: ақпараттық хабарды жіберу режимінде жоғалтуларды (25-50%) құратын шуы бар кванттік арнада пинг-понг хаттамаға қалқаланған шабуылдың ықтималдығы; КҚТБ жүйелерді тәжірибелік жүзеге асырудың қыйындығы; кубиттерді жіберудің жоғары емес жылдамдығы («женімді курьер» сияқты консервативті әдістерді қолдануға

үйренген отандық тұтынушылардың талаптарына қарап, жоғары жылдамдық – сынды параметр емес екенін айтуға болады); жоғары көлемді кванттік жадыны талап ету (кубиттерді блоктармен жіберуді қолданатын КҚТБ хаттамалар туралы); пинг-понг хаттаманың асимптотикалық қауіпсіздігі (нығайту мүмкіндігін жоғарыда қарастырдық); «адам ортасында» шабуылға әлсіздік (кванттық криптография да әлсіз болатын проблемалардың біреуі).

Әлемдік зерттеу орталықтардың ғылыми жұмысшылары (Northwestern University, BBN Technologies of Cambridge, TREL, NEC, Mitsubishi Electric, Лос-Аламос және басқа жерлерде Ұлттық зертханалар) кванттық криптография аймағында SECOQC (Secure Communication based on Quantum Cryptography) және EQCSPOT (European Quantum Cryptography and Single Photon Technologies) [1] сияқты жобаларды жүзеге асыруда белсенді қатысады.

Сонымен, осы жұмыста заманауи ақпараттық-коммуникациялық жүйелердің құпиялығын нығайту көз қарасынан кванттық қауіпсіз тікелей байланысының мүмкіндіктерін талдау жүргізілген. Кванттық қауіпсіз тікелей байланыс хаттамалар негізіндегі жүйелердің негізгі артықшылықтары мен кемшіліктері анықталған. Барлық жоғарыда көрсетілген негізінде кванттық байланысқа бүкіл әлемнің коммерциялық және әскері ұйымдарының үздіксіз құзығушылығы өсу туралы қорытынды шығаруға болады. Бүгін осы технологиямен тікелей айналысатын зерттеушілер оны зертханалардан нарыққа шығаруға жақындады.

Әдебиет

1. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Захист інформації. — 2010. — № 1. — С. 77–89.
2. Румянцев К.Е. Квантовая связь и криптография: Учебное пособие / К.Е. Румянцев, Д.М. Голубчиков — Таганрог: Изд-во ТТИ ЮФУ, 2009. — 122 с.

3. Килин С.Я. Квантовая криптография: Идеи и практика : Монография / С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. — Мінськ, 2008. — 398 с.
4. Василиу Е.В. Асимптотическая безопасность пинг-понг протокола квантовой прямой связи с трехкубитными состояниями Гринбергера-Хорна-Цайлингера // Georgian Electronic Scientific Journal: Computer Science and Telecommunications. – 2009, № . – P. 34.
5. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. — М. : Мир, 2006. — 824 с.
6. Имре Ш. Квантовые вычисления и связь: Инженерный подход / Ш. Имре, Ф. Балаж; Пер. с англ. под. ред. В.В. Самарцева. — М. : ФИЗМАТЛИТ, 2008. — 320 с.
7. Сейлова Н. А., Гнатюк С.О., Жмурко Т.О., Стоянович А. Метод подвешения защищенности систем защиты информации на базе квантовых технологий. Сборник 7 Всеукраинской научно-практической конференции SITS. 2015. - С. 93-97.

Баймульдин М.К., Абилдаева Г.Б., Каримова А.Н.

АҚПАРАТТЫҚ САЛАДА ЖҰМЫС ІСТЕЙТІН ҰЙЫМДАРДА ҚҰПИЯ АҚПАРАТТЫ ҚОРҒАУ

Қарағанды мемлекеттік техникалық университеті, Қарағанды, Қазақстан

Ақпараттық салада жұмыс істейтін ұйымдарда құпия ақпаратты қорғау аса маңызды мәселе болып табылады. Сондықтан бұл мәселені шешуге көп көңіл бөлінуі қажет. Біріншіден, құпия ақпаратты сақтайтын, оның дұрыс пайдалануын қадағалайтын адамдар тобын белгілеу керек – оларды шартты түрде ақпаратты қорғау маманы деп атайық. Екіншіден, жұмыс істейтін ақпараттың дәрежесін белгілеу керек. Ол дәрежелерді, мысал үшін келесідей

бөлуге болады: 1) өте құпия, 2) құпия, 3) жұмыс бабындағы ақпарат. Ақпараттың әрбір дәрежесіне қатынай алатын адамдар тобы белгіленеді.

Үшіншіден, құпия ақпаратпен жұмыс істеуге арналған арнайы бөлмелерді жабдықтау керек. Жұмыс бабындағы ақпарат жай бөлмелерде де өңделуіне болады. Ал құпия және өте құпия ақпарат тек арнайы бөлмелерде өңделуі тиіс. Бұл бөлмелердің техникалық қорғалуы алдыңғы тарауларда қарастырылған.

Ақпаратпен тиімді жұмыс істеуді ұйымдастыру тек қызметкерлерге ғана емес мекеме басшыларына да қатысты болуы керек, сол сияқты мекеменің бірінші басшысына да. Ақпаратты қарастырғанда мекеме басшысы ақпаратты қорғауды ұйымдастыру үшін келесі мәселелерді шешуі керек:

- ақпаратқа қатынай алатын қызметкерлер құрамы жөнінде дұрыс шешім қабылдауы,
- басшылардың құжаттармен жұмыс істеуі кезінде ол құжатпен басқалардың танысуына жол бермеу,
- келушілердің, қызметкерлердің және т.б., ақпаратты ұрлау немесе оның көшірмесін алу мүмкіндігін болдырмау,
- ақпараттың техникалық каналдар арқылы (визуальды, акустикалық және т.б.) сыртқа шығуын болдырмау. Мысал үшін қызметкерлердің құпия ақпаратты қорғалмаған байланыс линиялары бойынша немесе ортақ пайдаланыстағы орындарда (қоғамдық транспортта, паркттерде және т.б. жерлерде) немқұрайды талқылауы,
- қызметкерлердің құжаттарды алуын және қайтаруын белгілеп отыру ;
- ақпараттың физикалық сақталуын қамтамасыз ету және т.б.

Құжаттарды ақпаратты қорғау маманынан алар кезінде қызметкер немесе басшы арнайы есепке алу журналына қол қояды (ол журналдың электронды түрі де болуы тиіс). Бұл журналдың келесідей графалары болуы мүмкін:

1) құжаттың номері немесе шифры, аты (бірақ құжаттың тікелей мазмұнына сілтеме болатындай ат беруге болмайды)

2) құжат саны

- 3) құжатты алғандығы жөніндегі қолы
- 4) қайтарғандығы жөніндегі қолы
- 5) күні, уақыты.

Құпия ақпараты бар құжаттарды біреу арқылы алу және қайтару рұқсат етілмейді. Сол ақпаратқа тікелей қатысы бар және рұқсаты бар адамға ғана құжат беріледі және құжатты алған адам оны өзі қайтаруы тиіс.

Дәстүрлі және электрондық құпия құжаттар басшылар арасында немесе басшылар мен орындаушылар арасында тек ақпаратты қорғау маманы арқылы тасылады.

Басшылар қарастырып болғаннан кейін құжаттар арнайы операцияларды орындау үшін ақпаратты қорғау маманына қайтарылуы тиіс. Құжаттың есеп карточкасына құжаттарға қатынай алатын қызметкерлердің аты – жөні жазылады. Егер қызметкер құжаттың тек белгілі бөлігімен ғана жұмыс істей алатын болса, онда резолюцияда осы қызметкер жұмыс істей алатын бөлімдер, тер, қосымшалар міндетті түрде нақты көрсетілуі керек.

Мекеменің бірінші басшысына қарастырылуға берілмейтін құжаттар бөлімше бастықтарына (жұмыс бағытын белгілейтіндер), арнайы қызметкерлерге жіберіледі. Мұны ақпаратты қорғау маманы атқарады.

Басшыдан қайтарылған құжаттар мен тіркеуден өткен құжаттар танысуға, жұмысында қолдануға немесе орындауға қызметкерлерге бағытталады.

Құпия құжаттармен танысу арнайы бөлмелерде өтеді, танысқаннан кейін орындаушы танысу туралы мөр қояды. Орындаушыға арналған құжаттар оларды орындайтын қызметкерлердің жұмыс орнына беріледі.

Ақпаратты қорғау маманы құжаттарды берерде келесілерді орындауы керек:

- құжатты оған қатынауға рұқсаты жоқ адамға беруді болдырмау;
- қызметкерлердің алдында құжаттың физикалық бүтіндігін, барлық қосымшалардың, парақтардың және басқа да бөліктердің түгелдігін

тексеріп шығуы керек. Содан соң қызметкердің қол қоюымен құжатты беру фактын есеп карточкасында белгілеуі тиіс;

- қызметкерлерді құжаттың солраға қатысты ғана бөлігімен таныстыруы керек, қызметкерлерге олардың құжатпен танысу барысында жазба кітапшаларға, қағаздарға құжат мәтінінен жазулар жасауына рұқсат етілмеуі тиіс;
- құжатпен бөтен адамның танысуының кез – келген мүмкіндігін болдырмау;
- қолданыстағы құжаттардың есепке алынуын қамтамасыз ету, құжаттардың бүтіндігін жұмыс уақытында және одан басқа уақытта бақылау.

Электронды құжаттарды алу үшін орындаушы алдыменен ақпаратты қорғау маманының компьютерінде орналасқан электронды есеп карточкасына өзінің электронды цифрлық қолтаңбасын енгізеді. Содан кейін оның дұрыстығы тексерілгеннен кейін барып электронды құжаттар көшірмесі орындаушы компьютерінің дерекқорына жіберіледі [1].

Орындаушы алған барлық құжаттар (қағаз, электронды түрде) міндетті түрде орындаушының өзіндегі есеп карточкасында (ішкі есеп карточкасы) тіркелуі тиіс. Бұл ақпаратты қорғау маманының құжаттың қолданыста екендігін және қайтарылғанын бақылап отыру үшін қажет. Бұл есеп карточкасы орындаушыда сақталады, ал оның электронды аналогты ақпаратты қорғау маманының компьютерінде болады. Ішкі есеп карточкасының мынадай графалары болуы мүмкін: құжаттың номері немесе шифры, құпиялылық грифі, экземпляр саны, экземплярдағы парақтар саны, алу күні, қайтару туралы қолы және қайтару күні.

Құжатты ақпаратты қорғау маманына қайтару кезінде оның есеп формасына сәйкес келуі және барлық бөліктерінің, терінің бүтіндігі және тұтастығы тексеріледі. тер саны құжаттың алынуында, қайтарылуында міндетті түрде саналып, есеп формасына енгізіледі. Бұл құжаттың бүтіндігін,

тұтастығын растау үшін және оның ақпаратты қорғау маманының немесе орындаушының толық қабылдағандығын растау мақсатымен істеледі. Оған қоса терді аудару арқылы санау кезінде тердің бұзылуы (бір бөлігін жыртып алу, форматын өзгерту, т.б.) немесе ауыстыру факты тексеріледі.

Тек жоғарыдағы операцияларды орындағаннан кейін ғана ақпаратты қорғау маманының есеп карточкасында құжат, ішкі есеп карточкасында қайтарылғандығы жөнінде қол қоюға құқы болады. Ақпаратты қорғау маманы құжаттың жаңа орналасу жерін есеп карточкаларын бақылау журналында белгілейді.

Құпия құжаттармен жұмыс істеу оның мәтінін құру қиындығы мен бекітілген ережелерді ұстану қиындығымен ерекшелінеді.

Ақпаратты құжаттандыру шығармашылық жұмыс болып табылады және оны басшылар мен орындаушылар атқарады (мамандар). Құжаттарды орындаудың негізгі тікелей операциялары барлық уақыттың әдетте 10-12% ғана алады. Қалған операциялар формальды - логикалық және техникалық болады (ашу, жабу, сақтау, көшіру, өзгерту, жеткізу). Құпия ақпараттың құжаттандыру процесі кезінде құжаттың мәтіні құрылады және басқа да реквизиттер ресімделеді. Бұл реквизиттер құжатқа қажетті ақпараттылық (басқару мақсатында) және заңды күш беру үшін керек. Ең қиын да, маңызды да этап мәтінді құру болып табылады. Құпия құжатты құру кезінде келесідей ерекшеліктерді ескеру керек:

- құжатқа қосу керек құпия ақпараттың минимал құрамын анықтау,
- құпия ақпаратты құжаттандыру үшін бірінші басшының рұқсаты. Құпия ақпараттың қауіпсіздігін сақтауда маңызды элемент болып орындаушы жұмысының тиянақтылығы және кәсіби шеберлігі болып табылады [2].

Мекеме қызметкерлері құпия ақпаратпен жұмыс істегенде келесілерді орындауға міндетті:

- өзінің қызметтік міндеттеріне сәйкес рұқсат берілген құпия ақпаратпен ғана жұмыс істеуіне;
- бүтіндігі мен тұтастығын тексеру үшін қызметкер өзіндегі барлық құжаттарды ақпаратты қорғау маманына көрсетуге;
- ақпаратты қорғау маманымен бірге өзіндегі құжаттардың есебін жүргізуге;
- күнде жұмыс уақыты біткеннен кейін құжаттардың бар екендігін тексеріп, оларды ақпаратты қорғау маманына сақтауға тапсыруға,
- құжаттармен жұмыс істеп болғаннан кейін оларды ақпаратты қорғау маманына бірден тапсыруға;
- жұмыстан кеткенде, демалысқа шыққанда, жұмыс бабымен басқа жаққа жіберілгенде ақпаратты қорғау маманына өзіндегі құжаттардың барлығын тапсыруға;
- құжаттың бұзылғандығы, жоғалғандығы немесе кейбір терінің жетпей тұрғандығы, артық немесе ескерілмеген құжаттар бар екені айқындалған жағдайда бірден бірінші басшыға және ақпаратты қорғау маманына хабарлауға.

Әдебиеттер

1. Молдовян А. А., Молдовян Н. А., Советов Б. Я. «Криптография» - СПб.: «Лань» басылымы, 2001. – 224с.,ил. – (Жоғары оқу оындарына арналған оқулықтар. Арнайы әдебиет).
2. Мельников В. Комьпютерлік жүйелердегі ақпаратты қорғау. – М. Қаржы және Статистика, Электроинформ, 1997.

Баймульдин М.К., Савченко Н.К., Шакирова Ю.К., Абилдаева Г.Б.

**ИСПОЛЬЗОВАНИЕ СИСТЕМ ПЛАНИРОВАНИЯ БИЗНЕС-РЕСУРСОВ С
ЦЕЛЬЮ ПОВЫШЕНИЯ ПОТЕНЦИАЛА ПРЕДПРИЯТИЯ**

Карагандинский государственный технический университет, Караганда,
Казахстан

В современных условиях конкурентного рынка предприятие должно постоянно повышать свой потенциал - шанс получения прибыли в будущем. Повышение потенциала подразумевает совершенствование деятельности предприятия.

Повышение потенциала предприятия возможно за счет комплексного развития:

- Корпоративной культуры на базе СМК (Системы Менеджмента Качества) - для повышения качества основных процессов на предприятии, что ведет к повышению качества выпускаемой продукции;
- Методик ведения бизнеса - для снижения цены на выпускаемую продукцию;
- Инфраструктур бизнеса, базирующихся на Информационных Технологиях, основой которых является ERP-система (Enterprise Resource Planning - планирование ресурсов предприятия) - для налаживания системы планирования и организации работ "точно вовремя".

Повышение потенциала предприятия подразумевает непрерывное улучшение бизнес-процессов/BPI (Business Process Improvement) [1].

Выделяют пять уровней совершенства бизнес-процессов на предприятии:

1. Хаос - дисбаланс коммерческих, производственных и финансовых целей. Хаос характеризуется отсутствием системного взгляда; предприятие рассматривается как совокупность отдельных элементов.

2. Контроль - балансировка коммерческих, производственных и финансовых целей предприятия. Данный уровень подразумевает "налаженный" учет и контроль основных мероприятий на предприятии;

3. Оптимизация - оптимизация (упрощение) основных бизнес-процессов на предприятии, что ведет к снижению издержек.

4. Адаптация - адаптивность бизнес-процессов к условиям внешней среды.

5. Мировой класс - возможность предприятия формировать рынок.

Переходы предприятия с одного уровня на другой называются этапами, причем, на каждом из этапов используются ERP-система и Система Менеджмента Качества (рисунок 1).



Рисунок 1 – Использование ERP-системы и СМК в качестве инструментов непрерывного улучшения бизнес-процессов

Использование MRP II (Manufacturing Resource Planning – планирование производственных ресурсов) позволяет предприятию продвинуться от "Хаоса" к "Контролю" и осуществить балансировку коммерческих, производственных и финансовых целей предприятия за счет многоуровневого планирования [2].

Методика JIT (Just in time - точно вовремя) помогает предприятию оптимизировать достижение сбалансированных целей, вводя критерии оценки эффективности плана.

CSRP (Customer Synchronized Planning – планирование ресурсов в зависимости от потребностей Клиента) делает возможным планировать ресурсы предприятия в зависимости от потребности клиента, осуществляя адаптацию бизнес-процессов к внешней среде.

Переход с одного уровня ВРІ на вышестоящий реализуется за счет цикла совершенствования.

Цикл совершенствования подразумевает развитие методик ведения бизнеса на базе ERP-системы и СМК. Сердцевиной цикла является трехуровневое моделирование.

Разделение моделирования на уровни связано со следующей квалификацией деятельности на предприятии [3]:

- А - первичная деятельность (т.е. осуществление основных процессов на предприятии по управлению ресурсами и реализации продукции);
- В - вторичная деятельность, направленная на улучшение основной деятельности группы А;
- С - деятельность, направленная на улучшение деятельности группы В.

С помощью трехуровневого моделирования реализуется связь бизнес-методик с инструментами совершенствования деятельности предприятия, где:

- **Концептуальное моделирование** (для определения вектора развития предприятия) обеспечивает деятельность группы С.
- **Логическое моделирование** (для описания деятельности предприятия CASE-средствами с целью реорганизации процессов предприятия) обеспечивает деятельность группы В.
- **Нормативное моделирование** (для формализации деятельности предприятия средствами ERP-системы, т.е. создание нормативной модели предприятия) обеспечивает деятельность группы А.

Ключевая идея концептуального моделирования - использование эталонной модели производителя ERP-системы на самой ранней стадии. Это ведет к значительному сокращению времени создания концептуальной модели

и повышению эффективности её использования на уровнях логического и физического моделирования.

Литература

1. Дэниел О'Лири. ERP системы. Современное планирование и управление ресурсами предприятия, Вершина, 2004. 272 с.
2. С. В. Питеркин, Н. А. Оладов, Д. В. Исаев. Точно вовремя для России. Практика применения ERP-систем., Альпина Паблишер; 2010; 368с.
3. SAP - Экономия времени и снижение затрат, 2013, URL: <http://www.sap.com>

Барлыбаев А.Б., Сабыров Т.С.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В SMART-UNIVERSITY

Евразийский национальный университет им. Л.Н.Гумилева, Астана, Казахстан.

В данной работе мы опишем как необходимо строить информационную безопасность в интеллектуальных обучающих системах. Под понятием интеллектуальной обучающей системой мы понимаем систему умного электронного образования (смарт-образования) с адаптивным пользовательским интерфейсом, позволяющим вести письменный и устный диалог на естественном языке [1]. В таких сложных системах в обязательном порядке должна присутствовать информационная безопасность, так как в системе будут храниться личные данные пользователей, информация об учебных достижениях, информация внутреннего характера.

Информационная безопасность, иногда сокращается до ИБ, является практика защиты информации от несанкционированного доступа, использования, разглашения, разрушения, модификации, прочтения, осмотра, записи или уничтожения. Это общий термин, который может быть использован

независимо от формы данные могут принимать (например электронные, физические) [2].

Рассмотрим какие методы и подходы мы использовали в smart-university.

1) Необходимо выполнить следующие настройки над операционной системой (далее ОС):

- Минимизировать права технологической учетной записи системы управления базами данных (далее СУБД) Caché.
- Переименовать учетную запись администратора локального компьютера.
- Оставить в ОС только минимум необходимых пользователей.
- Своевременно устанавливать обновления безопасности для ОС и используемых служб и сервисов.
- Отключить или удалить неиспользуемые службы и сервисы.
- Ограничить доступ к файлам базы данных.
- Ограничить права на файлы данных Caché (оставить только у владельца и администраторов БД).

2) Настройки безопасности InterSystems Caché во время установки:

- Выбрать режим установки Maximum Security.
- Выбрать режим установки Custom Setup и в нем выбрать только те компоненты, которые минимально необходимы для работы прикладного решения.
- При установке указать порт SuperServer, отличный от стандартного для установок TCP порта 1972.
- При установке указать порт внутреннего веб сервера, отличный от стандартного для установок TCP порта 57772.
- В качестве пути для размещения экземпляра Caché указать отличный от стандартного путь (для Windows систем путь по умолчанию C:\InterSystems\Caché, для UNIX®/Linux систем - /usr/cachesys).

3) Настройки безопасности Caché после установки (большинство из них выполнено при режиме инсталляции Maximum Security):

- Отключены все сервисы и ресурсы, которые не используются прикладными системами сертифицируемого решения.
 - Для сервисов, использующих сетевой доступ, должны быть явно заданы IP адреса, с которых возможно удаленное взаимодействие.
 - Должны быть отключены неиспользуемые CSP веб приложения.
 - Для необходимых CSP приложений должен быть исключен доступ к ним без аутентификации и авторизации.
 - Должен быть закрыт паролем и ограничен доступ к CSP Gateway.
 - Должен быть включен аудит работы СУБД.
 - Для файла конфигурации должна быть включена опция шифрования.
- Также мы хэшируем пароли чтобы никто не смог прочесть их.

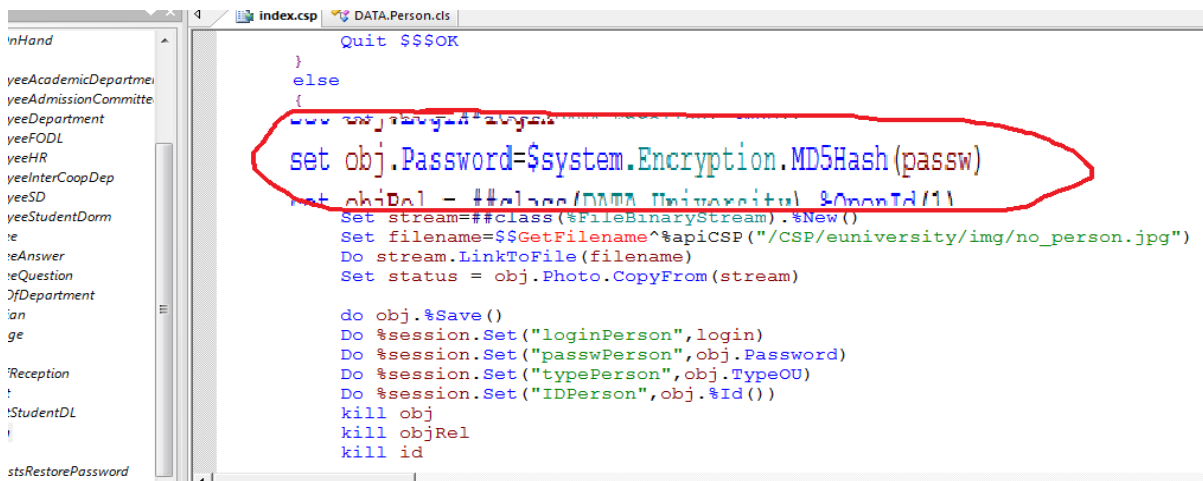
```
classmethod MD5Hash(text As %String) as %String
```

This method generates a 16-byte hash using the MD5 message digest algorithm. (See Internet Engineering Task Force Request for Comments 1321 for more information.)

Input parameter:

text - String to be hashed.

Return value: 16-byte MD5 hash.



```

Quit $$$OK
}
else
{
set obj.Password=$system.Encryption.MD5Hash(passw)
set objRel = ##class(DATA.University) %OpenId(1)
set stream=##class(%FileBinaryStream).%New()
set filename=$$GetFilename^%apiCSP("/CSP/euniversity/img/no_person.jpg")
do stream.LinkToFile(filename)
set status = obj.Photo.CopyFrom(stream)

do obj.%Save()
do %session.Set("loginPerson", login)
do %session.Set("passwPerson", obj.Password)
do %session.Set("typePerson", obj.TypeOU)
do %session.Set("IDPerson", obj.%Id())
kill obj
kill objRel
kill id

```

status	MiddleName	NID	Name	Nation	Other	DataOfID	Password	Photo	PlaceOB	PlaceOL	PlaceOR	RDegree	REducation	RExperience
			Rector	Kasax/Kazaxcra			éD(0(!)ú#bM	<binary>				sd	sd	

Литература

[1] Barlybayev A.B. An Intelligent System for Learning, Controlling and Assessment Knowledge. INFORMATION, 18 (5(A)). ISSN: 1343-4500. – Japan, 2015. P.1817-1828.

[2] Gordon, Lawrence; Loeb, Martin (November 2002). "The Economics of Information Security Investment". ACM Transactions on Information and System Security 5 (4): 438–457.

Бердибаев Р.Ш., Абулхасимова М.Б., Жаманкулова А.А.
ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА В БИОМЕТРИЧЕСКИХ СИСТЕМАХ
АУТЕНТИФИКАЦИИ

Казахский национальный исследовательский технический университет
 имени К.И. Сатпаева, г. Алматы, Казахстан

В последнее время наблюдается стремительный рост количества учебной, научной и научно-популярной литературы, посвященные вопросу исследования искусственного интеллекта. Это объясняется не только повсеместным внедрением современных информационных технологий, но и увеличением спектра задач, которые они могут решить.

Сегодня прогресс затрагивает все сферы жизни современного человека и термином «умная» техника уже никого не удивит. Мы стоим на пороге новой информационной революции, когда первенство будет закреплено за

искусственным интеллектом, а его влияние возможно лишь будет сопоставить с темпом развития Интернета.

Искусственный интеллект является сейчас «горячей точкой» научных исследований. В этой точке, как в фокусе, сконцентрированы наибольшие усилия кибернетиков, лингвистов, психологов, философов, математиков и инженеров. Именно здесь решаются многие коренные вопросы, связанные с путями развития научной мысли, с воздействием достижений в области вычислительной техники и робототехники на жизнь будущих поколений людей. Здесь возникают и получают права гражданства новые методы научных междисциплинарных исследований. Здесь формируется новый взгляд на роль тех или иных научных результатов и возникает то, что можно было бы назвать философским осмыслением этих результатов [1].

В настоящее время системы, основанные на применении искусственного интеллекта, фундаментом которого являются искусственные нейронные сети, схематически представляют прообраз человеческого мозга.

Нейронная сеть – множество нейронов, объединенных в сеть путем соединения входов нейронов одного слоя с выходами нейронов другого слоя, причем, входы нейронов первого слоя являются входами всей нейронной сети, а выходы нейронов последнего слоя являются выходами нейронной сети [2].

Преимуществом нейронных сетей перед классическими алгоритмами считается возможность обучаться и анализировать полученную информацию (рисунок 1).

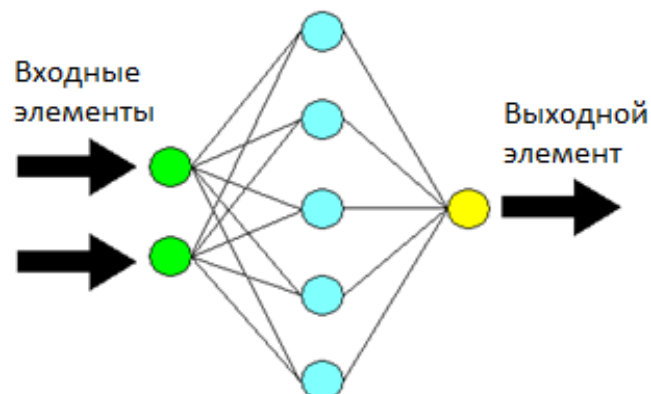


Рисунок 1 – Схема простой нейронной сети.

Стоит отметить, что сферы применения нейронных сетей различны, но наиболее широкое применение нашли в биометрических системах защиты информации.

Главной задачей биометрии в рамках информационной безопасности является усовершенствование систем защиты, которые должны идентифицировать пользователя в системе с минимальной погрешностью независимо от методов распознавания: статические или динамические.

В число статических методов распознавания личности можно включить: идентификацию по радужной оболочке глаза, папиллярному рисунку на пальцах, геометрии лица, сетчатке глаза, рисунку вен руки, геометрии рук. А к семейству методов, основанных на распознавании динамических характеристик можно отнести динамику рукописного почерка, идентификацию по голосу, сердечному ритму, походке [3].

На сегодняшний день среди статических методов наибольший интерес представляет распознавание по радужной оболочке глаза. Это обуславливается тем, что данный биометрический признак является уникальным и характеризует себя, как очень эффективный инструмент при использовании в системах биометрической идентификации.

Перспективным считается направление в области разработки систем идентификации личности по радужной оболочке с использованием нейронных сетей. Одним из преимуществ таких систем является возможность упрощения математического аппарата, что позволяет ускорить доступ зарегистрированных пользователей к ресурсам информационной системы.

Среди систем, которые используют динамические характеристики, наиболее широкое распространение получила технология биометрико-нейросетевой идентификации человека, основанная на анализе динамики его рукописного почерка [4]. Использование нейронной сети позволяет обеспечить

возможность минимизации ошибок первого и второго родов на основе ранее полученных измерений, по которым обучена сеть. Обученная нейронная сеть может идентифицировать личность человека, на основе выборки, по которой происходило обучение.

В целом процесс обучения нейронной сети схематически выглядит одинаково, как для статических, так и для динамических методов. На рисунке 2 представлена структурная схема обучения искусственной нейронной сети для биометрической аутентификации.

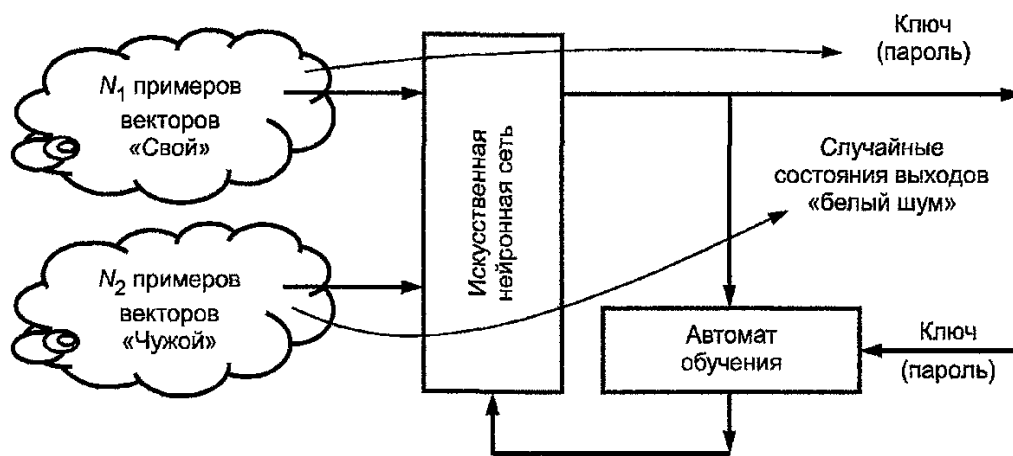


Рисунок 2 – Структурная схема обучения искусственной нейронной сети

Обучение средств высоконадежной биометрико-нейросетевой аутентификации сводится к обучению искусственной нейронной сети преобразовывать множество входных образов «Свой» в личный ключ пользователя и множество входных образов «Чужой» в случайный «белый шум» на каждом из выходов искусственной нейронной сети. Для обучения используется N_1 , примеров образов «Свой» и N_2 примеров образов «Чужой» [5].

Однако стоит отметить, что в процессе обучения нейронной сети остаются актуальными такие проблемы, как выбор наиболее подходящей структуры и построение оптимального алгоритма.

Для того, чтобы биометрические системы защиты информации, основанные на нейронных сетях, стали конкурентоспособными, необходимо усовершенствовать существующие и создавать новые методы для быстрого

обучения искусственных нейронных сетей. В связи с этим были проведены исследования относительно статических и динамических методов биометрической идентификации, на основании, которых можно сделать вывод: системы, построенные на использовании биометрических характеристик таких, как радужная оболочка глаза и рукописный почерк являются наиболее перспективными, так как обладают высокой степенью надежности и точности, по сравнению с другими.

В заключении хотелось бы отметить, что интерес к искусственным нейронным сетям в Казахстане и за рубежом стремительно растет. Возможность быстрого обучения и достоверность выводов позволяет рекомендовать системы, основанные на нейронных сетях, как один из обязательных инструментов не только в области защиты информации, но и во многих сферах жизни. Ярким примером является использование в прогнозировании котировок акций и курса валют.

Будущее за внедрением новых технологий, хотя это и трудоемкий процесс. Но на практике приложенные средства и усилия оправдываются и приносят преимущественное право, тем, кто их использует.

Литература

1. Кибернетика и сознание [Электронный ресурс]. – Электрон. дан. – Режим доступа: <http://cyber-intellekt.narod.ru/-----.-------.html>
2. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: Монография. / Алматы: ТОО «Издательство LEM», 2014 – 144 с.
3. Сейлова Н. А., Балтабай А.. Анализ биометрических методов аутентификации. Труды III Международной научно-практической конференции «Состояние, проблемы и задачи информатизации в Казахстане» – Алматы, КазНТУ, 2014. - Часть 1. - С. 425-436.

4. Безяев В. С. Оценка надежности и качества систем биометрико-нейросетевой аутентификации личности. Труды Международного симпозиума «Надежность и качество», Том 2, 2010. – С. 43.

5. ГОСТ Р 52633-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

Бердибеков А.Т., Доля А.В.

НЕКОТОРЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Национальный университет обороны имени Первого Президента Республики
Казахстан – Лидера Нации, г. Астана

Эффективность управления любой организацией, будто военной или гражданской, во многом зависит от решения задач оперативного и качественного формирования электронных документов, контроля их исполнения, а также продуманной организации их хранения, поиска и использования. Потребность в эффективном управлении электронными документами привела к созданию систем электронного документооборота (СЭД), под которыми понимают организационно-технические системы, облегчающие процесс создания, управления доступом и распространения электронных документов в компьютерных сетях, а также обеспечивающие контроль над потоками документов в организации. По данным ряда аналитиков, производительность труда персонала при использовании СЭД увеличивается на 20–25%, а стоимость архивного хранения электронных документов на 80% ниже по сравнению со стоимостью хранения бумажных архивов [1].

Система административного управления Вооруженными Силами характеризуется длительными сроками прохождения документов, большими трудозатратами личного состава на поиск и обработку требуемой информации,

ограниченными возможностями организации коллективной работы, особенно в случае территориальной удаленности соисполнителей друг от друга. В связи с этим, стоит острая необходимость повысить оперативность обмена информацией внутри структурных подразделений Министерства обороны, упростить контроль за исполнительской дисциплиной, обеспечить возможность оперативного поиска информации, чего невозможно добиться без внедрения системы электронного документооборота. Одной из самых главных задач организации системы электронного документооборота является защита информации.

Базовый элемент любой системы электронного документооборота - документ, внутри системы это может быть файл, а может быть запись в базе данных. Говоря о защите информации системы электронного документооборота, часто подразумевают именно защиту документов, защиту той информации, которую они в себе несут. В этом случае все сводится к задаче защиты данных от несанкционированного доступа. Здесь есть большое заблуждение, ведь речь идет именно о защите всей системы, а не только о защите данных внутри нее. Это значит, что нужно защитить также ее работоспособность, обеспечить быстрое восстановление после повреждений, сбоев и даже после уничтожения. Система - это как живой организм, не достаточно защитить только содержимое его клеток, необходимо защитить также связи между ними и их работоспособность. Поэтому к защите системы электронного документооборота необходим комплексный подход, который подразумевает защиту на всех уровнях СЭД. Начиная от защиты физических носителей информации, данных на них, и заканчивая организационными мерами [2].

Таким образом, необходимо защищать, во-первых, аппаратные элементы системы (компьютеры, серверы, элементы компьютерной сети и сетевое оборудование). Необходимо так же предусмотреть такие угрозы, как поломка оборудования, доступ злоумышленника к оборудованию, отключения питания

и т.д. Во-вторых, защита необходима файлам системы. Это файлы программного обеспечения и базы данных, уровень между аппаратными устройствами системы и логическими элементами системы и физическими составляющими. В противном случае появляется возможность влияния злоумышленником или внешними обстоятельствами на файлы системы электронного документооборота, не проникая в систему, т.е. как бы снаружи. Например, файлы базы могут быть скопированы злоумышленником или повреждены в результате сбоя операционной системы или оборудования. В-третьих, само собой, необходимо защищать документы и информацию, находящиеся внутри системы.

Используя такой подход, можно построить систему, защищенную на всех уровнях, и рубежи обороны от угроз на каждом уровне.

Угрозы для системы электронного документооборота достаточно стандартны и могут быть классифицированы следующим образом:

1) Угроза целостности - повреждение и уничтожение информации, искажение информации — как не намеренное в случае ошибок и сбоев, так и злоумышленное.

2) Угроза конфиденциальности - это любое нарушение конфиденциальности, в том числе кража, перехват информации, изменения маршрутов следования.

3) Угроза работоспособности системы - всевозможные угрозы, реализация которых приведет к нарушению или прекращению работы системы; сюда входят как умышленные атаки, так и ошибки пользователей, а также сбои в оборудовании и программном обеспечении.

Защиту именно от этих угроз в той или иной мере должна реализовывать любая система электронного документооборота.

Основные этапы проектирования системы комплексной защиты информации делятся на следующие четыре этапа.

Первый этап проектирования системы начинается с изучения среды функционирования, ее структуризации и определения основных условий.

Второй этап заключается в анализе уязвимости информационных потоков. При этом формируется система показателей уязвимости и система угроз информации. Разрабатываются соответствующие методы и модели угроз. Прогнозируются значения показателей уязвимости.

На третьем этапе определяются основные требования к системе защиты, формулируются цели и критерии оценки работоспособности проектируемой системы.

На четвертом этапе определяется набор функций механизмов защиты, выбираются соответствующие аппаратные и программные средства, разрабатываются и тестируются компоненты и модули системы. Если на этапе комплексного тестирования в условиях, максимально приближенных к реальной среде функционирования, будут обнаружены просчеты, процесс проектирования претерпевает дополнительные итерационные процедуры [3].

Разработка системы защиты информации системы электронного документооборота должна проводиться с учетом защиты от выявленных угроз и возможных информационных рисков, для которых определяются способы защиты, и на основе предложенного показателя оценки ее эффективности. При этом учитываются требования, которые предъявляются к созданию таких систем, а именно [4]:

– организация защиты информации осуществляется с учетом системного подхода, обеспечивающего оптимальное сочетание взаимосвязанных методологических, организационных, программных, аппаратных и иных средств;

– система должна развиваться непрерывно, так как способы реализации угроз информации непрерывно совершенствуются. Управление ИБ – это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования систем ИБ,

непрерывном контроле, выявление ее «узких» и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа (НСД);

– система должна предусматривать разделение и минимизацию полномочий по доступу к обрабатываемой информации и процедурам обработки;

– система должна обеспечивать контроль и регистрацию попыток НСД, содержать средства для точного установления идентичности каждого пользователя и производить протоколирование действий;

– обеспечивать надежность защиты информации и контроль за функционированием системы защиты, т.е. использовать средства и методы контроля работоспособности механизмов защиты.

Реализация перечисленных требований при создании системы защиты информации в системах электронного документооборота будет способствовать организации эффективного защищенного документооборота.

При проектировании системы электронного документооборота в различных сферах деятельности, необходимо трезво оценивать возможные угрозы и риски системы, а также величину возможных потерь от реализованных угроз. Комплекс организационных мер при создании системы электронного документооборота должен сводиться к главной задаче – обеспечение комплексной защиты системы на всех уровнях.

Литература

1. Макарова Н.В. Компьютерное делопроизводство: учеб. курс / Н.В. Макарова, Г.С. Николайчук, Ю.Ф. Титова. – СПб.: Питер, 2005. – 411 с.

2. Электронный ресурс:
<http://www.cnews.ru/reviews/free/security2006/articles/e-docs/>.

3. Астапенко Г.Ф. Аппаратно-программные методы и средства защиты информации / Г. Ф. Астапенко. – Минск : БГУ, 2008. 188с.

4. Аскеров Т.М. Защита информации и информационная безопасность / под общ. ред. К.И. Курбакова. – М.: Российская экономическая академия, 2001. – 386 с.

Бияшев Р.Г., Нысанбаева С.Е., Бегимбаева Е.Е.

ФОРМИРОВАНИЕ ЗАЩИЩЕННОГО ТРАНСГРАНИЧНОГО ИНФОРМАЦИОННОГО ОБМЕНА В ИНТЕГРИРОВАННОЙ СИСТЕМЕ

Институт информационных и вычислительных технологий КН МОН РК,
Алматы, Казахстан

Аннотация: Рассмотрена задача обеспечения трансграничного обмена в интеграционной системе. Трансграничное взаимодействие сторон информационного обмена в интегрированной системе обеспечивается за счет создания и использования интеграционного сегмента и национальных сегментов. Приведены основные задачи доверенной третьей стороны.

Ключевые слова: информационное взаимодействие, трансграничный информационный обмен, пространство доверия, информационная безопасность.

1 Введение

На сегодняшний день в силу глобализации мировых интеграционных процессов, обмен информацией (информационное взаимодействие) с использованием информационно-телекоммуникационных систем является неотъемлемым элементом отношений общества. Обеспечение защиты информации при трансграничном информационном взаимодействии с использованием информационно-телекоммуникационных систем становится одной из важных задач.

18 сентября 2014 года Решением Совета Евразийской Экономической Комиссии была утверждена Концепция использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов [1]. Концепция указывает на необходимость обеспечения юридической силы электронных документов при трансграничном информационном обмене. В этой связи вопросы укрепления доверия и безопасности между взаимодействующими сторонами в информационном процессе выходят на первый план. Обусловлено это тем, что актуализируется проблема равноправного участия Республики Казахстан в международном информационном обмене и в процессах международного регулирования информационной безопасности. Принимая во внимание трансграничный характер вопросов обеспечения информационной безопасности электронных документов при трансграничном информационном обмене, требуется дальнейшее совершенствование международного сотрудничества в данной области, соответствующего принципам равноправного международного информационного обмена.

2 Трансграничный информационный обмен в интеграционной системе

Электронное взаимодействие, а в особенности трансграничное электронное взаимодействие, подразумевает совместную работу множества разнородных информационных систем. Механизмы управления правами в каждой из них могут строиться на различных принципах и реализовываться различными способами [2].

Так как трансграничное взаимодействие – это взаимодействие субъектов различных правовых полей, то одной из основных проблем при трансграничном информационном взаимодействии является нерешенность комплекса организационных, технологических и правовых вопросов обеспечения юридической значимости электронной информации в интегрированной

системе. В число основных проблем обеспечения информационного взаимодействия входит разработка эффективного и надежного механизма управления правами субъектов и обеспечения каждой из сторон этого взаимодействия собственной информационной безопасности и защиты своего информационного суверенитета.

Взаимодействующие стороны при трансграничном обмене используют национальные стандарты криптографических алгоритмов и алгоритмов создания и проверки цифровой подписи (ЦП). По причине различного подхода обеспечения информационной безопасности взаимодействующих сторон и несовместимости способов реализации криптографических алгоритмов, возникает проблема применения единых криптографических средств ЦП. Но такой подход в настоящее время невозможен, поскольку к использованию сторон допускаются только сертифицированные по национальным стандартам средства криптографической защиты.

Решение задач надежной и эффективной интеграции территориально распределенных государственных информационных ресурсов и информационных систем органов государств-членов, обеспечения взаимодействия органов власти государств-членов в электронном виде, в том числе предоставление возможности обмена электронными документами, имеющими юридическую силу (или взаимно признаваемыми таковыми), является одним из ключевых направлений работ по созданию и внедрению интегрированной информационной системы Евразийского экономического союза [1].

Взаимодействие в электронном виде между взаимодействующими сторонами информационного обмена в интегрированной системе обеспечивается за счет создания и использования интеграционного сегмента и национальных сегментов. Эти сегменты представляют собой совокупность защищенной системы передачи данных и интеграционных шлюзов, входящих в состав каждого узла взаимодействующих сторон информационного обмена.

Обеспечение трансграничного обмена в интеграционной системе реализуется на основе применения службы доверенной третьей стороны. Инфраструктура доверенной третьей стороны должна быть размещена в интеграционном шлюзе, как и удостоверяющий центр. Доверенные третьи стороны организуются на уровне каждой взаимодействующей стороны.

Основными задачами доверенной третьей стороны являются:

- осуществление подтверждения подлинности электронных документов и ЦП субъектов информационного взаимодействия в фиксированный момент времени;
- осуществление гарантий доверия в трансграничном обмене электронными документами;
- обеспечение правомерности применения ЦП в исходящих и входящих электронных документах и сообщениях в соответствии с правилами и требованиями законодательства той взаимодействующей стороны, где находится доверенная третья сторона [3].

При документообороте в трансграничном пространстве доверия могут возникать конфликтные ситуации. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения электронного документа, а также использованием в данных документах ЦП. Разрешение конфликтных ситуаций должно входить в задачи доверенной третьей стороны. Конфликтные ситуации могут возникать в следующих случаях:

- неподтверждение подлинности защищенных электронных документов средствами проверки ЦП получателя;
- оспаривание факта идентификации владельца ЦП, подписавшего электронный документ;
- заявление отправителя или получателя электронного документа об его искажении;

- оспаривание факта отправления и (или) получения защищенного электронного документа;
- оспаривания времени отправления и (или) получения защищенного электронного документа;
- иные случаи возникновения конфликтных ситуаций.

Выполнение правовой функции электронного документооборота обеспечивается за счет реквизитов документа.

Заключение

При решении задач обеспечения защищенного трансграничного информационного обмена должен учитываться комплекс как организационных, технологических особенностей такого взаимодействия, так и правовых вопросов обеспечения юридической значимости электронной информации в интегрированной системе.

Литература

1. Концепция использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов // <http://www.tks.ru/news/law/2014/10/08/0006>.
2. Сазонов А.В. Инфраструктура и технология управления правами субъектов в трансграничном пространстве // Общие вопросы безопасности информации и объектов №3, 2012, С.83-87.
3. Модельный закон «О трансграничном информационном обмене электронными документами» // <http://www.pvti.ru/>.

Боранбаев С.Н., Тасмагамбетов О.К., Сейткулов Е.Н.

ТРЕБОВАНИЯ ПРИ ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Евразийский национальный университет имени Л.Н.Гумилева, г. Астана,
Республика Казахстан

1. Введение

Информационная система (ИС) поддержки правоохранительной деятельности предназначена для автоматизации деятельности аналитических групп по контролю за преступлениями. Система служит для сбора, обработки и анализа информации об объектах анализируемой обстановки (лица, организации, организационно преступные группировки, и т.д.), их взаимосвязях в различные моменты времени и событиях происходящих с ними, осуществления оценки сложившейся ситуации, анализа ее дальнейшего развития, обеспечения поддержки деятельности служб при планировании мероприятий, направленных на пресечение незаконной деятельности.

Основной целью информационной системы является увеличение эффективности деятельности аналитических служб, а также использование анализа и прогноза в рассматриваемой предметной области в оперативных целях за счет: более полного охвата и учета различных факторов внешней среды; улучшения качества информационного обслуживания и обеспечения целостного восприятия ситуации аналитиками и руководителем; заблаговременного выявления позитивных и негативных тенденций и проблемных областей на основе информации из различных источников; анализа и оценки эффективности проводимых и планируемых мероприятий по пресечению преступлений на территории Республики Казахстан (РК); усиления взаимодействия и обмена информацией между различными организациями, занимающимися борьбой с преступностью, как на территории РК, так и за ее пределами; для дальнейшего использования накапливаемой информации - ведение архива информации о физических и юридических лицах, задействованных в преступлениях, проводимых ими мероприятиях, их связях и контактах в Республике Казахстан (РК) и за рубежом. При проектировании

информационной системы использованы некоторые методы и подходы изложенные в работах [1-4].

Разработка информационной системы основывается на реорганизации бизнес-правил, моделировании организационной структуры, проектировании баз данных и знаний, обосновании системы математических моделей, реализации пользовательского интерфейса, выборе архитектуры сети и технических средств. Разнообразие задач приводит к появлению проблем взаимодействия специалистов и необходимости согласования этапов проектирования и компонент информационной системы. При этом должно обеспечиваться единство тезауруса в рамках определенной предметной области. Современные технологии проектирования информационных систем в некоторой мере позволяют решить перечисленные проблемы. В настоящее время используются CASE-технологии (Computer Aided Software/System Engineering), предоставляющие ряд нотаций для разработки описательных моделей. Использование CASE-технологий позволяет ускорить разработку информационных систем (ИС) за счет решения ряда организационных проблем – взаимодействия между различными специалистами, этапами проектирования и отдельными компонентами информационной системы, создания документации, единства тезауруса и репозитория моделей. Методологии, технологии и CASE-средства составляют основу проекта любой ИС. Методология реализуется через конкретные технологии и поддерживающие их стандарты, методики и инструментальные средства, которые обеспечивают выполнение процессов жизненного цикла информационных систем (ЖЦ ИС). На рисунке 1 представлена методология проектирования ИС, поддерживающая основные процессы обследования, анализа и конструирования [3].

Основное содержание технологии проектирования составляют технологические инструкции, состоящие из описания последовательности технологических операций, условий, в зависимости от которых выполняется та или иная операция, и описаний самих операций.

Информационная технология, как и любая другая, должна отвечать следующим требованиям:

- обеспечивать высокую степень расчленения всего процесса обработки информации на этапы (фазы), операции, действия;
- включать весь набор элементов, необходимых для достижения поставленной цели;
- иметь регулярный характер. Этапы, действия, операции технологического процесса могут быть стандартизированы и унифицированы, что позволит более эффективно осуществлять целенаправленное управление информационными процессами.

Разработанная технология для проектирования ИС, базируется на методах структурно-функционального и объектно-ориентированного анализа.

Важное место в системном анализе и проектировании занимают объектно-ориентированные методы, основанные на объектной декомпозиции предметной области, представляемой в виде совокупности объектов, взаимодействующих между собой посредством передачи сообщений. Данный подход не является противопоставлением структурному подходу, более того, фрагменты методологий структурного анализа (базовые модели DFD, ERD, STD) используются при объектно-ориентированном анализе для моделирования структуры и поведения самих объектов.

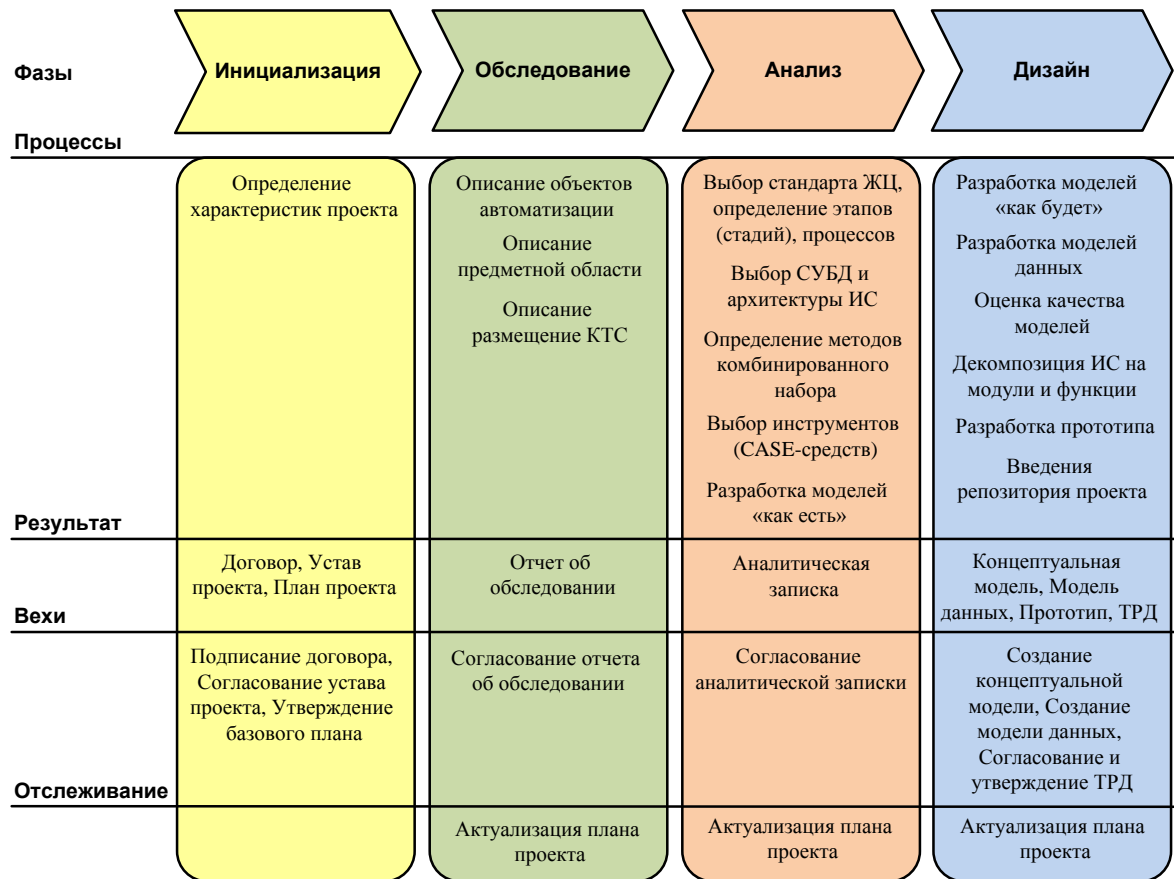


Рис. 1 - Методология проектирования ИС

2. Требования при проектировании информационной системы поддержки правоохранительной деятельности

В действующей практике контроль и управление следственной деятельностью осуществляется в соответствии с требованиями уголовного-процессуального кодекса Республики Казахстан (УПК РК), ведомственными нормативными правовыми актами, указаниями руководства органов министерства внутренних дел (МВД) на различных уровнях управления.

В качестве автоматизированной информационной системы обеспечения следственной деятельности используется ведомственный банк данных, где осуществляется учет: документов; правовых оценок оперативных материалов, материалов доследственной проверки; уголовных дел; правонарушений; переданных материалов; мероприятий; участников уголовного процесса; плановых позиций.

Банк данных является инструментально-техническим элементом системы информационного обеспечения оперативной, следственной, аналитической и организационно-управленческой деятельности правоохранительных органов и предназначен для автоматизированного решения информационно-справочных, информационно-логических и статистических задач, а также является информационной основой для других информационных систем. Применяется технология «толстого» клиента. В банке данных осуществляется накопление и систематизация информации, на основе оперативных, следственных, аналитических, организационно-управленческих документов МВД и других материалов. В преимущественном большинстве в качестве пользователей выступают работники информационно-аналитических подразделений (ИАП). Следственными работниками информационный массив используется редко в виду централизации учета информации. Основа банка данных представляет собой совокупность взаимодействующих между собой структурных звеньев.

Обмен информации между центральным звеном и структурными звеньями осуществляется на основе распределенной системы обмена информации (РСОИ). На организационно-технологическом уровне обеспечение информационной безопасности осуществляется путем разграничения доступа по направлениям деятельности, территориям и по уровню занимаемой должности.

Процесс работы с банком данных, регламентируется различными нормативными правовыми актами, касающимися вопросов организации работы с ним, предоставления и выдачи информации, администрирования, практическим руководством ввода и поиска информации, технологическими картами, определяющими порядок действий на участках, а также указаниями, направляемыми в рамках координации информационной работы.

Клиентская часть имеет интерфейс с выбором элементов управления, обеспечивающих доступ к функциональным возможностям банка данных, а также диалоговое взаимодействие «человек-компьютер».

В качестве достоинств существующей практики управления следует отметить относительно четкую юридическую регламентированность действий субъектов уголовно-процессуального законодательства в сравнении с другими процессами в органах МВД.

Необходимость дальнейшего развития системы информационного обеспечения следственной деятельности обусловлена следующими недостатками:

- используется большое количество информационных систем со своими отдельными базами данных, организационно и технологически не связанных между собой, разработанных в различное время и реализованные на различной программно-аппаратной платформе;

- основной архитектурой является так называемый «толстый» клиент, в которой все компоненты, выполняющие обработку данных, размещаются на клиентской рабочей станции;

- в разработанных системах практически отсутствует инструментарий для реализации аналитических функций, либо применяются устаревшие технологии;

- не регламентированность информационных потоков;

- необходимость достаточной информационной основы для принятия решений на различных уровнях управления в следственной деятельности;

- отсутствие возможности ведения в электронном формате уголовных дел и контроля хода их производства;

- подготовка процессуальных документов не формализована.

В целом ИС единого электронного пространства органов МВД должна удовлетворять следующим требованиям:

- 1) Многоплатформенность (операционные системы и аппаратные средства) и поддержка гетерогенной сетевой среды. Должна быть возможность функционирования на различных программно-аппаратных платформах;

2) Компонентная структура. Должна строиться на основе компонентной структуры, которая позволит при необходимости применить имеющиеся типовые решения;

3) Современная техническая платформа. Должна быть построена с использованием современных технологий хранения, обработки, визуализации и управления данными;

4) Открытость стандартов. Должна основываться на открытых индустриальных стандартах, поддерживаемых широким кругом производителей;

5) Надежность технических средств. Технические средства должны обеспечивать надежную и бесперебойную работу, резервирование и восстановление данных;

6) Модульность. Программное обеспечение должно быть модульным, чтобы обеспечить оптимальную стартовую конфигурацию с возможностью дальнейшего поэтапного развития, возможность настройки под изменения объекта автоматизации (информационно-аналитических процессов, требований к ним) в процессе эксплуатации;

7) Масштабируемость. Должна обеспечиваться масштабируемость по количеству пользователей, объему хранимых данных, интенсивности обмена данными, скорости обработки запросов и данных, набору предоставляемых сервисов, способам обеспечения доступа;

8) Возможность гибкой настройки. Должен быть предусмотрен набор настроек и средств разработки, достаточный для сокращения сроков внедрения и обеспечения эксплуатации;

9) Удобство эксплуатации. Пользовательские интерфейсы должны обладать информативностью, смысловой определенностью, согласованностью и структурированностью;

10) Сопровождаемость. Организационное обеспечение работы должно включать в себя техническую поддержку аппаратных средств, системного

программного обеспечения (в том числе, своевременное обновление его версий) и прикладного программного обеспечения, обучение эксплуатационного персонала, поддержку технической документации в актуальном состоянии;

11) Локализация. Должна обеспечиваться поддержка на уровне баз данных, предоставляемых информационных ресурсов на казахском и русском языках;

12) Должна поддерживаться работа пользователей на территориально распределенных объектах;

13) Должно быть обеспечено поэтапное наращивание, как производительности, так и функционала;

14) Должна быть обеспечена возможность интеграции с другими информационными системами органов МВД, информационными ресурсами государственных органов и других организаций во внутреннем контуре, программными продуктами. Должен быть реализован принцип открытой архитектуры построения, обеспечивающий возможность встраивания и взаимодействия с любыми другими системами (открытые интерфейсы для развития и интеграции).

15) Должна позволять обеспечить работу пользователей минимум на двух языках: государственный, русский (интерфейс пользователя).

Задачи, решаемые информационной системой, можно разделить на несколько уровней.

Задачи, решаемые на оперативном уровне:

1. Анализ и оценку эффективности реализации государственных и международных программ по борьбе с преступностью;
2. Анализ эффективности работы правоохранительных служб, включающий в себя:
 - а. Выявление критических зон, с точки зрения проникновения на территорию Республики международной преступности;

- b. Создание аналитических и поведенческих моделей;
- c. Оптимизация распределения средств охраны, мониторинга и контроля;
- d. Разработка системы управления в случае возникновения чрезвычайных ситуаций.

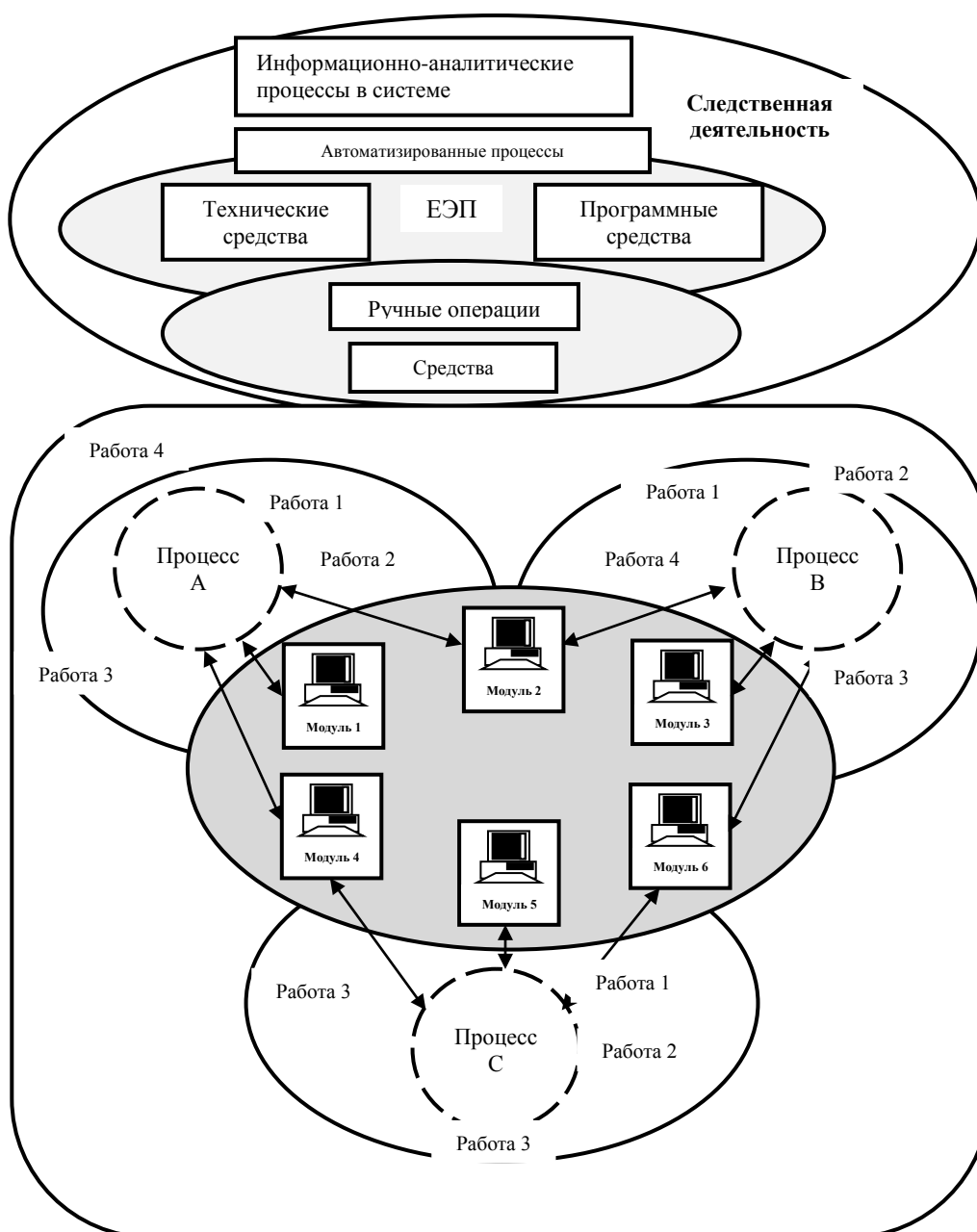


Рис.2 - Модель организации работы

Задачи, решаемые на стратегическом уровне:

1. Обеспечение информационного обмена, взаимодействие и координация действий со службами и организациями, занимающимися проблемой правоохранительной деятельности;
2. Анализ информации о зонах преступности на территории Республики, а так же об организациях и персоналиях, напрямую или косвенно связанных с ними;
3. Анализ финансовых потоков и выявление источников финансирования незаконной деятельности.

Заключение

ИС должна соответствовать следующим общим принципам:

1) единая точка входа;

2) однократная авторизация при получении доступа;

3) защищенный, масштабируемый и надежный доступ.

4) автоматическая система определения уровня доступа при авторизации, основанная на данных кадрового подразделения, создание и назначение специфических прав доступа (профиль пользователя/роль);

5) пользовательский интерфейс должен быть сформирован в соответствии с определенным профилем, правами доступа к подсистемам, информационным ресурсам, модулям/инструментам системы;

6) интерфейсы пользователей должны быть дружественными, интуитивно-понятными, многоуровневыми и содержать стандартные и общепринятые элементы управления, навигации, виды заголовков, закладок и т.д.

7) работа клиентской части без установки какого-либо специального программного обеспечения, за исключением браузера и офисных приложений,

для возможной выгрузки отчетных форм, информации (использование веб-технологий для снижения общей стоимости внедрения);

8) поддержка работы комплекса на двух языках (казахский, русский), с возможностью переключения непосредственно из интерфейса, без использования специальных шрифтов для операционных систем;

9) интерактивность – диалоговый режим и помощь посредством реализации функции доступа к инструкциям непосредственно из интерфейса клиентской части;

10) агрегация и консолидация любых данных комплекса в любом количестве, составе и виде.

11) бесконфликтное наращивание функций, расширение состава и числа пользователей, при условии адекватного увеличения производительности аппаратного обеспечения.

12) создание и модификация структуры информационных объектов без внесения изменений и дополнений в исходные коды программ;

13) реализация неограниченного числа автоматизированных рабочих мест;

14) позволять интеграцию с унаследованными (при необходимости миграция данных из них) и создаваемыми информационными системами.

Список литературы

1. Боранбаев С.Н. Методы разработки информационных систем. Астана: ТОО «Мастер ПО», 2012. -256 с.
2. Боранбаев С.Н., Бигаринов Р.А. Информационные системы поддержки принятия решений. Астана: ЕНУ имени Л.Н. Гумилева, 2010. -220 с.
3. Боранбаев С.Н., Байдюсенов Р.Б. Разработка технологии проектирования информационных систем с использованием шаблонов. Вестник НАН РК, 2010, №4, с.32-35.

4. Boranbayev S.N., Boranbayev A.S., Altayev S.A. Development of a mathematical model for designing reliable information systems and its properties. The 2014 International Conference on Software Engineering Research and Practice (SERP'14), Las Vegas, USA, 2014, -P. 286-290.

Боранбаев С.Н., Тасмагамбетов О.К., Сейткулов Е.Н.

**СТРУКТУРА И ФУНКЦИОНАЛЬНЫЕ ЗАДАЧИ ИНФОРМАЦИОННОЙ
СИСТЕМЫ ПОДДЕРЖКИ ПРАВООХРАНИТЕЛЬНОЙ
ДЕЯТЕЛЬНОСТИ**

Евразийский национальный университет имени Л.Н.Гумилева,
г. Астана, Республика Казахстан

1. Введение

Разработка информационной системы поддержки правоохранительной деятельности является сложной задачей. Большая размерность и сложность объектов автоматизации предопределяет итерационный характер методов разработки, и требует глубокую формализацию технологии выполнения всех этапов проекта. Существующие сегодня методы, безусловно, решают задачу разработки программного обеспечения, однако, не обладают в достаточной степени промышленными свойствами.

Высокая сложность объектов автоматизации определяет характер работ, начиная с самых ранних этапов, заключающихся в обследовании, моделировании и анализе предметной области. При этом разработка информационной системы имеет свои особенности, которые должны находить отражение в специальных мероприятиях по поддержанию логической целостности результатов на протяжении всего проекта.

В работах [1-5] предложена технология разработки информационных систем, которую можно применить при разработке информационной системы поддержки правоохранительной деятельности. В качестве модели для

проектирования информационной системы предлагается использовать ориентированную связанную сеть, отражающую ход выполнения проекта и предназначенную для анализа логической структуры проекта. Сеть имеет единственную входную и единственную выходную вершины. Каждая вершина – это работа в проекте. Простой сетью называется участок исходной сети, имеющая единственную входную вершину и единственную выходную вершину и состоящая из линейной последовательности работ проекта. Все работы входящие в простую сеть выполняются последовательно с первой до последнего. Исходная сеть рассматривается как совокупность конечного числа простых сетей. Последовательность выполнения простых сетей отображает ход выполнения проекта. Используем некоторые обозначения из [1-5]. Введено понятие интегральной сети. Из сети $S=(M, R, m_0)$ можно получать интегральные сети до тех пор, пока не будет получена интегральная сеть некоторого m -го ранга. На рисунках 1-2 показан пример сети $S=(M, R, m_0)$ и его интегральная сеть 2-го ранга.

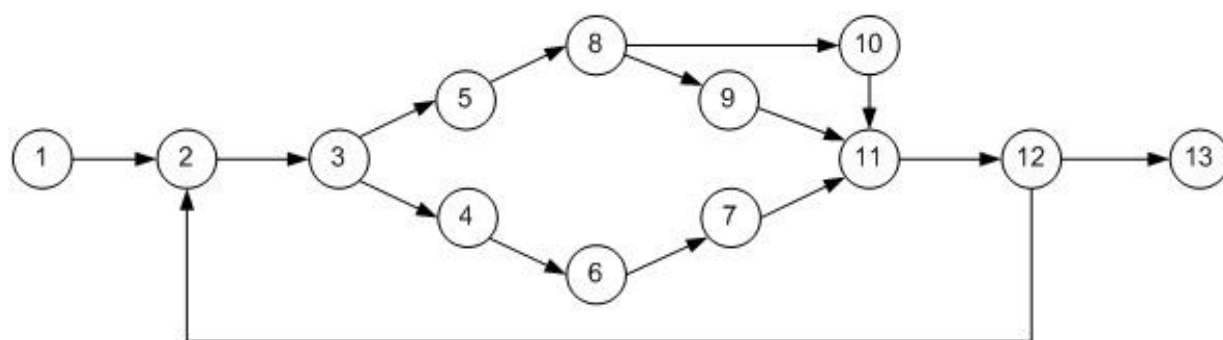


Рисунок 1 – сеть S

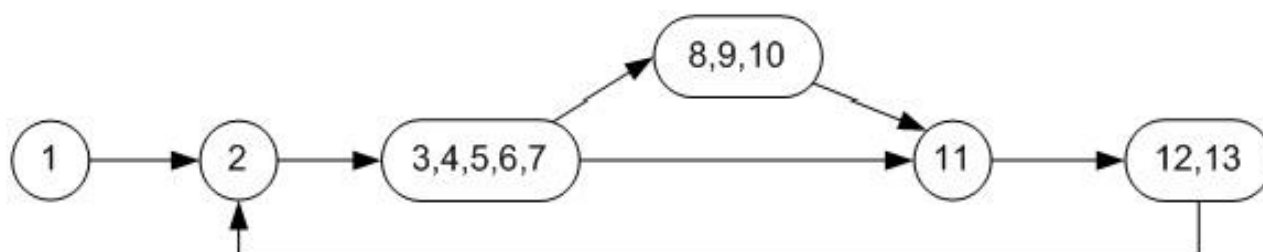


Рисунок 2 – интегральная сеть 2-го ранга

Сетевая модель этапов работ, позволяет укрупнять работы, для более осмысленного восприятия всех необходимых работ при проектировании информационной системы. Представление этапов работ проекта в виде сетевой модели позволяет оценивать масштабы информационной системы, является основой для дальнейшего планирования и распределения ресурсов при реализации ИС на последующих этапах.

2. Структура и функциональные задачи информационной системы поддержки правоохранительной деятельности

Информационная система поддержки правоохранительной деятельности должна содержать:

1) средства систематизации и накопления информации в рамках информационно-аналитических процессов следственной деятельности (создание, удаление, просмотр, редактирование, модификация информационных объектов);

2) средства поиска информации (контекстный поиск, поиск по различным подключенным информационным ресурсам, сложнозависимый поиск по характеристикам связанных объектов) и сохранения постоянных запросов;

3) средства (инструменты/модули), позволяющие обрабатывать информацию с возможностью подготовки и выдачи выводных отчетных форм, таблиц, статистических диаграмм (в форматах RTF, PDF, MS Excel и MS/Open Office);

4) средства и механизмы создания, управления информационно-аналитическими процессами (создание/перестроение процессов), потоками данных, модулей/инструментов системы (профили пользователей/права доступа);

5) средства изменения структуры и внешнего вида, интерфейсов пользователей в общих и частных случаях (создание, модификация, удаление

информационных объектов, полей, словарей, шаблонов документов, отдельных элементов интерфейса);

б) средства хранения информации и администрирования (резервное копирование данных с возможностью восстановления информации, управление правами доступа и функциями системы, журналирование всех действий и т.д.).

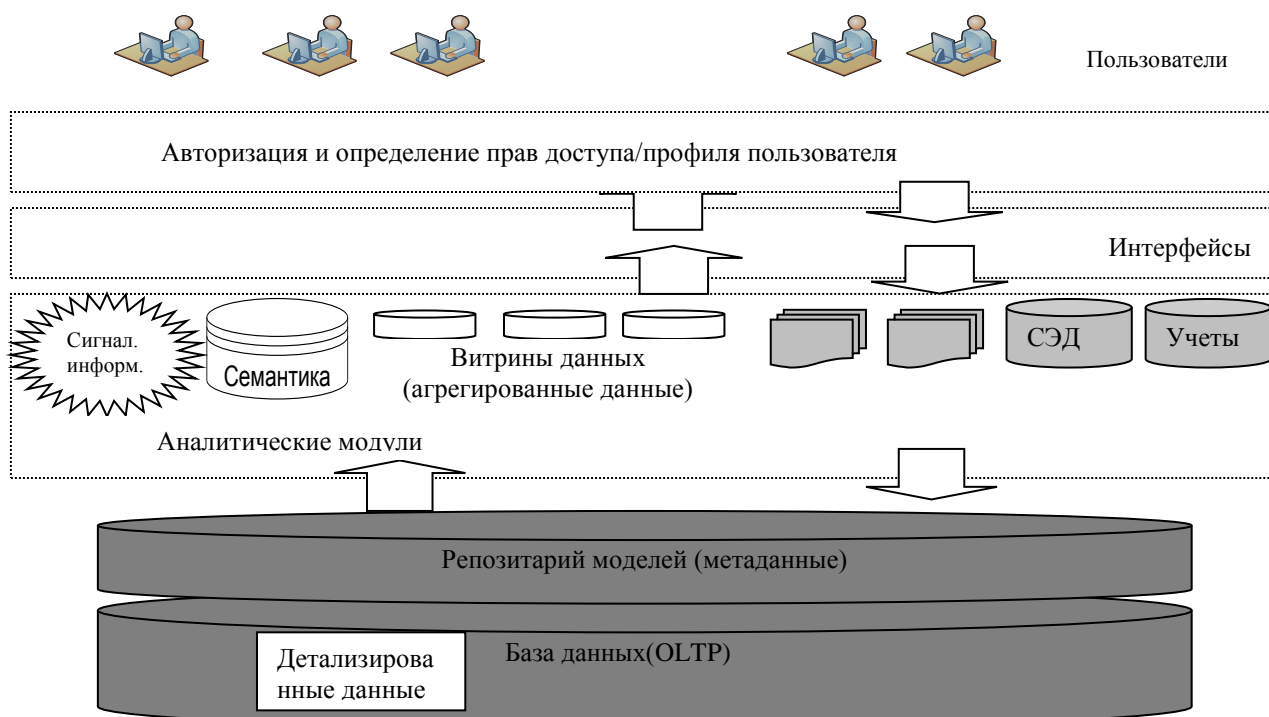


Рисунок 3 - Подсистемы ИС

Доступ к функциям/модулям по накоплению и систематизации информации, хранению, обработки и выдачи предоставляется пользователям в зависимости от участка, направления и уровня управления администратором системы.

В соответствии с осуществляемыми процессуальными действиями и принимаемыми процессуальными решениями в рамках процесса доследственной проверки предоставляется доступ к шаблонам документов для их подготовки и учета. При возбуждении уголовного дела в автоматизированном рабочем месте (АРМ) работника ответственного за учет уголовных дел появляется документ являющийся основанием для его заведения (постановление). Возбужденные уголовные дела после их учета появляются в АРМ работников, в чьем производстве они находятся. На этапе проведения предварительного следствия и дознания в соответствии с осуществляемыми процессуальными действиями и принимаемыми процессуальными решениями предоставляется доступ к шаблонам документов для их подготовки и учета.

На этапе завершения расследования уголовного дела в автоматическом режиме должен формироваться проект обвинительного (оправдательного) приговора, для дознания протокол. На этом этапе должна быть возможность перемещения материалов по уголовному делу в электронном виде, в случае необходимости. На всех этапах обеспечивается методическая поддержка, возможность контроля хода и сроков проверки, расследования, статистических и иных отчетных данных.

Подсистема информационного обеспечения следственной деятельности должна позволять:

- подготовку процессуальных документов на этапе доследственной проверки;

- подготовку процессуальных документов при проведении расследования уголовного дела (УД);
- помощь в расследовании много эпизодных уголовных дел;
- помощь в коллективном расследовании УД следственно-оперативной группой;
- автоматизированное формирование обвинительного заключения;
- обеспечение нормативной-правовой, методической и консультационной поддержки при проведении расследования УД, ведение методической базы;
- обеспечение возможности передачи УД по подследственности в электронном виде (внутри органов МВД);
- планирование и контроль планов расследования УД;
- текущее планирование работы следственных подразделений и дознания;
- автоматизированное формирование статистической отчетности (стат.формы и карточки) учета по УД;
- формирование статистической отчетности по подразделению;
- контроль за расследованием УД, включая контроль процессуальных сроков, автоматизированное предоставление справки по УД;

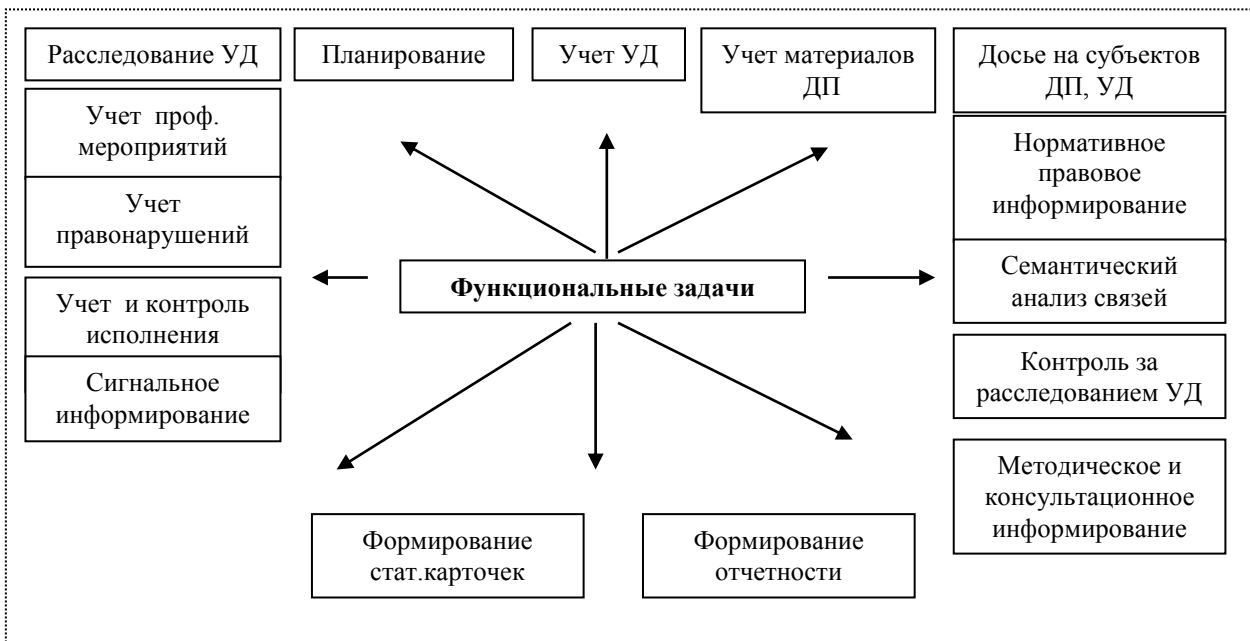


Рисунок 4 – Функциональные задачи

- учет и контроль поступивших заявлений, сообщений, жалоб и т.д.;
- возможность формирования досье на лиц и организаций (субъектов УД)
- возможность учета правонарушений;
- возможность учета переданных материалов;
- возможность учета профилактических мероприятий;
- возможность семантического анализа связей субъектов;
- сигнальное информирование по субъектам УД по запросам;
- учет правонарушений;
- учет переданных материалов.

В соответствии со СТ РК 34.025-2006 определены следующие стадии и этапы работ.

Таблица 1- стадий и этапы работ

Стадии	Этапы работ
1.Формирование требований к ИС и планирование работ	1.1. Обследование объекта. 1.2. Формирование и анализ требований пользователей к ИС. 1.3. Оформление отчета о выполненной работе 1.4. Построение плана-графика выполнения работ
2.Разработка концепции ИС	2.1. Изучение объекта; 2.2. Проведение необходимых исследовательских работ; 2.3. Разработка концепции АИС, удовлетворяющего требованиям пользователя; 2.4. Оформление отчета о выполненной работе.
3. Эскизный проект	3.1. Разработка предварительных проектных решений по ИС и ее частям; 3.2. Разработка документации на ИС и ее части.
4. Технический проект	4.1. Разработка ИС и ее частей 4.2. Разработка частных технических заданий на

	части ИС
5. Рабочая документация	5.1. Разработка рабочей документации 5.2. Разработка программного обеспечения
6. Ввод в действие	6.1. Подготовка объекта автоматизации к вводу модернизируемой архитектуры в действие. 6.2. Подготовка персонала 6.3. Комплектация системы поставляемыми изделиями (программными и техническими средствами) 6.4. Монтажные работы 6.5. Пусконаладочные работы 6.6. Проведение предварительных испытаний 6.7. Проведение опытной эксплуатации 6.8. Проведение приемочных испытаний
7. Сопровождение	7.1. Обеспечение функционирования системы. При запуске выполнение работ подрядчиком в соответствии с гарантийными обязательствами.

Список литературы

5. Боранбаев С.Н. Методы разработки информационных систем. Астана: ТОО «Мастер ПО», 2012. -256 с.
6. Боранбаев С.Н., Бигаринов Р.А. Информационные системы поддержки принятия решений. Астана: ЕНУ имени Л.Н. Гумилева, 2010. -220 с.
7. Боранбаев С.Н., Байдюсенов Р.Б. Разработка технологии проектирования информационных систем с использованием шаблонов. Вестник НАН РК, 2010, №4, с.32-35.
8. Boranbayev S.N., Boranbayev A.S., Altayev S.A. Development of a mathematical model for designing reliable information systems and its

properties. The 2014 International Conference on Software Engineering Research and Practice (SERP'14), Las Vegas, USA, 2014, -P. 286-290.

9. Боранбаев С.Н., Боранбаев А.С., Алтаев С.А. Разработка математической модели проектирования надежных информационных систем и ее свойства. Вестник Евразийского национального университета имени Л.Н. Гумилева. -2014, №4, с.120-127.

Гафуров Х.

СТЕГОАНАЛИЗ В СРЕДЕ ПРОГРАММЫ MathCAD11

Таджикский государственный университет права, бизнеса и политики, г.

Худжанд, Республика Таджикистан

Одним из актуальных проблем цифровой стеганографии является стегоанализ направленный на обнаружение информации скрытой внутри другого информационного объекта называемого контейнером, в качестве которого могут быть использованы файлы фотографий различных форматов [1]. Естественно в сегодняшних условиях необходимо иметь возможность программного решения этой проблемы. С этой точки зрения представляется интересным рассмотрение возможности программы MathCAD11, предназначенный для решения различных математических и научно-технических задач, для стегоанализа файлов фотографий.

Известно, что для скрытия информации в фотографических файлах разработаны различные программы, в числе которых можно назвать и программу Jphswin.exe. Используя эту программу разместим, скрытно, разные степени сложности объекты в виде рисунков и попробуем анализировать полученные рисунки в среде программы MathCAD11 с целью обнаружения разницы по сравнению с оригиналом использованного файла фотографии.

Для начала создадим два файла разными именами одной и той же фотографии достаточно хорошего качества и определим их разницу используя функции программы MathCAD11 выполнением следующих операций.

Используя файл фотографии, в среде программы MathCAD11, создадим ее матрицу.

$$D := \text{READRGB}("D:\text{Pic}\text{DES.jpg} ")$$

Таким образом мы получили матрицу фотографии размером $2500 \times 2000 = 5000000$ пиксель, название файла которого DES.jpg.

Матрицу этой же фотографии но сохраненную с названием файла DES01056.jpg получаем за счет следующей функции:

$$D1 := \text{READRGB}("D:\text{Pic}\text{DES01056.jpg} ")$$

На основе полученных матриц можем создать рисунки в среде программы которые приводятся на рис.1.



Рис.1 Два рисунка в среде MathCAD11 на основе матриц D1 и D

Визуально эти рисунки не имеют разницу и для определения их разницы выполним операцию вычитания матриц D1 и D используя такую возможность программы результатом которого будет третья матрица имеющий такой же размер что и матрица анализируемых фотографий.

$$G1 := D1 - D$$

Если между двумя фотографиями будет разница то это отразится на содержание третьей матрицы.

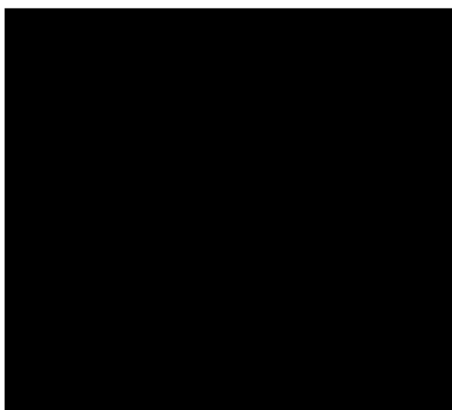


Рис.2 Рисунок разницы матриц $D1$ и D в среде MathCAD11

Эту разницу можно визуализировать путем формирования фотографии на основе данных третьей матрицы. Для рассмотренного случая когда нет скрытой информации внутри файлов рисунков DES.jpg и DES01056.jpg мы получаем изображение состоящего из черного прямоугольника который представлен на рис.2.

Полностью однотонный черный четырёхугольник является признаком отсутствия разницы в анализируемых рисунках DES.jpg и DES01056.jpg, а следовательно и дополнительной скрытой информации.

Используя стеганографическую программу Jphswin.exe разместим внутри одного из рисунков, а именно DES01056.jpg рисунок однотонного квадрата зеленого цвета и полученный стегофайл сохраним под именем D_G.jpg. Создаем матрицу этого файла в среде MathCAD11.

```
D_G:=READRGB(D:\Pic\D_G.jpg)
```

Определи разницу матриц фотографий со скрытой информацией и оригиналом.

```
G := D_G - D
```

Создаем ее рисунок который представлен на рис.3.



Рис.3 Рисунок разницы матриц оригинала и фотографии со скрытой информацией

В полученном рисунке мы видим множества светлых пятен которые являются свидетелями наличия дополнительной информации в фотографии имеющий название D_G.jpg. Конечно пока не известно в чем состоит разница фотографий, однако факт обнаружения дополнительной информации в среде программы MathCAD11 несомненно является хорошим результатом.

По рассмотренному принципу были получены разницы фотографий с оригиналом при скрывании внутри исследуемой фотографии объектов разной сложности. Полученные результаты и сами объекты показаны на рис.4 и 5.

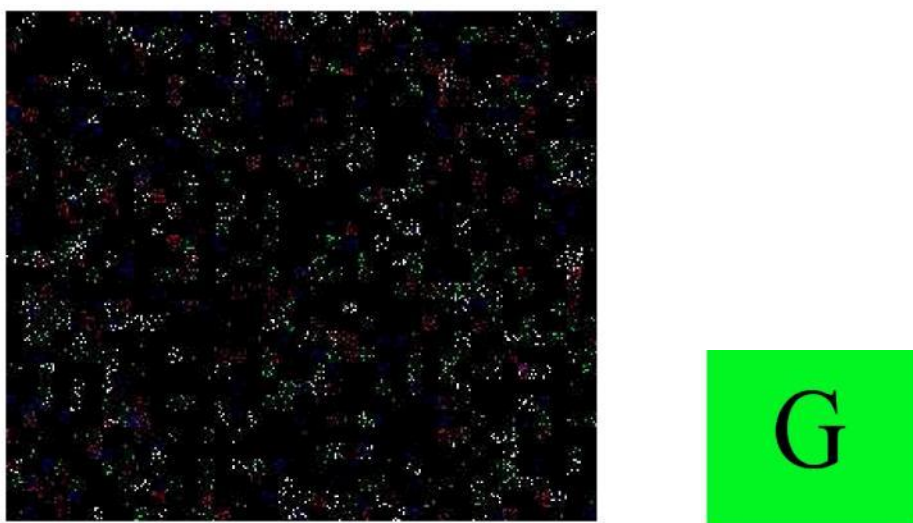


Рис.4 Фотография разницы и изображение объекта скрытого внутри исследуемой фотографии в виде квадрата с одним символом

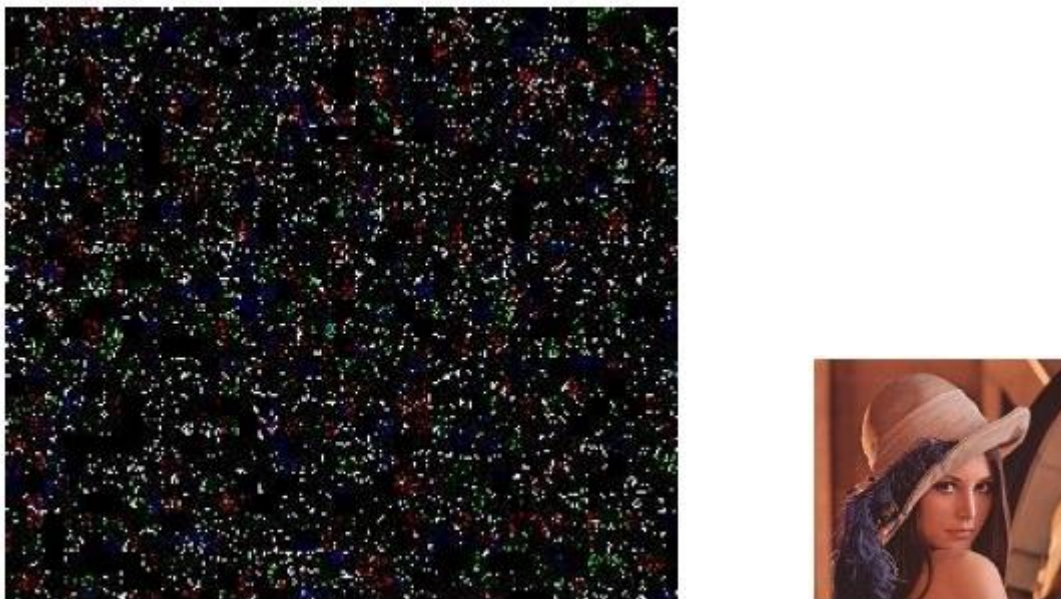


Рис.5 Фотография разницы и изображение объекта скрытого внутри исследуемой фотографии в виде сложного изображения

На основе сравнения результатов можно сказать, количество неоднородности разницы фотографий со скрытой информацией и оригинала зависит от степени сложности скрываемого объекта.

Таким образом на основе анализа результатов применения стеганографической программы Jphswin.exe в среде программы MathCAD11 можно сделать следующие выводы.

1. В среде программы MathCAD11 имеется возможность анализа фотографий в виде матрицы их данных которые легко обрабатываются.
2. На основе анализа матрицы фотографий легко можно обнаружить их разницу по сравнению с оригиналом который может быть образован в результате применения цифровой стеганографии.
3. Среда программы MathCAD11 может быть использована для стеганографического анализа файлов фотографий и других видов информации.

Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография М.: Солон-Пресс, 2009. — 265 с.

Джамбеков А.М.

**НЕЧЕТКОЕ СИТУАЦИОННОЕ УПРАВЛЕНИЕ ПРОЦЕССАМИ
ЗАЩИТЫ ИНФОРМАЦИИ НЕФТЕГАЗОВОГО ПРЕДПРИЯТИЯ**
ФГБОУ ВПО «Астраханский государственный технический университет»,
Астрахань, Россия

В настоящее время для крупных промышленных предприятий, в том числе и нефтегазовых, важное значение имеет комплексная защита их информационных ресурсов и систем. Защита информационных систем является сложной комплексной задачей, призванной решать вопросы обеспечения конфиденциальности, целостности и доступности информации. В зависимости от сложности и разветвленности структуры нефтегазового предприятия разрабатываются и реализовываются те или иные методы защиты информации от вредоносных атак.

К основным видам вредоносных воздействий при перехвате относятся: простое прослушивание сети, внедрение ложного информационного объекта, атакующее воздействие с передачей паразитного трафика, изменение критически важных информационных ресурсов и др.

Предлагается подход к защите информационных объектов на нефтегазовом предприятии на основе ввода в заблуждение потенциальных нарушителей зон информационной системы относительно истинных целей, характеристик, задач, решаемых объектом защиты. Одним из путей осуществления данного подхода является создание ложных информационных объектов.

Ложный информационный объект информационной системы является аналогом реального информационного объекта и наделен его основными функциями и свойствами. При этом система защиты информационных ресурсов нефтегазового предприятия будет включать совокупность определенного количества ложных информационных объектов. Структурный состав ложных

информационных объектов, их количество и уровень противодействия вредоносным атакам должны соответствовать их глубине и интенсивности. Так как модель злонамеренного воздействия на информационную систему имеет нечеткий характер, то делаем предположение о нечеткости модели системы противодействия вредоносным атакам. Описание нечеткого характера поведения информационных объектов производится на основе теории нечетких множеств.

К нечисловым параметрам, которые характеризуют вредоносную атаку, необходимо отнести параметры двух типов: качественные оценочные параметры и параметры, отражающие степень влияния оценок соответствующих показателей на суммарную оценку ущерба информационной системе нефтегазового предприятия.

С целью обозначения приведенных выше параметров введем лингвистические переменные: $\langle y_i, T_i, D_i \rangle$ с названием $y_i = \text{«ОЦЕНКА}_i\text{»}$ и $\langle z_k, S_k, H_k \rangle$ с названием $z_k = \text{«ЗНАЧИМОСТЬ}_k\text{»}$ [1].

Для терм-множеств лингвистических переменных «ОЦЕНКА» и «ЗНАЧИМОСТЬ» накладываются следующие условия [2]:

$$\left\{ \begin{array}{l} \mu_{C_1}(\inf D) = 1, \\ \mu_{C_J}(\sup D) = 1, \\ \forall T_j \in T \setminus \{T_J\} \ 0 < \sup \mu_{C_j \cap C_{j+1}}(d) < 1, \\ \forall T_j \in T \ \exists d \in D \mid \mu_{C_j}(d) = 1, \\ \exists d_1, d_2 \in D \mid \forall d \in D (d_1 < d < d_2). \end{array} \right.$$

где $T = \{T_j \mid j = \overline{1, J}\}$ - упорядоченное терм-множество в соответствии с правилом:

$$\forall T_j, T_k \in T (j > k) \Leftrightarrow \exists d_j, d_k \in D (d_j > d_k),$$

которое означает, что терм с левее расположенным носителем обладает меньшим порядковым номером. Данное условие означает, что обозначаемые выше указанными лингвистическими переменными понятия должны

представлять собой множества, ранжированные по качественным значениям признака.

В основу построения функций принадлежности нечетких множеств будет положено использование π -функции, определяемой системой выражений [3]:

$$\mu_{C_j}(d) = \pi(d, \eta_j, d_j^I, d_j^II)^{2^s},$$

$$\pi(d, \eta_j, d_j^I, d_j^II) = \begin{cases} s(d, d_j^I - 2\eta_j, d_j^I - \eta_j, d_j^I), \text{ нпу } d \leq d_j^I, \\ 1, \text{ нпу } d_j^I \leq d \leq d_j^II, \\ 1 - s(d, d_j^II, d_j^II + \eta_j, d_j^II + 2\eta_j), \text{ нпу } d \geq d_j^II, \end{cases}$$

$$s(d, \xi, \tau, \delta) = \begin{cases} 0, \text{ нпу } d \leq \xi, \\ \frac{2(d - \xi)^2}{(\delta - \xi)^2}, \text{ нпу } \xi \leq d \leq \tau, \\ 1 - \frac{2(\delta - d)^2}{(\delta - \xi)^2}, \text{ нпу } \tau \leq d \leq \delta, \\ 1, \text{ нпу } d \geq \delta. \end{cases}$$

В памяти ЭВМ функция принадлежности $\mu_{C_j}(d)$ представляется четырьмя параметрами: d_j^I и d_j^II , задающие интервал номинальных значений базовой переменной d , для которых степень принадлежности терму $T_j \in T \setminus \{T_1, T_J\}$ равна 1; η_j определяющим относительно значений d_j^I и d_j^II значения базовой переменной d , для которых степень принадлежности терму $T_j \in T \setminus \{T_1, T_J\}$ равна 0,5; параметром s , который характеризует функцию принадлежности в интервалах:

$$[d_j^I - 2\eta_j; d_j^I], [d_j^II; d_j^II + 2\eta_j].$$

Для количественной оценки лингвистических переменных воспользуемся процедурой дефаззификации методом «центра тяжести» [4]:

$$\hat{T} = \frac{\int_{d=d^I-2\eta^I}^{d^I+2\eta^I} d \mu_T(d) d(d)}{\int_{d=d^I-2\eta^I}^{d^I+2\eta^I} \mu_T(d) d(d)}$$

На основании указанного подхода, любая информационная система газоперерабатывающего предприятия способна определить глубину, степень и интенсивность вредоносных атак и на основе анализа сгенерировать определенное количество ложных информационных объектов. Структура данных объектов формируется путем анализа поведения нарушителя системы и интегрируется при использовании типовых сервисов и служб в зависимости от текущей оценки системой вредоносной атаки.

Приведенный подход определения уровня потенциальных угроз информационной системе можно использовать и в других задачах информационной безопасности газоперерабатывающих предприятий, где свойства и признаки объектов могут быть представлены на основе нечеткого ситуационного подхода.

Литература

1. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. - М.: Горячая линия - Телеком, 2007. - 284 с.
2. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2003. – 736 с.
3. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. - М.: Горячая линия - Телеком, 2006. - 452 с.
4. Усков А.А., Кузьмин А.В. Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика. - М.: Горячая линия – Телеком, 2004. - 144с.

Доля А.В., Бердибеков А.Т.

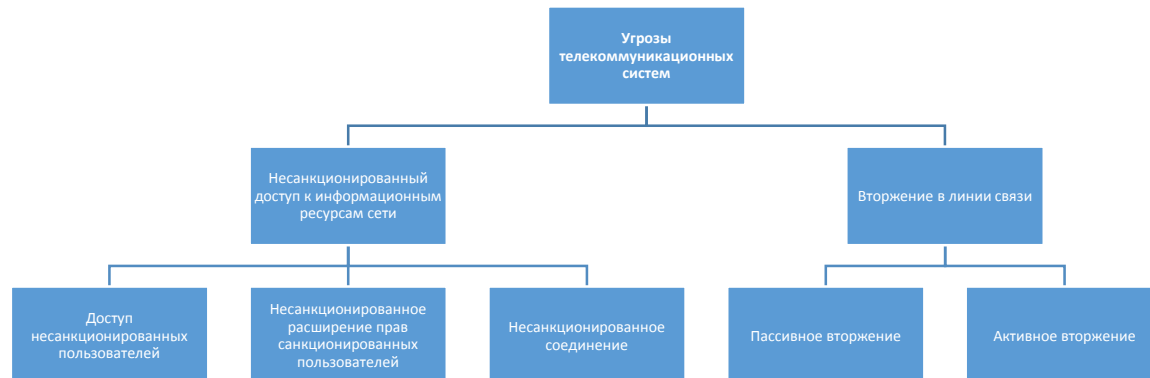
**ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ
СИСТЕМАХ**

Национальный университет обороны имени Первого Президента Республики
Казахстан – Лидера Нации, г. Астана

Телекоммуникационные системы, как и любая информационная система, работают в условиях воздействия многочисленных угроз безопасности информации, циркулирующей в них.

Современные телекоммуникационные системы (ТКС) предназначены для обмена сообщениями и базируются на элементах компьютерных сетей [1].

Как и для других информационных систем, угрозы для ТКС можно классифицировать как угрозы конфиденциальности информации, целостности и доступности. Для ТКС, как систем с распределенной структурой, имеющей территориально разнесенные элементы, соединенные каналами связи все множество угроз условно можно представить следующей диаграммой:



Несанкционированный доступ к информационным ресурсам сети осуществляется с целью копирования, чтения, модификации, а также уничтожения данных или программ.

Являясь объектом коллективного использования, телекоммуникационной системе присуще также такой вид угрозы как несанкционированное расширение прав санкционированных пользователей. При выполнении различных действий пользователями (хранение, создание, передача

информации) существует угроза, что разрешенный пользователь может попытаться произвести в системе неразрешенные ему действия, в том числе расширения своих полномочий в системе, используя для этого недостатки программно-аппаратных средств телекоммуникационной системы или с помощью применения внедрённого программного обеспечения.

Несанкционированное соединение к информационным ресурсам сети осуществляется нарушителем, выдавшим себя за разрешенного пользователя, с другим разрешенным пользователем с целью получения от него важной информации или дезинформирования.

При пассивном вторжении в линию связи нарушитель только просматривает сообщения, передаваемые по линиям связи, не нарушая их передачу. При этом нарушитель делает попытку читать передаваемые сообщения и проводить анализ трафика сообщений, передаваемых по каналам связи, с целью выявления идентификаторов объектов сети, длину сообщения, адреса и прочие параметры сети.

При активном вторжении в линию связи нарушитель осуществляет всевозможные манипуляции над сообщениями во время соединения. В этом случае сообщения могут быть уничтожены, скопированы, модифицированы, задержаны, может быть изменен порядок следования сообщения, а также введены в сеть сообщения ложного характера.

Для защиты от несанкционированного доступа используются процедуры управления доступом. За каждым субъектом (пользователем, процессом) закрепляется определенная информация, называемая идентификатором, позволяющая идентифицировать только его. Идентификаторы всех санкционированных субъектов регистрируются в сети, и при входе в сеть идентификатор проверяется. При положительном результате соответствия идентификатора происходит процедура аутентификации, то есть проверка подлинности субъекта). В результате процедуры аутентификации путем предъявления индивидуального пароля, который знает только

санкционированный субъект, пользователю предоставляются регламентированные полномочия.

При разнесенном взаимодействии двух субъектов через каналы передачи данных перечисленных мер может оказаться недостаточно, поэтому возникает проблема подтверждения подлинности соединения абонентов. Она заключается в том, что получатель должен быть уверен в истинности источника данных и истинности самих данных посредством применения технологии электронной цифровой подписи (ЭЦП). Тогда как сам отправитель должен получить подтверждение в получении (уведомление) и быть уверен в доставке данных получателю и в истинности доставленных данных. Эта процедура реализуется также с помощью ЭЦП. При этом для доказательства отправителю истинности переданного сообщения, уведомление о получении включает модификацию ЭЦП полученного сообщения. При этом в силу свойств ЭЦП отправитель не может отрицать ни факта отправления сообщения, ни его содержания, а получатель не может отрицать ни факта получения сообщения, ни истинности его содержания.

При отправке сообщений по каналам электронной почты получатель не является активным в момент пересылки. Это означает, что:

- взаимоподтверждение подлинности невозможно;
- ЭЦП проверяется в более позднее время, когда получатель забирает сообщение;
- получение уведомления отправителя о доставке сообщения также откладывается.

В связи с этим защита электронной почты требует специальных протоколов подтверждения подлинности отсроченных процедур.

Специфические проблемы, связанные с подтверждением передачи сообщений, возникают при организации телеконференций. Здесь для обеспечения взаимодействия участников также должны использоваться специальные протоколы.

Для всего рассмотренного выше предполагалось, что взаимодействуют взаимодоверяющие субъекты в недружественном сетевом окружении. То есть, считалось, что источник угроз по отношению к соединению находится вне его. Более сложно обеспечить защиту при передаче сообщений между недружелюбными субъектами, когда никто никому не доверяет. Это заставляет входить в соединение, обмениваясь минимумом (или одинаковой по важности) идентификационной информацией. Процедуры защиты, используемые при этом, получили название - подписание контракта.

Использование двухуровневой защиты линий связи, при которой защищается трафик и текст сообщения позволяет противодействовать пассивным вторжениям в линии связи.

Защита от активных вторжений сводится, по существу, к действиям, позволяющим устанавливать факт атаки на линию связи, при этом работа сети может быть временно нарушена.

Из рассмотренных выше подходов к защите телекоммуникационных систем можно выделить следующие задачи системы защиты:

- защищать данные во время их хранения и передаче по каналам связи;
- необходимо идентифицировать субъекты и подтверждать их подлинность;
- предоставлять полномочия и осуществлять контроль доступа, при этом быть управляемой только со стороны уполномоченного субъекта и недоступной для модификации для всех остальных пользователей.

На сегодняшний день все вышесказанные задачи системы защиты телекоммуникационных систем решаются применением криптографии, ЭЦП, протоколов идентификации и аутентификации, межсетевых экранов.

Возможности злоупотребления информацией, передаваемой по телекоммуникационным каналам, развиваются и совершенствуются не менее интенсивно, чем средства их предупреждения. По этой причине проблема

защиты информации требует организации целого комплекса специальных мер с целью предупреждения потери информации, циркулирующей в телекоммуникационных каналах.

Комплексный подход к информационной безопасности предусматривает комплексное развитие всех методов и средств защиты информации. Таким образом, в сферу влияния современной технологии защиты информации, передаваемой по телекоммуникационным каналам, попадают не только каналы связи, но и центры коммутации, периферийные устройства, терминалы, администраторы связи, локальные компьютерные сети и т.д.

Литература

1. Голиков В.Ф., Курилович А.В. Криптографическая защита информации в телекоммуникационных системах: учеб. пособие / В.Ф. Голиков, А.В. Курилович – Минск : БГУИР, 2006. 77с.

Жангисина Г.Д.

СОВРЕМЕННЫЕ ТРЕБОВАНИЯ К НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ: ИНФОРМАЦИОННЫЙ АСПЕКТ

Центрально-Азиатский университет

В настоящее время в условиях усиления глобализации вопросы национальной безопасности государства являются актуальными для Республики Казахстан. **Информационная безопасность** - это атрибут национальной безопасности государства.

В разных странах название документов, раскрывающих содержание концепции национальной безопасности, различное. В частности, в США — это «Стратегия национальной безопасности», в Канаде и Турции — «Политика национальной безопасности», в Италии — «Стратегическая концепция национальной обороны». В Великобритании, Германии, Китае, Японии и ряде

других стран подобными документами являются так называемые «Белые книги». Положения всех этих документов являются базой для формирования и осуществления единой общегосударственной концепции национальной безопасности государства в различных сферах деятельности (военной, экономической, социальной, экологической, информационной и других).

В данном докладе затрагивается информационный аспект.

В связи с новейшими научно-техническими достижениями в области информатики и информационных технологий современное соперничество государств и других объектов социальной природы характеризуется появлением нового фактора - **информационного**. Через целевое воздействие на информационную среду реализуются угрозы национальной безопасности в различных сферах человеческой деятельности. В политической сфере все большую значимость приобретает информационно-психологическое воздействие с целью формирования отношений в обществе, его реакции на происходящие процессы. В экономической сфере растет уязвимость экономических структур от недостоверности, запаздывания и незаконного использования рыночной информации. В военной сфере исход вооруженной борьбы все в большей степени зависит от качества добываемой информации и уровня развития информационных технологий, на которых основываются системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием. В сфере духовной жизни возникает опасность развития в обществе, в результате применения электронных средств массовой информации, агрессивной потребительской идеологии, распространения идей насилия и нетерпимости, а также других негативных воздействий на сознание и психику человека.

Информационная безопасность - защищенность информационной среды личности, общества и государства от преднамеренных и непреднамеренных угроз и воздействий.

1. Внутренние угрозы национальной безопасности Казахстана в информационной сфере

Информационная сфера Казахстана характеризуется активным развитием современных средств информационного обмена и различного типа технических средств. Слабое внимание, уделяемое проблемам обеспечения информационной безопасности, создает объективные условия для незаконного доступа к закрытой информации, ее хищения или разрушения. Особую опасность имеет возможность манипуляций различного рода информацией для негативного воздействия на процесс принятия стратегических решений. Одновременно игнорирование факторов информационной безопасности может привести к сдерживанию процессов становления системы национальной безопасности во всех других ее сферах и серьезно осложнить задачи управления информационными ресурсами в этой области. К внутренним угрозам национальной безопасности Казахстана в данной сфере относятся:

1) стратегическое отставание Казахстана от ведущих стран мира по уровню информатизации; 2) нарушение информационных прав и свобод частных и юридических лиц; 3) несанкционированный доступ к информации во всех сферах деятельности, циркулирующей в системах электронной обработки данных и автоматизированных сетях связи, с целью ее хищения, искажения или уничтожения; 4) противоправное содействие со стороны отдельных граждан и организаций деятельности специальных служб иностранных государств; 5) ограничение законных прав средств массовой информации и журналистов на законное получение, сбор и передачу информации.

2. Внешние угрозы национальной безопасности Казахстана в информационной сфере

К основным внешним угрозам национальным интересам Казахстана в информационной сфере относятся:

- 1) недопущение Казахстана к участию на равноправной основе в международном информационном обмене;
- 2) возможность преднамеренных воздействий на государственные и общественные информационные системы для нарушения их функционирования или несанкционированного доступа к ним;
- 3) использование дезинформации для воздействия на общественное мнение и принимаемые решения стратегического руководства; действия, связанные с расхищением информационных ресурсов Казахстана.

Основные задачи по реализации и защите национальных интересов на современном этапе развития Казахстана в информационной сфере:

- Принятие закона о концепции информационной безопасности Казахстана, определяющего систему сбалансированных политических, юридических, организационных и научно-технических мероприятий по обеспечению устойчивости государственных и военных информационных средств и структур в условиях воздействия различных видов «информационного оружия».
- Обеспечение свободы получения и распространения информации гражданами, другими субъектами общественных отношений в интересах формирования гражданского общества, демократического правового государства, развития науки и культуры.
- Обеспечение надежной защиты информационного потенциала Казахстана (т.е. совокупности информации, обеспечивающей национальные интересы страны; систем ее получения, хранения, переработки и распространения; его субъектов) от неправомерного его использования в ущерб охраняемым законом интересам личности, общества и государства.
- Осуществление контроля и надзора за экспертом из страны интеллектуальной продукции, а также информационных банков данных.

Организация эффективной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности.

- Развитие взаимодействия государственных и негосударственных систем информационного обеспечения в целях более эффективного использования информационных ресурсов страны.

- Совершенствование системы нормативно-правовых актов, регулирующих отношения собственности и соблюдения баланса интересов личности, общества и государства в сфере формирования, хранения и использования информационных ресурсов. Формирование и развитие федеральных и региональных центров сертификации систем информационной защиты и их элементов.

- Противодействие целенаправленным действиям по дезинформированию органов власти, населения страны, использованию каналов информационного обмена для нарушения систем управления различными сферами жизнедеятельности государства.

- Создание общего информационного пространства стран СНГ в интересах содействия интеграционным процессам, повышения эффективности взаимодействия в реализации общих интересов. Включение Казахстана в международную систему информационного обмена с учетом обеспечения национальных интересов и противодействия акциями информационной интервенции.

- Обеспечение на международном уровне принятия решений о безусловном запрете на использование информационного оружия в мирное время.

Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» регулирует правовые отношения в области национальной безопасности Республики Казахстан и определяет содержание и принципы обеспечения безопасности человека и

гражданина, общества и государства, систему, цели и направления обеспечения национальной безопасности Республики Казахстан.

Видами **национальной безопасности** являются:

1) **общественная безопасность** - состояние защищенности жизни, здоровья и благополучия граждан, духовно-нравственных ценностей казахстанского общества и системы социального обеспечения от реальных и потенциальных угроз, при котором обеспечивается целостность общества и его стабильность;

2) **военная безопасность** - состояние защищенности жизненно важных интересов человека и гражданина, общества и государства от внешних и внутренних угроз, связанных с применением военной силы или намерением ее применения;

3) **политическая безопасность** - состояние защищенности основ конституционного строя, деятельности системы государственных органов и порядка государственного управления от реальных и потенциальных угроз, при котором обеспечивается соблюдение прав и свобод граждан, социальных групп и баланс их интересов, стабильность, целостность и благоприятное международное положение государства;

4) **экономическая безопасность** - состояние защищенности национальной экономики Республики Казахстан от реальных и потенциальных угроз, при котором обеспечивается устойчивое ее развитие и экономическая независимость;

5) **информационная безопасность** - состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны;

6) **экологическая безопасность** - состояние защищенности жизненно важных интересов и прав человека и гражданина, общества и государства от

угроз, возникающих в результате антропогенных и природных воздействий на окружающую среду.

В статье 23 - «Обеспечение информационной безопасности»

(Закон Республики Казахстан «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 07.11.2014 г.) говорится:

1. Информационная безопасность обеспечивается решениями и действиями государственных органов, организаций, должностных лиц, направленными на:
 - 1) недопущение информационной зависимости Казахстана;
 - 2) предотвращение информационной экспансии и блокады со стороны других государств, организаций и отдельных лиц;
 - 3) недопущение информационной изоляции Президента, Парламента, Правительства и сил обеспечения национальной безопасности Республики Казахстан;
 - 4) обеспечение бесперебойной и устойчивой эксплуатации сетей связи в целях сохранения безопасности Республики Казахстан, в том числе в особый период и при возникновении чрезвычайных ситуаций природного, техногенного характера, карантинных, иных чрезвычайных ситуаций;
 - 5) выявление, предупреждение и пресечение утечки и утраты сведений, составляющих государственные секреты и иную защищаемую законом тайну;
 - 6) недопущение информационного воздействия на общественное и индивидуальное сознание, связанного с преднамеренным искажением и распространением недостоверной информации в ущерб национальной безопасности;
 - 7) обнаружение и дезорганизацию механизмов скрытого информационного влияния на процесс выработки и принятия государственных решений в ущерб национальной безопасности;

8) поддержание и развитие эффективной системы защиты информационных ресурсов, информационных систем и инфраструктуры связи, в которых циркулируют сведения, составляющие государственную, коммерческую и иную защищаемую законом тайну.

Для сравнения дадим анализ современного состояния национальной безопасности наших ближних соседей России и Китая, а также государства США.

1) О национальной безопасности России.

Россия переживает непростой этап формирования нового социально-экономического и политического строя. Происходит это в условиях крайне противоречивого, на грани кризиса, переходного периода, затрагивающего все стороны нашей жизни. В современном мире перед Россией встала неотложная задача, заключающаяся, прежде всего, в обеспечении национальной безопасности. Она диктуется наличием реально существующих угроз: угрозы государству - его целостности и независимости, угрозы обществу - его демократическим институтам, угрозы личности - ее правам и свободам. Нуждается в существенной доработке и Концепция национальной безопасности. В Концепции выделяется 9 основных сфер деятельности государства, понимаемых как объекты безопасности: международная, внутриведомственная, социальная, военная, пограничная, экономическая, информационная, духовная, экологическая. Вместе с тем, Концепция не выделяет технологическую и продовольственную составляющие, а также региональные и правоохранные аспекты безопасности.

Мониторинг законодательной основы национальной безопасности Российской Федерации выявил отсутствие в ней целостности и системности. Внутриведомственная ориентированность нормативных правовых актов в сфере национальной безопасности, с одной стороны, выступает инструментом организации деятельности конкретных органов исполнительной власти, с

другой - является причиной фрагментарности и разрозненности правовых норм, регулирующих отношения в области национальной безопасности. Противоречия и декларативность положений законов, регулирующих сферу национальной безопасности, препятствуют их эффективному и целенаправленному исполнению.

2) О национальной безопасности США.

В настоящее время национальная безопасность подразделяется в зависимости от местонахождения источника угрозы на два типа - внутреннюю и внешнюю безопасность/3/. В данный момент и в обозримой перспективе угрозы национальной безопасности государства носят преимущественно внутренней характер и сосредоточены во внутривнутриполитической, экономической, социальной, экологической, информационной и духовной сферах. Данное обстоятельство дополнительно повышает значимость проблемы обеспечения внутренней безопасности страны.

Принципиально иными стали внутренние угрозы безопасности и соответственно изменяются задачи по их своевременному выявлению, предупреждению и парированию. Среди этих угроз особо опасными является рост преступности, коррупции, контрабанды, незаконной миграции, незаконного оборота оружия, боеприпасов, взрывчатых и отравляющих веществ, наркотических средств, деятельность незаконных вооруженных формирований, ставящих своей целью насильственное изменение конституционного строя государства и насильственный захват власти.

Наиболее отработанная и развитая система формирования концептуальных основ национальной безопасности в настоящее время сложилась в США. Само понятие «национальная безопасность» широко вошло в международную практику с 1947 года, когда в США был принят Закон «О национальной безопасности». При этом под «национальной безопасностью» в США понимают состояние защищенности государства от враждебных актов

или других видов вмешательства, в том числе от внутренних угроз. Понятие «национальная безопасность» включает как национальную оборону, так и внешние отношения государства в политической, экономической и других сферах. В Соединенных Штатах Америки Закон «О национальной безопасности» 1947 года не предусматривал деления национальной безопасности на внутреннюю и внешнюю. В период «холодной войны» жесткая конфронтация в военной и идеологической областях определила приоритет внешнеполитического и военно-политического подхода к проблемам национальной безопасности в США. Поэтому стратегия национальной безопасности США во все года «холодной войны» касалась только внешней безопасности, практически не затрагивая внутренних сфер. Однако, трагические события 11 сентября 2001 года вынудили американскую администрацию повернуться лицом к проблемам внутренней безопасности. Война против террористов с глобальной досягаемостью объявлена долгосрочной задачей мирового масштаба. Впервые в американской истории появился и стал официально использоваться термин «внутренняя безопасность», как согласованные национальные усилия по предотвращению террористических действия на территории Соединенных Штатов, по снижению уязвимости Америки от терроризма, по минимизации ущерба и ликвидации последствий возможных терактов»/4/.

В соответствии с положениями «Национальной стратегии внутренней безопасности» обеспечение внутренней безопасности США организуется на четырех базовых элементах - **право, достижения науки и технологии, современные информационные технологии и международное сотрудничество**. Сочетание этих четырех основополагающих факторов дает возможность оценить реальный уровень внутренней безопасности и определить масштабы необходимых государственных ассигнований в эту сферу. Именно право позволяет правительству выбрать конкретные механизмы соответствующих действий и в то же время ограничивает масштабы этих

действий определенными рамками. Федеральные законы не должны задавить законодательную инициативу штатов и в то же время не допустить чрезмерной федерализации борьбы с терроризмом. В США уже созданы правовые основы обеспечения внутренней безопасности. Они закреплены, прежде всего, в Конституции и Своде законов США. В «Законе Патриота США» дополнено определение понятия «международный терроризм», но главное - впервые в американском законодательстве терроризм разделен на международный и внутренний. Американская администрация особо подчеркивает криминальный характер современного терроризма, резко усиливает санкции за преступления террористического характера и расширяет карательные возможности федерального правительства в борьбе с терроризмом как частью организованной преступности.

3) О национальной безопасности Китая.

Традиционные угрозы для Китая дают о себе знать преимущественно в политической и военной сферах. После окончания холодной войны традиционными угрозами остаются гегемонизм и политика с позиции силы. В настоящее время они проявляются следующим образом.

Во-первых, сохраняется тенденция к росту числа локальных войн и вооруженных конфликтов, отличительными особенностями которых являются продолжительность, сравнительно высокая географическая концентрированность, а также сложность и многообразие причин. В 2008 году на нашей планете произошло 46 локальных войн и вооруженных конфликтов, в то время как в 2007-м их было гораздо меньше – 33. Кроме того, после холодной войны для них характерно применение высоких и информационных технологий.

Во-вторых, крупные мировые державы постоянно наращивают военные расходы для трансформации своих вооруженных сил, ядром которой служат информационные технологии. Мировым лидером являются Соединенные

Штаты. В 2008-м США израсходовали на военные нужды 481,4 млрд долларов (не учитывая средств, потраченных на ведение войн). КНР необходимо постоянно увеличивать финансирование армейского строительства в процессе модернизации народного хозяйства в четырех областях, с тем чтобы подготовить высококвалифицированных специалистов и повысить боеспособность военнослужащих в эпоху информационных технологий.. К 2020 году, когда будет обеспечен среднезажиточный уровень жизни населения, завершится механизация вооруженных сил с ориентацией на переход к информационным технологиям. А к 2050-му, когда Китай осуществит модернизацию во всех областях и выйдет в ряды среднеразвитых стран, закончится и процесс информатизации вооруженных сил. НОАК обретет способность одерживать победы в войнах локального характера с применением информационных технологий.

В-третьих, в центре внимания мирового сообщества находится вопрос о нераспространении ядерного оружия. Ядерные проблемы на Корейском полуострове и в Иране остаются самыми острыми вопросами международной безопасности.

В настоящее время Китай обладает огромным влиянием на геополитическое соотношение сил в Центральной Азии. Ускоренный экономический рост и другие факторы придают ему статус центра силы в регионе, где отчетливо прослеживается возвышение Китая до уровня мировой державы. Активизация Китая на центральноазиатском направлении является очевидным. Регион, представляющий стратегическую важность для Пекина, имеет огромный экономический потенциал, который Китай может использовать в целях собственного развития. Если экономика КНО будет и дальше сохранять нынешние высокие темпы роста, то она все больше и больше будет нуждаться в масштабных закупках нефти и газа, которыми так богата Центральная Азия(особенно Казахстан и Туркмения). Китайские политологи объясняют интерес к региону всевозрастающей потребностью в

энергоресурсах. В этой связи обеспечение прочных позиций и предотвращение доминирования третьей стороны в регионе являются главными задачами политики КНР и Центральной Азии. Реализация внешнеполитической стратегии в ЦАР производится на основании следующих факторов:

1)Геополитический фактор. КНР стремится путем распространения своего влияния в ЦА обезопасить «тылы», обеспечив тем самым безопасность и развитие Синьцзяна и других западных провинций. Геополитическое преобладание в Центральной Азии необходимо Китаю для противодействия политике США по сдерживанию его дальнейшего роста и противостояния однополярной системе и доминирующему положению Соединенных штатов на экономическом, политическом и военном уровнях.

2)Энергетический фактор. В обозримом будущем Пекин не планирует менять основные маршруты поставки нефти в страну. Руководство КНР стремится диверсифицировать поставщиков, способы транспортировки и варианты закупки углеводородов.

3)Фактор необходимости развития западных территорий. Для Пекина решение торгово-экономических вопросов не только способствует реализации его планов по укреплению своих позиций в регионе, но и отвечает задачам развития западных провинций КНР. Рынки стран Центральной Азии являются для производителей западных районов Китая идеальным вектором внешнеэкономической активности, так как удаленность от мировых морских коммуникаций усложняет их выход на основные рынки мира. В результате на сегодняшний день свыше 80% от общего товарооборота КНР с Центральной Азией приходится на СУАР.

4. Транзитный потенциал региона. Центральная Азия важна для Пекина как транспортный коридор, который в перспективе может обеспечить КНР сухопутный выход в Иран и далее в Европу. Появление возможности прокладки сухопутных магистралей через территорию стран ЦА важно для

Пекина в контексте диверсификации сухопутных маршрутов в Европу, а также сокращения сроков доставки китайской продукции.

Все вышесказанное в совокупности позволяет говорить о том, что Китай в силу своего геополитического веса, военной мощи (наличия сдерживающего стратегического арсенала), политического статуса (постоянного членства в совете безопасности ООН) и социальной притягательности для большой группы стран уже превращается из региональной державы в **центр силы глобального порядка**.

Можно утверждать, что именно Китай в перспективе может сыграть существенную роль в процессе становления нового стратегического равновесия и геополитической стабильности, а также создания новой системы международных отношений. Важное требование к системе безопасности - ее обязательное сопряжение с глобальной системой безопасности, международными региональными (общеевропейской, азиатско-тихоокеанской и др.) системами безопасности и национальными системами безопасности других стран, прежде всего соседних. Особое место здесь должна занять система коллективной безопасности стран СНГ.

Общая концепция национальной безопасности Казахстана, согласованная и утвержденная высшим руководством страны, должна упорядочить, скоординировать деятельность всех государственных органов, а значит усилить государство и внутри и вовне. Она послужит основой для исключения возможности нанесения ущерба национальной безопасности Казахстана. Если мы говорим **о безопасности личности**, то, в первую очередь, - это реализация всех ее возможностей, всестороннего развития, создания условий адаптации в быстро меняющемся мире. Поэтому **наука, образование, культура** занимают важнейшее место в сфере обеспечения **национальной безопасности**. Их разрушение - угроза безопасности не только личности, но и государства, чреватая уничтожением национальных корней граждан.

Уменьшение интеллектуального слоя общества – одна из самых серьезных угроз национальной безопасности хотя бы потому, что эти люди способны видеть и понимать суть процессов общественного развития, в том числе и в сфере национальной безопасности, через них работает механизм обратной связи между принимаемыми решениями в политической, социальной, экономической сферах и результатами реальных процессов, отражающих качество жизни граждан.

Современные угрозы безопасности для любого государства носят комплексный характер. Порой их трудно разделить на внутренние и внешние, "индивидуализировать" в плане того, грозят ли они лишь нам или другим странам тоже. Успех в экономике позволит смягчить комплекс сопутствующих взаимосвязанных угроз - нарастание опасности социальных потрясений, национализма, экологических бедствий, подрыв физического и духовного здоровья граждан, дальнейший рост криминализации общества и хозяйственной деятельности, сращивание криминальных и властных структур, истощение природных ресурсов. Национальные интересы не могут быть сформированы, осознаны и реализованы в отрыве от духовных традиций, без охранения и приумножения сугубо специфических российских ценностей, без создания определенных условий для творческого самовыражения духа российского общества. Обладая ограниченными ресурсами, отразить, смягчить эти угрозы мы сможем вместе только действуя сплоченно и на единой основе, которой должна стать концепция национальной безопасности.

Литература

- 1) Мусабеков Р.И. О растущей роли Китая в мировой геополитике. Оборонный вестник. Март 2014 год. С 26-27.
- 2) Озеров В.А. Национальная безопасность России: проблемы законодательного обеспечения безопасности РФ. Москва. 2010 год.

- 3) Чернигова, Н. К. (Надежда Константиновна). Правовое обеспечение внутренней безопасности страны в современных условиях : На опыте Соединенных Штатов Америки : Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность 05.26.02 - Безопасность в чрезвычайных ситуациях /Н. К. Чернигова; Науч. рук. Ю. Г. Шпаковский. -М.,2007. -28 с.-Библиогр. : с . 28.3.
- 4) National Strategy for Homeland Security. July 2002.P. 2.

Жук А. П., Осипов Д. Л., Гавришев А. А.

**АНАЛИЗ МЕТОДОВ ОЦЕНКИ ЗАЩИЩЕННОСТИ
БЕСПРОВОДНОЙ СИГНАЛИЗАЦИИ**

ФГАОУ ВПО «СКФУ», г. Ставрополь, Россия

В настоящее время происходит развитие беспроводных сигнализаций, в том числе охранно-пожарных и автомобильных [1]. Вместе с этим можно говорить о появлении негативной тенденции – участились атаки на технические системы охраны с нарушением их работы [2]. К таким атакам относятся [3]: перехват, просмотр и подмена. Таким образом, как для разработчиков, так и для пользователей беспроводных сигнализаций интерес представляют методы, позволяющие провести оценку защищенности (ОЗ) беспроводных сигнализаций (БС) от данных атак.

Целью данной статьи является анализ существующих методик ОЗ радиоканала БС от несанкционированного доступа (НСД).

Проведем обзор методик ОЗ БС как радиотехнических систем (РТС). Методики ОЗ разделим на следующие группы: вероятностная ОЗ специализированных РТС, оценка скрытности РТС, оценка имитозащиты РТС, оценка надежности РТС.

Рассмотрим вероятностную ОЗ РТС специального назначения (СН), которые выведены в отдельную группу в силу следующих особенностей:

наличие средств для радиоэлектронной борьбы и подавления, наличие возможности физического разрушения пунктов управления. В работах [4, 5] предлагаются следующие методики ОЗ радиоканала РТС СН (таблица 1):

Таблица 1 – методики ОЗ РТС специального назначения

Название	Область применения	Используемый математический аппарат	Полученный результат
Оценка разведзащищенности (РЗ) см. [4]	РТС СН		
Энергетическая		Теория вероятности (ТВ), теория надежности (ТН)	Оценка энергетической РЗ
Временная		ТВ, ТН	Оценка временной РЗ
Оценка помехоустойчивости см. [4]	РТС СН		
Энергетическая		ТВ, ТН	Оценка помехоустойчивости
временная		ТВ, ТН	Оценка помехоустойчивости
3) РЗ узлов связи см. [5]	РТС СН	ТВ	Комплексная оценка РЗ

Преимуществом рассматриваемых ОЗ является возможность оценки в сложных условиях, когда РТС работают в экстремальных условиях. Однако данные ОЗ малоприменимы для распространенных недорогих гражданских РТС. Кроме того, они отличаются сложной элементной базой и математическим аппаратом.

Рассмотрим методики оценки скрытности РТС. Она оценивается по следующим основным критериям: оценка энергетической скрытности (ЭС), оценка структурной скрытности (СС) (таблица 2).

Рассмотрим ЭС, под которой понимается малая вероятность обнаружения неизвестных сигналов по энергии. В работе [6] рассматривается ЭС радиолокационных сигналов (РЛС). Оценкой ЭС предлагается формула полной вероятности. Преимуществом данной оценки ЭС является возможности оценки РЛС с большой базой. В работе [7] ЭС предлагают оценивать как произведение алгоритмической скрытности R на число отчетов сигнала N_0 . Данная оценка отличается простотой расчетов.

Рассмотрим СС, под которой понимается процесс затруднения раскрытия структуры сигнала. В работе [8] предлагается оценка СС способа защиты информации со стохастическим применением ансамблей дискретных

ортогональных многоуровневых сигналов (АДОМС), зависящая от характеристик бидиагональной симметрической матрицы. Из-за малой проработанности вопросов АДОМС данная оценка может найти применение в ограниченном круге решений. В работе [9] предлагается оценка СС РТС, использующих хаотические последовательности. Конечная формула данной оценки отличается сложностью математических расчетов.

Таблица 2 – методики оценки скрытности РТС

Источник	Область применения	Используемый математический аппарат	Полученный результат
см. [6]	РТС	ТВ	Оценка ЭС
см. [7]	РТС	ТВ	Оценка детерминированных и стохастических сигналов
см. [8]	РТС	ТВ, комбинаторика	Оценка защищенности АДОМС
см. [9]	РТС	ТВ	Оценка СС

Рассмотрим методики оценки имитозащиты РТС (таблица 3). В работе [10] для оценки предлагается использовать гипергеометрическую стратегию имитонападения. Данная оценка отличается сложностью математических выкладок. В работе [11] предлагается оценка вероятности навязывания ложной информации. Данная оценка отличается простотой математического аппарата, однако возможность ее применения ограничена РТС СН. В работе [12] предлагается оценка имитозащиты РТС СН. Основным недостатком данной оценки является адаптированность для РТС СН, что затрудняет ее использование для гражданских РТС.

Таблица 3 – методики оценки имитозащиты РТС

Источник	Область применения	Используемый математический аппарат	Полученный результат
см. [10]	Автоматизированные системы радиосвязи	ТВ, геометрическое представление	оценка имитостойкости РТС
см. [11]	РТС СН	ТВ	оценка имитозащиты РТС
см. [12]	РТС СН	ТВ, теория графов	оценка имитозащиты РТС

Рассмотрим оценку надежности РТС. В работе [13] приводится оценка влияния угроз информационной безопасности (ИБ) на коэффициент готовности телекоммуникационных сетей. Данная оценка отличается простотой математического аппарата, однако она учитывает угрозы ИБ как проводных,

так и беспроводных систем и, кроме того, необходимо рассчитать время восстановления работоспособности. В работе [14] предлагается агрегатная имитационная модель функционирования систем радиосвязи в условиях преднамеренных помех, позволяющая проводить оценку эффективности их функционирования. Преимуществом данной оценки является простота математического аппарата.

Таким образом, сейчас не существует совершенных методик ОЗ БС: многие методики обладают сложным математическим аппаратом и, следовательно, сложны в программной реализации. Кроме того, все они обладают общим недостатком – ОЗ не носит комплексного характера и направлена на одну или несколько угроз ИБ. Так же присутствует проблема технологий «двойного назначения», препятствующих переносу специальных решений на гражданские системы. Из этого можно сделать вывод: разработка методик ОЗ БС представляет значительный научный и практический интерес. Наличие простой, и одновременно с этим эффективной методики ОЗ БС позволит найти наиболее рациональное решение задачи оценки защищённости. Одним из перспективных направлений построения методики, по мнению авторов, является использование нечёткой логики. Данное утверждение основывается на простоте математических расчетов, наличии количественных и качественных показателей, легкости в программной реализации.

Литература

- 1 Копытов В.В., Лепешкин О.М., Жук А.П. Комплексные средства безопасности и технические средства ОПС. – М.: Гелиос АРВ, 2009 – 288 с.;
- 2 <http://ru-bezh.ru/content/2014/07/30/veb-kamera-dropcam-okazalas>;
- 3 Осипов Д.Л., Гавришев А.А., Бурмистров В.А. К вопросу об защите датчиков технических систем охраны // Сборник трудов I МНПК «Информационная безопасность в свете Стратегии Казахстан-2050». – Астана, 2013 г., с. 463-467;

4 Эффективность систем военной связи и методы ее оценки. Боговик А.В., Игнатов В.В. – СПб.: ВАС, 2006. – 184 с.;

5 Мельник В.Г. и др. Показатели оценки разведывательной защищенности узлов связи пунктов управления систем военной связи // Материалы МНТК, приуроченной к 50-летию МРТИ-БГУИР, Минск: в 2 ч. – Ч. 1. – с. 211-212;

6 Куприянов А.И. и др. Скрытность сверхширокополосных радиолокационных импульсных сигналов // Технологии ЭМС. 2009. № 2. с. 13-18.;

7 Энергетическая скрытность сигналов и защищенность радиолиний: учеб. пособие / В.П. Литвиненко. Воронеж: ГОУ ВПО «ВГТУ», 2009. 166 с.;

8 Жук А.П. и др. Оценка структурной скрытности сигналов в системе передачи информации с ортогональными последовательностями // Известия ЮФУ. Тематический выпуск «Информационная безопасность». 2007. №1(76). с. 167-171;

9 Сивашенко С.И. Скрытность радиосистем со сложными и хаотическими сигналами // Системи упр., навігації та зв'язку. 2009. № 3. с. 56-58;

10 Орошук И.М. Оценка эффективности имитозащиты автоматизированных систем радиосвязи на основе гипергеометрической стратегии имитонападения // IV МК «Цифровая обработка сигналов и их применение». М., 2003 – с. 353-356;

11 Воронов Д.Н. Критерии оценки имитостойкости командно-телеметрических радиолиний // Системи обробки інформації. 2007. № 4(62). с. 14-16;

12 Романов А.М. Методика оценки уровня имитозащиты сигналов управления в радиосети специального назначения // Наука и бизнес: пути развития. 2014. № 2 (32). с. 42-44;

13 Митрохин В.Е. и др. Оценка влияния угроз информационной безопасности на доступность телекоммуникационной сети // Доклады ТУСУРа. 2014. № 2(32). с. 121-124;

14 Зайцев И.В. и др. Оценка эффективности систем радиосвязи в условиях преднамеренных помех на основе агрегативного имитационного моделирования их функционирования // Сборник докладов III ВНК ИММОД-2007. Том I / СПб.: ФГУП ЦНИИ ТС, 2007, с. 134-138;

Жумагулова С.К., Турсынғалиева Г.Н.
СОЗДАНИЕ ПРОГРАММНОГО КОМПЛЕКСА
КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ
КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ МЕТОДОМ ПРЯМОЙ
ЗАМЕНЫ

Карагандинский Государственный Университет им.Е.А.Букетова,
г.Караганда, Республика Казахстан

То, что информация имеет ценность, люди осознали очень давно - недаром переписка сильных мира сего издавна была объектом пристального внимания их недругов и друзей. Тогда-то и возникла задача защиты этой переписки от чрезмерно любопытных глаз. Еще в древние времена люди пытались использовать для решения этой задачи самые разнообразные методы, и одним из них была тайнопись - умение составлять сообщения таким образом, чтобы его смысл был недоступен никому кроме посвященных в тайну [1].

Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения [2].

В настоящее время особо актуальной стала оценка уже используемых криптоалгоритмов. Задача определения эффективности средств защиты зачастую более трудоемкая, чем их разработка, требует наличия специальных знаний и, как правило, более высокой квалификации, чем задача разработки.

Эти обстоятельства приводят к тому, что на рынке появляется множество средств криптографической защиты информации, про которые никто не может сказать ничего определенного. При этом разработчики держат криптоалгоритм (как показывает практика, часто нестойкий) в секрете. Однако задача точного определения данного криптоалгоритма не может быть гарантированно сложной хотя бы потому, что он известен разработчикам. Кроме того, если нарушитель нашел способ преодоления защиты, то не в его интересах об этом заявлять. Поэтому обществу должно быть выгодно открытое обсуждение безопасности систем защиты информации массового применения, а сокрытие разработчиками криптоалгоритма должно быть недопустимым [3].

Среди разнообразнейших способов кодирования информации можно выделить алгоритм прямой (простой) замены, когда буквы шифруемого сообщения заменяются другими буквами того же самого или некоторого другого алфавита.

При написании данной программы шифрования был применен метод прямой замены. Суть этого метода состоит в том, что используется таблица замены символов, которая позволяет отправителю зашифровать сообщение, а получателю расшифровать его. В случае шифрования данных, хранимых на магнитных или иных носителях информации, ключ позволяет зашифровать информацию при записи на носитель и расшифровать при чтении с него.

Данная программа обладает довольно качественным и понятным интерфейсом, поэтому пользователь без труда может сориентироваться при запуске приложения. Также одним из достоинств программы является то, что диалог пользователя с программой осуществляется при помощи понятных и довольно удобных диалоговых окон. Следует также заметить то, что в целом, программа выполнена в классическом варианте для приложений, разработанных для операционной Windows. То есть, это удобная, не надоедливая цветовая гамма, которая не раздражает после долгой работы органы зрения пользователя.

Разработанный программный продукт предназначен для шифрования конфиденциальной информации и выполняет следующие функции:

- обеспечение конфиденциальности информации;
- шифрование/дешифрование информации.

Для возможности работы с данным программным продуктом необходима ПЭВМ на базе процессора Intel Pentium 4 и выше, со свободным дисковым пространством не менее 1 Gb, оперативной памятью – 512 Mb. ПЭВМ на которой будет эксплуатироваться предоставляемая программа должна быть обеспечена операционной системой Windows XP или системами совместимыми с ней.

Разработанная система предназначена для шифрования информации методом прямой замены.

Запуск приложения осуществляется двойным нажатием левой кнопкой мыши по ярлыку файла Project1.exe. После чего на экране появится окно для шифрования/дешифрования информации (рисунок 1).

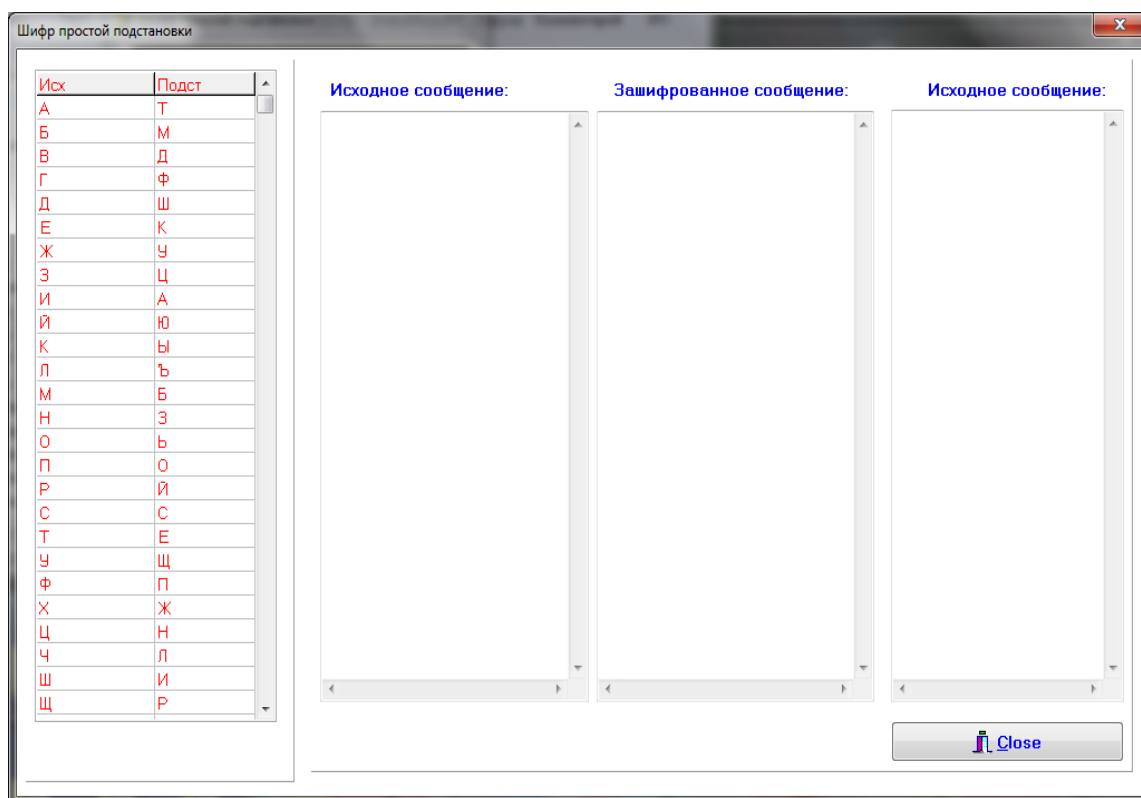


Рисунок 1. Меню Шифратор/Дешифратор

При помощи команды **Зашифровать** необходимо ввести текстовый файл для шифрования (рисунок 2).

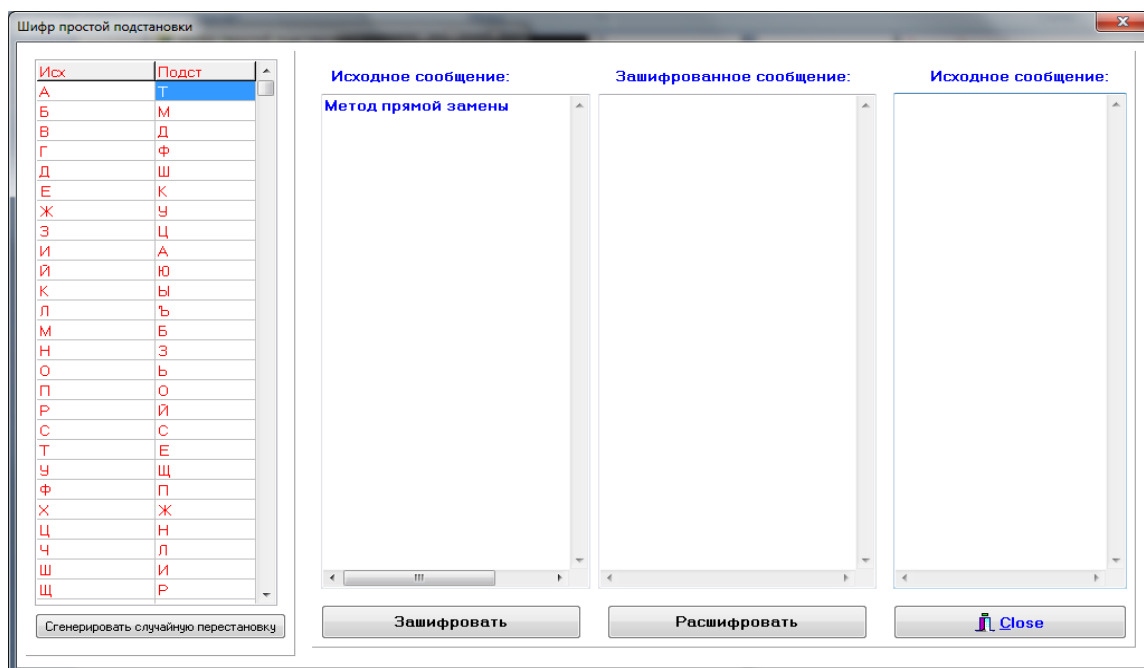


Рисунок 2. Результат шифрования

Зашифрованный текст представлен на рисунке 3.

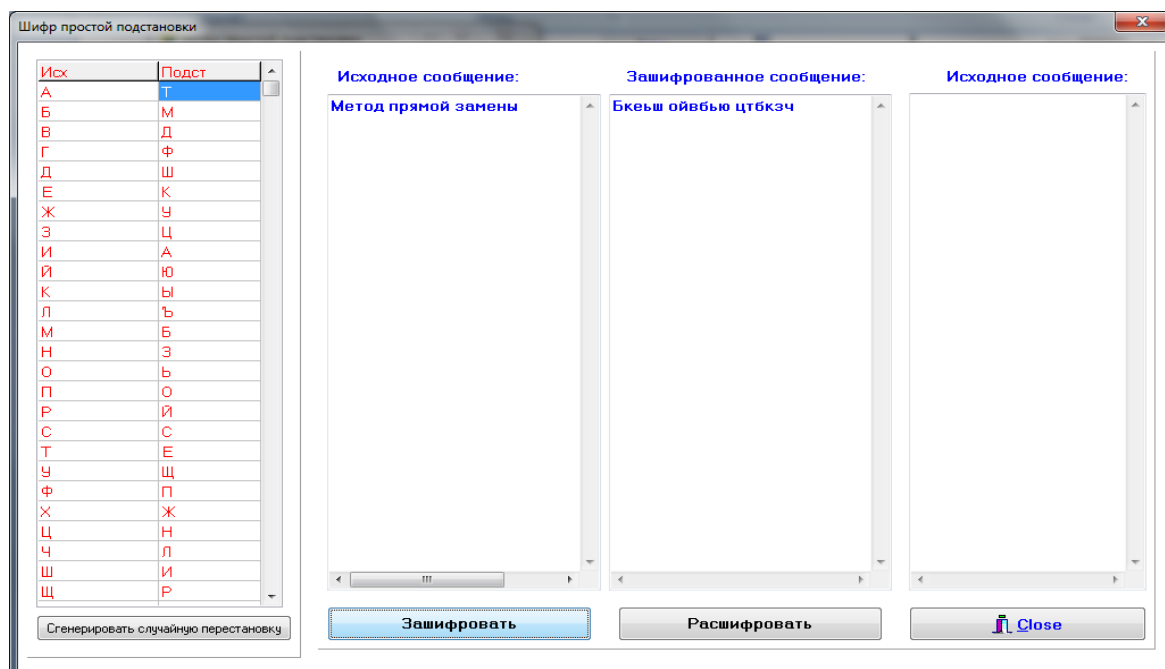


Рисунок 3. Вид зашифрованного текста

При необходимости можно вернуть исходный текст с помощью команды **Исходное сообщение** (рисунок 4).

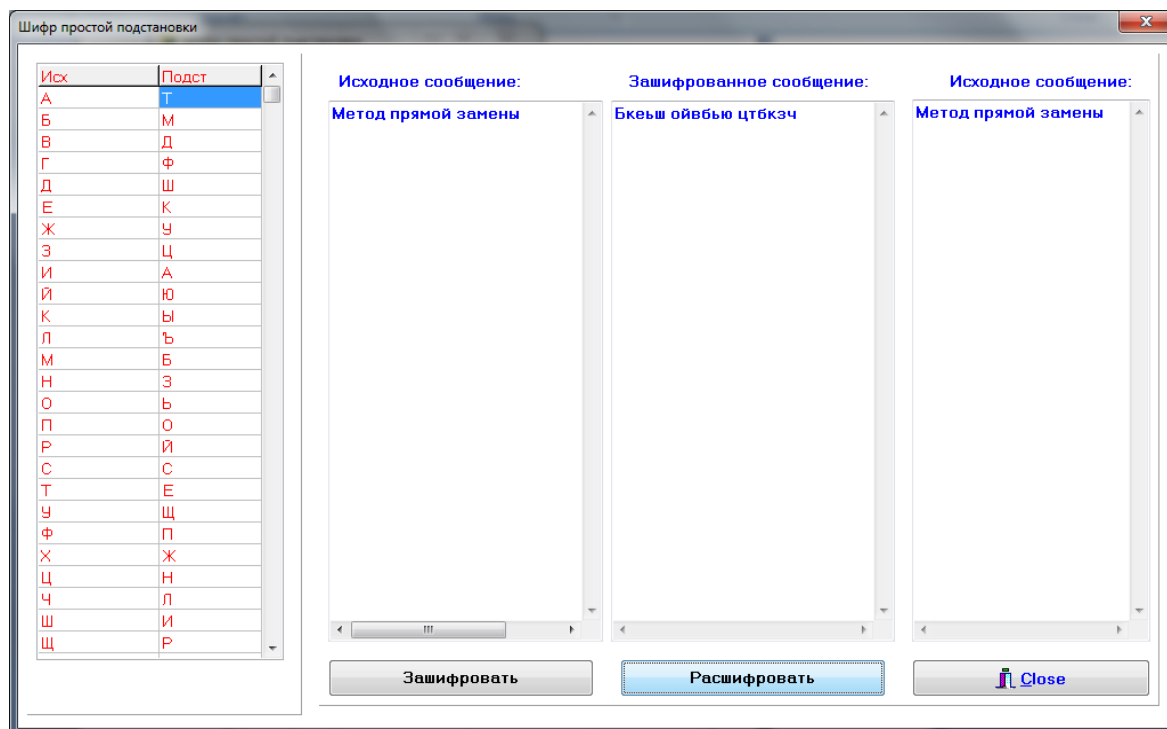


Рисунок 4. Исходный текст

Выйти из программы шифрования можно выбрав команду Close.

Даже простое преобразование информации является весьма эффективным средством, дающим возможность скрыть ее смысл от большинства неквалифицированных нарушителей.

Реализация данного проекта была проведена с помощью мощных средств Borland Delphi 7.0 , что позволило создать программный продукт максимально ориентированный на пользователя.

Литература

1. Шеннон К. Теория связи в секретных системах/Сб.: «Работы по теории информации и кибернетике»- М.: Иностранная литература, 2003-С.333-402.
2. Грушо А.А,Тимонина Е.Е.Теоретические основы защиты информации.- М.:Издательство агенства «Яхтсмен»,1996-71с.
3. Пшенин Е.С. Теоретические основы защиты информации. Еч.пос.Алматы;КазНТУ,2000-452с

Заурбек А., Ахметов Б.С., Джурунтаев Д.З, Сейлова Н.А.

Схема генератора акустического шума для защиты речевой информации от скрытой звукозаписи

Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Алматы, Республика Казахстан

В настоящее время немалую часть передаваемых по техническим каналам связи данных составляет речевая информация. Человеческая речь является универсальным средством общения, обладает уникальными свойствами эффекта присутствия, информационной избыточностью, поэтому широко используется во многих системах связи и передачи информации. Речевая информация может содержать сведения, составляющие конфиденциальную информацию о деятельности предприятия, коммерческую тайну, персональные данные о личной жизни работника государственного сектора, политика, бизнесмена. В этой связи задача защиты речевой информации от утечки по различным каналам занимает одно из ведущих мест в решении общей проблемы информационной безопасности.

Для нелегального съема (прослушивания) речевой информации злоумышленники могут использовать широкий набор технических средств (закладные устройства, диктофоны, магнитофоны, лазерные акустические локационные устройства, направленные микрофоны и т. д.) и с их помощью перехватывать речевую информацию по акустическому, виброакустическому и опто-электронному каналам.

Следует отметить, что при проведении практических работ по защите речевой информации от утечки из помещений по акустическим и виброакустическим каналам не достаточно выполнение только пассивных мер защиты, например: усиление звукоизоляции и виброизоляции конструкций, введение звукопоглощения и вибропоглощения в тракты утечки речевых сигналов, применение обнаружителей диктофонов: металлодетекторов,

нелинейных локаторов и т. д. [1-3]. Кроме того, дорогостоящие предварительные проверки помещений на наличие звукозаписывающих и подслушивающих устройств, оказываются бесполезными, если эти устройства попадают в помещение накануне проведения конфиденциальных переговоров или вносятся непосредственно участниками этих переговоров. В таких случаях для гарантированной защиты целесообразно использование активных мер защиты речевой информации путем создания дополнительных акустических и вибрационных маскирующих помех. При этом для эффективного воздействия помехи на устройство перехвата речевой информации, уровень помехи должен в несколько раз, а иногда и на порядок превосходить уровень речевого (полезного) сигнала в канале передачи. Для того, чтобы устройству перехвата было сложнее отфильтровать помеху, ее спектр должен находиться как можно ближе к речевому спектру (диапазону частот от 300 Гц до 3400 Гц). В результате маскирования речевого сигнала шумовой помехой, «злоумышленники» в своих приемниках (наушниках) слышат вместо полезной речевой информации шумы.

В данной статье рассматривается вопрос защиты речевой информации от скрытой звукозаписи с применением диктофонов. Современные диктофоны (аналоговые или цифровые) не только являются микроминиатюрными по габаритным размерам, но и они позволяют вести запись информации (на микрокассету или флеш-память) больших объемов. Некоторые аналоговые диктофоны позволяют осуществить запись на микрокассету до 6 часов непрерывной работы, другие диктофоны снабжены беззвучным автостопом, системой VOX (автоматического включения записи при появлении акустического сигнала) и системой дистанционного включения/выключения [1,4]. Однако самыми удобными для несанкционированной записи речевой информации являются цифровые диктофоны, которые имеют микроминиатюрные размеры, отличаются высоким

качеством записи (на микрочипы, карты: SmartMedia, MemoryStick и др) и воспроизведения.

Диктофоны бывают встроенными(стационарными) и переносными (носимыми) и их выбор зависит от разных факторов, в частности от условий, при которых приходится вести звукозапись. Встроенные диктофоны должны быть компактными и иметь относительно малые размеры для обеспечения их скрытности. Однако при этом их возможности по времени непрерывной работы для ведения скрытой звукозаписи речевой информации существенно ограничиваются. На практике более широко применяются переносные диктофоны. Переносной диктофон хорошо камуфлируется под любой элемент личных вещей посетителя-«злоумышленника»(в виде пуговицы на костюме или рубашке, колпачка от авторучки и т. д.), поэтому его не сложно пронести в кабинет руководителя организации или помещение, где будут проходить важные деловые переговоры или совещание.

Обнаружение у посетителя руководителя организации или участника совещания диктофона с применением металлодетектора в принципе не представляет особой трудности. Однако проведение такого мероприятия (открытого досмотра лиц и носимых ими предметов: портфеля, кейсов, сумок и т. д.) перед важным совещанием как правило не желательно, так как может вызвать отрицательную реакцию посетителя переговоров или участника совещания. Для контроля за проносом диктофона можно использовать нелинейные локаторы («детекторы нелинейных переходов»), которые позволяют обнаруживать звукозаписывающие устройства на относительно больших расстояниях, чем металлодетекторы при входе в помещение. Однако при этом необходимо учитывать безопасность руководителя организации, в кабинете которого будет находиться и эксплуатироваться нелинейный локатор (с относительно высоким уровнем ВЧ-излучения) в течение относительно длительного времени.

Таким образом, для защиты от скрытой звукозаписи с помощью диктофонов целесообразно применение активных мер защиты речевой информации, т. е. целесообразно использование генераторов акустического шума [1,5-7], которые своими колебаниями маскируют звуковые сигналы. При этом для эффективного маскирования эти колебания (шумовые помехи) должны иметь структуру речевого сообщения, т. е. по своему спектральному составу должны быть близкими звуковому сигналу.

Для маскирования речевых сигналов, т. е. для защиты переговоров от скрытой звукозаписи на диктофон, прослушивания с помощью радиозакладки и перехвата их по оптико-электронному каналу в работе предлагается электрическая схема генератора псевдослучайной последовательности импульсов, которая создает акустическое и виброакустическое зашумление (рисунок 1). В состав генератора псевдослучайной последовательности импульсов входят пятиразрядный последовательный (сдвигающий) регистр на триггерах D-типа, мультивибратор (генератор тактовых импульсов), логические элементы: «исключающее ИЛИ», «И» и «ИЛИ», с помощью которых осуществляется обратная связь, и активный фильтр низких частот второго порядка на операционном усилителе (ОУ). Сигнал обратной связи U одновременно подается на входы сдвигающего регистра и активного фильтра низких частот [8].

Рассмотрим принцип действия схемы генератора акустического шума для защиты речевой информации. 0-ое состояние сдвигающего регистра, когда триггеры всех разрядов находятся в состоянии логического 0 (выходные сигналы триггеров $Q_1 = Q_2 = Q_3 = Q_4 = Q_5 = 0$) является не рабочим. Для исключения 0-ого состояния регистра в схему вводится логический элемент (ЛЭ) «И», на входы которого подаются сигналы с инверсных выходов триггеров всех разрядов регистра.

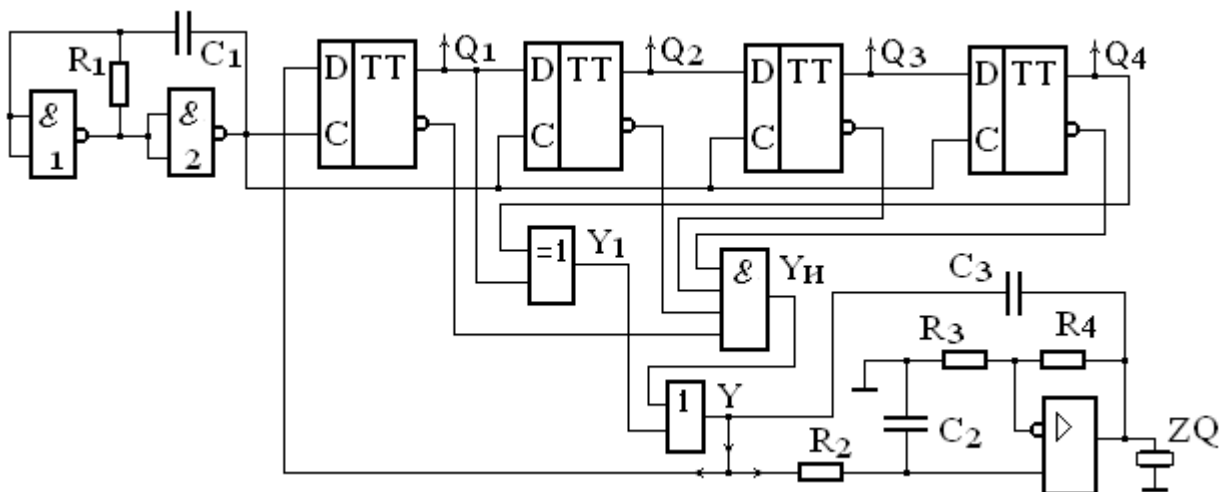


Рисунок 1 – Электрическая схема генератора акустического шума
для защиты речевой информации

При 0-ом состоянии регистра на выходе ЛЭ «исключающее ИЛИ» будет сигнал логического 0 ($Y_1 = 0$), а на выходе ЛЭ «И» - логическая 1 ($Y_{И} = 1$) и этот единичный сигнал через элемент «ИЛИ» по цепи обратной связи ($Y = 1$) поступает на вход сдвигающего регистра. Следует отметить, что сигнал логической 1 на выходе ЛЭ «И» ($Y_{И} = 1$) будет только при 0-ом состоянии регистра, а в остальных случаях сигнал $Y_{И} = 0$.

После поступления первого тактового импульса мультивибратора сигнал $Y = 1$ с выхода генератора записывается в триггер первого разряда регистра и одновременно с этим содержимое регистра сдвигается на один разряд вправо. При этом в регистре будет число 1 ($Q_1 = 1, Q_2 = Q_3 = Q_4 = Q_5 = 0$), а сигнал обратной связи Y (он же является выходным сигналом логического элемента «ИЛИ» и генератора псевдослучайной последовательности импульсов) будет равен логическому 0, так как $Y = Y_1 + Y_{И} = 0 + 0 = 0$. Поэтому после подачи второго тактового импульса в триггер первого разряда записывается сигнал логического 0, а содержимое регистра вновь сдвигается вправо на один разряд и в регистре будет число 2 ($Q_1 = 0, Q_2 = 1, Q_3 = Q_4 = Q_5 = 0$). Сигнал обратной связи Y будет равен 1 ($Y = 1$). Этот 1-чный сигнал записывается в триггер первого разряда после подачи 3-го тактового импульса и после сдвига содержимого регистра в нем будет число 5. Далее после подачи последующих

тактовых импульсов мультивибратора состояние разрядных триггеров и содержимое регистра (число в регистре) будут меняться в соответствии с таблицей состояний 1 генератора псевдослучайной последовательности импульсов. Как видно из таблицы состояний 1 после 31-го тактового импульса мультивибратора в регистре будет число 16 ($Q_1 = Q_2 = Q_3 = Q_4 = 0, Q_5 = 1$), а сигнал $Y = 1$, поэтому 32-й тактовый импульс возвращает регистр (генератор) в начальное состояние, соответствующее числу 1 ($Q_1 = 1, Q_2 = Q_3 = Q_4 = Q_5 = 0$), $Y = 1$. Состояние регистра, когда все триггеры находятся в состоянии логического 0 ($Q_1 = Q_2 = Q_3 = Q_4 = Q_5 = 0$), как отмечено выше, исключается как нерабочее. Далее генератор будет генерировать псевдослучайные импульсы с длиной (периодом повторения), равным 31 в той же последовательности, как указано в таблице состояний 1.

В общем случае при n -разрядном сдвигающем регистре можно генерировать m - кодовые последовательности псевдослучайных импульсов, где $m = 2^n - 1$. Псевдослучайная последовательность кодов чисел(импульсов) отличается от истинно случайной периодичностью, хотя внутри периода ничем не отличается от истинно случайной. Последовательность 1011010110010001111101011001000, соответствующую $m = 2^n - 1$ можно снять с выхода триггера любого разряда сдвигающего регистра, так как та же самая последовательность поступает с временным сдвигом с выхода триггера каждого разряда. При относительно большом значении n псевдослучайная последовательность практически не отличается от случайной последовательности.

Акустический шум, создаваемый генератором псевдослучайной последовательности импульсов обеспечивает также защиту от прослушивания (с помощью закладных устройств) переговоров в кабинете руководителя организации или переговоров, проводимых в специально выделенных для этой цели помещениях. Для создания акустического шума к выходу генератора псевдослучайной последовательности импульсов подключается активный

фильтр низких частот (ФНЧ) второго порядка на основе операционного усилителя, нагрузкой которого является пьезокерамический преобразователь ZQ (рисунок 1).

Таблица 1 - Таблица пятиразрядного генератора псевдослучайной последовательности импульсов

№ тактовых импульсов		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Число в Рг Вых. сигналы	0	1	2	5	10	21	11	23	14	29	27	22	12	24	17	3
Q ₁	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1
Q ₂	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1
Q ₃	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0
Q ₄	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0
Q ₅	0	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0
Y	1	0	1	1	0	1	0	1	1	0	0	1	0	0	0	1
Q ₁	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0
Q ₂	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0
Q ₃	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0
Q ₄	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0
Q ₅	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1
Y	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1

Операционный усилитель включен по схеме неинвертирующего усилителя (повторителя). Активный ФНЧ, частота среза которого мала по сравнению с частотой тактовых импульсов мультивибратора, осуществляет преобразование цифрового шума (псевдослучайной последовательности импульсов) в аналоговый. Цифровой шум представляет собой временной случайный процесс, близкий по своим свойствам к процессу физических шумов и поэтому называется «псевдослучайным процессом». Схема активного ФНЧ второго порядка, называемая также схемой Саллена-Ки (рисунок 1) позволяет реализовать большую крутизну спада амплитудно-частотной характеристики по сравнению со схемой активного ФНЧ первого порядка [6,8]

Следует отметить, что акустическое зашумление помещения обеспечивает эффективную защиту информации в нем, если акустический

генератор расположен к акустическому приемнику злоумышленника ближе, чем источник информации. Например, когда подслушивание возможно через дверь или, когда перехват речевой информации осуществляется через оконное стекло с помощью лазерного устройства, то акустический генератор целесообразно прикрепить к двери или разместить на подоконнике, вблизи от зашумляемого оконного стекла. Если местонахождение акустического приемника злоумышленника (например, закладного устройства) неизвестно, то размещение акустического генератора между говорящими людьми не гарантирует надежную защиту информации. Кроме того, повышение уровня шума вынуждает собеседников к более громкой речи, что создает дискомфорт и снижает эффект от зашумления. Оптимизация режима работы генератора акустического зашумления позволит снизить уровень шумов и обеспечить большую комфортность ведения разговоров в защищаемом помещении.

При использовании лазерного устройства в направлении источника звука (кабинета руководителя организации или комнаты, где ведутся важные переговоры конфиденциального характера) посылается зондирующий луч. Возникающие при разговоре акустические волны, распространяясь в воздушной среде, воздействуют на оконное стекло и вызывают его колебания в диапазоне частот, соответствующих речевому сообщению. Оконное стекло вибрирует под действием окружающих звуков и модулирует своими колебаниями лазерный луч. Таким образом, лазерное излучение, падающее на внешнюю поверхность оконного стекла, в результате виброакустического преобразования речевого сообщения оказывается промодулированным сигналом. Отраженный модулированный сигнал принимается оптическим приемником лазерного устройства, в котором осуществляется восстановление речевой информации из кабинета руководителя организации.

Предложенную в работе схему генератора псевдослучайной последовательности импульсов можно использовать также для защиты речевой информации от прослушивания лазерным микрофоном. Пьезокерамический

вибратор генератора псевдослучайной последовательности импульсов, прикрепляемый (приклеиваемый) к поверхности оконного стекла, вызывает его колебание по случайному закону с амплитудой, превышающей амплитуду колебаний стекла от акустической волны речевого сигнала. При этом на приемной стороне возникают трудности в детектировании речевого сигнала.

Данная работа относится к области обеспечения информационной безопасности переговоров в кабинете руководителя организации или служебном помещении, выделенном для этой цели, с помощью акустического зашумления на частотах звуковых сигналов и может быть использовано в системах защиты конфиденциальной речевой информации.

Следует отметить также, что генераторы псевдослучайных последовательностей импульсов на сдвигающих регистрах с обратными связями можно использовать для защиты телефонных разговоров, а также в криптографии для создания алгоритмов поточного шифрования [2,7]. Вместе с тем следует отметить, что программная реализация алгоритмов функционирования генераторов псевдослучайных последовательностей импульсов на базе линейных сдвиговых регистров представляет собой достаточно сложную задачу.

ЛИТЕРАТУРА

1. Андрианов В. И., Соколов А.В. Шпионские штучки. Устройства для защиты объектов и информации: справ.пособие. – СПб.: Лань, 1996. - 254 с.
2. Хорев А.А. Техническая защита информации. Т.1:Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.
3. Герасименко В.Г., Лаврухин Ю.Н.,Тупота В.И. Методы защиты акустической речевой информации от утечки по техническим каналам. – М.: РЦИБ «Факел», 2008. – 258 с.
4. Дворянкин С.В., Мишуков А.А. Маскирование речевой информации: Перспективные методы и средства. – М.: журнал «Спецтехника и связь», №3, 2009. – С. 46-51.

5. Горбатов В.С. Контроль защищенности речевой информации в помещениях. – М.: НИЯУ МИФИ, 2014. – 248 с.
6. Горшков Ю.Г. Анализ и маскирование речи. Учебное пособие. – М.: МГТУ им. Н.Э. Баумана, 2006. – 58 с.
7. Адамян А. Защита речевой информации руководителя организации от скрытой записи посетителем. <http://daily.sec.ru>, 17.08.2007.
8. Джурунтаев Д.З. Схемотехника. Учебник. – Алматы: Эверо, 2005. – 276 с.

Золотарев В.В., Овечкин Г.В., Ташатов Н.Н.

**ПРИМЕНЕНИЕ ПРИНЦИПА ДИВЕРГЕНЦИИ
ПРИ ДЕКОДИРОВАНИИ СВЁРТОЧНЫХ КОДОВ**

Институт космических исследований РАН, Москва, РФ

Рязанский государственный радиотехнический университет, Рязань, РФ

Евразийский национальный университет, Астана, РК

Помехоустойчивое кодирование стало неотъемлемой частью современных систем передачи и хранения информации. Это стало возможным благодаря существенным прорывам, достигнутым теорией кодирования за последние годы. Представленные в [1] основные достижения оптимизационной теории кодирования свидетельствуют о том, что построенные на новых постулатах этой теории многопороговые декодеры (МПД) к настоящему моменту достигли уже весьма высокого уровня эффективности при умеренной сложности. В гауссовских каналах эти алгоритмы работают с вероятностью ошибки на бит $P_b(e) < 10^{-5}$ при уровне битовой энергетике $E_b/N_0 \sim 1,3$ дБ. Организовать столь же эффективную работу декодеров низкоплотностных (LDPC) кодов, при таком уровне шума уже весьма сложно, а для высокоскоростных каналах и невозможно.

С другой стороны, возможность реализации декодеров МПД на основе технических решений [2] позволяет сохранять хорошие энергетические характеристики декодирования на высокие скорости передачи канала, в том числе выше, чем 1 Гбит/с [3, 4]. К тому же ресурсы улучшения характеристик для МПД алгоритмов ещё не полностью исчерпаны, что позволяет и в дальнейшем ожидать от них дальнейшего улучшения эффективности работы при больших уровнях шума. Представленные в [5, 6] результаты исследований показывают, что символьные многопороговые декодеры (QMПД) существенно перекрывают по своей эффективности коды Рида-Соломона и практически реализуемые QLDPC коды, оставаясь столь же простыми в реализации, как и их прототипы – двоичные МПД.

Главная причина столь высокой степени преимущества МПД декодеров всегда заключается в том, что и для весьма высоких уровней шума канала они обеспечивают такое же декодирование, как и оптимальные переборные методы, но при линейной сложности. Для многих сочетаний характеристик кодов и каналов эффективность МПД разных модификаций при малой энергетике канала столь значительна, что других методов, которые работоспособны в этих условиях, вообще назвать нельзя. Таким образом, преодолев уровень эффективности реальных декодеров LDPC кодов, алгоритмы МПД фактически заявили о своём первенстве по эффективности и сложности реализации вообще для всех значимых приложений в системах передачи, хранения, контроля и восстановления цифровых данных.

Однако в настоящее время недостаточно применения в декодерах итеративного типа только простых средств обработки цифровых потоков на базе мажоритарной логики. Использование только мажоритарной логики, видимо, не даст существенно приблизиться к пропускной способности канала. В настоящей работе предлагаются новые направления развития итеративных алгоритмов, которые могут помочь значительно приблизить допустимые уровни кодовых скоростей к пропускной способности каналов.

Рассмотрим схему простого свёрточного кодирования с кодовой скоростью $R=1/2$, представленную на рис. 1. Она состоит из регистра сдвига, в левой части которого сгруппированы ячейки, с выходов которых поступают значения их содержимого на входы полусумматора (mod 2 сумматор), с выхода которого проверочные символы кода отправляются в канал. Для упрощения описания будем полагать код систематическим. Поэтому вместе с проверочным символом кода в канал на каждом такте работы кодера уходит и один информационный символ из нулевой ячейки регистра сдвига.

Принципиальным моментом для описания работы данного кодера является наличие далеко в правой части кодирующего регистра ещё одной ячейки, содержимое которой также поступает на вход полусумматора, с которого данные уходят в канал.

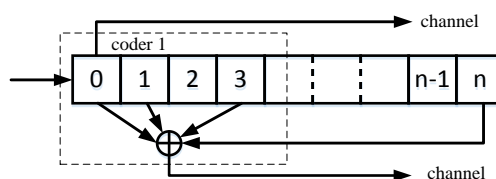


Рисунок 1 – Кодер дивергентного кода

На рис. 2 показан декодер свёрточного кода, соответствующий кодеру, представленному на рис. 1. Он построен по идеям МПД и содержит 2 пороговых элемента (ПЭ), находящихся в левой и правой частях декодера. Левый ПЭ (ПЭ 1) и соответствующие части информационного и синдромного регистров, с которыми он взаимодействует, выделены пунктирным квадратом и названы Decoder1 (D1).

Полный декодер со вторым пороговым элементом (ПЭ 2) в правой части регистров декодеров подобен D1. Но на вход ПЭ 2 поступает ещё и

дополнительная проверка кода, которая появляется в декодере намного позже символов компактной группы проверок, связанных с первым ПЭ1.

При работе в канале первый ПЭ1 принимает решения об информационных ошибках на основании только своей группы проверок. Если шум канала и код выбраны правильно, то после первого ПЭ 1 плотность таких ошибок будет меньше, чем до этого порога, а достигнув второго ПЭ 2, эти ошибки согласно принципам работы МПД будут подчищены. А поскольку на входы ПЭ 2 поступает на одну большее число проверок, чем в ПЭ 1, то и корректирующие возможности второго ПЭ 2 будут более высокими, что позволит усилить процесс коррекции, так как второй ПЭ 2 работает с кодом, у которого минимальное расстояние d как бы выросло на единичку по сравнению с первым ПЭ 1. Важно, что этого удалось добиться без привлечения методов каскадирования, которые отнимают избыточность у первого кода (и первого ПЭ 1), что заметно уменьшает корректирующие возможности первого декодера.

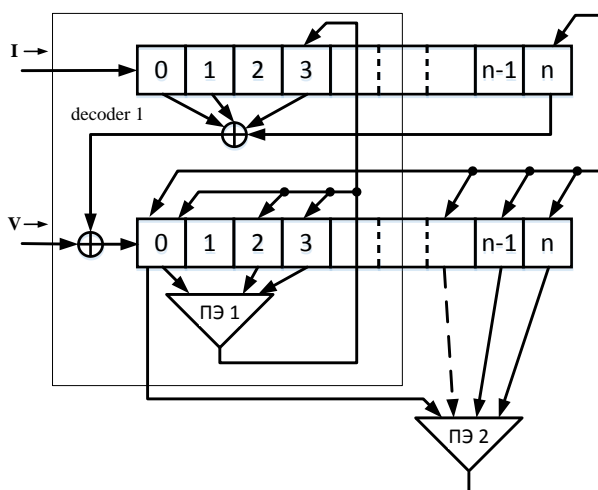


Рисунок 2 – Декодер дивергентного кода

Очевидно, что предложенный код сам может быть первой частью ещё более длинного кода с подобной же структурой. Тогда на двух таких условных

"каскадах" кодирования/декодирования минимальное расстояние d уже будет увеличено на 2 и т.д.

Получившаяся схема декодирования стала намного более сложной, так как эффект роста кодового расстояния, крайне ценного ресурса, не может быть получен просто так. Первый декодер на рис. 2 часть ошибок, которые он не исправил, пропускает направо ко второму ПЭ2. И тогда с ячейки n через два полусумматора эти ошибки попадают в синдромный регистр. Значит, первый ПЭ1 работает при немного возросшем уровне шума, что ухудшает его характеристики. Но если ПЭ1 справляется с этим возросшим потоком ошибок и ухудшает свои характеристики немного, а второй ПЭ2 помогает первому, то можно ожидать, что вместе они справятся с таким более сложным потоком ошибок, что и позволяет продолжить анализ этой схемы для определения её возможностей при высоком уровне шума.

Рассмотрим характеристики такой дивергентной схемы (с растущими, "расходящимися" значениями d), представленные на рис. 3. На нём также представлены приближённые зависимости вероятности ошибки декодеров $P_b(e)$ от уровня шума канала для алгоритма Витерби (VA) и для МПД декодеров с кодами, имеющими некоторое кодовое расстояние d и $d+1$. Характеристики имеют типичные изгибы, которые находятся в точках, где вероятности ошибки МПД при уменьшении уровня шума (вправо) достигают оптимальных минимальных значений для используемых кодов. Левее точек перегибов алгоритмы уже не могут работать из-за высокого шума канала. Рисунок демонстрирует принцип дивергентного кодирования, при котором МПД, работающий в такой схеме с кодом, имеющим расстояние $d+1$ обеспечивает декодирование при уровне шума $\sim 1,7$ дБ, хотя сам МПД работает в обычном режиме только при уровне шума порядка 1,8 дБ.

Характеристики МПД с кодом, имеющим минимальное расстояние d , близки к оптимальным до энергетики 1,6 дБ. Установим уровень шума для него 1,7 дБ. Это точка 1 на диаграмме. Теперь подключим в кодере и декодере

дополнительную далёкую проверку, влияние которой мы обсуждали по рис. 1 и 2. Если дополнительный шум от этой проверки невелик и может быть выражен как увеличение шума канала примерно на 0,1 дБ, с которым первый МПД с кодом, имеющим расстояние d , ещё справляется, то характеристики этого МПД сместятся из точки 1 в точку 2 и пока останутся оптимальными. Но тогда во второй декодер с ПЭ2 действительно попадает поток информационных ошибок из первого декодера с гораздо меньшей плотностью, чем вероятность ошибок в канале. А это и создаёт условия, при которых второй ПЭ2 действительно тоже дополнительно снизит плотность ошибок, пришедших к нему от первого ПЭ1 (точка 3). Но это произойдёт уже при уровне шума, примерно на 0,1 дБ большем, чем тот, при котором ПЭ2 мог работать без поддержки ПЭ1. Разумеется, применяя этот принцип несколько раз, можно значительно продвинуться в область более высоких шумов канала.

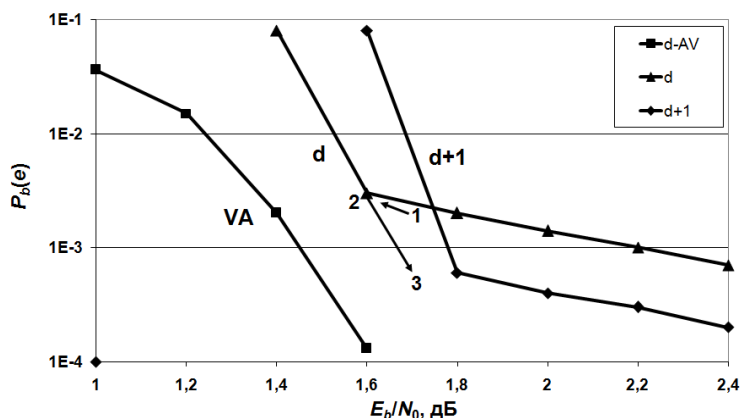


Рисунок 3 – Характеристики дивергентного кода

Обращаясь далее к графику для АВ, который приведён на рис. 3, можно заметить, что он не имеет таких перегибов, как кривые для МПД. Кроме того, обычно графики для длинных, но ещё реализуемых в плане сложности декодеров АВ лежат левее графиков для МПД, как это и показано на рис. 2. Это значит, что если вместо первого ПЭ1 поставить достаточно эффективный декодер АВ, то применение принципа дивергенции может быть ещё более эффективным.

Разнообразные сопоставления эффективности многих алгоритмов декодирования показали также, что единственной группой методов, которые измеряют расстояние своих решений до принятого сообщения, являются МПД, QМПД (декодеры символьных кодов) и алгоритм Витерби. В работе показано, что они успешно применяются совместно, в том числе для дивергентного кодирования.

Литература

1. В.В. Золотарёв, Ю.Б. Зубарев, Г.В. Овечкин. Многопороговые декодеры и оптимизационная теория кодирования. // Под редакцией академика РАН В.К. Левина. М., «Горячая линия – Телеком», 2012, 238 с.

2. Патент РФ №2377722.

3. Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В. Высокоскоростной многопороговый декодер для систем передачи больших объемов данных // Научно-технический сборник «Техника средств связи», серия «Техника телевидения», юбилейный выпуск, МНИТИ, 2010, с.41–43.

4. В.В. Золотарёв. Г.В. Овечкин. Применение многопороговых методов декодирования помехоустойчивых кодов в высокоскоростных системах передачи данных // "Электросвязь, М., 2014, №12, с.10-14.

5. Zolotarev V.V., Averin S.V. Non-Binary Multithreshold Decoders with Almost Optimal Performance. 9-th ISCTA' 07, July, UK, Ambleside, 2007.

6. Ovechkin G.V., Zolotarev V.V. Non-binary multithreshold decoders of symbolic self-orthogonal codes for q-ary symmetric channels – 11-th ISCTA'09, July, UK, Ambleside, 2009.

Ибраев Н.С.

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФАКТОР УСПЕШНОГО
ПЛАНИРОВАНИЯ ВОЕННЫХ (СПЕЦИАЛЬНЫХ) МЕРОПРИЯТИЙ**

КОЛЛЕКТИВНЫХ СИЛ ОПЕРАТИВНОГО РЕАГИРОВАНИЯ ОРГАНИЗАЦИИ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ

Национальный университет обороны имени Первого Президента Республики
Казахстан – Лидера нации, г. Астана, Республика Казахстан

В статье рассматриваются вопросы обеспечения информационной безопасности в ходе планирования военных (специальных) мероприятий (действий) коллективных сил оперативного реагирования Организации Договора о коллективной безопасности.

Ключевые слова: информационная безопасность, планирование военных (специальных) действий, коллективные силы оперативного реагирования (далее КСОР), Организация Договора о коллективной безопасности (далее ОДКБ).

Концепция информационной безопасности Республики Казахстан до 2016 года (далее – Концепция) выражает совокупность официальных взглядов на сущность и содержание деятельности Республики Казахстан по обеспечению информационной безопасности государства и общества, их защите от внутренних и внешних угроз. Концепция определяет задачи, приоритеты, направления и ожидаемые результаты в области обеспечения информационной безопасности личности, общества и государства. Она является основой для конструктивного взаимодействия органов государственной власти, бизнеса и общественных объединений для защиты национальных интересов Республики Казахстан в информационной сфере [1].

Концепция является критически важным нормативно-правовым актом, которая определяет перспективы деятельности Вооруженных Сил Республики Казахстан (далее – ВС РК) в информационной сфере.

В Законе Республики Казахстан (п.4. статья 18.) говорится:

4. Часть состава Вооруженных Сил может входить в объединенные вооруженные силы или находится под объединенным командованием в

соответствии с международными договорами, ратифицированными Республикой Казахстан [2].

В декабре 2008 года в Казахстане на неформальном саммите ОДКБ главами государств-членов Организации принято Решение о формировании в рамках ОДКБ группировки сил быстрого реагирования.

4 февраля 2009 года в Москве на внеочередной сессии Совета коллективной безопасности ОДКБ (далее – СКБ) президентами государств-членов ОДКБ подписано Решение «О Коллективных силах оперативного реагирования Организации Договора о коллективной безопасности» по итогам которого воинские контингенты от ВС РК вошли в состав КСОР.

Коллективные силы оперативного реагирования ОДКБ предназначены для оперативного реагирования на вызовы и угрозы безопасности государств-членов ОДКБ.

К основным задачам КСОР, относятся [3]:

развертывание на территории любой из Сторон с целью демонстрации готовности к применению военной силы;

- участие в предотвращении и отражении вооруженного нападения, в том числе агрессии, локализации вооруженных конфликтов;

- участие в мероприятиях по борьбе с международным терроризмом, незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров, оружия и боеприпасов, другими видами транснациональной организованной преступности;

- участие в выполнении мероприятий по защите населения от опасностей, возникающих при ведении или вследствие военных действий, а также ликвидации чрезвычайных ситуаций и оказании чрезвычайной гуманитарной помощи.

Состав КСОР включает два компонента: воинские контингенты; формирования сил специального назначения (далее – формирования сил СпН).

Планирование оперативного развертывания КСОР на территориях Сторон заблаговременно осуществляется Объединенным штабом ОДКБ (далее – ОШ ОДКБ) во взаимодействии с заинтересованными министерствами и ведомствами. В структуре ОШ ОДКБ предусмотрено создание и функционирование в мирное время Оперативного центра КСОР ОДКБ.

Немаловажным фактором является слаженность органов управления и контингентов КСОР при ведении ими совместных действий. В этой связи особое внимание уделяется подготовке и проведению совместных мероприятий оперативной и боевой подготовки контингентов КСОР.

Применение КСОР осуществляется в форме совместной операции, при этом подготовка и определение способов ее проведения осуществляется Командующим КСОР во взаимодействии с заинтересованными министерствами и ведомствами. Для управления контингентами КСОР при подготовке и проведении операций создается Командование КСОР. Штаб является основным органом управления контингентами КСОР при выполнении им поставленных задач. Свою работу Штаб осуществляет на основе решений, приказов, директив и указаний Командующего.

Мероприятия по планированию применения КСОР являются важной частью заблаговременной и непосредственной подготовки военных (специальных) действий.

Военные (специальные) действия воинских контингентов и формирований сил СпН КСОР будут характеризоваться возросшим размахом, интенсивностью, применения их как самостоятельно, так и в составе международных, коалиционных группировках войск и сил. С применением разнообразной сложной боевой техники, высокой динамичностью и маневренностью действий, ведением их в условиях отсутствия сплошного фронта, дистанционного поражения, быстрых изменений обстановки, ожесточенной борьбой за захват и удержание инициативы, сильного радиоэлектронного и **информационного противодействия**.

В этих условиях, процесс планирования применения КСОР значительно усложнится и будет все больше приобретать характер реализации заранее разработанных вариантов решений, программирования и моделирования предстоящих военных (специальных) действий КСОР. Высокий уровень планирования операций (специальных операций, действий) станет главной предпосылкой эффективного управления воинскими контингентами и формированиями сил СпН КСОР. **Информационная безопасность** как составная и неотъемлемая часть при планировании применения КСОР в военных (специальных) действиях становится одним из ключевых **факторов** успешного выполнения поставленных задач. **Целью информационной безопасности на этапе планирования**, вероятно, будет являться создание системы обеспечения информационной безопасности, гарантирующей защиту деятельности органов управления, воинских контингентов и формирований сил СпН КСОР в информационной сфере.

Таким образом, при обеспечении информационной безопасности в ходе планирования применения воинских контингентов и формирований сил СпН КСОР в совместных операциях (специальных операциях, действиях) целесообразно решение некоторых задач:

1) развитие (создание) системы управления информационной безопасностью, позволяющей обеспечить защищенность информационной инфраструктуры КСОР и единого информационного пространства в ходе выполнения задач;

2) разработка и реализация единой технической политики в сфере обеспечения информационной безопасности, в т.ч. развитие и укрепление системы защиты информации;

3) защита прав военнослужащих, сотрудников правоохранительных органов, органов безопасности и других компетентных органов из состава КСОР ОДКБ в информационной сфере;

4) развитие информационного пространства на национальных территориях государств-участников КСОР ОДКБ;

5) внесение необходимых изменений в нормативную правовую базу, регламентирующую деятельность Объединенного штаба ОДКБ и сил, и средств системы коллективной безопасности в информационной сфере.

СПИСОК ЛИТЕРАТУРЫ

1 Концепция информационной безопасности Республики Казахстан до 2016 года, утверждена Указом Президента Республики Казахстан от 14 ноября 2011 года № 174. Астана, 2011 г.

2 Закон Республики Казахстан «Об обороне и Вооруженных Силах Республики Казахстан» *(с изменениями и дополнениями по состоянию на 03.07.2013 г.)*

3 Коллективные силы оперативного реагирования Организации Договора о коллективной безопасности / Пресс-служба Секретариата ОДКБ, www.dkb.gov.ru, e.mail: odkb@gov.ru

Исмоилов Д.

ОБ ОДНОМ ПРИМЕНЕНИИ АРИФМЕТИКИ В КРИПТОГРАФИИ

Инновационный Евразийский Университет

г. Павлодар, Республика Казахстан

В настоящем сообщении исследуется одна задача, связанная с теорией вероятностей, а именно, с «выборкой» последовательностей (символов) с последующим применением в криптографии (теории кодирования).

Пусть

$$(1) \quad \{x_0, x_1, \dots, x_{g-1}\}; \quad g > 1$$

некоторая последовательность символов или чисел. Каждому элементу этой последовательности ставим в соответствие его индекс, т.е.: $x_j \Leftrightarrow j$, тогда получим следующее взаимно однозначное соответствие:

$$(2) \quad \{x_0, x_1, \dots, x_{g-1}\} \Leftrightarrow \{0, 1, \dots, g-1\}$$

Далее, будем рассматривать расположения элементов x_j друг за другом (кортеж) из n наборов $1 < n < g-1$. В результате образуется множество n -значных кортежей, которое в дальнейшем обозначим через множество

$$(3) \quad S(g; n) = \{s = x_j x_k \dots x_n\},$$

где индексы независимо друг от друга пробегают целые неотрицательные числа из множества $\{0, 1, 2, \dots, g-1\}$, индексы могут быть и равными друг другу, т.е. элементы могут повторяться.

В заданном кортеже будем считать: **позиция элемента x_j чётная или нечётная в зависимости от чётности или нечётности его индекса.** Разобьем множество $S(g; n)$ на три подмножества, которые будем называть соответственно: **чётные**, **нечётные** и **смешанные**. Любой набор (кортеж) из n -значных чисел будем называть **чётным** или **нечётным**, если все члены данного набора состоят соответственно только из **чётных** или **нечётных** элементов. Например, кортеж $a = x_2 x_2 x_4 \dots x_0 x_{2k}$ является чётным, а кортеж $b = x_1 x_5 x_7 \dots x_3 x_{2k+1}$ является нечётным. Кортеж называем **смешанным**, если хотя бы два элемента в данном кортеже имеют позиции разных чётностей. Например, $c = x_1 x_2 \dots x_{2k} x_{2k+1}$. В результате получим три непересекающихся подмножества: $S_1(g; n)$, $S_2(g; n)$, $S_3(g; n)$. При этом имеем формулы:

$$(4) \quad S_n(g) = S_1(g; n) \cup S_2(g; n) \cup S_3(g; n); \quad \emptyset = S_1(g; n) \cap S_2(g; n) \cap S_3(g; n).$$

Заметим, что любой элемент из последовательности (1), в частности, из $\{0, 1, \dots, g-1\}$ считается однозначным и будет в зависимости от номера индекса элемента чётным или нечётным. В этом случае смешанные кортежи отсутствуют, а их множество считается пустым. Следовательно, смешанные кортежи существуют в случаях $n \geq 2$.

Как известно из теории делимости целых чисел [1], всякое множество целых чисел, состоящее из g элементов, попарно несравнимых по модулю g , называется полной системой вычетов по модулю g , а последовательность $\{0, 1, \dots, g-1\}$ называется наименьшими неотрицательными вычетами по модулю g . На основании формулы Евклида (деление с остатком), каждое целое число a представляется однозначно в «многочленном» виде

$$(5) \quad a = a_k g^k + a_{k-1} g^{k-1} + \dots + a_1 g + a_g = \overline{a_k a_{k-1} \dots a_1 a_g};$$

где $1 \leq a_k < g$, $0 \leq a_j < g$, $j = g, 1, 2, \dots, k-1$; a_g – выражает остаток при делении числа a на g , т.е. $a = bg + a_g$; $0 \leq a_g \leq g-1$. Представление (5) называют также систематическое представление числа a по основанию g . На практике часто (в криптографии, теории кодирования, нумерологии и др.) пользуются некоторыми образованиями (кортежами), состоящих из слов, символов, а также из кортежа многозначных чисел, расположенных друг за другом. В наших рассуждениях мы будем исследовать случай, когда основание числа a в представлении (5) равно $g=10$. Тогда будем иметь в качестве основного множества $\{x_0, x_1, \dots, x_{g-1}\}$; $g > 1$ множество целых чисел, состоящее из полной системы вычетов по модулю 10, т.е. $\{0, 1, 2, \dots, 9\}$, и на их основе будем рассматривать всевозможные n -значные числа вида (3).

Следовательно, имеем следующие однозначные базовые множества:

$$(6) \quad S_1(10;1) = \{1, 3, 5, 7, 9\}; S_2(10;1) = \{0, 2, 4, 6, 8\}.$$

Далее все n -значные числа вида (3) формируются на базе элементов двух базовых множеств: $S_1(10;1) = \{1, 3, 5, 7, 9\}$; $S_2(10;1) = \{0, 2, 4, 6, 8\}$, где число элементов в каждом из них поровну, т.е. по 5, а число смешанных элементов равно нулю.

Примеры: $a = 1357591$ – нечётный семизначный кортеж, составленный из нечётных чисел, принадлежащих множеству $S_1(10;1)$, $b = 2064248$ – чётный семизначный кортеж, составленный из чётных чисел множества $S_2(10;1)$ и $c = 1054749$ – смешанный семизначный кортеж, составленный из элементов обоих множеств.

Далее исследуем вероятностный смысл каждого подмножества по отношению к множеству n -значных чисел для любого натурального числа $n \geq 2$. и базовых однозначных подмножеств $S_1(10;1), S_2(10;1)$.

Сформулируем общую задачу в общепринятом виде.

В ящике (урне) имеются шары трёх видов, пронумерованные n -значными числами из множества $S_1(10;1); S_2(10;1)$. Другими словами, в урне имеются шары, пронумерованные n -значными числами, имеющими только нечётные, чётные и смешанные цифры.

1. Найти общее количество всех n -значных чисел, определить из них количество с нечётными, чётными и смешанными цифрами кортежей.

2. При извлечении случайным образом одного шара из ящика, найти вероятность $p_i = P\{X = N_i(n)\}$ появления каждого n -значного числа.

3. Построить закон распределения дискретной случайной величины $X(n) = \{N_1(n), N_2(n), N_3(n)\}$; где $N_1(n), N_2(n), N_3(n)$ - количество элементов в каждом подмножестве, а также числовые характеристики случайной величины $X(n)$: математическое ожидание, дисперсия и стандарт.

Решение. Для полноты изложения сначала исследуем случай $n = 2$. Имеем:

$$S_1(10;2) = \{11, 13, 15, 17, 19; \dots; 91, 93; \dots; 99\} \Rightarrow N_1(2) = 25,$$

$$S_2(10;2) = \{20, 22, 24, 26, 28; \dots; 80, 82; 84; 86; 88\} \Rightarrow N_2(2) = 20.$$

Общее количество двузначных чисел равно $99 - 9 = 90$. Следовательно, число смешанных двузначных чисел равно $90 - 45 = 45$, т.е. $N_3 = 45$. Следовательно, в нашем случае мы получаем случайную величину с соответствующими вероятностями: $X(2) = \{N_1(2), N_2(2), N_3(2)\}$; $p_1 = 25/90$; $p_2 = 20/90$; $p_3 = 45/90$;

Таким образом, в этом случае закон распределения случайной величины $X(2)$ и таблица распределения будет выглядеть так:

$X(2)$	$N_1(2)$	$N_2(2)$	$N_3(2)$
$P(2)$	25/90	20/90	45/90

Основные числовые характеристики находятся по известным формулам

(например, см.[2]): $MX(2) = \sum_{i=1}^3 p_i \cdot N_i(2) \approx 33,89$, $D_{X(n)} = M[X^2(2)] - [MX(2)]^2 \approx$
 $\approx 126,268$; $\sigma_{X(n)} = \sqrt{D_{X(n)}} \approx 11,237$. Аналогично рассматривается случаи $n \geq 3$.

Решение задачи в общем случае. Для случаев $n \geq 2$ основное множество $S(10;n)$ распадается на три подмножества n -значных чисел: $S_1(10;n)$, $S_2(10;n)$, $S_3(10;n)$ при этом условимся, что все чётные кортежи, для которых число ноль находится спереди, учитывается только в одном единственном случае, когда рассматриваются однозначные кортежи. В остальных случаях все числа, представленные в кортеже должны быть n -значными в соответствии с формулой (5) т.е. старший коэффициент разложения a_k должен быть отличным от нуля. Пусть $n > 2$, тогда общее количество всех n -значных чисел вычисляется по формуле $N(n) = 10^n - 1 - (10^{n-1} - 1) = 9 \cdot 10^{n-1}$. С другой стороны имеем: $N(n) = N_1(n) + N_2(n) + N_3(n)$. Нетрудно показать, что имеют место равенства: $N_1(n) = 5^n$; $N_2(n) = 4 \cdot 5^{n-1}$; отсюда получим $N_3(n) = 9 \cdot 5^{n-1} \cdot (2^{n-1} - 1)$. Найдем соответствующие вероятности:

$$(7) \quad p_1 = 5/9 \cdot 2^{n-1}, \quad p_2 = 4/9 \cdot 2^{n-1}, \quad p_3 = (2^{n-1} - 1)/2^{n-1}.$$

Закон распределения случайной величины $X(n) = \{N_1(n), N_2(n), N_3(n)\}$ задаётся следующей таблицей:

$X(n)$	$N_1(n)$	$N_2(n)$	$N_3(n)$
$P(n)$	$5/9 \cdot 2^{n-1}$	$4/9 \cdot 2^{n-1}$	$(2^{n-1} - 1)/2^{n-1}$

Далее, математическое ожидание, дисперсия и стандарт находятся по известным формулам: именно $MX(n) = \sum_{i=1}^3 N_i(n) \cdot p_i = \frac{5^{n-1}}{9 \cdot 2^{n-1}} \cdot [41 + (9 \cdot (2^{n-1} - 1))^2]$, аналогично находятся: $D_{X(n)} = M[X^2(n)] - [MX(n)]^2$; $\sigma_{X(n)} = \sqrt{D_{X(n)}}$ при каждом n .

На практике часто пользуются шестизначными числами, т.е. когда $n = 6$. Выпишем значения основных величин: $N(6) = 900000$; $N_1(6) = 15625$;

$$N_2(6)=12500; N_3(6)=871875; X(6) = \{15625;12500;871875\},$$

$$p_1 = N_1(6)/N(6) \approx 0,0174; p_2 = N_2(6)/N(6) \approx 0,0139; p_3 = N_3(6)/N(6) \approx 0,9687;$$

При этом выполняется равенство: $p_1 + p_2 + p_3 = 1$, т.е. мы имеем *полную группу событий*. Теперь найдём числовые характеристики:

$$MX(6) \approx 845030, 9375; D_{X(6)} \approx 91408784728, 0635; \sigma_{X(6)} \approx \sqrt{D_{X(6)}} = 302338, 8575.$$

Вывод: когда число знаков в номере шариков увеличивается, то число наборов с четными цифрами убывает по сравнению с числом наборов с нечетными цифрами, а число смешанных наборов стремительно растёт. Таким образом, при кодировании указанными наборами естественно наиболее выгодными являются наборы с четными цифрами, т.е. **дешифровать** случай с четными наборами труднее в отличие от двух других случаев. Однако, всегда у **«взломщиков»** остаётся надежда на случайность. Также отметим, что в общем случае аналогичные задачи можно исследовать с иными условиями разбиения элементов базового множества $\{x_0, x_1, \dots, x_{g-1}\}$; $g > 1$. На этом мы ограничимся.

Литература

1. И.М. Виноградов «Основы теории чисел», Наука, Москва 1981 г., 176с
2. М.С. Бокаева, Д. Исмоилов, Н.Д. Сарбасова «Курс лекций по теории вероятностей и математической статистике», ИнЕУ, Павлодар, 2014г, 430с (А4)

Капалова Н. А., Дюсенбаев Д.С.

**ПОЗИЦИЯЛЫҚ ЕМЕС ПОЛИНОМДЫҚ САНАУ ЖҮЙЕСІНЕ
НЕГІЗДЕЛГЕН ШИФРЛЕУ АЛГОРИТМДЕРІНЕ СЫЗЫҚТЫҚ
КРИПТОТАЛДАУДЫ ҚОЛДАНУ**

ҚР БҒМ ҒК «Ақпараттық және есептеуіш технологиялар институты»

Алматы, Қазақстан Республикасы

Дәстүрлі емес шифрлеу мен электрондық сандық қолтаңбаны қалыптастыру және криптографиялық кілттерді тарату алгоритмдер мен әдістерін дамыту мен

зерттеуде позициялы емес полиномды санау жүйесін (ПЕПСЖ) қолдану криптографиялық рәсімдердің сенімділігі мен тиімділігін айтарлықтай арттырады [1-5]. Қалдықтар классының классикалық жүйесіне қарағанда ПЕПСЖ модульдік негіздері коэффициенттері екілік жүйеде болатын келтірілмейтін көпмүшеліктерден (немесе $GF(2)$ өрісінде) тұрады. Позициялы емес полиномды санау жүйесін пайдаланып құрылған криптографиялық алгоритмдердің криптографиялық беріктілігін бағалау үшін сызықтық анализ жүргізілді.

Сызықтық криптоанализ – сызықтық емес теңдеулерден, кілтке, ашық және жабық мәтінге қатысты сызықтық теңдеулер құру мүмкіндігіне негізделген [6].

Біріншіден, шифрлау алгоритм белгілі болуы тиіс. Екіншіден, сызықтық теңдеулер жүйесін құрудағы сызықтық қиындық қаншалықты.

Жұмыстың негізгі мақсаты позициялы емес полиномды санау жүйесі негізінде көпмүшеліктерді модуль бойынша көбейту арқылы шифрлау алгоритміне сызықтық криптоанализ жүргізу әдістерін қарастыру.

ПЕПСЖ қалыптастыру [2-4] айтылған: осы негіздердің дәрежелері m_1, m_2, \dots, m_s болатын, сәйкесінше

$$p_1(x), p_2(x), \dots, p_s(x) \quad (1)$$

$GF(2)$ өрісінде келтірілмейтін көпмүшеліктер таңдалады.

Әрбір i үшін $GF(2^{m_i})$ кеңейтілген ақырлы өрісінде дәрежесі m_i болатын $p_i(x)$ - келтірілмейтін көпмүшелігі бойынша $GF(2)$ өрісінде $GF(2)[x]/(p_i(x))$ факторсақиналарын құрайды.

Алдымен жұмыс негізі біреу болған жағдайы, яғни бір келтірілмейтін көпмүшелік деп қарастырайық. Позициялы емес полиномді санау жүйесі арқылы құрылған

$$f(x) * \varphi(x) = g(x)(\text{mod } p(x)), \quad (2)$$

шифрлауды қарастырайық [2, 5].

Берілген (2) алгоритмде дешифрлау мына формула бойынша орындалады

$$g(x) * \varphi^{-1}(x) = f(x)(\text{mod } p(x)), \quad (3)$$

мұндағы $\varphi(x) * \varphi^{-1}(x) = 1 \pmod{p(x)}$.

$\exists s(x) \in GF(2)[x]/(p(x))$ - көпмүшелігі табылады және

$$g(x) * \varphi^{-1}(x) \oplus p(x) * s(x) = f(x), \quad (4)$$

теңдігін қанағаттандырады.

Онда (4) теңдігінен төмендегідей теңдеулер жүйесін аламыз.

$$\begin{cases} c_{n-1} * d_{n-1} \oplus k_n * s_{n-2} = 0 \\ c_{n-1} * d_{n-2} \oplus c_{n-2} * d_{n-1} \oplus k_n * s_{n-3} \oplus k_{n-1} * s_{n-2} = 0 \\ \dots \\ c_{n-1} * d_1 \oplus c_{n-2} * d_2 \oplus \dots \oplus c_1 * d_{n-1} \oplus k_n * s_0 \oplus k_{n-1} * s_1 \oplus \dots \oplus k_2 * s_{n-2} = 0 \\ c_{n-1} * d_0 \oplus c_{n-2} * d_1 \oplus \dots \oplus c_0 * d_{n-1} \oplus k_{n-1} * s_0 \oplus \dots \oplus k_1 * s_{n-2} = a_{n-1} \\ c_{n-2} * d_0 \oplus c_{n-3} * d_1 \dots \oplus c_0 * d_{n-2} \oplus k_{n-2} * s_0 \oplus k_{n-3} * s_1 \oplus \dots \oplus k_0 * s_{n-2} = a_{n-2} \\ \dots \\ c_2 * d_0 \oplus c_1 * d_1 \oplus c_0 * d_2 \oplus k_2 * s_0 \oplus k_1 * s_1 \oplus k_0 * s_2 = a_2 \\ c_1 * d_0 \oplus c_0 * d_1 \oplus k_1 * s_0 \oplus k_0 * s_1 = a_1 \\ c_0 * d_0 \oplus k_0 * s_0 = a_0 \end{cases} \quad (5)$$

$c = (c_{n-1}, c_{n-2}, \dots, c_2, c_1, c_0)$ сандар тізбегі шифр мәтіннің бит түріндегі пішіні болғандықтан, олар бізге белгілі.

$$a = (a_{n-1}, a_{n-2}, \dots, a_2, a_1, a_0), k = (k_n, k_{n-1}, \dots, k_2, k_1, k_0),$$

$$d = (d_{n-1}, d_{n-2}, \dots, d_2, d, d_0) \text{ және } s = (s_{n-2}, s_{n-3}, \dots, s_2, s_1, s_0)$$

тізбектері белгісіз айнымалылар.

Қандай криптоанализ жүргізілсе де осы (5) теңдеулер жүйесінен шығады. Бұл теңдеулер жүйесі кілттің, ашық және жабық мәтіннің мәндерін байланыстыратын басты схема.

Криптоаналитик ең алдымен шифртекстің әлсіз жерлерін іздейді, яғни көпмүшеліктердің көбейтіндісінің дәрежесі келтірілмейтін көпмүшеліктің (модуль негізі) дәрежесінен кіші болатын жағдайларды қарастырады. Өйткені, ол жағдайларда (5) теңдеулер жүйесінде k_i және s_i айнымалыларына қатыссыз, тек d_i және a_i айнымалыларына қатысты сызықтық теңдеулер жүйесі шығады. Сондықтан кілтті таңдау кезінде ондай жағдайды жібермеуі керек.

Егер келтірілмейтін көпмүшеліктің p_n және p_0 коэффициенттерінің 1 болатынын ескерсек, онда (5) теңдеулер жүйесіндегі s_i айнымалыларынан толық құтылып, теңдеулер жүйесі d_i , k_i және a_i айнымалыларына қатысты болатын теңдеулердің саны n болады. Яғни жүйедегі теңдеулердің санын $2n-1-$

ден n -ге дейін азайтамыз. Теңдеулер жүйесінің шешімдері көп. Бізге ақиқат шешімін табу керек. Ол шешімді табу үшін әртүрлі әдістерді қолдануға болады. a_i айнымалылары ашық мәтіннің бит түріндегі пішіні болғандықтан оларды өзіміз жорамалдау арқылы береміз. k_i айнымалылары келтірілмейтін көпмүшеліктердің коэффициенттері де белгісіз, сондықтан оларды теру арқылы тексереміз.

Егер k және a айнымалылар тізбегін таңдадық десек, онда теңдеулер жүйесінде $d = (d_{n-1}, d_{n-2}, \dots, d_2, d_1, d_0)$ айнымалылары қалады.

Теңдеулер жүйесіндегі теңдеулердің саны мен айнымалылар саны тең.

Теңдеулер жүйесінің шешімі болуы үшін, осы жүйенің мәндерінен құрылған сәйкесінше матрицаның рангі айнымалылардың санына тең болу керек. Яғни, теңдеулер жүйесінің шешімі $(d'_{n-1}, d'_{n-2}, \dots, d'_2, d'_1, d'_0)$ болсын. Онда келесі сандар тізбегін кему ретімен сәйкесінше коэффициенттері болатын көпмүшеліктерге модуль бойынша көбейтеміз, дешифрлаудағы есептеулер бойынша дешифрланған мәтін ашық мәтіннің ережелерін қанағаттандырмаса, оқылмаса, онда келесі таңдауға көшеміз. Дәл осылай ашық мәтін шыққанша орындалады. Келтірілмейтін көпмүшеліктердің дәрежесі артқан сайын, іздеу қиындығы да артады (таблица 1-2).

Осы алгоритм $m = \sum_{i=1}^s m_i$ – кілттің ұзындығы болғандықтан теңдеудің әрбір m_i дәрежелі келтірілмейтін көпмүшелігіне сәйкес m қадам бойынша тексеріледі.

Ендігі жұмыс іздеу қиындығын есептеу. Сонда біз сызықтық криптоанализдың тұрақтылығы қаншалықты екеніне жауап береміз.

Таблица 1. Кілтке қатысты ашық мәтінді іздеу мүмкіндігі.

Кілт ұзындығы	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Келтірілмейтін көпмүшеліктердің саны	2	3	6	9	18	30	56	99	186	335	630	1161	2182	4080
Ашық мәтенді таңдау саны	8	16	32	64	116	116	232	464	928	1856	3712	7424	13456	13456

Мүмкін болу саны	16	64	256	832	2920	6400	19392	65328	237936	859696	3198256	11817520	41178512	96078992
Ықтималдылығы	0,0625	0,015625	0,003906	0,001202	0,000342	0,000156	5,16E-05	1,53E-05	4,2E-06	1,16E-06	3,13E-07	8,46E-08	2,428E-08	1,041E-08

Таблица 2. Стандартты кеңейтілген файлдардың бастапқы байттары.

байт	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
.docx	50	4b	03	04	14	00	06	00	08	00	00	00	21	00		
.jpg	ff	d8	Ff	e0	00	10	4a	46	49	46	00	01	01	01	01	2c
.pdf	25	50	44	46	2d	31	2e									
.pdf*	ef	bb	Bf	25	50	44	46	2d	31	2e						
.htm	3c	21	44	4f	43	54	59	50	45	20	68	74	6d			
.doc	d0	cf	11	e0	a1	b1	1a	e1	00	00	00	00	00	00	00	00
.zip	50	4b	03	04												
.exe	4d	5a	90	00	03	00	00	00	04	00	00	00	ff	ff	00	00

Екінші әдіс. $\frac{3}{4}$ ықтималдылықпен $xu \oplus x \oplus u = 1$ теңдігін қарастыруға болады.

Егер (5) теңдеулер жүйесіндегі айнымалылардың көбейтіндісін $xu = x \oplus u \oplus 1$ өрнегімен жуықтау арқылы сызықтық теңдеулер жүйесін аламыз.

Егер теңдеулердегі $xu = x \oplus u$ қателіктері жұп болып кездесетін болса, онда олар ақиқаттықты береді. Осы құрылған теңдеулер жүйесінде алғашқы әдістегідей арнайы таңдалған ашық мәтінтерді теру арқылы шығарамыз.

Кілт бөлікшесінің барлық мүмкін мәндерін таңдауға айнымалылардың мүмкін мәндеріне келтірілмейтін көпмүшеліктердің санына көбейткенге тең. Ашық мәтіннің статистикалық кездесу мүмкіндігі, сол көлемдегі барлық мүмкін мәндерінен кіші болғандықтан, теңдеулер жүйесін шешудегі мүмкіндігі ашық мәтіннің кездесу мүмкіндігі мен келтірілмейтін көпмүшеліктердің санына көбейткенмен тең. Кілтті толық табу үшін, осылай біртіндеп бөліктеп табуға болады. Осы әдістерді тексеруде бағдарлама жазылуда, оның тексеру мүмкіндігі кілт бөлікшелерінің ұзындығына тәуелді.

Пайдаланылган әдебиеттер тізімі

1. Бияшев Р. Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10.1985: утв. 28.03.1986. - М., 1985.
2. Амербаев В.М., Бияшев, Р.Г., Нысанбаева С.Е. Применение непозиционных систем счисления при криптографической защите // Изв. Нац. акад. наук Республики Казахстан.–Сер. физ.-мат.– Алматы:Гылым, 2005. - № 3. – С. 84-89.
3. Biyashev R., Nyssanbayeva S., Kapalova N. The Key Exchange Algorithm on Basis of Modular Arithmetic // Proceedings of International Conference on Electrical, Control and Automation Engineering (ECAE2013), Hong Kong-Lancaster, U.S.A.:DEStech Publications, 2013. – P.16.
4. R. Biyashev, M. Kalimoldayev, S. Nyssanbayeva, N. Kapalova, R. Khakimov. Program Modeling of the Cryptography Algorithms on Basis of Polynomial Modular Arithmetic / The 5th International Conference on Society and Information Technologies (ICSIT 2014, march 4-7, 2014- Orlando, Florida, USE) – IIS. pp. 49-54
5. Бияшев Р.Г., Нысанбаева С. Е., Капалова Н.А. Секретные ключи для непозиционных криптосистем. Разработка, исследование и применение. – LAB LAMBERT Academic Publishing, 2014, с. 126.
6. Л.К. Бабенко, Е.А. Ищукова. Современные алгоритмы блочного шифрования и методы их анализа // Москва. Гелиос АРВ – 2006.

Каполёз Г.В.

АНАЛИЗ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА КАК СРЕДЫ РЕАЛИЗАЦИИ ИНФОРМАЦИОННОГО ВЛИЯНИЯ

Центр военно-стратегических исследований Национального университета
обороны Украины имени Ивана Черняховского, Киев, Украина

Средой реализации информационных воздействий при различных уровнях напряженности в информационных отношениях между субъектами информационного сообщества является информационное пространство, в рамках которого осуществляется накопление, обработка, хранение информации обмен ею между людьми организациями, государствами и межгосударственными объединениями.

К.Б. Водолазская [1] отмечает, что информационное пространство имеет структурные и динамические характеристики и может принадлежать как отдельному человеку, так и группе, социальным слоям и слоям общества, а также обществу в целом. Учитывая сложность феномена, который обозначается термином “информационное пространство”, во время его описания, воспользуемся предложением В.В. Баранюка [2] рассматривать информационное пространство с оперативной, технологической и организационной точек зрения.

С оперативной точки зрения информационное пространство целесообразно рассматривать как совокупность информации, которая образует “информационный ресурс”. Информация как сообщение некоторых сведений не имеет самостоятельной ценности. Ее значение определяется приростом знаний получателя сообщения, соотнесенных с его потребностью или с целью субъекта, который поместил информацию в информационное пространство. Анализ подходов В.Б. Толубко [3], В.В. Балабина, И. Замаруевой, С.В. Лескова, А.А. Рось [4], С.М. Пустовит [5] к определению понятия “информационный ресурс” позволяет нам рассматривать его как продукт интеллектуальной и практической деятельности человека, коллектива, сообщества, который представлен в виде информации (данные, сведения, сообщения и т.п.), знаний (совокупность сведений, образующих целостное описание объекта или процесса, взаимосвязанная совокупность сведений, информационное представление, которое содержит взаимосвязанную совокупность сведений об

объекте или процессе и т.п.) подготовленных для использования в конкретной сфере индивидуальной, групповой, государственной деятельности в общественной и производственной сферах.

По уровню подготовленности к использованию целесообразно различать актуальный и потенциальный информационные ресурсы. Актуальный информационный ресурс содержит информацию и знания, которые подготовлены к использованию в конкретной сфере государственной, производственной или общественной деятельности. Потенциальный информационный ресурс содержит совокупность информации и (или) знаний, требующих ресурсных (времени, денег, материальной и экспериментальной базы, привлечения подготовленных специалистов) расходов на их преобразование (анализ, научные исследования и т.п.) в актуальный информационный ресурс. В зависимости от конкретных задач и обстоятельств информационный ресурс может быть использован:

1) для обеспечения необходимыми исходными данными лиц (руководства государства, силовых структур, соответствующих организаций, граждан и т.п.) при принятии решений в политической, экономической, военной, культурной и т.д. сферах;

2) для активного вторжения в информационное пространство и выполнение в нем специальных задач: удовлетворение познавательных, культурных потребностей личности, формирование менталитета нации, дезинформация противника, защита "собственного информационного пространства" в мирное и военное время, придания ему свойств живучести и независимости (инвариантности) от вмешательства со стороны враждебных информационных воздействий и др.

Таким образом, информационный ресурс будучи продуктом деятельности человека, коллектива, сообщества, используется как механизм преобразования знаний (информации) в силу, которая влияет на факторы развития общества. С одной стороны, он обеспечивает принятие решения, часто является

первопричиной умственной деятельности (новая информация об объекте меняет отношение к нему, что требует переосмысления), а с другой – побуждает исполнителей к деятельности (реализации решений) на предметном уровне (полученное указание или изменение представления об объекте вызывают действия или бездействие в отношении последнего).

С технологической точки зрения информационное пространство целесообразно рассматривать как сочетание хранилищ информации; средств ее введения и представления, коммуникационных систем и сетей; совокупности структурных подразделений (должностных лиц), осуществляющих наполнение и ведение хранилищ информации и администрирование информационных ресурсов, обеспечивающих реализацию информационных процессов.

Под информационной технологией, как правило, понимают совокупность методов, средств и способов сбора, накопления, хранения, обработки данных с целью целенаправленного преобразования, использования, распространения информации (знания) в информационном пространстве. Информационные технологии направляются на обеспечение автоматизации, алгоритмизации работы субъектов информационного пространства. В структуре информационных технологий (ИТ) можно выделить три основных компонента: технические средства принятия, обработки и передачи информации (телерадиостанции, спутниковые системы коммуникации, ЭВМ и сопряженная с ней высокопроизводительная аппаратура и т.д.), инструментарий (методологическое обеспечение информационной борьбы, математическое и программное обеспечение ЭВМ и т.д.), специально созданные структуры органов управления применением технических средств и инструментария.

С организационной точки зрения информационное пространство целесообразно рассматривать как совокупность взаимосвязанных субъектов информационного сообщества, обеспечивающих информационные процессы в системе обмена информацией по общим правилам их описания и формализации.

В информационном пространстве функционируют субъекты и объекты информационного воздействия. Среди объектов информационного воздействия в широком смысле целесообразно выделить личность, группу, общественные слои, страны с их политическими интересами, в узком смысле – информационные системы, обеспечивающие принятие решения, функционирование элементов вооруженной защиты и нападения, системы образования и культуры. Как правило, в структуре объектов информационного влияния можно выделить органы управления (психика личности, лидеры малых и больших групп, общественных слоев населения, органы государственного и военного управления и т.п.), силы и средства (знания, убеждения, традиции, общественное мнение, научно исследовательские учреждения, учебные заведения, научно-промышленный комплекс страны, телекоммуникационные узлы, центры спутниковой связи, каналы международного информационного обмена, образцы вооружения и техники и т.д.).

Субъектами информационного воздействия следует считать лиц, органы, структуры, занимающиеся исследованием информационного пространства, определением целей, планированием и осуществлением информационного воздействия.

Заключение.

Таким образом, информационное пространство целесообразно рассматривать как среду реализации информационных воздействий, а в его структуре различать информационные ресурсы, источники информационных потоков, потребителей информации (объекты воздействия), системы, формирующие информационные потоки (субъекты воздействия).

Информационное пространство целесообразно рассматривать с разных точек зрения: оперативной (как совокупность информации, образует "информационный ресурс") технологической (как сочетание хранилищ информации; средств ее введения и представления, коммуникационных систем и сетей; совокупности структурных подразделений (должностных лиц),

осуществляют наполнения и ведения хранилищ информации и администрирования информационных ресурсов, обеспечивающих реализацию информационных процессов), организационной (как совокупность взаимосвязанных субъектов информационного сообщества, обеспечивающих течение информационных процессов в системе обмена информацией по общим правилам их описания и формализации).

Литература

1. Водолазька К.Б. Модель інформаційного простору особистості як об'єкту вербального впливу // Науково-технічний збірник. – К.: ННДЦ ОТ і ВБ України, 1999. – Вип. 3. – С. 174-179.
2. Баранюк В.В. Единое информационное пространство ВС РФ: проблемы создания // Военная мысль. – 2003. №3. – С. 36-38.
3. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): Монографія. – К.: НАОУ, 2003. – 320 с.
4. Балабін В.В. Інформаційні системи нового покоління як чинник забезпечення національних інтересів / В.В. Балабін, І.В. Замаруєва, С.В. Лесков, А.О. Рось // Наука і оборона. – №1, 2007. – С. 40-45.
5. Рось А.О. Інформаційні ресурси: сутність і класифікація / А.О. Рось, С.М. Пустовіт // Науково-технічний збірник. – К.: ННДЦ ОТ і ВБ України, 1999. – Вип. 3. – С. 25-34.

Касенов Т.А.

РОЛЬ ВОЕННОЙ ПОЛИЦИИ США В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Национальный университет обороны имени Первого Президента Республики
Казахстан – Лидера нации, г. Астана, Республика Казахстан

Рассматривается опыт деятельности военной полиции США по связи с общественностью и средствами массовой информации.

Ключевые слова: информационная безопасность, военная полиция, средства массовой информации.

Противоборство в информационной сфере стало носить многопрофильный характер общественно-экономических, военно-политических и государственных отношений. Ее целью стало не только повышение эффективности боевых действий путем завоевания информационного превосходства, но и завоевание всестороннего всеобщего превосходства над потенциальным противником, дабы обеспечить свои экономические, политические, а если необходимо, то и военные цели [1].

В силу своих имманентных качеств информация обладает свойством распространяться невзирая на границы и устанавливаемые пределы. Одной из наиболее популярных характеристик современного общества является его определение как «информационного общества». Многие члены современного общества заняты производством, обработкой, передачей, распространением, потреблением информации. Более того, чем более человек вовлечен в информационный процесс, тем больше он подвержен воздействию информационной агрессии [2].

История последних десятилетий показала, что оказывается возможным разгромить мощное государство, его экономику, его военно-промышленный комплекс, все его важнейшие структуры вообще без применения военной силы (Советский Союз). Того же самого можно добиться и с применением военной силы, но принципиально с иным подходом, чем ранее (Ирак, Югославия), где методы ведения войны, нацеленные на достижение победы, наряду с поражением и физическим уничтожением неприятеля, включают его дезинформацию, снижение морально-психологической устойчивости, паралич воли к сопротивлению, создание благоприятной социально-политической обстановки в зоне ведения боевых действий.

Наибольший эффект информационно-психологического воздействия достигается в ходе соответствующих специальных технологий, получивших название PR-технологии. Недавние события в Ливии, Египте, и других странах Северной Африки особенно очевидно показали, насколько тяжкими могут быть последствия нарушения информационной безопасности.

Как мы видим, информация стала стратегическим ресурсом и приобрела такие свойства и масштабы, которые позволяют глобально воздействовать на национальную безопасность.

Осуществление технологий информационно-психологического воздействия включает предварительное подробное изучение общественного мнения, общественных настроений и ожиданий, на основе итогов которого готовится и корректируется соответствующая информация, подбираются и используются наиболее эффективные приемы и методы информационного воздействия

В этой связи, особое внимание за рубежом уделяется структурам по работе с общественностью в системе органов военного управления, в полномочия которых входит разработка рекомендаций командному составу по вопросам формирования и реализации информационной политики.

Так, в рамках программ по связи с общественностью органам управления вооруженных сил обеспечивается возможность посредством средств массовой информации довести своевременную и точную информацию до мировой общественности о содержании целей и задач военных компаний и операций, а также донести до потенциального противника сведения о своих намерениях и возможностях.

Необходимо отметить, что немаловажную роль в организации работы Вооруженных Сил США с гражданским населением, трактуемых как действия командиров по установлению и поддержанию отношений между подчиненным им войскам и гражданскими властями, организациями и местным населением в районах развертывания войск и воинских формирований, занимает

деятельность военной полиции США по взаимодействию со средствами массовой информации (СМИ). В документах Сухопутных войск США говорится, что военные полицейские могут периодически контактировать с представителями масс-медиа, поскольку установление доверительных отношений со СМИ позволяет устранять возникающие недоразумения между военными и общественностью.

В то же время здесь также существует определенный регламент. Как отмечается в документах, командование военной полиции имеет право отказывать СМИ в предоставлении напрямую запрашиваемой информации. При этом сообщается, где и у кого могут быть востребованы интересующие СМИ сведения. Каналы получения и содержание информации уточняются через офицера по связям с общественностью (СО), который является штатным сотрудником военной полиции и подчиняется соответствующему командиру. Как правило, офицер СО информирует о проводимых военной полицией мероприятиях и развитии обстановки, в первую очередь исходя из интересов командования. Одновременно это же лицо предоставляет командиру всю необходимую информацию о настроении населения и возможной реакции общества в отношении проводимых мероприятий. В интересах поддержки действий военной полиции офицер по СО может готовить пресс-релизы с информацией открытого характера. Для ее распространения используются различные медийные каналы, включая ТВ, радио, прессу, а также рекламную продукцию, такую как плакаты и листовки.

С помощью СМИ ведется широкая разъяснительная работа, а также устанавливаются контакты между вооруженными силами, местными властями и общественностью. Кроме того, масс-медиа нередко используются для обращения к населению с просьбой оказать содействие военной полиции при решении ряда задач, в том числе по профилактике правонарушений. Активный информационный обмен служит надежным индикатором взаимоотношений СМИ и военного ведомства в целом, полагают американские эксперты [3].

Деятельность военной полиции США по взаимодействию с общественностью и СМИ позволяет выполнять следующие задачи обеспечения информационной безопасности:

- формирование благоприятного общественного мнения в отношении решений принимаемых органами военного управления и командованием подразделений военной полиции;

- информационная поддержка действий войск и подразделений военной полиции;

- защита секретной информации о состоянии и деятельности национальных вооруженных сил;

- противодействие распространению подрывной и неконструктивной информации.

Таким образом, опыт деятельности военной полиции США по связи с общественностью и СМИ необходимо перенять в качестве одного из направлений совершенствования деятельности Вооруженных Сил Республики Казахстан по обеспечению информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

- 1 Тактика гибридной войны gosman.com/articles/taktika-gibridnoi-voyni-79.html.
- 2 Информационная война <http://www.echo.msk.ru/blog/aillar/1408258-echo/>.
- 3 Военная полиция США <http://www.modernarmy.ru/article/370/voennaya-policia-ssha>.

Кацалап В.А.

ПРЕДВАРИТЕЛЬНОЕ ПЛАНИРОВАНИЕ ИНФОРМАЦИОННОЙ ОПЕРАЦИИ

Национальный университет обороны Украины имени Ивана Черняховского,
г. Киев, Украина

Предварительное планирование относительно достижения большей эффективности при проведении информационной операции без применения насилия – возможно и востребовано, к тому же, подобное планирование не является чем-то новым. Существует много различных примеров планирования информационных мероприятий (акций, атак, отдельных актов) в недавнем прошлом.

Планирование информационных мероприятий осуществлялось и раньше при проведении небольших кампаний, таких как: «автобусный» бойкот, «сидячая» забастовка в буфете против расовой сегрегации в Соединенных Штатах Америки. Аналогично, в течение нескольких десятилетий велись тактические разработки для продолжительных маршей протеста (в течение дней или недель) за мир, социальную справедливость, избирательные права женщин, гражданские права, права человека и защиту окружающей среды.

Планирование и подготовка информационных мероприятий осуществлялись также при проведении различных повсеместных забастовок за экономические и политические права, происшедших в нескольких странах. Еще в период с 1765 по 1775 годы, когда колониальная Америка вела борьбу против Британского правления ненасильственными методами, осуществлялось не только тактическое, но и долгосрочное стратегическое планирование возможных информационных мероприятий которые в наше время во всей совокупности называется информационной операцией.

Случаи, когда идет речь об отдельной информационной акции или атаке можно считать необыкновенной интуицией, что само по себе очень - редко, поскольку только обрисовав контуры необходимых информационных действий и при этом выработав определенную стратегию возникает необходимость реализации в тактических этапах.

Например, в Польше в 1980-ых годах массы людей принимали участие в борьбе независимого профсоюзного объединения «Солидарность» и близких по духу групп, руководствуясь историческим опытом ведения информационных

действий – крича на улицах свои требования и только столкнувшись с агрессивными действиями властей они сумели провести организованные митинги и добиться своих целей. В Сербии в 2000 году проводились предварительные расчеты и подготовительные информационные мероприятия, рассматривались вопросы деятельности и стратегического планирования информационной операцией в целях устранения диктатуры Милошевича. Однако, во многих конфликтах, которые проводились без применения насилия, планирование не осуществлялось. Зачастую планирование не соответствовало действительности при полном отсутствии стратегических расчетов. Тем не менее, существуют примеры достижения значительных успехов в хаотических информационных мероприятиях.

Необходимо также отметить наличие достаточного количества примеров достижения весьма скромных результатов. Есть примеры сокрушительного поражения и ужасных жертв как случилось в Сирии. В будущем необходимо снижать возможность подобных поражений и жертв, одновременно повышая вероятность достижения успехов используя только спланированную за местом и временем информационную операцию.

Более полное и качественное стратегическое планирование информационной операции в будущем может помочь повысить эффективность борьбы без применения насилия против угнетения и снизить количество жертв. Но это все зависимость от внешних советников по вопросам планирования может быть рискованной и недальновидной.

Желательно, чтобы знания по разработке стратегий информационной операции были доступными, так чтобы люди, при столкновении с диктаторским режимом и другими видами угнетения, могли осуществлять предварительное планирование информационной операцией по смещению режима собственными силами.

Поскольку единичные митинги менее эффективны и не обеспечивают такого глубокого влияния на население, как спланированная их волна

внимательное то это на сегодняшний день будет являться главной составляющей информационной операции. Предварительно спланированные митинги с подобранной целевой аудиторией можно считать основой любой информационной операции.

По этому рассматривая вопрос предварительного планирования информационной операцией необходимо подходить с создания модели по информационному влиянию на отдельных лиц и группы лиц, желающих изменить свое состояние в обществе при этом реализовать потенциальные возможности ненасильственных методов борьбы против тирании. Также эта модель может помочь людям развить свои знания, способности мыслить и понимать, чтобы научиться действовать более эффективно в конфликтах с противником. Для успешной реализации этой цели необходимо внимательно изучить информационное пространство, методы мотивации людей, а также проанализировать все возможные информационные угрозы, в ситуации острого политического конфликта, когда со стороны противника можно ожидать жестких репрессивных мер.

Предварительно спланированная информационная операция и продуманная генеральная стратегия позволят участникам информационной борьбы действовать такими методами, которые в совокупности обеспечат скорейшее достижение поставленных целей в конфликте.

Таким образом, в данной статье отражено основные компоненты предварительной планированной информационной операции совокупность которых позволит достичь одновременного успеха не силовыми методами.

Клиновой Д.В., Рогов П.Д., Белокур Н.А.

**ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССА
ДЕЦЕНТРАЛИЗАЦИИ УПРАВЛЕНИЯ ПРИРОДНЫМИ РЕСУРСАМИ
ГОСУДАРСТВА**

Государственное учреждение «Институт экономики природопользования и устойчивого развития Национальной академии наук Украины», г. Киев,
Украина

Децентрализация в управлении природными ресурсами в мире, как показывает мировой опыт, основывается на конституционных нормах отдельно взятой страны и зависит, в первую очередь, от системы административно-территориального устройства государства (унитарное государство или федерация). В обоих случаях децентрализация является одним из наиболее распространенных преобразований, осуществляемых во многих странах. Одним из ключевых вопросов в процессе децентрализации является информационный вопрос, а именно – информационное сопровождение и, соответственно, информационная безопасность передачи государством на местный уровень определенных полномочий. Таким образом, децентрализация представляет соответствующим образом информационно обеспеченный и открытый процесс передачи правительством полномочий и функций в управлении природными ресурсами местным институтам, среди которых главную роль играют такие как: отраслевые подразделения местных органов публичной власти (называется деконцентрацией или делегированием); органы местного государственного управления и самоуправления (политическая децентрализация); группы пользователей (деволюция) [1, с.36].

Опыт децентрализации в управлении природными ресурсами показывает разную ее эффективность для разных стран. В первую очередь это связано со стартовыми условиями проведения реформ на определенный момент. Как можно лучше децентрализация в управлении природопользованием происходит там, где есть стойкий, переосмысленный для местных условий, опыт самостоятельного природопользования на местном уровне (пример: Польша, Финляндия) или же давние или стойкие традиции федеральных отношений (пример: Швейцария, США). В любом случае залогом эффективной

децентрализации является, с одной стороны, информационная открытость в управлении природными ресурсами и соблюдение правил информационной безопасности, построенных на принципах открытого доступа граждан и местных общин к информации и природным ресурсам, а с другой стороны, соблюдение принципа контроля государством информации о передаче прав местным сообществам и защиты стратегически важной информации о природных ресурсах, которая носит, в необходимой степени, закрытый характер (например, информация об определенных полезных ископаемых, составляющая государственную тайну). Таким образом, информационная безопасность в процессе децентрализации власти предполагает как закрытие доступа к определенной информации, так и наоборот – открытие информации о том, какие права и полномочия относительно каких ресурсов передаются местным органам власти.

Опыт стран Восточной Европы, Балкан, Азии, Южной Америки [2] показывает, что, как правило, децентрализованные институты демонстрируют неудовлетворительные результаты по следующим причинам:

- реформа имеет информационно-закрытый характер, не создает подотчетные, репрезентативные местные институты, теряется местный контроль над ресурсами;
- на местный уровень не передаются ни информация о природных ресурсах, ни конструктивные полномочия или не оговариваются точно такие полномочия, на практике ресурсы не передаются в ведение местных общин;
- наоборот, на местный уровень передаются полномочия, которые местное сообщество осуществить объективно не может в силу отсутствия финансовых, информационных или иных средств;
- местным сообществам передаются более широкие полномочия, нежели это необходимо, при этом государство теряет контроль над

стратегически важными ресурсами, местные общины, по сути, присваивают государственную монополию на такие ресурсы;

- не определены и не согласованы политические и социально-экономические интересы, как местных общин, так и государства, которые являются движущим фактором процесса децентрализации.

Европейские исследователи выделяют три фактора, которые особенно серьезно влияют на результат процесса децентрализации [3]: информационный, технический и финансовый потенциал местного сообщества; степень социально-экономического равенства, уровень развития гражданского общества и информационной свободы; всеобъемлющий информационный характер и подотчетность местной институциональной базы.

Этот процесс должен быть в необходимой мере информационно открытым и иметь необходимое информационное обеспечение. Так, в открытом доступе для органов центральной и местной власти и должны находиться реестры (кадастры) земельных, водных, лесных и минерально-сырьевых ресурсов. Например, для некоторых ресурсов в современных условиях в Украине крайне сложно решить вопросы децентрализации полномочий из-за отсутствия необходимой информации. Так, согласно мнению М.А. Хвесика и соавторов [4], передача части властных полномочий относительно управления отечественным фондом недр сейчас является преждевременной, поскольку отсутствует необходимая информационная составляющая, обеспечивающая экономическую безопасность страны и её регионов. С 2012 года Государственный информационный геологический фонд Украины прекратил выпуск ежегодного справочника “Минеральные ресурсы Украины”, данные о балансовых запасах полезных ископаемых, их погашении, о количестве месторождений отсутствуют уже 4 года. В таких условиях делегирование прав местным органам самоуправления на предоставление специальных разрешений для добычи полезных ископаемых не может быть эффективно обеспечено.

Подобные явления характерны и для других видов природных ресурсов – водных, земельных, лесных, биологических, рекреационных.

Задачей обеспечения информационной безопасности любого государства в процессе децентрализации в управлении природными ресурсами является создание как можно более полноценной информационной системы с обратной связью, обеспечивающей защиту интересов, как государства, так и регионов при передаче управления природными ресурсами в местные сообщества. Управление природными ресурсами при участии местных сообществ (УПРМС) представляет собой форму управления природными ресурсами, которое контролируется и санкционируется самым местным сообществом (например, в Украине - территориальной общиной, которую представляет орган местного самоуправления). Оно может касаться разных прав собственности на ресурсы и комплексы ресурсов. Этот процесс должен иметь всестороннюю информационную поддержку таким образом, чтобы вся необходимая информация о природных ресурсах, которые передаются в использование местным сообществам, находилась в распоряжении соответствующих органов и граждан. Одновременно с этим необходимо обеспечить защиту информации о природных ресурсах, которая зачастую носит закрытый характер и не может быть вынесена для открытого доступа.

Особенно важным в процессе децентрализации в управлении природными ресурсами является аспект информационной безопасности для вопросов, касающихся системы прав собственности на природные ресурсы, в которых право собственности предоставляется сообществу, а оно, в свою очередь выделяет землю или другие ресурсы членам сообщества.

Выводы:

1. Отличительной чертой децентрализации в управления природными ресурсами местными сообществами является необходимость информационного обеспечения и, соответственно, информационной безопасности, этого процесса для всех участников процесса.

2. Государство должно принимать непосредственное участие в процессах децентрализации, направляя свои усилия на понимание происходящих процессов; создание рабочих законов (а не законов декларативного характера); управление процессами децентрализации, предполагающими мероприятия координации, организации, распорядительства, прогнозирования, обеспечения и контроля, а также обеспечения региональной информационной безопасности без участия иностранных “помощников-консультантов”.

3. Местным сообществам, равно как и государственной власти, в процессе децентрализации необходимо четко понимать связанные с ним задачи, права, обязанности и ограничения, которые должны быть определены и четко сформулированы с учетом фактора информационной безопасности.

Литература

1. Основы системы прав собственности на природные ресурсы: Памятка реформаторам в странах Восточной Европы, Кавказа и Центральной Азии. Отдел по анализу и оценке экологической результативности. Директорат по охране окружающей среды: ОЭСР, 2011. – 54 с.
2. Ribot J.C. Waiting for Democracy. The Politics of Choice in Natural Resource Decentralization, WRI Report World Resources Institute: Washington, DC, 2004. – 142 p.
3. Meinzen-Dick R., di Gregorio M., Dohrn S. Decentralization, Pro-poor Land Policies and Democratic Governance// CAPRI Working Paper: CGIAR and UNDP, № 80, June 2008. – 36 p.
4. Економічні аспекти управління природними ресурсами та забезпечення сталого розвитку в умовах децентралізації влади в Україні / [за наук. ред. акад. НААН України, д.е.н., проф. М.А. Хвесика, д.г.-м.н., проф. С.О. Лизуна; Державна установа «Інститут економіки природокористування та сталого розвитку Національної академії наук України»]. – К. : ДУ ІЕПСР НАН України, 2015. – 72 с.

Корченко А.Г.¹, Казмирчук С.В.¹, Алимсеитова Ж.К.², Жекамбаева М.Б.²

ПРОГРАММНОЕ СРЕДСТВО ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОБРА

¹Национальный авиационный университет, Киев, Украина,

²Казахский национальный исследовательский университет имени
К.И. Сатпаева, Алматы, Республика Казахстан

На сегодняшний день существует достаточно широкое множество инструментальных средств анализа и оценивания риска (САОР). В работе [1] осуществлен анализ понятия риска, в различных предметных областях человеческой деятельности, для последующей его интерпретаций в области информационной безопасности (ИБ). Также в [2] была предложена кортежная модель базовых характеристик риска (КМР). Такой подход дает возможность относительно КМР унифицировать процесс исследования соответствующих САОР и повысить эффективность осуществления их выбора.

В связи с этим, целью данной работы является проведение исследования САОР (с использованием предложенного в [2] подхода) для определения их набора характеристик, по которым можно осуществить сравнительный анализ таких средств. Это повысит эффективность решения задач в области ИБ.

В качестве исходного материала исследования было взято наиболее известные и используемые на практике САОР – СОБРА, CRAMM.

Методика СОБРА (Consultative Objective and Bi-Functional Risk Analysis, разработчик – C & A Systems Security Ltd, Великобритания) ориентирована на поддержку требований стандарта ISO 17799 посредством тематических вопросников (checklist's), используемых в ходе оценки рисков информационных активов и электронных бизнес транзакций компании [5]. В комплект программного обеспечения (ПО) входят модули СОБРА ISO 17799 Security Consultant, СОБРА Policy Compliance Analyst и СОБРА Data Protection Consultant, а также менеджер модуля СОБРА, используемый для настройки и

изменения снабжаемой базы знаний. На основе инициализации тематического вопросника осуществляется оценка и анализ риска по следующим категориям: высокоуровневая; безопасности информационных технологий (ИТ); оперативная ИТ и бизнеса; инфраструктуры электронной коммерции. Модули тематического вопросника информационно поддерживают отдельные приложения, например: APP-MAN (Application level security management) – управления безопасностью; APPAUDIT (Application level Auditing) – аудит; APPCNTRL (Application Staff control) – контроль штата; APPDEPND (Application Staff dependency) – зависимость штата; AUDIT (System Audit) – проверка системы и т.д.

Как видно из запроса, здесь нет конкретизации по украденному, что не позволяет четко определить степень урона и на какие характеристики безопасности ресурсов информационных систем (ИС) повлиял тот или иной инцидент. Такой подход дает возможность реализовать лишь достаточно грубое оценивание риска. Воровство (с учетом [3]) есть субъективной активной угрозой КИД-типа, конфиденциальность, целостность и доступность в этом случае нарушается, например, с исчезновением единственного экземпляра определенных информационных ресурсов, кража также может быть связана с подменой данных перед их вводом или в процессе вывода [3] и т.д. Относительно базовых характеристик риска [2] для методики COBRA можно получить отображения таких составляющих: BC_1 , BC_2 . Так, компоненту BC_1 (исходя из указанного примера) соответствует, например, значение BC_{11} = «Кража». Это действие приводит к нарушению определённых характеристик безопасности атакованных ресурсов и может быть связано со значением BC_{27} = «НКЦД».

После обработки инициализированных данных система генерирует отчет, в котором описана детальная оценка (Detailed Risk Assessment (continued)) по следующим характеристикам риска: категория (RISK CATEGORY); уровень (RISK LEVEL); оценка (RISK ASSESSMENT). Например: КАТЕГОРИЯ

РИСКА – «Непредвиденная ситуация в бизнесе»; УРОВЕНЬ РИСКА – 96,61%; ОЦЕНКА РИСКА – «Персонал плохо подготовлен к непредвиденным ситуациям, нет планирования действий в непредвиденных ситуациях и не выполняются требования к ним». Отметим, что в анализируемой методике риск отображается тремя базовыми характеристиками, первая и последняя из которых несут в себе BC_1 и BC_2 , составляющие (название категории и комментарии к ней), а оставшаяся – составляющую, которой соответствует «УРОВЕНЬ РИСКА», представленный в процентах (вероятность наступления риска), в связи с этим (учитывая [2]) уровень риска можно отобразить через компонент BC_3 . Все рассматриваемые действия (BC_1), которые отображаются в запросах, собраны в категории риска, например, действие рассмотренное в примере запроса BC_{11} входит в категорию риска «Непредвиденная ситуация в бизнесе (НСБ)», следовательно характеристику в данной категории риска можно представить как $BC_{НСБ} = \{BC_{НСБ1}, BC_{НСБ2}, \dots, BC_{НСБbc_1}\}$, где $BC_{НСБ1} =$ «Кража» (bc_1 – количество идентификаторов угроз для категории НСБ) [2].

Анализ показал, что прямого использования компонента BC_2 в системе нет, но прослеживается логическая связь с ним, поэтому считаем его присутствие косвенным. Здесь и далее для обозначения косвенных характеристик в кортеже будет использоваться символ *, т.е. BC_2^* . После проведенного анализа с учетом КМР [2] кортеж для этой методики можем представить в виде $\langle BC_1, BC_2^*, BC_3 \rangle$.

Система Risk Watch (разработчик – компания Risk Watch, США) отображает требования стандартов ISO/IEC 27001 и ISO/IEC 27002, NIST а также COBIT IV. Процесс анализа и оценивания риска производится в четыре фазы. Фаза 1 – описание ИС организации с точки зрения ИБ (определение предмета исследования). Здесь описываются такие параметры предприятия, как тип организации, состав исследуемой системы, базовые требования в области ИБ. Фаза 2 – ввод данных. Для выявления уязвимостей инициализируется тематический вопросник (ТВ), база которого содержит более 600 запросов.

Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов (активов) (рис. 1), на основании чего рассчитывается эффективность внедрения средств ЗИ [4].

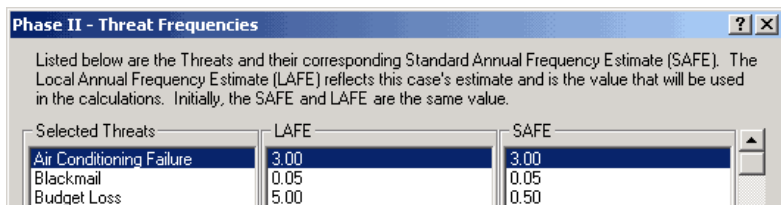


Рис. 1. Окно инициализации параметров

По аналогии с ПО СОБРА в Risk Watch (для упрощения ввода и обработки данных) множество запросов ТВ

инициируются посредством выбора данных из набора вариантов. Фаза 3 – оценка риска. Рассчитывается профиль рисков, и выбираются меры обеспечения ИБ. Для этого устанавливаются связи между ранее определенными ресурсами, потерями, угрозами и уязвимостями, а риск оценивается посредством ожидаемых потерь за год. Например, если стоимость сервера $v = 150\,000\$$, а вероятность его уничтожения при пожаре в течение года $p = 0,01$, то ожидаемые потери составят $m = 1\,500\$$, т.е. $m = p \times v$, где p – вероятность возникновения угрозы, а v – стоимость ресурса. Отметим, что Risk Watch базируется на таких данных NIST, как LAFE (Local Annual Frequency Estimate) и SAFE (Standard Annual Frequency Estimate), соответственно отражающих годовую частоту реализации угроз в локализованной (например, в городе) и глобализованной (например, в Северной Америке) области. Получить оценки LAFE и SAFE, например, для Казахстана проблематично, поскольку нет необходимой статистики. Фаза 4 – генерация отчета. Формируются диаграммы и таблица детального представления соответствия и несоответствия (относительно запросов) требованиям стандарта, а также диаграмма потерь. С учетом стоимости ресурса осуществляется оценка ожидаемых потерь (по конкретному активу) от реализации одной угрозы (ALE) [4] $ALE = A \times EF \times F$, где: A (AssetVal) – стоимость ресурса (данные, программы, аппаратура и т.д.); EF (ExposureFactor) – коэффициент воздействия (процентная часть от стоимости актива, подвергаемой риску); F (Frequency) – частота возникновения

нежелательного события. Например, пусть аппаратное средство стоит $A=10\ 000\$$, коэффициент воздействия на него $EF=0,5$, а частота $F=0,2$, то ожидаемые потери составят $AEL=1000\$$. После идентификации активов и воздействий оценивается общий риск для ИС (сумма всех частных значений). Для оценивания отдельно взятой пары «угроза-ресурс» используется формула $ALE = ARO \times SLE$. Эффект от внедрения средств безопасности определяется параметром ROI (Return on Investment – возврат инвестиций), показывающий отдачу от вложений за период времени.

Относительно КМР с учетом [2] для Risk Watch определим кортеж. Так компоненту BC_1 (исходя из указанного примера категорий потерь) соответствуют, например, значения BC_{11} = «Задержка и отказ в обслуживании», BC_{12} = «Раскрытие информации», BC_{13} = «Уничтожение оборудования» и т.д. Эти действия приводят к нарушению определенных характеристик ИБ атакованных ресурсов и соответственно связываются со значениями BC_{23} = «НД», BC_{21} = «НК», BC_{25} = «НЦД». Анализ риска происходит во время обработки данных инициируемых через ТВ, который используется при прохождении фазы 1. Для определения ALE используется компонент BC_5 , а риском являются ожидаемые потери за год, которые также можно интерпретировать как расходы (BC_6). С учетом КМР, кортеж для этой методики можно представить в виде $\langle BC_1, BC_2^*, BC_5, BC_6 \rangle$.

Таким образом, в работе с учетом предложенного в [2] подхода, проведено исследование САОР в виде соответствующего ПО и определен набор базовых характеристик, по которым можно осуществить сравнительный анализ соответствующих средств оценивания и выбрать наиболее подходящие для решения определенного класса задач ЗИ.

Литература

- [1]. Алексеев А. Управление рисками. Метод СРАММ / А. Алексеев // IT Expert. – Электрон. дан. – М. : ЗАО «ИТ Эксперт», 2010. – Режим доступа:

WorldWideWeb. – URL:
http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf. – Загл. с экрана
(просмотрено 19 декабря 2014).

- [2]. Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Б. Кортежная модель базовых характеристика риска / Вестник КазНТУ – 2015. – №6.
- [3]. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : «МК-Пресс», 2006. – 320с.
- [4]. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ [Электронный ресурс] / И. С. Медведовский // SecurityLab. Электрон. дан. – Мн. : SecurityLab, 2004. – Режим доступа: WorldWideWeb. – URL: <http://www.ixbt.com/cm/informationssystem-risks012004.shtml>.
- [5]. Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA. [Electronic resource] / Security Risk Analysis & Assessment, and ISO 27000 Compliance –Electronic data – Macclesfield : The Leading Security Risk , 2010– Access mode: World Wide Web. – URL: <http://www.riskworld.net/>.

Корченко А.Г.¹, Казмирчук С.В.¹, Ахметова С.Т.², Жекамбаева М.Б.²

**ПРОГРАММНОЕ СРЕДСТВО ОЦЕНИВАНИЯ РИСКОВ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ CRAMM**

¹Национальный авиационный университет, Киев, Украина,

²Казахский национальный исследовательский университет имени
К.И. Сатпаева, Алматы, Республика Казахстан

Существует множество инструментальных средств анализа и оценивания риска (САОР). В работе [2] осуществлен анализ понятия риска, в различных предметных областях человеческой деятельности, для последующей его интерпретаций в области информационной безопасности (ИБ). Также в [2] была

предложена кортежная модель базовых характеристик риска (КМР). Такой подход дает возможность относительно КМР унифицировать процесс исследования соответствующих САОР и повысить эффективность осуществления их выбора.

В связи с этим, целью данной работы является проведение исследования САОР (с использованием предложенного в [2] подхода) CRAMM для определения набора характеристик. Это повысит эффективность решения задач в области ИБ.

Метод CRAMM (CCTA Risk Analysis and Management Method, разработчик – Центральное агентство по компьютерам и телекоммуникациям (CCTA – Central Computer and Telecommunications Agency, Великобритания) реализован фирмой Insight Consulting Limited в одноименном программном продукте, в котором предусматривается поэтапный и строгий подход к анализу и оцениванию риска, охватывающий аспекты безопасности как технического (например, ИТ-оборудование и программное обеспечение), так и нетехнического характера (например, физического и человеческого) [4]. В дальнейшем будем рассматривать программное инструментальное средство CRAMM, в котором процесс оценивания реализуется в три этапа. На первом – проводится идентификация физических, программных и информационных ресурсов, содержащихся внутри границ системы. Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения. Для данных и ПО выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10. Например, шкала оценки по критерию «Финансовые потери, связанные с восстановлением ресурсов» отображается через следующие значения [1, 4]: 2 балла – менее \$1000; 6 баллов – от \$1000 до \$10 000; 10 баллов – свыше \$100 000 и т.д.

На втором этапе рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. Оценивается зависимость пользовательских сервисов от определенных групп ресурсов и

существующий уровень угроз и уязвимостей, а также вычисляются уровни рисков и анализируются результаты. Ресурсы группируются по типам угроз и уязвимостей. Программное средство CRAMM для каждой группы ресурсов (и каждого из 36 типов угроз) генерирует список запросов, для которых после инициализации данных оценка уровней осуществляется, например, как очень высокий, высокий, средний, низкий, очень низкий (для угрозы), и как высокий, средний и низкий (для уязвимости). Рассмотрим пример запроса для «оценки угрозы»: «Сколько раз за последние три года сотрудники организации пытались получить несанкционированный доступ к хранящейся в ИС информации с использованием прав других пользователей?» Также, для дальнейшей обработки, предлагаются варианты инициализации данных запросу посредством присваивания определенного количества баллов: а) ни разу (0 баллов); ... д) в среднем чаще одного раза в год (30 баллов) и т.д. На основе этой информации рассчитываются уровни рисков (риск определяется как возможность потерь в результате какого-либо действия или события, способного нанести ущерб [1]) в дискретной шкале с градациями от 1 до 7. Программное средство CRAMM объединяет угрозы и уязвимости в матрице риска, а для создания шкал, например, используются данные из табл. 1 (для уровней угроз и уязвимостей).

Таблица 1. Шкалы для уровней угроз и уязвимостей

Шкалы		Описание	Значение
Шкала оценки уровней угрозы (частота возникновения)	оценки угрозы	Инцидент происходит в среднем, не чаще, чем каждые 10 лет	очень низкий
		Инцидент происходит в среднем один раз в 3 года	низкий
		Инцидент происходит в среднем раз в год	средний
		Инцидент происходит в среднем один раз в четыре месяца	высокий
		Инцидент происходит в среднем раз в месяц	очень высокий
Шкала оценки		В случае возникновения инцидента, вероятность развития	низкий

уровня уязвимости (вероятность успешной реализации угрозы)	событий по наихудшему сценарию меньше 0,33	
	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию от 0,33 до 0,66	средний
	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию выше 0,66	высокий
	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию меньше 0,33	низкий

Анализ риска проводится на первом и втором этапах, после чего осуществляется его оценивание. Во время анализа предлагается проставить коэффициенты для каждого ресурса с точки зрения частоты возникновения угрозы и вероятности реализации угрозы, в связи с этим с учетом [2] здесь можно выделить компоненты BC_5 и BC_3 .

Исходя из оценок стоимости ресурсов защищаемой ИС, угроз и уязвимостей, определяются «ожидаемые годовые потери». На рис. 1 приведен пример матрицы оценки ожидаемых потерь [1], где второй столбец слева содержит значения стоимости ресурса, верхняя строка заголовка таблицы – оценку частоты возникновения угрозы в течение года (уровня угрозы), нижняя строка заголовка – оценку вероятности успеха реализации угрозы (уровня уязвимости).

Значения ожидаемых годовых потерь (Annual Loss of Expectancy) переводятся в баллы, показывающие уровень риска, согласно шкалы, представленной на рис. 2 (в этом примере размер потерь приводится в фунтах стерлингах) и далее в соответствии с матрицей (рис. 3) выводится оценка риска. Здесь, с учетом [2], годовые потери можно отразить через компонент BC_6 .

	0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1 1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2 10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3 300000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4 1000000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5 3000000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6 10000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7 30000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8 1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9 3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10 1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

Рис. 1. Матрица ожидаемых годовых потерь

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

Рис. 2. Шкала оценки

Третий этап исследования заключается в поиске адекватных контрмер. Здесь CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Относительно представления КМР для CRAMM (аналогично методике COBRA) можно определить значения: BC_1, BC_2^* . Компонент BC_1 отображается действием, которое привело к нарушению характеристик ИБ, что можно показать на примере «оценки угрозы», а именно BC_{12} = «Несанкционированный доступ» может привести к BC_{21} = «Нарушение конфиденциальности (НК)».

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Рис. 3. Матрица оценки риска

После прохождения всех этапов в результате имеем полное описание ИС. Оценка угроз и уязвимостей осуществляется на основе оценки риска по двум факторам – риск рассматривается как комбинация вероятности реализации угрозы и уязвимости, а также ущерб [1, 4]. В процессе оценивания угрозы и уязвимости все баллы суммируются и полученное значение относительно определенного диапазона, отображает их степень. Например, если сумма баллов для угрозы равна 25, то она определяется как средняя, при этом используемая шкала для степени угрозы следующая: до 9 баллов – очень низкая; от 20 до 29 – средняя; 40 и более – очень высокая. Аналогично для уязвимости. Эта методика подходит для уже существующих систем и малоприменяется на стадиях их разработки, поскольку для качественной оценки риска требуется полное описание ИС компании. После проведенного анализа с учетом [2] составим КМР для данного метода: $\langle BC_1, BC_2^*, BC_3, BC_5, BC_6 \rangle$.

Таким образом, в работе с учетом предложенного в [2] подхода, проведено исследование САОР в виде соответствующего ПО и определен набор базовых

характеристик, наиболее подходящие для решения определенного класса задач ЗИ.

Литература

- [1]. Алексеев А. Управление рисками. Метод CRAMM / А. Алексеев // IT Expert. – Электрон. дан. – М. : ЗАО “ИТ Эксперт”, 2010. – Режим доступа: WorldWideWeb. – URL: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf. – Загл. с экрана (просмотрено 19 декабря 2014).
- [2]. Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Б. Кортежная модель базовых характеристика риска / Вестник КазНТУ – 2015. – №6.
- [3]. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : «МК-Пресс», 2006. – 320с.
- [4]. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ [Электронный ресурс] / И. С. Медведовский // SecurityLab. Электрон. дан. – Мн. : SecurityLab, 2004. – Режим доступа: WorldWideWeb. – URL: <http://www.ixbt.com/cm/informationssystem-risks012004.shtml>.
- [5]. Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA. [Electronic resource] / Security Risk Analysis & Assessment, and ISO 27000 Compliance –Electronic data – Macclesfield : The Leading Security Risk , 2010– Access mode: World Wide Web. – URL: <http://www.riskworld.net/>.

Куламбаева К.К.

НЕКОТОРЫЕ ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Национальный университет обороны имени Первого Президента Республики
Казахстан – Лидера нации, г. Астана, Республика Казахстан

Закон Республики Казахстан «О национальной безопасности Республики Казахстан» гласит «информационная безопасность - состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны» [1]. Следовательно, безопасность определяется как «... положение, при котором не угрожает опасность кому-либо или чему-либо...» [2, 38].

Предлагаем при проведении исследований указанной нами темы рассматривать существующие в отечественной и зарубежной науке определения безопасности, в том числе и данные Викторовым А.Ш. в работе «Введение в социологию безопасности» [3].

В ней автор разбивает определения безопасности на три группы:

- безопасность как отсутствие опасностей (на основе принципа дихотомии, т.е. некое целое, которое состоит из двух противоположных частей, в данном случае, это целое - существование человека);

- безопасность - это определенная деятельность по обеспечению или по предупреждению каких-либо угроз, опасностей (т.е. это деятельностный подход, связанный с уровнем развития общественного производства, благодаря которому и создаются те или иные защитные (предупреждающие) действия;

- безопасность - это осознанная потребность, ценность, интерес, так или иначе связанные с тем или иным целеполаганием.

Для нас актуален вывод Викторова А.Ш. сделанный в данной работе о том, что безопасность всегда связана с определенной исторической практикой обеспечения жизнедеятельности человека или его существования.

Потому как, если любое состояние безопасности есть взаимосвязанное единство тех или иных действий конкретного субъекта, благодаря которому достигается тот или иной результат, то закономерно, что полученные результаты

субъекта будут определять гуманитарную сторону его деятельности по обеспечению информационной безопасности.

Средства и методы деятельности субъекта по обеспечению информационной безопасности это рефлексивные гуманитарные методы и средства: понимание, объяснение, интерпретация сущности потребностей и интересов всех субъектов информационных отношений, а также и субъектов информационных угроз (личности, общества, государства).

А так как общеизвестно, что деятельность имеет в своей структуре ряд компонентов: цель, субъект, объект, процессы, средства, методы и результаты, то исследователям логично рассмотреть в рамках изучения данной темы среди других работ монографию доктора педагогических наук профессора Л.В. Астаховой «Информационная безопасность: герменевтический подход» [4].

Мнение автора во многом схожи с нашим мнением, что деятельность по обеспечению информационной безопасности состояния защищенности субъекта, выражающееся в безопасности информации субъекта и его информационно-психологической безопасности обеспечивают существование, и развитие субъекта как человека, наивысшей ценности государства.

Осуществляется гуманитарная информационно-психологическая безопасность субъекта при оперировании с содержанием информации и с ее формой, создании, передаче, представлении, получении, обработке, хранении информации [4, 5-25.].

Однако в реализации гуманитарных аспектов информационной безопасности имеются проблемы, потому, что деятельности субъекта в стадии своего формирования всегда проходит преобразования: институционализацию, профессионализацию, технологизацию, социализацию.

Астахова Л.В. раскрывает эти преобразования следующим образом: институционализация это формирование системы специализированных учреждений, служб, подразделений в составе различных организаций, ведомств. Профессионализация - формирование профессионального

сообщества и системы профессиональных коммуникаций кадров, определение основных каналов миграции специалистов из смежных отраслей, выработка основных квалификационных требований к профессии, поиска решений в области профессионального образования. Технологизация - формирование технологий и методов деятельности. Социализация - становление и признание значимости отрасли в глазах общественности (появление ученых, которые путем пропаганды и популяризации доносят до внимания общественности актуальность вопросов отрасли) [4, 25-50].

Дорохов В.Э., Моисеев А.В. [5] акцентируют свое внимание на том, насколько реализован нормативно-правовой компонент информационной безопасности, который для нас это является одним из основных гуманитарных аспектов информационной безопасности, так как в нем раскрывается нацеленность на человека и его безопасности.

Авторы считая, что формирование нормативно-правового компонента, начинается с момента осознания обществом необходимости создания особых защитных механизмов от воздействия реальных и потенциальных угроз и опасностей, снижения риска их проявления [5, 106-110] позволяют нам сделать вывод, что регулирование отношений и взаимодействий в сфере информационной безопасности это определение ее приоритетов, целей и направлений.

Немало важны и другие компоненты информационной безопасности – организационный, так как он представлен государственными органами власти и управления, в функциональные задачи и компетенцию которых входят вопросы информационной безопасности, социально-культурный компонент (культура информационной безопасности личности), который необходим для формирования адекватной среды - сферы информационной безопасности.

Шерстюк В.П. [6] раскрывает, что когнитивный компонент информационной безопасности при выработке гуманитарных критериев информационной безопасности, определении ее целей и приоритетов,

представляют собой большую область современного научного поиска потому, что сама природа экономики информационного общества выдвигает сегодня на первое место человека, его личность.

В настоящее время сложилась система подготовки специалистов по защите информации. Развивается система профессиональных коммуникаций. Накоплен значительный объем научной и учебной профильной литературы, что оказывает свое влияние на профессионализацию, потому как процесс институционализации информационной безопасности (ИБ) всегда сопровождался и подкреплялся профессионализацией.

Технологии защиты информации постоянно совершенствуются, что связано с развитием новых информационных технологий (технологическими знаниями, методикой и инструментарием данной деятельности) [7, 101-113].

К их числу относятся организационные и управленческие технологии в сфере информационной безопасности, технологии документационного обеспечения защиты информации, технологии формирования и развития культуры информационной безопасности и др.

Изобретение печатного станка и книгопечатания, электрические средства связи (телефон, телеграф, радио, телевидение), компьютерная техника и технологии, положившие начало экранной, цифровой культуре привело к увеличению скорости передачи информации, а, следовательно - и ускорению процесса распространения информации по миру.

Процесс распространения информации ведет нас к активному исследованию гуманитарных аспектов информационной безопасности, как на содержательном уровне, так и на представительном уровне при создании, передачи, представления, получения, обработки, хранения информации.

Повышение статуса информационной безопасности актуализирует изучение проблем гуманитарных аспектов состояния защищенности информационного пространства, а также вопросов защиты и обеспечения прав, интересов человека и гражданина, общества и государства в информационной

сфере от реальных и потенциальных угроз, что будет темой последующих исследований.

Литература

1 Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан».

2 Ожегов С.И. Словарь русского языка / С.И. Ожегов. - М.: Русский язык, 1986. - 478 с.

3 Викторов А.Ш. Введение в социологию безопасности / А.Ш. Викторов, - М.: Канон, 2008. - 568 с.

4 Астахова Л.В. Информационная безопасность: герменевтический подход: монография / Л.В. Астахова. - М.: РАН, 2010. - 185 с

5 Дорохов В.Э., Моисеев А.В. Обзор нормативно-правовых актов Российской Федерации в области информационной безопасности // Безопасность информационных технологий, 2013. - № 3. - С. 106-110.

6 Шерстюк В.П. МГУ: научные исследования в области информационной безопасности / В.П. Шерстюк // Информационное общество. - 2005. - Вып. 1. - С. 48-53.

7 Советов Б.Я. Технологии защиты информации / Советов Б.Я. Информационные технологии: учебник - 6-е изд. - М.: Издательство Юрайт, 2012 - 263 с.

Кулатаев С.А.

РОЛЬ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В СОВРЕМЕННЫХ КОНФЛИКТАХ

Национальный университет обороны имени Первого Президента Республики

Казахстан – Лидера нации, г. Астана, Республика Казахстан

В данной статье проведен анализ некоторых вооруженных конфликтов конца XX – начала XXI века и возрастание роли информационного противоборства в современной войне.

Ключевые слова: *вооруженные конфликты, информационное противоборство, информационная война.*

Войны могут выигрываться на поле боя, а проигрываться в сознании людей. Информационные войны сопровождают всю историю человечества. Сейчас в связи с бурным развитием технических средств передачи информации, информация оперативно доводится до народных масс. И ведется активная борьба с носителями чужих идей и навязывание той, которая выгодна то или иной противоборствующей стороне[1]. Это особенно ярко выражается в вооруженных конфликтах последних десятилетий.

Анализ современных вооруженных конфликтов показывает изменение характера вооруженной борьбы. Вооруженные конфликты конца XX – начала XXI века показывают возрастающую роль информационного противоборства (ИПб). Существует следующие определения информационного противоборства [2]:

1) форма межгосударственного противоборства, предусматривающая целенаправленное использование специально разработанных средств для воздействия на информационный ресурс противостоящей стороны и защиты собственных ресурсов в интересах достижения поставленных политических и военных целей;

2) форма межгосударственного соперничества, реализуемая посредством информационного воздействия на системы управления других государств и их вооруженные силы, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации (СМИ) этих государств для достижения поставленных целей при одновременной защите от аналогичных действий своего информационного пространства.

Рассмотрим роль информационного противоборства в вооруженных конфликтах в рамках данного периода [3]:

В операции «Буря в пустыне» в Ираке 1991 года, вооруженная борьба носила в основном воздушный и наземный характер. *Высокое влияние информационного противоборства в военных действиях.* Коалиционный характер, дезориентация общественного мнения в отдельных государствах и мирового сообщества в целом. В результате полный разгром группировки Ирака в Кувейте.

Военный конфликт НАТО - Югославия 1999 год. Вооруженная борьба носила в основном воздушный характер. *Высокое влияние информационного противоборства в военных действиях.* Широкое использование непрямых, неконтактных и других (в том числе нетрадиционных) форм и способов действий, дальнего огневого и электронного поражения; *активное информационное противоборство; дезориентация общественного мнения в отдельных государствах и мирового сообщества в целом.* Стремление к дезорганизации системы государственного и военного управления; применение новейших высокоэффективных (в том числе основанных на новых физических принципах) систем вооружения и военной техники. Возрастание роли космической разведки. В результате поражение войск Югославии, полная дезорганизация военного и государственного управления

Операция «Несгибаемая свобода» Афганистан. 2002 год. Вооруженная борьба носила наземный и воздушный характер с широким применением сил специальных операций. *Высокое влияние информационного противоборства в военных действиях.* Коалиционный характер. Управление войсками осуществлялось через космос. Возрастание роли космической разведки. В результате вооружённой борьбы основные силы талибов разгромлены.

Операция «Свобода Ираку» 2003 год. Вооруженная борьба носила в основном воздушно-наземный характер, управление войсками осуществлялись через космос. *Высокое влияние информационного противоборства в военных*

действиях. Коалиционный характер. Возрастание роли космической разведки. Широкое использование не прямых, неkontaktных и других (в том числе нетрадиционных) форм и способов действий, дальнего огневого и электронного поражения; *активное информационное противоборство, дезориентация общественного мнения в отдельных государствах и мирового сообщества в целом*; маневренные действия войск (сил) на разрозненных направлениях с широким применением аэромобильных сил, десантов и войск специального назначения. В результате полное поражение вооружённых сил Ирака. Смена политической власти.

Военные действия Российской Федерации на Северном Кавказе (1994-2000 гг.) показали, что помимо чисто военных действий, незаконные воинские формирования (НВФ) активно использовали информационно-психологическое воздействие на население региона и России в целом, на военнослужащих федеральных сил. Были созданы специальные подразделения занимающиеся «психологической войной», имеющие подвижные телевизионные станции, полиграфическое оборудование, активно использовались возможности «Интернета».

Данные подразделения использовали приемы и методы информационного противоборства. С помощью зарубежных спецслужб готовились специалисты «психологической войны». В итоге Россия и ее вооруженные силы были дискредитированы, и перед мировым общественным мнением представлены как агрессоры, в отношении самопровозглашенной Республики Ичкерии.

Но, Россия сделала правильные выводы, о чём свидетельствуют события 2014 года по присоединению Крыма к России, где в Российских средствах массовой информации официально заявлено о том, что присоединение Крымского полуострова и Черноморского флота к России произошло по воле народов, проживающих в Крыму. Эту «операцию» можно назвать самой поучительной, где немаловажную роль сыграли СМИ, в которой информация преподносилась в той форме, в которой нужно было. Общественное мнение

разделено на двое, по сферам влияния той же СМИ, западные СМИ эти события считают не законными и трактуют как захват, а в Российских СМИ, как помощь или спасение народов, проживающих в Крыму.

Результаты анализа данных конфликтов показал, что с помощью сил и средств информационного противоборства, можно достичь преимущества над противником и в дальнейшем обеспечить успех действий своих войск.

При этом, успех применения сил и средств информационного противоборства в военных операциях зависит от своевременности организации и качества проведения подготовительных мероприятий по организации ИПБ.

Вперспективном плане развития ВС РК: «Основные направления строительства и развития Вооруженных Сил Республики Казахстан до 2020 года» указано, что одним из основных усилий должно быть формирование органов управления и подразделений информационного противоборства в Министерстве обороны, видах и родах войск Республики Казахстан[4].

Для достижения этого необходимо выполнить ряд задач:

- совершенствование законодательно-правовой базы в сфере информационного противоборства;
- создание комплексной системы, способной адекватно и своевременно отразить любые виды информационных, кибернетических атак, и вести эффективную информационную борьбу
- подготовку специалистов в области информационного противоборства и обеспечение их современным специальным оборудованием;
- общую подготовку всех пользователей, имеющих доступ, а информации ограниченного доступа;
- в структурных подразделениях всех уровней Вооруженных Сил РК необходимо иметь пресс-службу или представителей пресс-служб, для взаимодействия со СМИ, с целью правильного информирования и исключения фальсификации информации.

Таким образом, можно сделать вывод, что в современной войне недостаточно одержать победу в вооружённой борьбе, а ещё необходимо иметь контроль над информационной средой, информационного превосходства, в противном случае мировое сообщество победителя может представить, как новую угрозу мира, с вытекающими отсюда выводами.

Список использованных источников:

1 <http://psyfactor.org/psyops/infowar7.htm>

2 Информационное противоборство в современных условиях: учебное пособие./ Р.А. Таиров. Астана: Жаркын Ко, 2013.- с.26

3 Вооруженные силы зарубежных государств. Информационно-аналитический сборник. Москва. Военное издательство. 2009. с. 321-324.

4 Учебный материал по дисциплине «Военное строительство и строительство Вооруженных Сил Республики Казахстан». Направления развития ВС РК. Щучинск. 2011. инв. 2170. секр. с. 43

Курымбаев С.Г., Бакей Д.К.

ЗНАЧЕНИЕ ПРИМЕНЕНИЯ ИНФОРМАТИЗАЦИИ НА ТРАНСПОРТЕ

Карагандинский Государственный Университет им.Е.А.Букедова,
г.Караганда, Республика Казахстан

Неотъемлемой частью деятельности транспорта является процесс циркуляции и переработки информации (информационный процесс). Это вызвано тем, что, во-первых, незначительная часть информации на транспорте потребляется в том виде, в котором она поступает извне или вырабатывается внутри системы; во-вторых, большая часть информации подлежит обработке, хранению, передаче, сбору, доведению до пользователя. При этом в роли предмета труда выступает информация (данные). Средствами труда выступают аппаратные и программные средства автоматизации, воздействующие на

объект (предмет) труда. Поэтому информация на транспорте вместе со средствами труда считается частью средств производства, составляющих транспортный процесс.

Информация на предприятие поступает от источников внешней информации или от источников внутренней информации.

Внешняя информация – информация из внешней среды, является приблизительной, не точной, отрывистой, противоречивой, она касается рынка и конкурентов, прогнозов, процентных ставок и цен налоговой политики, политической ситуации, носит вероятностный характер. Для обработки используются экспертные информационные системы. Высшее руководство в основном использует внешнюю информацию.

Внутренняя информация - возникает в самой системе управления и отражает в различные временные интервалы его финансовое положение.

Информация - это сведения являющиеся объектом хранения, передачи и преобразования.

Основная информация используемая на предприятии касается: состояние подвижного состава, расписание перевозок, объема груза, маршрут перевозок.

В настоящее время большое распространение получила передача данных с помощью информационно–вычислительных сетей. Информационно-вычислительные сети представляют динамичную и эффективную отрасль автоматизированной технологии процесса ввода, передачи, обработки и выдачи информации. На данном предприятии информация между отделами передается по локальной сети, в устной форме и документальной письменной.

Доведение информации до пользователя - это преобразование сведений о течении транспортного процесса и сведений, влияющих на ход этого процесса в форму, обеспечивающую оперативное и безошибочное восприятие пользователем и непосредственная выдача сведений. До пользователя информация доводится по: телефону, факсу, Интернету. Информацию пользователь получает и по документам.

Информационная система на транспорте - это, во-первых, совокупность процессов циркуляции и переработки информации и, во-вторых, описание этих процессов. Целью реализации информационной системы на транспорте является повышение эффективности транспортного процесса на базе использования современных компьютеров, распределенной переработки информации, распределенных баз данных, различных информационно-вычислительных сетей, путем обеспечения циркуляции и переработки информации.

Общая структурная схема информационной системы АТП включает комплекс взаимосвязанных автоматизированных рабочих мест: АРМ отдела кадров, АРМ технического отдела, АРМ бухгалтерии, АРМ планового отдела, РМ ремонтной службы, АРМ администратора системы (базы данных).

Внедрение информационной системы в АТП необходимо выполнять в определенной последовательности.

На первой стадии запускаются рабочие места, обеспечивающие систему нормативно – справочной информацией, на второй стадии – текущей (первичной) информацией, на третьей стадии – формирующиеся выходные формы.

При реализации комплексной системы предприятия в первую очередь необходимо запустить АРМ отдела кадров, АРМ технического отдела, поскольку без сведений о подвижном составе, водителях и ремонтных рабочих и другом персонале ни одна из подсистем работать не будет или произойдет сбой в транспортном процессе.

На втором этапе необходимо реализовать подсистемы работы диспетчерской службы, обработки путевой документации, учет топлива. В результате комплексной обработки путевых листов будут формироваться сведения о расходах топлива, отработке водителей (часы) и о пробегах автомобилей.

На третьем этапе возможна реализация рабочих мест бухгалтерии (начисление зарплаты) и планового отдела (формирование форм анализа работы предприятия).

На четвертом этапе, после того как в системе налажен учёт пробегов, можно реализовать АРМ ремонтной зоны (планирование ТО-1 и ТО-2).

Далее предстоит внедрение системы мониторинга и навигации на основе GPS/Глонасс [1].

Высокие темпы роста экономики Казахстана доказывают эффективность построения и реализации собственной модели развития, основанной на долгосрочном планировании. основополагающим документом, провозгласившим долгосрочные приоритеты развития государства в области развития транспортной сферы, является Транспортная стратегия Республики Казахстан до 2015 года. Стратегия определяет приоритетные направления государственной транспортной политики до 2015 года и представляет собой совокупность политико-экономических и организационно-правовых мер, принципов, приоритетов развития транспортных сооружений, то есть транспортной инфраструктуры и транзитной политики, призванных обеспечить комплексность и единство транспортной системы и создать основу для разработки соответствующих отраслевых программ.

В основных принципа Транспортной стратегии отражено и инновационное развитие национальной транспортной системы, которое должно быть, прежде всего, направлено на повышение доступности транспортных услуг и снижение грузоемкости экономики; на внедрение новых технологий, задача которых обеспечивать унификацию транспортных процессов, осуществляемых внутри республики, с процессами глобальной транспортной системы [2].

Роль транспортной отрасли производства в современной экономике очень велика. От ее эффективности зависит эффективность работы других отраслей промышленности, а следовательно, и экономического благосостояния страны.

Транспорт - очень разнообразная отрасль. Все его виды, выполняя главную функцию - обеспечения хозяйственного комплекса страны в грузовых и пассажирских перевозках, вступают между собой и большинством сфер производства во взаимодействие. Это даёт основание рассматривать транспорт как систему, а весь механизм формирования и развития её - в неразрывном единстве со всей экономикой страны.

Современное развитие транспортных предприятий осуществляется на основе больших финансовых вложений для приобретения нового подвижного состава. Но зачастую развитие связано и с возникновением проблем, связанных с управлением предприятием. Возрастает необходимость более грамотного планирования перевозочной деятельности для обеспечения стабильной работы парка, более жесткого контроля за своевременным поступлением денежных средств. Таким образом, перед предприятием встает задача перестроить всю систему управления предприятия, чтобы в результате нового подхода к управлению контроль за расходами и доходами (а соответственно и за себестоимостью и прибылью) был максимально информативен и, самое главное, был оперативным и позволял гибко изменять все имеющиеся недостатки в работе автопредприятия.

Основой формирования нововведений на транспортных предприятиях является анализ того, что представляет собой это предприятие в настоящее время и оценка его потенциала.

Для обеспечения гармоничного и скоординированного развития всех секторов транспортного комплекса, повышения управляемости отдельных его секторов, а также обеспечения оптимального распределения финансовых и материальных ресурсов требуется комплексная информатизация на транспорте.

На основе внедрения современных систем телекоммуникаций и связи необходима модернизация существующей системы управления и контроля на транспорте.

В настоящее время у многих ведомств и организаций возникает необходимость оперативного слежения за местоположением и состоянием подвижных объектов, а также передачи на них оперативной информации.

Информация является решающим фактором который определяет развитие технологии транспортного процесса и ресурсов в целом. Цель реализации информационных технологий на транспорте - это повышение эффективности транспортного процесса на базе использования современных компьютеров распределенной переработки информации, баз данных, различных информационно- вычислительных сетей путем обеспечения циркуляции и переработки информации.

В последние годы настоятельно ставится задача о внедрении новых надежных технических средств, которые позволили бы осуществлять автоматизированный сбор диспетчерской информации с подвижных объектов, а также передавать информацию на объекты [3].

Литература

1. Информационные технологии и средства связи на автомобильном транспорте: Учеб. пособие / А.Э. Горев I СПб. гос. архит.-строит, ун-т. -СПб., 1999.-162 с.
2. О Транспортной стратегии Республики Казахстан до 2015 года. Указ Президента Республики Казахстан от 11 апреля 2006 года N 86
3. Козырев А.А. Информационные технологии в экономике и управлении: Учебник. - 2-е, изд. - СПб.: Изд-во Михайлова В.А., 2001. - 360 с.

Курьязов Д.М., Саттаров А.Б.

МЕТОД ПОСТРОЕНИЯ АЛГЕБРАИЧЕСКОЙ СИСТЕМЫ УРАВНЕНИЙ, ОПИСЫВАЮЩЕЙ S – БЛОК

Ташкентский университет информационных технологий, Ташкент, Узбекистан.

1. Для определения криптостойкости алгоритмов шифрования требуется оценить их известными современными методами криптоанализа. Условием применения методов криптоанализа к алгоритмам шифрования является наличие у криптоаналитика в достаточном объеме необходимого материала (соответствующих открытых и закрытых текстов) и вычислительной мощности (производительность процессора и объем памяти). При отсутствии возможности достичь хотя бы одного из указанных параметров считается, что алгоритм шифрования стойкий к указанному методу криптоанализа. Исходя из этого, одной из актуальных задач в сфере криптоанализа остается вопрос создания нового эффективного метода криптоанализа или усовершенствования уже существующих методов.

В данной статье предложены отдельные решения для формирования системы уравнений для блоков замен (S-блоков) с целью повышения эффективности алгебраического метода криптоанализа блочных симметричных алгоритмов шифрования.

2. Сущность алгебраического метода анализа заключается в построении системы уравнений, описывающей нелинейные преобразования S-блоков, и определении ключа шифрования путем решения полученной системы уравнений [1-6]. Исходя из этого, сложность алгебраического метода анализа сводится к построению и решению системы уравнений.

3. Для построения системы формируются уравнения, связывающие вход и выход блоков замены (обозначим их X и Y соответственно). Для отражения нелинейности выполняемой операции искомые уравнения содержат произведения битов входа и выхода блоков. В формуле (1) представлен один из известных методов формирования уравнений для построения системы уравнений S-блоков, заключающийся в построении всех возможных вариантов уравнений и проверки их на соответствие заданному S-блоку [1-6].

$$\sum a_{ij}x_i x_j \oplus \sum \beta_{ij}y_i y_j \oplus \sum \gamma_{ij}x_i y_j \oplus \sum \delta_{ij}x_i \oplus \sum \varepsilon_{ij}y_i \oplus \eta = 0 \quad (1)$$

где x_i и y_i – соответственно входные и выходные биты S-блока, $\alpha, \beta, \gamma, \delta, \varepsilon, \eta$ – коэффициенты, принимающие значения 0 или 1.

4. Согласно данному методу, для блока замены размером $n \times n$ бит (т.е. число бит на входе и выходе равно n) нужно проверить 2^t уравнений, где t – число одночленов, встречающихся в уравнениях. Параметр t вычисляется по формуле (2).

$$t = C_{2n}^2 + 2n + 1 \quad (2)$$

5. Несмотря на то, что данный метод является очень простым и всегда дает правильный результат, его сложность сильно зависит от размера S-блока. Например, для S-блока (4x4) нужно проверить 2^{37} уравнений, а для S-блока (8x8) – 2^{137} уравнений, что, по сути, невозможно реализовать на практике. Очевидно, что для формирования уравнений, описывающих S-блок, требуется использовать другой метод. Ниже предложен один из методов формирования системы уравнений, описывающих S – блок, который более эффективен, чем вышеуказанный.

Известно, что сложность решения системы уравнений над полем $GF(2)$, зависит от количества уравнений, разреженности системы и степенью её алгебраической нелинейности (\deg). Вне зависимости от того, какой метод был использован для формирования системы уравнений, для криптоанализа имеют важность только линейно независимые уравнения с меньшей степенью нелинейности.

Для произвольного блока замены число линейно независимых уравнений равняется $r \geq t - 2^n$, в силу следующей теоремы [4].

Теорема. Для любого блока замены размером $n \times m$ бит: $F(x_1, \dots, x_n) \rightarrow (y_1, \dots, y_m)$, и для любого подмножества T из t всех возможных одночленов (2^{n+m}), если выполняется условие $t > 2^n$, то существует по меньшей мере $t - 2^n$ линейно независимых уравнений, содержащих одночлены из множества T и выполняющиеся с вероятностью 1.

Допустим, рассматривается вопрос формирования системы уравнений для S-блока (4x4). В соответствии с теоремой, число линейно независимых уравнений для данного S-блока не меньше чем 21.

Из формулы (1) следует, что всевозможные одночлены, встречающиеся в этом уравнении, следующие: $x_4, x_3, x_2, x_1, y_4, y_3, y_2, y_1, x_4x_3, x_4x_2, x_4x_1, x_4y_4, x_4y_3, x_4y_2, x_4y_1, x_3x_2, x_3x_1, x_3y_4, x_3y_3, x_3y_2, x_3y_1, x_2x_1, x_2y_4, x_2y_3, x_2y_2, x_2y_1, x_1y_4, x_1y_3, x_1y_2, x_1y_1, y_4y_3, y_4y_2, y_4y_1, y_3y_2, y_3y_1, y_2y_1$. Из этого списка видно, что существуют 26 выходных одночленов (т.е. y_i, y_iy_j, x_iy_j), которые определяются входящими значениями S-блока (т.е. x_4, x_3, x_2, x_1). Очевидно, что количество уравнений со степенью $deg \leq 2$, описывающих любой S-блок (4x4), не больше чем 26. Выражая все 26 выходных одночленов в виде булевых функций (т.е.: $y_4=f_1, y_3=f_2, y_2=f_3, y_1=f_4, x_4y_4=f_5, x_4y_3=f_6, x_4y_2=f_7, x_4y_1=f_8, x_3y_4=f_9, x_3y_3=f_{10}, x_3y_2=f_{11}, x_3y_1=f_{12}, x_2y_4=f_{13}, x_2y_3=f_{14}, x_2y_2=f_{15}, x_2y_1=f_{16}, x_1y_4=f_{17}, x_1y_3=f_{18}, x_1y_2=f_{19}, x_1y_1=f_{20}, y_4y_3=f_{21}, y_4y_2=f_{22}, y_4y_1=f_{23}, y_3y_2=f_{24}, y_3y_1=f_{25}, y_2y_1=f_{26}$), можно составить уравнения (АНФ) для этих функций, с помощью их таблиц истинности. Для всех этих уравнений удовлетворяется условие $deg \leq 4$. Используя эти уравнения, можно сформировать уравнения, удовлетворяющие условию $deg \leq 2$.

Рассмотрим данное преобразование более подробно.

Известно, что в составе уравнения со степенью $deg=4$, существует только один одночлен вида " $x_4x_3x_2x_1$ ". В составе уравнения со степенью $deg=3$, могут существовать одночлены " $x_4x_3x_2$ ", " $x_4x_3x_1$ ", " $x_4x_2x_1$ " или " $x_3x_2x_1$ ". Допустим, для n ($n>1$) уравнений удовлетворяется $deg(f_{1,2,\dots,n})=4$. Выбрав любое одно из этих уравнений (назовем его *образующим*), осуществим его сложение со всеми остальными по модулю два (\oplus). В итоге образуется $n-1$ уравнений, удовлетворяющих $deg \leq 3$.

Далее, используя комбинации $(f_i \oplus f_j)$ из оставшихся уравнений, можно сформировать или выбрать четыре таких уравнений (следующие *образующие*), в составе которых будут присутствовать по одному одночлену третьей степени, которые будут отличаться друг от друга. При помощи образующих уравнений

третьей степени можно сформировать уравнения, удовлетворяющие $deg \leq 2$. Для этого, соответствующие оставшиеся уравнения (не образующие) складываются по модулю два с образующими, чем достигается сокращение одночленов третьей степени.

Следовательно, после этих двух этапов снижения степени уравнений для S-блока (4x4) можно составить по меньшей мере 21 линейно независимое уравнение, удовлетворяющее $deg \leq 2$.

Используя предложенный метод, можно сформировать системы уравнений с минимальной алгебраической степенью для S-блоков произвольного размера.

Ниже приведен пример формирования системы уравнений для S-блока.

1-таблица. S-блок (4x4).

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Y	7	12	15	4	6	10	8	2	1	14	3	0	11	5	9	13

2-таблица. Таблица истинности S-блока(4x4).

Вход				Выход	f ₅	f ₆	f ₇	f ₈	f ₉	f ₁₀	f ₁₁	f ₁₂	f ₁₃	f ₁₄	f ₁₅	f ₁₆	f ₁₇	f ₁₈	f ₁₉	f ₂₀	f ₂₁	f ₂₂	f ₂₃	f ₂₄	f ₂₅	f ₂₆	
x	x	x	x	ffff																							
4	3	2	1	уууу	x ₄ y ₄	x ₄ y ₃	x ₄ y ₂	x ₄ y ₁	x ₃ y ₄	x ₃ y ₃	x ₃ y ₂	x ₃ y ₁	x ₂ y ₄	x ₂ y ₃	x ₂ y ₂	x ₂ y ₁	x ₁ y ₄	x ₁ y ₃	x ₁ y ₂	x ₁ y ₁	y ₄ y ₃	y ₄ y ₂	y ₄ y ₁	y ₃ y ₂	y ₃ y ₁	y ₂ y ₁	
0	0	0	0	0111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	
0	0	0	1	1100	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	
... ..																											
1	1	1	0	1001	1	1	0	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0
1	1	1	1	1101	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1	1	0	1	0	1	0	0

Первоначально составленные уравнения:

1. $f_1: y_4 \oplus x_1 \oplus x_2 \oplus x_4 x_2 \oplus x_4 x_3 \oplus x_4 x_2 x_1 = 0,$
2. $f_2: y_3 \oplus x_3 x_1 \oplus x_3 x_2 \oplus x_3 x_2 x_1 \oplus x_4 \oplus x_4 x_1 \oplus x_4 x_2 x_1 \oplus x_4 x_3 x_1 \oplus x_4 x_3 x_2 \oplus 1 = 0,$

3. $f_3: \mathbf{y}_2 \oplus x_1 \oplus x_3 x_1 \oplus x_3 x_2 \oplus x_3 x_2 x_1 \oplus x_4 \oplus x_2 x_4 \oplus x_4 x_3 \oplus x_4 x_3 x_1 \oplus x_4 x_3 x_2 \oplus 1 = 0,$
4. $f_4: \mathbf{y}_1 \oplus x_1 \oplus x_3 \oplus x_3 x_1 \oplus x_4 x_3 \oplus 1 = 0,$
5. $f_5: \mathbf{x}_4 \mathbf{y}_4 \oplus x_4 x_1 \oplus x_4 x_2 x_1 \oplus x_4 x_3 = 0,$
6. $f_6: \mathbf{x}_4 \mathbf{y}_3 \oplus x_4 x_1 \oplus x_4 x_2 x_1 \oplus x_4 x_3 x_2 x_1 = 0,$
7. $f_7: \mathbf{x}_4 \mathbf{y}_2 \oplus x_4 x_1 \oplus x_4 x_2 \oplus x_4 x_3 \oplus x_4 x_3 x_2 x_1 = 0,$
8. $f_8: \mathbf{x}_4 \mathbf{y}_1 \oplus x_4 \oplus x_4 x_1 \oplus x_4 x_3 x_1 = 0,$
9. $f_9: \mathbf{x}_3 \mathbf{y}_4 \oplus x_3 x_1 \oplus x_3 x_2 \oplus x_4 x_3 \oplus x_4 x_3 x_2 \oplus x_4 x_3 x_2 x_1 = 0,$
10. $f_{10}: \mathbf{x}_3 \mathbf{y}_3 \oplus x_3 \oplus x_3 x_1 \oplus x_3 x_2 \oplus x_3 x_2 x_1 \oplus x_4 x_3 \oplus x_4 x_3 x_2 \oplus x_4 x_3 x_2 x_1 = 0,$
11. $f_{11}: \mathbf{x}_3 \mathbf{y}_2 \oplus x_3 \oplus x_3 x_2 \oplus x_3 x_2 x_1 \oplus x_4 x_3 x_1 = 0,$
12. $f_{12}: \mathbf{x}_3 \mathbf{y}_1 \oplus x_4 x_3 = 0,$
13. $f_{13}: \mathbf{x}_2 \mathbf{y}_4 \oplus x_2 \oplus x_2 x_1 \oplus x_4 x_2 \oplus x_4 x_2 x_1 \oplus x_4 x_3 x_2 = 0,$
14. $f_{14}: \mathbf{x}_2 \mathbf{y}_3 \oplus x_2 \oplus x_3 x_2 \oplus x_4 x_2 \oplus x_4 x_3 x_2 \oplus x_4 x_3 x_2 x_1 = 0,$
15. $f_{15}: \mathbf{x}_2 \mathbf{y}_2 \oplus x_2 \oplus x_2 x_1 \oplus x_3 x_2 \oplus x_4 x_3 x_2 x_1 = 0,$
16. $f_{16}: \mathbf{x}_2 \mathbf{y}_1 \oplus x_2 \oplus x_2 x_1 \oplus x_3 x_2 \oplus x_3 x_2 x_1 \oplus x_4 x_3 x_2 = 0,$
17. $f_{17}: \mathbf{x}_1 \mathbf{y}_4 \oplus x_1 \oplus x_2 x_1 \oplus x_4 x_3 x_1 = 0,$
18. $f_{18}: \mathbf{x}_1 \mathbf{y}_3 \oplus x_1 \oplus x_3 x_1 \oplus x_4 x_2 x_1 \oplus x_4 x_3 x_1 \oplus x_4 x_3 x_2 x_1 = 0,$
19. $f_{19}: \mathbf{x}_1 \mathbf{y}_2 \oplus x_3 x_1 \oplus x_4 x_1 \oplus x_4 x_2 x_1 \oplus x_4 x_3 x_2 x_1 = 0,$
20. $f_{20}: \mathbf{x}_1 \mathbf{y}_1 \oplus x_4 x_3 x_1 = 0,$
21. $f_{21}: \mathbf{y}_4 \mathbf{y}_3 \oplus x_1 \oplus x_2 \oplus x_3 x_1 \oplus x_3 x_2 \oplus x_4 x_2 \oplus x_4 x_2 x_1 \oplus x_4 x_3 x_2 = 0,$
22. $f_{22}: \mathbf{y}_4 \mathbf{y}_2 \oplus x_2 \oplus x_2 x_1 \oplus x_3 x_1 \oplus x_3 x_2 \oplus x_4 x_1 \oplus x_4 x_2 \oplus x_4 x_3 \oplus x_4 x_3 x_1 = 0,$
23. $f_{23}: \mathbf{y}_4 \mathbf{y}_1 \oplus x_2 \oplus x_2 x_1 \oplus x_3 x_2 \oplus x_3 x_2 x_1 \oplus x_4 x_2 \oplus x_4 x_2 x_1 \oplus x_4 x_3 \oplus x_4 x_3 x_1 \oplus x_4 x_3 x_2 = 0,$
24. $f_{24}: \mathbf{y}_3 \mathbf{y}_2 \oplus x_1 \oplus x_3 x_2 \oplus x_3 x_2 x_1 \oplus x_4 \oplus x_4 x_2 x_1 \oplus x_4 x_3 x_1 \oplus x_4 x_3 x_2 \oplus 1 = 0,$
25. $f_{25}: \mathbf{y}_3 \mathbf{y}_1 \oplus x_1 \oplus x_3 \oplus x_3 x_1 \oplus x_4 \oplus x_4 x_1 \oplus x_4 x_3 \oplus 1 = 0,$
26. $f_{26}: \mathbf{y}_2 \mathbf{y}_1 \oplus x_1 \oplus x_3 \oplus x_3 x_1 \oplus x_4 \oplus x_4 x_1 \oplus x_4 x_2 \oplus x_4 x_2 x_1 \oplus 1 = 0.$

После этапов снижения степени уравнений:

Образующие уравнения: $\mathbf{g}_0 = f_6$; $\mathbf{g}_1 = f_1$; $\mathbf{g}_2 = f_8$; $\mathbf{g}_3 = f_1 \oplus f_{13}$; $\mathbf{g}_4 = f_8 \oplus f_{11}$.

1. $f_2 \oplus \mathbf{g}_1 \oplus \mathbf{g}_2 \oplus \mathbf{g}_3 \oplus \mathbf{g}_4: \mathbf{y}_3 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_3 \mathbf{y}_2 \oplus x_3 \oplus x_2 x_1 \oplus x_2 \oplus x_4 x_2 \oplus x_3 x_1 \oplus x_4 \oplus x_4 x_1 \oplus 1 = 0,$

2. $f_3 \oplus g_2 \oplus g_3 \oplus g_4: \mathbf{y}_2 \oplus \mathbf{y}_4 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_3 \mathbf{y}_2 \oplus \mathbf{x}_3 \oplus \mathbf{x}_2 \mathbf{x}_1 \oplus \mathbf{x}_4 \oplus \mathbf{x}_3 \mathbf{x}_1 \oplus \mathbf{x}_4 \mathbf{x}_2 \oplus 1=0,$
3. $f_4: \mathbf{y}_1 \oplus \mathbf{x}_1 \oplus \mathbf{x}_3 \oplus \mathbf{x}_3 \mathbf{x}_1 \oplus \mathbf{x}_4 \mathbf{x}_3 \oplus 1=0,$
4. $f_5 \oplus g_1: \mathbf{x}_4 \mathbf{y}_4 \oplus \mathbf{y}_4 \oplus \mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_1=0,$
5. $f_7 \oplus g_0 \oplus g_1: \mathbf{x}_4 \mathbf{y}_2 \oplus \mathbf{x}_4 \mathbf{y}_3 \oplus \mathbf{y}_4 \oplus \mathbf{x}_1 \oplus \mathbf{x}_2=0,$
6. $f_9 \oplus g_0 \oplus g_1 \oplus g_3: \mathbf{x}_3 \mathbf{y}_4 \oplus \mathbf{x}_4 \mathbf{y}_3 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_2 \mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_3=0,$
7. $f_{10} \oplus g_0 \oplus g_1 \oplus g_3 \oplus g_4: \mathbf{x}_3 \mathbf{y}_3 \oplus \mathbf{x}_4 \mathbf{y}_3 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_4 \mathbf{y}_1 \oplus \mathbf{x}_3 \mathbf{y}_2 \oplus \mathbf{x}_4 \oplus \mathbf{x}_2 \mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_2 \oplus \mathbf{x}_3 \mathbf{x}_1 \oplus \mathbf{x}_4 \mathbf{x}_3=0,$
8. $f_{12}: \mathbf{x}_3 \mathbf{y}_1 \oplus \mathbf{x}_4 \mathbf{x}_3=0,$
9. $f_{14} \oplus g_0 \oplus g_1 \oplus g_3: \mathbf{x}_2 \mathbf{y}_3 \oplus \mathbf{x}_4 \mathbf{y}_3 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_2 \mathbf{x}_1 \oplus \mathbf{x}_4 \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_2=0,$
10. $f_{15} \oplus g_0 \oplus g_1: \mathbf{x}_2 \mathbf{y}_2 \oplus \mathbf{x}_4 \mathbf{y}_3 \oplus \mathbf{y}_4 \oplus \mathbf{x}_1 \oplus \mathbf{x}_4 \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_3 \oplus \mathbf{x}_4 \mathbf{x}_1 \oplus \mathbf{x}_2 \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_2=0,$
11. $f_{16} \oplus g_3 \oplus g_4: \mathbf{x}_2 \mathbf{y}_1 \oplus \mathbf{y}_4 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_4 \mathbf{y}_1 \oplus \mathbf{x}_3 \mathbf{y}_2 \oplus \mathbf{x}_3 \oplus \mathbf{x}_4 \oplus \mathbf{x}_4 \mathbf{x}_1 \oplus \mathbf{x}_1 \oplus \mathbf{x}_4 \mathbf{x}_3 \oplus \mathbf{x}_2=0,$
12. $f_{17} \oplus g_2: \mathbf{x}_1 \mathbf{y}_4 \oplus \mathbf{x}_4 \mathbf{y}_1 \oplus \mathbf{x}_4 \oplus \mathbf{x}_4 \mathbf{x}_1 \oplus \mathbf{x}_1 \oplus \mathbf{x}_2 \mathbf{x}_1=0,$
13. $f_{18} \oplus g_0 \oplus g_2: \mathbf{x}_1 \mathbf{y}_3 \oplus \mathbf{x}_4 \mathbf{y}_3 \oplus \mathbf{x}_4 \mathbf{y}_1 \oplus \mathbf{x}_4 \oplus \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_1=0,$
14. $f_{19} \oplus g_0: \mathbf{x}_1 \mathbf{y}_2 \oplus \mathbf{x}_4 \mathbf{y}_3 \oplus \mathbf{x}_3 \mathbf{x}_1=0,$
15. $f_{20} \oplus g_2: \mathbf{x}_1 \mathbf{y}_1 \oplus \mathbf{x}_4 \mathbf{y}_1 \oplus \mathbf{x}_4 \oplus \mathbf{x}_4 \mathbf{x}_1=0,$
16. $f_{21} \oplus g_1 \oplus g_3: \mathbf{y}_4 \mathbf{y}_3 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_2 \mathbf{x}_1 \oplus \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_2=0,$
17. $f_{22} \oplus g_2: \mathbf{y}_4 \mathbf{y}_2 \oplus \mathbf{x}_4 \mathbf{y}_1 \oplus \mathbf{x}_4 \oplus \mathbf{x}_2 \oplus \mathbf{x}_2 \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_1 \oplus \mathbf{x}_3 \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_3=0,$
18. $f_{23} \oplus g_1 \oplus g_2 \oplus g_3 \oplus g_4: \mathbf{y}_4 \mathbf{y}_1 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_3 \mathbf{y}_2 \oplus \mathbf{x}_3 \oplus \mathbf{x}_4 \mathbf{x}_3=0,$
19. $f_{24} \oplus g_1 \oplus g_2 \oplus g_3 \oplus g_4: \mathbf{y}_3 \mathbf{y}_2 \oplus \mathbf{x}_2 \mathbf{y}_4 \oplus \mathbf{x}_3 \mathbf{y}_2 \oplus \mathbf{x}_3 \oplus \mathbf{x}_4 \oplus \mathbf{x}_2 \mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_2 \oplus \mathbf{x}_1 \oplus 1=0,$
20. $f_{25}: \mathbf{y}_3 \mathbf{y}_1 \oplus \mathbf{x}_1 \oplus \mathbf{x}_3 \oplus \mathbf{x}_3 \mathbf{x}_1 \oplus \mathbf{x}_4 \oplus \mathbf{x}_4 \mathbf{x}_1 \oplus \mathbf{x}_4 \mathbf{x}_3 \oplus 1=0,$
21. $f_{26} \oplus g_1: \mathbf{y}_2 \mathbf{y}_1 \oplus \mathbf{y}_4 \oplus \mathbf{x}_2 \oplus \mathbf{x}_4 \mathbf{x}_3 \oplus \mathbf{x}_3 \oplus \mathbf{x}_3 \mathbf{x}_1 \oplus \mathbf{x}_4 \oplus \mathbf{x}_4 \mathbf{x}_1 \oplus 1=0.$

При анализе приведенного выше 21 уравнения видно, что все они линейно независимые и для всех удовлетворяется $deg=2$.

Приведенный в данной статье метод построения алгебраической системы уравнений может быть использован как одно из средств для повышения

эффективности применения алгебраического метода криптоанализа к блочным симметричным алгоритмам шифрования.

Литература

1. **Courtois N., Pieprzyk J.** Cryptanalysis of block ciphers with overdefined systems of equations // ASIACRYPT, 2002. – P. 267-287.

2. **Бабенко Л.К., Ищукова Е.А.** Анализ симметричных криптосистем // Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 136-147.

3. **Бабенко Л.К., Маро Е.А.** Алгебраический криптоанализ упрощенного алгоритма шифрования Rijndael // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 187-199.

4. **Бабенко Л.К., Маро Е.А.** Анализ стойкости блочных алгоритмов шифрования к алгебраическим атакам // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 110-119.

5. **Грушо А.А., Тимонина Е.Е., Применко Э.А.** Анализ и синтез криптоалгоритмов. Курс лекций. – Йошкар-Ола: Изд-во МФ МОСУ, 2000. +5+

6. **Маро Е.А.** Разработка и исследование алгоритмов алгебраического криптоанализа // Материалы I Всероссийской молодежной конференции по проблемам информационной безопасности ПЕРСПЕКТИВА – 2009. – Таганрог: Изд-во ТТИ ЮФУ, 2009. – С. 259 – 265.

Лившиц И.И.

ФОРМИРОВАНИЕ КОНЦЕПЦИИ МГНОВЕННЫХ АУДИТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ООО «Газинформсервис», Санкт-Петербург, Российская Федерация

Введение. Проблема выполнения аудитов (как процесс оценки) для больших и/или сложных систем рассматривалась в классических трудах Н. Винера, Р. Кини, Х. Райфа, И. Пригожина [1 – 3]. В настоящее время представлены

различные материалы по актуальной проблеме противодействия угрозам «нулевого дня» (“zero-day”). В частности отмечается, что «любые процессы, управляемые людьми, ненадёжны», поэтому крупнейшие поставщики средств ИБ предлагают «единственный» вариант – только постоянное совершенствование технических средств защиты информации (СрЗИ), в частности, Check Point Threat Emulation и Qualys Continuous Monitoring [4 – 6]. Подобная оценка представляется коммерчески выгодной, но весьма далекой от решения хорошо известной технической проблемы – противостояния СрЗИ как «брони» и угроз – как «снаряда».

Очевидно, что «гонка вооружения» между целевыми (таргетированными) атаками (“advanced persistent threats”, АТР) не приведет в ближайшем времени к повышению уровня защищенности объектов, и это отмечается многими экспертами [8 – 9]. В этой ситуации предлагается применять не только технический подход (СрЗИ) для противодействия угрозам «нулевого дня», но предложить комбинированный метод, основанный на концепции мгновенных аудитов ИБ. Методической базой концепции мгновенных аудитов является семейство стандартов ISO серии 27001, дополненное множеством (расширяемым) метрик ИБ для формирования количественной оценки уровня защищенности объекта [7]. Для формирования концепции мгновенных аудитов ИБ, как средства противодействия АТР, представляется полезным применить известное математическое понятие предела функции, точнее, предела слева, которое позволит формировать количественные оценки защищенности в процессе выполнения аудитов ИБ.

Постановка задачи. Реализация требований ИБ в предлагаемой концепции дополняется еще одним важным параметром – требуемой частотой выполнения аудитов с целью максимального повышения осведомленности и скорости принятия адекватных решений об уязвимостях, которые могут быть использованы злоумышленниками для реализации АТР, об объективной оценке текущего уровня обеспечения ИБ. В этих условиях постановка задачи

формулируется следующим образом – разработка концепции мгновенных аудитов ИБ на методической базе риск-ориентированных стандартов ISO, с целью обеспечения комплексного подхода для оценивания защищенности ценных для бизнеса объектов с любой требуемой частотой.

Обоснование практической ценности мгновенных аудитов. Практическая ценность предлагаемой концепции мгновенных аудитов основана на известных фактах, что порядка 96% успешных взломов можно было бы избежать, если бы был внедрен ряд простых мер ИБ, а более 75% атак использовали уже известные уязвимости, которые могли бы быть «закрыты» регулярными патчами безопасности [4 – 6]. При этом отмечается, что 85% реально произошедших вторжений были обнаружены спустя месяцы (среднее время обнаружения – 5 месяцев) [4 – 6].

В качестве мер противодействия угрозам «нулевого дня» в настоящее время применяются различные подходы, направленные, в основном, на пресечение последствий потенциально возможных угроз, но не на выявление и устранение уязвимостей, например:

1. «Песочницы», имитирующие рабочие станции организации,
2. Анализ аномальной сетевой активности,
3. Поведенческий анализ рабочих станций.

Соответственно, для атак «нулевого дня» (реакция на которые крайне критична по времени) указанные выше примеры дают известный эффект только при постоянном наращивании вычислительных ресурсов для сокращения времени «аналитических» проверок СрЗИ в режиме, близком к режиму реального времени. При этом не инициируется объективный анализ всей совокупности потенциальных уязвимостей и не затрагивается уровень технологических, программных и иных уязвимостей [8, 9].

Важным преимуществом предложенной концепции является акцентирование именно на получении численных оценок, а не простого «соответствия» или «несоответствия». Именно периодическое систематическое

получение измеримых численных оценок ИБ, представляется практически полезным для лиц, принимающих решение (ЛПР).

Концепция мгновенных аудитов СМИБ. Концепция мгновенных аудитов предполагает реализацию принципа выполнения аудитов ИБ с частотой, определяемой высшим менеджментом (ЛПР) и зависящей от предыдущего состояния «слева» уровня защищенности объекта [8, 9]. Иными словами, если предыдущий Аудит_1 ИБ, проведенный, предположим, месяц назад (отметка t_0) выявил ряд несоответствий (в терминах [7]) и показал, что 40% компьютеров по-прежнему работают под Windows XP с SP2, на 60% рабочих станций пользователи обладают правами администратора, на 70% ноутбуков обновление антивируса не выполняются и/или отключены, то оценка (отметка t_1) текущего уровня защищенности $R_{base} | t_1 \leq R_{base} | t_0$, т.е. не выше предыдущей (см. рис. 1).

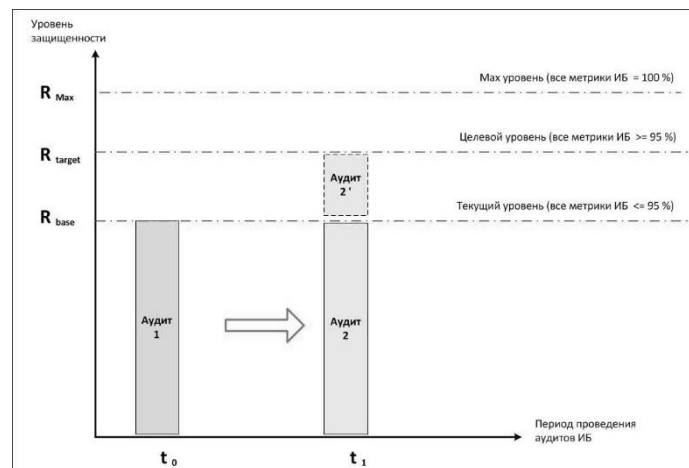


Рис. 1. Оценка достижения уровней защищенности

Обоснование математической базы концепции мгновенных аудитов. Для формирования оценки защищенности по результатам аудитов ИБ необходимо применять достоверные математические понятия, дающие обоснование предложенной концепции, в частности одностороннего предела (точнее, предела функции слева).

$$\lim_{\Delta x \rightarrow 0} = \frac{f(x + \Delta x) - f(x)}{\Delta x} = \lim \frac{d}{dx} f(x) = f'(x)$$

Соответствующий односторонний предел называют левой производной, обозначают $f'_-(x)$ [10]. Левая производная позволяет оценить требуемый интервал, на котором допустимо (по времени) могут быть выполнены необходимые изменения в СМИБ и обосновано проведение нового аудита ИБ. Для цели противодействия угрозам «нулевого дня» рассмотрим действительную функцию переменных:

$$y = f(x_1, x_2, x_3, \dots, x_n)$$

где, например, первые 4 переменные описывают атрибуты аудитов ИБ:

x_1 – частота проведения аудитов, определяемая как отношение кол-ва аудитов в СМИБ к наблюдаемому периоду;

x_2 – объем программы аудитов, определяемый как отношение кол-ва охваченных процессов к общему кол-ву процессов в заявленной области сертификации СМИБ;

x_3 – метрика достижения уровня защищенности, определяемая как мера результативности СМИБ $R_{\text{base}} / R_{\text{Max}}$;

x_4 – метрика выполнения корректирующих действий, запланированных на интервал проведения аудитов ИБ.

Для одной изменяемой переменной x_1 (например, частоты проведения аудитов ИБ) оценим практическое значение частной производной (при неизменности иных переменных), получаем оценку скорости роста уровня защищенности СМИБ:

$$\frac{\partial}{\partial x_1} = f'_{x_1}(x_1, x_2, x_3, \dots, x_n) = \frac{\Delta R_k}{\Delta t k}$$

Реализация концепции мгновенных аудитов для оценки защищенности ценных для бизнеса активов с любой требуемой частотой, может быть продемонстрирована как сокращение периода (увеличение частоты) проведения аудитов ИБ при использовании предела слева функции переменных. При этом объективно повышается способность системы (СМИБ или ИСМ) эффективно

противодействовать угрозам «нулевого дня» в режиме, близком к режиму реального времени. В примере для одной переменной x_1 продемонстрировано увеличение скорости роста уровня защищенности СМИБ $\frac{\Delta R_k}{\Delta t k}$ при известных переменных процесса аудитов ИБ (см. рис. 2).

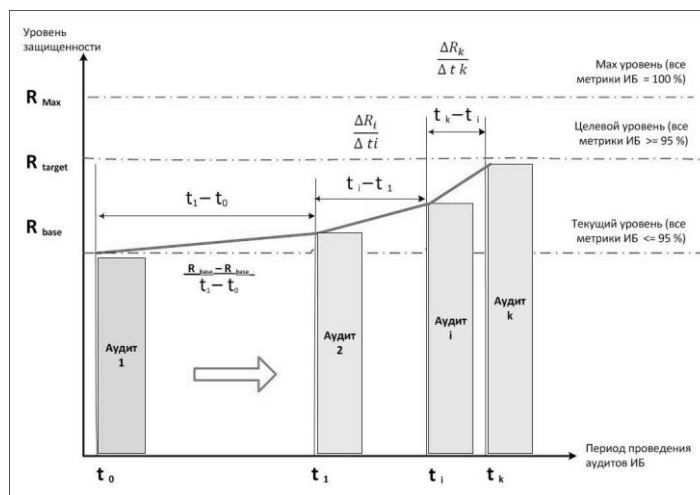


Рис. 2. Пример увеличения скорости роста уровня защищенности

Литература

1. Винер Н. Кибернетика, или управление и связь в животном и машине. – 2-е издание. – М.: Наука; Главная редакция изданий для зарубежных стран, 1983. – 344 с.
2. Р.Л. Кини, Х. Райфа. Принятие решений при многих критериях: Предпочтения и замещения: Пер. с англ./ Под ред. И.Ф. Шехнова. – М.: Радио и Связь. 1981. – 560 с.
3. Пригожин И., Стенгерс И. Время. Хаос. Квант. К решению парадокса времени. М.: Едиториал УРСС, 2003. – 240 с.
4. Сотников Павел. Защита Информации 2.0, непрерывный аудит безопасности Qualys <http://www.infosecurityrussia.ru/2013/expo/qualys> (дата обращения 07.07.2015)
5. An Osterman Research White Paper «Dealing with Data Breaches and Data Loss Prevention», Published March 2015, Osterman Research, Inc.

6. *Wall Street Journal*, 9/18/14 “Chinese Hacked U.S. Military Contractors, Senate Panel Say”, опубликовано <http://www.slideshare.net/SelectedPresentations/08-smorodinsky>, дата обращения 23.03.2015
7. Information technology – Security techniques – Information security management systems – Requirements: ISO/IEC 27001:2013, International Organization for Standardization, 2013. – 23 pages.
8. *Лившиц И.И.* Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI и ISO // Информатизация и Связь, 2013, вып. 6; с. 62 – 67;
9. *Лившиц И.И.* Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества, 2013, вып. 1; с. 22 – 34;
10. *Г. Корн, Т. Корн*, Справочник по математике для научных работников и инженеров, М.: Наука, 1978. — 832 с.

Лившиц И.И., Танатарова А.Т.

**ПОВЫШЕНИЕ УРОВНЯ ОБЕСПЕЧЕНИЯ ИБ ПРИ ВНЕДРЕНИИ СМИБ
В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ГОСТ Р ИСО/МЭК 27001**

ООО «Газинформсервис», Санкт-Петербург, Российская Федерация;

НЭУ им. Т. Рыскулова, Алматы, Республика Казахстан

Введение. Актуальность проблемы повышения уровня ИБ является закономерным следствием увеличения количества и серьезности последствий угроз (внешних и внутренних) для защищаемых активов, а также постоянным ростом сложности требований, в том числе соответствия комплексу требований «регуляторов». Для решения поставленной проблемы для высшего руководства организации рекомендуется в качестве оптимального способа обеспечения безопасности бизнес-процессов рассматриваться внедрение систем

менеджмента информационной безопасности (СМИБ). При оценке результативности СМИБ должны быть приняты во внимание требования стандартов ГОСТ Р ИСО/МЭК 27001 и отраслевых стандартов.

Статистика сертификации СМИБ. Традиционно высокий рейтинг в мире стандартов ISO/IEC серии 27000 отмечается в ежегодных отчетах ISO. Из данных отчета «The ISO Survey of Management System Standard Certifications – 2013» (октябрь 2014 г.), следует, что в мире насчитывалось свыше 22.000 сертификатов, выданных органами по сертификации на соответствие требованиям ISO/IEC 27001:2005. Динамика прироста сертификатов по сравнению с предыдущим годом составляет 14% (см. рис.1). Стандарт ISO 27001 несколько лет подряд демонстрирует двузначный стабильный рост. Соответственно, высший менеджмент решает проблему обеспечения безопасности либо внедрением СМИБ по «целевому» стандарту ISO 27001 как отдельно, так и составе ИСМ.

Standard	number of certificates in 2013	number of certificates in 2012	evolution	evolution in %
ISO 9001	1 129 446	1 096 987	32 459	3 %
ISO 14001	301 647	284 654	16 993	6 %
ISO 50001	4 826	2 236	2 590	116 %
ISO 27001	22 293	19 620	2 673	14 %
ISO 22000	26 847	23 278	3 569	15 %
ISO/TS 16949	53 723	50 071	3 652	7 %
ISO 13485	25 666	22 317	3 349	15 %
TOTAL	1 564 448	1 499 163	65 285	4 %

Рис. 1 Динамика сертификации в мире по стандартам ISO

Предпосылки для разработки и внедрения СМИБ. В соответствии с требованиями стандарта ISO 27001 в СМИБ должен реализовываться цикл постоянного улучшения PDCA (в новой версии 2013 г. п. 10.2) и выполняться анализ со стороны руководства на периодической основе (в новой версии 2013 г. п. 9.3). Этот принцип постоянного улучшения (известный также как принцип Деминга) наилучшим образом способствует адекватной реакции на изменение экономической ситуации и отражения политики СМИБ, целей в области ИБ и

менеджмента рисков применительно к выбранным значимым (существенным для бизнеса) активам СМИБ.

Проблема оценки результативности СМИБ в соответствии с требованиями стандартов ГОСТ Р ИСО/МЭК серии 27001 является достаточно известной, особенно для СМИБ, созданных с учетом дополнительных отраслевых стандартов. В случае, когда высшее руководство организации принимает решение о внедрении (сертификации) СМИБ, представляется необходимым выработать решение о комплексе мероприятий, которые следует предпринять для целей обеспечения соответствия СМИБ требованиям стандарта ISO. Одним из важнейших требований, включенных в цикл PDCA, является требование постоянного повышения результативности. Эти достоверные оценки должны быть представлены высшему руководству для принятия адекватных управленческих решений. Для реализации управляемых условий данного процесса в СМИБ предлагается несколько примеров расчета результативности СМИБ, прошедших практическую апробацию.

Расчет результативности СМИБ. Для расчета результативности СМИБ можно рекомендовать к применению формулы, учитывающие отдельно события ИБ и инциденты ИБ. В этом варианте особую роль приобретает техническая оснащенность службы безопасности, позволяющая «селектировать» из многих тысяч событий в режиме, близком к режиму реального времени. На этапе проектирования СМИБ эти вопросы должны рассматриваться при определении области распространения (*scope*). Соответственно, результативность СМИБ рассчитывается следующим образом:

Расчет результативности событий ИБ:

$$K_c = \left(1 - \left(\frac{C_{тек.}}{C_{max}} \right) \right) * 100\% \quad (1)$$

Где:

K_c – коэффициент результативности по идентификации событий ИБ;

Стек – идентифицированное количество событий ИБ в конфигурации *scope*;

C_{max} – максимально возможное количество событий ИБ за предыдущий период.

Расчет результативности инцидентов ИБ:

$$K_{и} = \left(1 - \left(\frac{И_{тек.}}{И_{max}} \right) \right) * 100\% \quad (2)$$

Где:

$K_{и}$ – коэффициент результативности по идентификации инцидентов ИБ;

$И_{тек}$ – идентифицированное количество инцидентов ИБ в конфигурации *scope*;

$И_{max}$ – максимально возможное количество инцидентов ИБ за предыдущий период.

С учетом положений (1) и (2) общий показатель результативности СМИБ рассчитывается:

$$K_{смиб} = (K_{с} * \alpha + K_{и} * \beta) \quad (3)$$

Где:

$K_{смиб}$ – общий показатель результативности СМИБ

$K_{с}$ – коэффициент результативности по идентификации событий ИБ;

$K_{и}$ – коэффициент результативности по идентификации инцидентов ИБ;

α – весовой коэффициент для определения важности идентификации $K_{с}$;

β – весовой коэффициент для определения важности идентификации $K_{и}$.

В качестве практических метрик ИБ рекомендуются к применению дополнительно:

— $K_{с} = (1 - C_{тек} * 100\% / C_{max})$ – для оценки динамики событий ИБ;

— $K_{р} = (1 - K_{с}(\text{повторных}) * 100\% / K_{с})$ – для оценки динамики повторных событий ИБ (рецидив);

— $K_{д} = (C_{max} - C_{тек}) / (K_{max} - K_{тек})$ – для оценки динамики приращений событий ИБ и инцидентов ИБ.

Рассмотрим пример графического расчета результативности СМИБ при равной важности событий ИБ и инцидентов ИБ; $\alpha = \beta = 0,5$ (рис. 2)

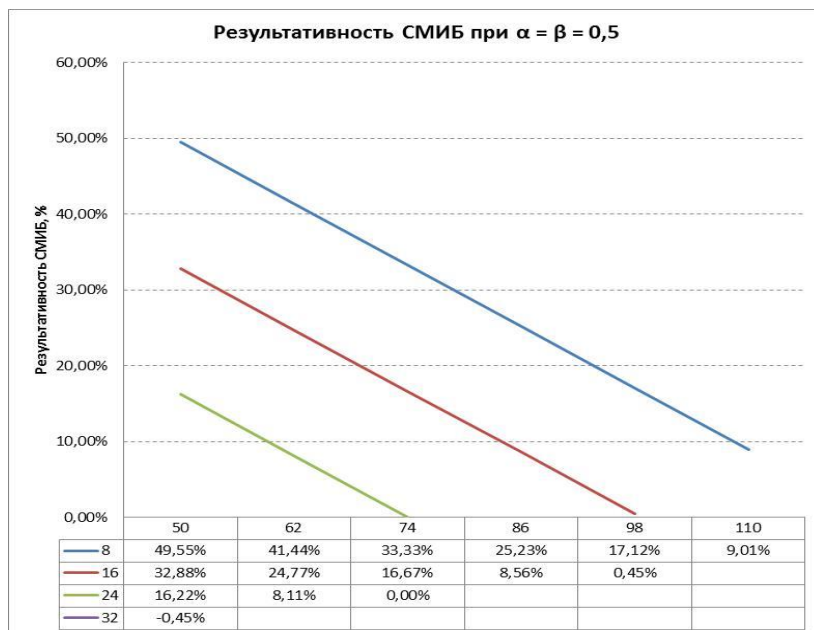


Рис. 2. Расчет результативности СМИБ при $\alpha = \beta = 0,5$

С целью снижения издержек (это одна из приоритетных задач любого бизнеса и наиболее «презентабельная» форма оценки результативности службы ИБ), могут быть применены метрики, показывающие степень достижения возможного максимума (плана продаж, выполнения в срок проектов и пр.). Соответственно, могут быть предложены различные типы метрик:

- простые метрики (например, количество выявленных инцидентов ИБ, предотвращенных утечек);
- сложные метрики (например, отношение стоимости мер защиты к стоимости ИТ активов);
- комплексные метрики (например, число произошедших инцидентов ИБ, приведших к ущербу (вынужденному простое) в ИС, определенных как критичные для бизнеса).

Выводы

Внедрение и сертификация СМИБ на базе стандарта серии 27001 будет способствовать обеспечению требуемого уровня обеспечения ИБ благодаря следующим факторам:

- СМИБ позволяет получать оперативные и достоверные оценки уровня защищённости значимых для бизнеса активов (в процессе аудитов ИБ или проверок со стороны надзорных органов);
- СМИБ позволяет повысить объективность и корректность оценки уровня обеспечения ИБ, например, в рамках периодического анализа СМИБ со стороны руководства с учетом множества требований международных стандартов ISO и отраслевых особенностей (например, с помощью полиномиальных расчетов и конкретных весовых коэффициентов);
- Для обеспечения постоянного повышения результативности СМИБ необходимо формировать сопоставимые метрики ИБ, которые позволят сформировать обоснованные цели в области СМИБ, направленные на обеспечение стабильного развития бизнеса организации.

Библиография

- [1] The ISO Survey of Management System Standard Certifications – 2013
- [2] ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

В. Ф. Лукичев

ПРИНЦИПЫ СОЗДАНИЯ ЕДИНОЙ СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ООО «Управляющая компания «Лекс», г. Тюмень, Россия

«Когда имена неправильные,

**суждения несоответственны;
когда суждения несоответственны,
дела не исполняются».
Конфуций.**

Ни один масштабный проект, в том числе такой, как **«Создание единой системы национальной безопасности»**, сегодня не обсуждается с точки зрения сущности и смысла той терминологии, тех понятий, которые применяются в таких проектах.

Считается, что если применяются «общепринятые» понятия, термины, то всем все понятно.

На самом деле, как показывает анализ реализации международных, общенациональных проектов, неучет данного момента при обсуждении конкретных проектов приводит, практически всегда или к негативным результатам, или к невозможности даже приступить к реализации этих проектов.

Ведь если у строителей дома нет образа дома, или этот образ различен у каждого строителя, то дом никогда не будет построен. Это – аксиома. Но факты сегодняшнего дня говорят об обратном. У человечества, у наций нет образа того, что они пытаются реализовать в масштабах отдельных стран, крупных регионов и даже всего мира.

Именно поэтому, ни в одной стране мира так и не была создана единая система национальной безопасности, а также не была построена экономика, тем более эффективная и тем более рациональная, т.е. разумная (латынь). И это есть закономерность сегодняшнего дня.

Более того, это был и есть предсказуемый результат потому, что еще в древнекитайской книге «Го юй» («Речи царств») говорится: «Китайская философия, как новый образ мышления и познания мира, вероятно,

окончательно сформировалась, когда она стала заниматься понятиями и терминами».

Когда мы начинаем реализовывать масштабные проекты, например – «Единая система национальной безопасности», то нам нужен образ этих проектов для их реализации. И образ этот должен соответствовать сущности и смыслу абсолютных законов природы. Но в том то и дело, что таких образов вообще не сформировано в мире. И, в то же время, мы тратим и тратим впустую огромные ресурсы, в том числе и такой абсолютный ресурс, как время.

На самом деле, к такому выводу можно было прийти в самом начале, т.е. до начала реализации конкретного проекта.

На основании вышеизложенного обратимся к созданию образа «**информационная безопасность**» с точки зрения подлинного и собственного значения слова – слова в его собственном, своем смысле. И мы увидим, что данный образ будет значительно отличаться от общепринятого.

Информация (с точки зрения человека) – то, что определяет естественную, подлинную, истинную внутреннюю сущность и смысл человека и, тем самым, способствует рождению (возникновению) у человека естественного, подлинного желания, стремления знать в совершенстве суть и смысл всего сущего и законов природы, а также подлинное и собственное значение слова – слово в его собственном, своем смысле (прямая речь).

Таким образом, **информация** есть внутреннее свойство человека. Но не каждый человек обладает информацией, т.е. данным внутренним свойством.

Безопасность – знание истинной природы, сущности опасности (прямая речь).

Знание – установление, определение и защита человеком сути и смысла самого себя, всего сущего и законов природы, используемых человеком для внутреннего качественного изменения себя и воздвижения богатого, изобильного, с плодородными и многоводными землями Отечества (Родины)

истины и справедливости (Веры), счастья, чтобы человек жил в радости, пахал и сеял всегда в гармонии с Землей и Природой (празык).

Слово «**знание**» имеет только единственное число. Нет старого, нового или неполного знания. Знание не подвластно времени. Оно или есть, или его нет. Другого не дано.

Опасность – воистину, в высшей степени естественный, подлинный источник, препятствующий созданию человеком абсолютного организующего начала познания им самого себя, всего сущего, законов природы и своего будущего и воздвижения человеком надежной защиты и охраны своей жизни, а также богатого, изобильного, с плодородными и многоводными землями Отечества (Родины) истины и справедливости (Веры), счастья, чтобы человек жил в радости, пахал и сеял всегда в гармонии с Землей и Природой (празык).

Таким образом, главной опасностью для человека, нации, человечества является сам человек, сама нация, само человечество. Но именно это, вообще не отображено в документах ведущих стран мира, касающихся вопросов национальной безопасности. Все устремления этих стран направлены на создание определенной технико – технологической системы надежной защиты и охраны. Идет всемирная гонка технического, технологического оснащения стран. И, в первую очередь, это касается именно военного аспекта проблемы безопасности стран.

На самом деле, и об этом говорили наши далекие предки, технико – технологического решения (в современном понимании) человеческих проблем не существует.

Надо всегда помнить, что только человек вводит в кризис коммерческие организации, страны и человечество в целом. И только человек способен вывести их из кризиса. Другого варианта не существует в природе вовсе.

В тоже время, абсолютным фактом является то, что те, кто завел человечество, отдельные страны или объединения стран, коммерческие организации в кризис, никогда не выведут их из кризиса.

Таким образом, для создания действительно надежной единой системы национальной безопасности надо знать **«человека»** и уметь управлять им.

Человек – большая открытая живая комплексная, самоуправляемая, саморазвивающаяся, самоорганизующаяся, самовосстанавливающаяся, противоречивая, неустойчивая, неравновесная (нестабильная), асимметричная, асинхронная, информационно – энергетическая система.

Сегодня, в принципе, никто не занимается реальным человеком. И происходит это потому, что те, кто обязан заниматься этим, не знают кто есть человек с точки зрения его сущности и смысла. Человек для них всего лишь трудовой или иной ресурс.

Именно поэтому, так называемые «экономисты» и «управленцы» говорят сегодня об управлении страной, регионами, коммерческими организациями, проектами, технологическими процессами, финансовыми потоками, капиталами, деньгами, продажами, издержками, стоимостями и конечно же машинами, но при этом не говорят об управлении реальным человеком, людьми. На самом деле, единственным объектом и субъектом управления является именно человек и только он потому, что **«управление»** означает **«успокаивать, облегчать участь, унимать, усмирять, склонять к чему – либо, делать уступчивым, подчинять человека словом»** (празык).

Государственное управление – механизм решения всех человеческих проблем через слово (празык).

Конечная цель управления – достижение истины и справедливости, т.е. Веры.

На основании вышеизложенного, только человек обладающий знанием может действительно создать надежную систему защиты и охраны своей жизни – единую систему национальной безопасности. Таким человеком, является, на самом деле, управленец – человек обладающий знанием, интуицией (мышление образами) и памятью, вобравшей в себя все достижения человечества за всю его историю.

Именно управленцы должны стоять во главе инновационных процессов преобразования социально – экономических систем различного уровня. А инновационные процессы, в свою очередь, должны стать основой развития и интеграции людей. И это действительно так.

Инновация (латынь) – внутреннее обновление, изменение, преобразование и преображение (реформирование).

Инновация – рождение внутреннего организующего начала жизненного пути познания человеком самого себя, всего сущего и законов природы, что способствует внутреннему качественному изменению человека (праязык).

Инновации – есть функция управления именно человеком, а не новые продукты и технологии.

Интеграция – естественный, подлинный источник (начало) рождения сущности и смысла внутреннего качественного изменения человека, обеспечивающего познание им самого себя, всего сущего и законов природы и действительное, истинное объединение людей, представляющее собой единое целое, для создания надежной защиты и безопасности их жизни и земли и воздвижения ими богатого, изобильного, с плодородными и многоводными землями Отечества (Родины) истины и справедливости (Веры), счастья, чтобы жить в радости, пахать и сеять всегда в гармонии с Землей и Природой (праязык).

Поэтому, интегрироваться могут только люди определенного уровня развития. Общества таких людей представляют собой единое целое.

И тогда, и только тогда в стране действительно можно создать единую систему национальной безопасности, т.е. решить все человеческие проблемы. Это под силу только обществу разумных людей. Еще Конфуций говорил: «У разумных людей нет проблем».

Лунин А.В.

ВОПРОСЫ ФОРМИРОВАНИЯ ЕДИНОГО ПРОСТРАНСТВА ДОВЕРИЯ ПРИ МЕЖДУНАРОДНОМ ЭЛЕКТРОННОМ ВЗАИМОДЕЙСТВИИ

Технический комитет по стандартизации «Криптографическая защита информации», г. Москва, Российская Федерация

Существенным вкладом в формирование единого пространства доверия при международном электронном взаимодействии должна, в частности, стать стандартизация механизмов защиты информации, а также однозначная недвусмысленная идентификация в международном масштабе любого объекта реального мира путем использования объектных идентификаторов, также определяемых через процедуру стандартизации.

Для обеспечения юридически значимого документа широко используются такие криптографические механизмы, как электронная подпись и функция хэширования, позволяющие обеспечить доказуемость целостности и авторства документов. В СНГ приняты и продолжают действовать стандарты ГОСТ 34.310-2004 и ГОСТ 34.311-95, предназначенные в том числе и для целей межгосударственного общения. В ЕАЭС прорабатываются вопросы использования технологии третьей доверенной стороны, позволяющей обеспечить трансграничное взаимодействие. Однако на наш взгляд, по мере принятия новых межгосударственных (региональных) стандартов необходимость в ее применении отпадет.

Россия наряду с другими странами активно участвует в общем процессе разработки, поддержания и развития, как на международном уровне, так и на национальном, системы и правил однозначной недвусмысленной идентификации объектов реального и виртуального мира на основе описания древообразной структуры идентификации, называемой “международное дерево идентификаторов объектов” с использованием понятия “идентификатор объекта”. Объектные идентификаторы национальных деревьев Казахстана и России заложены в проект развития общих информационных систем ЕЭК.

Практическая значимость обсуждаемых вопросов уже ярко проявилась в ходе работ по созданию Интегрированной информационной системы внешней и взаимной торговли Таможенного союза (ИИСВТ) и планируемом ее дальнейшем развитии и преобразовании в Интегрированную информационную систему Евразийского экономического союза (ИИС). Темой 2015 года в рамках конференции названа информационная безопасность государств - членов Организации Договора о коллективной безопасности. Представленные на конференции государства являются участниками и других международных форматов, таких как ШОС, АТЭС, ЭСКАТО и др. Отсюда вытекает насущная необходимость активизации работ в региональных и международных организациях по стандартизации, таких как Межгосударственный совет по стандартизации метрологии и сертификации (МГС) Содружества Независимых Государств (СНГ), Международная организация по стандартизации (ИСО), либо в рамках вновь создаваемых систем стандартизации.

Метлинов А.Д.

СКОРОСТНЫЕ ХАРАКТЕРИСТИКИ СИММЕТРИЧНОЙ РЮКЗАЧНОЙ КРИПТОСИСТЕМЫ С ОБЩЕЙ ПАМЯТЬЮ. NIST – ТЕСТИРОВАНИЕ

Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия

В начальных вариациях построения ассиметричной рюкзачной криптосистемы предложено использовать сверхвозрастающие рюкзачные базисы. Однако, подход, основанный на таких базисах, оказался небезопасным [1, 2]. В работе [3] представлен новый подход к конструкции рюкзачных криптосистем, позволяющий обойти атаку Шамира и L^3 – атаку. Главная его идея состоит в отказе от асимметрии в пользу симметричного ключа и введении общей памяти между парой (Sender, Receiver) в канале связи, подмножества которой «параметрически влияют» на построение базисов рюкзачной схемы

шифрования. Такие базисы не обладают свойством сверхвозрастания и не могут подвергаться атакам типа L^3 .

В статье обсуждаются особенности скоростных характеристик симметричной блочной рюкзачной криптосистемы с общей памятью, которые установлены с помощью экспериментальных оценок скорости работы алгоритмов по сравнению с известными стандартами шифрования. В работе [3] доказана равномерная по d_e единственность и логарифмическая скорость получения разложения

$$S = (\sum k_i * f_i(d_e)) + \Delta(S), i = 1, \dots, l, \quad (1)$$

где $S \in N$, k_i принадлежащее GF_2 - элементы ключевой последовательности, $f_i(d_e)$ - элементы базиса и Δ - некоторое аддитивное слагаемое. Представление (1) получено однопроходным алгоритмом, просматривающим элементы базисов $f_i(d_e) \leq S$ сверху вниз. В рамках конструкции (1), основанной на общей памяти D в любом параметризованном базисе $\{f(d_e)\}$ устанавливается однозначное битовое соответствие

$$S \leftrightarrow (e_1, \dots, e_n, k_1, k_2, \dots, k_l, \Delta_2), \quad (2)$$

где Δ_2 - обычное двоичное представление остаточного слагаемого.

На основе приведенной конструкции (2) в реализации алгоритма [3] построен масштабируемый блочный симметричный шифр, с несколькими режимами работы, в том числе и режимами кодовой книги (рис.1) и сцепления блоков (рис.2). В этом шифре симметричный ключ имеет два сегмента, один из которых отвечает за выборку элементов общей памяти и параметрически влияет на базис задачи рюкзака.

Зафиксируем достаточно большие натуральные n и l в (1), (2) и обозначим \bar{S} максимально возможное натуральное число в представлении (1). Пусть S - любой двоичный файл произвольной длины. Зададим конкатенацию блоков $S = S_1 // S_2 // \dots // S_m$, где $S_i \in GF_2$, где длина каждого блока, за исключением последнего, фиксирована. Считая выполненным равномерно по всем индексам $S_i \leq \bar{S}$, для каждого блока применим представление (2). Алгоритм, который

находит (2) есть функция шифрования блока, которую обозначим $F_k(d_e, S)$. Обратный алгоритм – функция дешифрования $F_k^{-1}(d_e, [e_1, \dots, e_n, k_1, \dots, k_l, \Delta_2])$.



Рисунок 1 – Симметричный блочный шифр в режиме кодовой книги

В режиме зацепления блоков каждый блок открытого текста, кроме вектора инициализации, побитово складывается по модулю 2 с предыдущим результатом шифрования. Пусть B_0 – вектор инициализации (блок формируется с помощью определенного одностороннего алгоритма на основе общей памяти), тогда:

$$B_i = F_k^{d_e}(S_i \oplus B_{i-1}), \quad (3)$$

где i – номер текущего блока; $F_k^{d_e}$ – алгоритм шифрования, используемый в спроектированной ранее симметричной рюкзачной криптосистеме с общей памятью и плотностью укладки больше единицы; S_i – блок открытого текста.

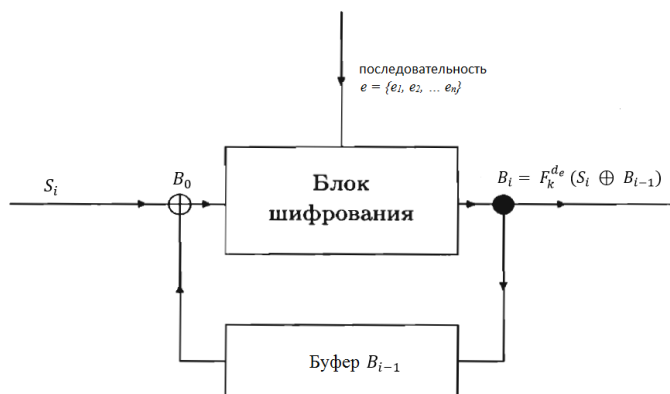


Рисунок 2 – Симметричный блочный шифр в режиме зацепления блоков

В реализованной конструкции (3) блочного шифра длина блока текста равна 64 битам, максимально возможный размер общей памяти оценивается в 2^{64} бит и $\Delta_{max} = 3$ бита. Длина ключа соответственно $n + l + \Delta_{max}$ бит. Для практического подтверждения грубых асимптотических оценок скорости работы алгоритма, приведенных в [3], блочный шифр подвергся

экспериментальным прогонам по двум направлениям. Одно из них – тестирование на скорость работы шифрования и сравнение с соответствующими скоростями работы криптосистем Меркла - Хеллмана и на основе базиса Цекендорфа. Второе – NIST – тестирование для практического доказательства криптостойкости. Результаты тестов направлены на подтверждение того факта, что последовательность, являющаяся результатом работы блочного шифра, похожа на случайную.

В ходе первого тестирования было отобрано десять различных типов файлов (сжимаемых и несжимаемых). Для каждой из трех криптосистем и для каждого типа файла проведено по 30 контрольных экспериментов (всего порядка тысячи), результаты которых показали, что спроектированный алгоритм шифрования криптосистемы с общей памятью работает в среднем на 25-28% быстрее, чем рюкзак Меркла - Хеллмана и на 7-9% быстрее, чем рюкзак, в основе которого лежит базис Цекендорфа (рис.3).

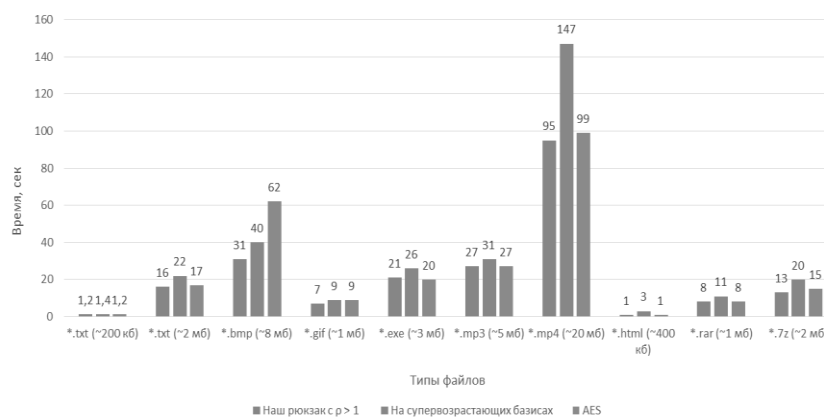


Рисунок 3 – Сравнение скоростей с известными стандартами шифрования

На основе реализации блочного шифра с помощью стандартной схемы свертки блоков за счет общей памяти впервые появляется возможность построения параметризованного по наличию общей памяти стандартного алгоритма хеширования, применяемого для контроля достоверности передаваемой информации от отправителя к получателю. Свертка блочного шифра порождает такую хэш-функцию для пары (Sender, Receiver), которая является строго индивидуальной. В самом деле, все построения, в том числе и

хеш-функция непрерывно зависят от согласованного параметра d_e общей памяти этой и только этой пары (Sender, Receiver).

В качестве вектора инициализации хеш-функции $H_0 = const$ будем использовать массив данных, полученный на основе общей памяти с помощью специального необратимого преобразования, в качестве которого выступает односторонняя функция, о значении которой отправитель и получатель договариваются заранее.

В качестве алгоритма формирования выходного значения хеш-функции – итогового хеш-значения (хеш-суммы) будем использовать любой ключевой алгоритм. Ключом в данном алгоритме будет служить последовательность k_1, k_2, \dots, k_l , полученная в ходе разложения секрета S

$$H_i = (M \oplus H_{i-1})_{k_i} \quad (4)$$

Разработанная криптосистема показала свои отличные результаты в прохождении NIST – тестов. Сводная статистика прохождения некоторых из тестов представлена в таблице 1.

Таблица 1 – Результаты NIST - тестирования

Название теста	Описание	Результат теста
Частотный побитовый тест	$m \rightarrow p(0) = 0,489$ и $p(1) = 0,511$	тест пройден
Энтропийный тест	Энтропии бит: 0,9996211 и энтропии байт: 6,949998	тест пройден
Серийный тест	Каждая последующая серия в 2 раза короче предыдущей	тест пройден
Тест рангов бинарных матриц	Всего матриц : 16567 и Количество вырожденных матриц: 9947	тест пройден

Спроектированные алгоритмы шифрования и дешифрования работают заметно быстрее, чем в аналогичных рюкзачных криптосистемах. Изложенные скоростные характеристики позволяют делать выводы о возможности применения приведенного алгоритма в композициях с другими стандартами, такими как AES, DES и GOST1989. В частности, для встраивания алгоритма шифрования в протоколы передачи данных https, где конструкцию шифрования

/ дешифрования AES можно соответственно заменить на композиции $AES(F_k^{de}(S)) / F_k^{de^{-1}}(AES^{-1}(S))$.

Литература

1. Odlyzko A. M. and Lagarias J. C. Solving Low-Density Subset Sum Problems // J. Association Computing Machinery. 1985. V. 32. No.1. P. 229–246.
2. Александров А.В., Метлинов А.Д. «К вопросу об особенностях реализации симметричной рюкзачной криптосистемы с общей памятью и плотностью укладки больше единицы» // XXXIII Всероссийская НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем», г. Серпухов, сборник научных трудов, часть 4, с. 161-167, 2014.
3. Александров А.В., Метлинов А.Д. Симметричная рюкзачная криптосистема с общей памятью и плотностью укладки больше единицы // Журнал «Проблемы информационной безопасности. Компьютерные системы», №4 2014, с. 58-65.

Мусиралиева Ш.Ж., Абдаким Г.

ЗАМАНАУИ ТЕХНИКАЛЫҚ ҚАУІПСІЗДІК ЖҮЙЕЛЕРІ ҮШІН ПРОЕКТІЛІК ШЕШІМДЕР

әл-Фараби атындағы ҚазҰУ, Алматы

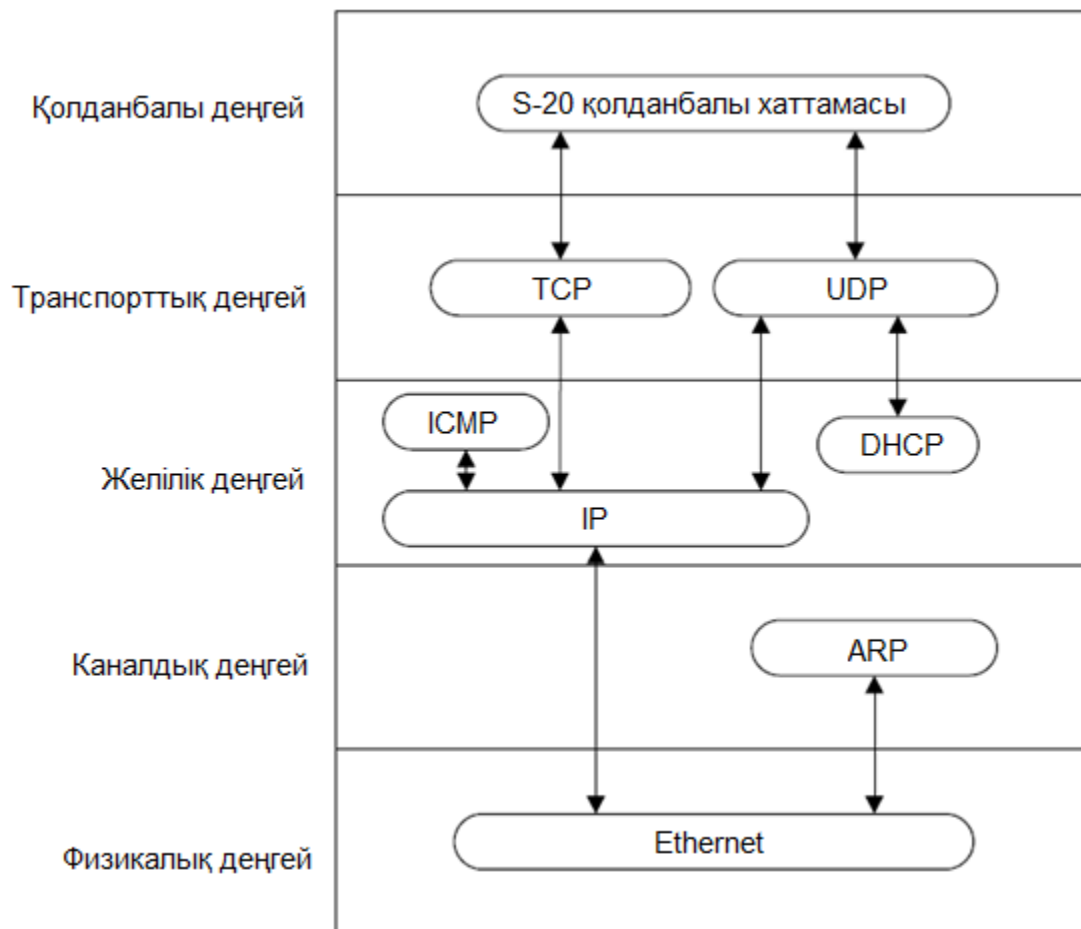
Қазіргі кезде кез келген кәсіпорынның тіршілік әрекетін қауіпсіздіктің енгізілген жүйесінсіз елестету қиын. Егер бұрын талап периметрдің қорғанысымен шектелсе және бейне бақылау ғана болса, ал бүгін қауіпсіздіктің техникалық жүйесі басқа да көптеген міндеттерді шешеді. Кәсіпорынның басқарылуының қамтамасыз етілуі, объектілерді қорғау, еңбектиімділігінің жоғарылауы, экономикалық тиімділік көптеген мәселелердің бірі болып табылады, олардың шешу жолдарын қазіргі қауіпсіздіктің жүйелерінің мүмкіндіктерімен толықтыруға болады. Осылайша, жүйе өзін-өзі қорғаныс

құралдары мен инженерлік-техникалық құралдардан тұратын интегралданған кешен ретінде таныстыруы керек; ұйымдастыру шаралары; ақпарат қорғауды жүзеге асыру міндеттерін қажетті хаттамамен бағдарламалық қамтамасыз ету; жиынның бағдарламалық қаражаты және деректерді визуализациялау және тағы басқа ([1,2]).

Ұсынылып отырған баяндамада авторлар *PERCo-S-20* техникалық қауіпсіздік жүйесіне сүйене отырып жоғары оқу орындары үшін проектілік шешімдер ұсынып отыр.

Желілік бақылауыштардың қызмет етуі үшін Ethernet 10-BaseT, 100-BaseTX немесе 1000-BaseTX желі қажет. Деректерді жіберу үшін бақылауыштардың тікелей IP-адрестерін, сонымен бірге UDP хаттаманы пайдаланады. *PERCo-S-20* жүйесін қолданатын объектілердегі деректерді жіберуді дұрыс күйге келтіру үшін дайын жүзеге асырылған механизмді түсіну қажет. ([3]). Жүйеде деректер алмасу үшін келесі хаттамалар тобы қолданылады (1-сурет):

Бірлестірілген хаттамалар бойынша функционалды қызмет жасайтын, ортақ байланыс сызықтары мен мәліметтер қорын қолданатын, ортақ программалық ядро арқылы басқарылатын, барлық кішігірім жүйелердің бір үлкен комплексті жүйеге біріктіру техникалық қауіпсіздік жүйесін құрудың қазіргі заманғы көзқарасы болып табылады. Бірақ қауіпсіздік жүйені толығымен автоматтандырылған түрде жасауға болмайды. Өйткені ұйымда дәл қазіргі уақытта болып жатқан және болашақта болуы мүмкін барлық жағдайларды қарастыру мүмкін емес. Моделдеуді құрал-жабдықтардың көмегімен жасау мүмкіндігін қолдана отырып осы мақаланың авторлары еңбектің тиімділігін жоғарылату үшін Ақпараттық жүйелер кафедрасына арналған проектілік жоба жасады және тест жүргізді.



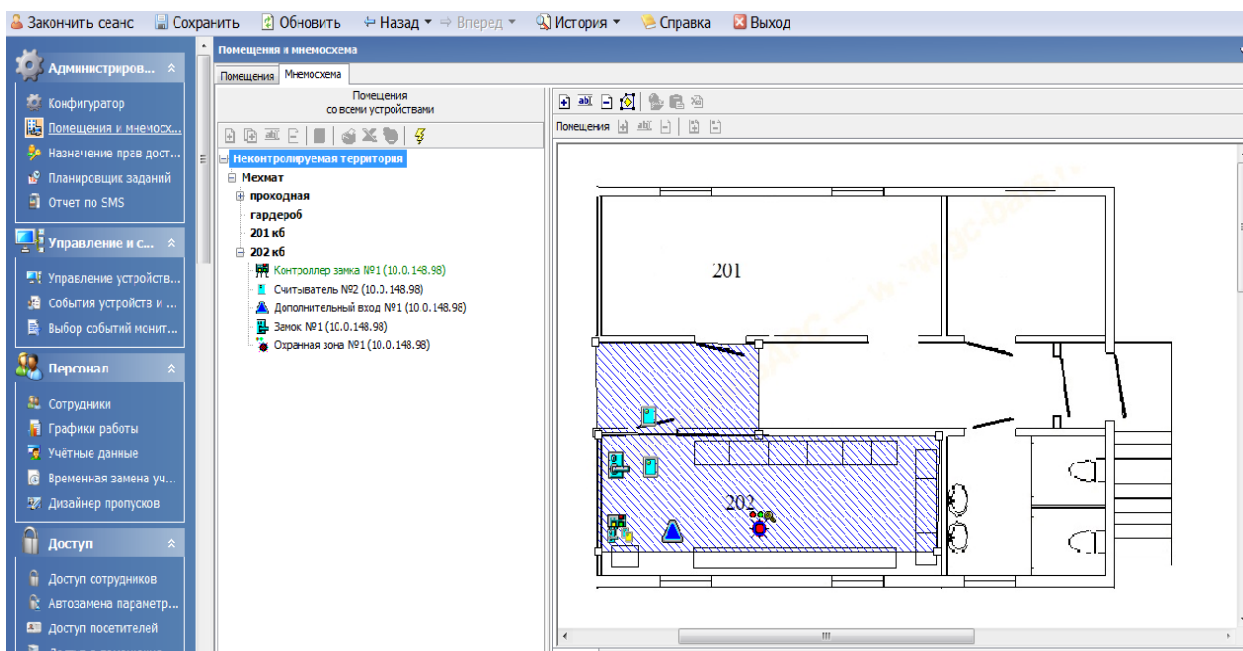
1-сурет. Деректер алмасуға арналған хаттамалар

Бастапқы кезеңде қауіпсіздік жүйесінің сырт пішіні жасалады. Бұл кезең *PERCo-S-20* қауіпсіздік жүйесінің программалық қамтамасыз ету және құрылғылардың параметрлерінің жұмыс істеуін сипаттауға арналған. Бұл кезде жүйеге жаңа құрылғыларды қосу немесе құрылғыларды алып тастау, құрылғылардың жұмысын қалыпқа келтіру, әр түрлі оқиғаға байланысты құрылғылардың реакциясын бақылау сияқты жұмыстар атқарылады.

Моделдеу сатысы КІТ оңтайлы зертханалық стендінде жүзеге асырылды. КІТ жиынтығы *PERCo-CT/L-04* контроллерінен және екі *PERCo-IR0X* сериясындағы есептегіштен, өткізгіш құрылғыдан тұрады.

Қызметкерлердің мәліметтер қоры жасалды, жұмыс кестесі құрылды, кіруге мүмкіндік беретін карточкалар берілді және кіруге шек қою жасалды. Мынадай жағдайларда: мұғалімнің сабаққа 10 минуттан көп кешігуіне

байланысты немесе мұғалімнің аудиторияда сабақтың соңына дейін болмауы кезінде тәртіп бұзу туралы журнал құрылады. Механика-математикалық факультеттің екінші қабатының сол жақ қанатының мнемосхемасы жасалды. 2-суретте көрсетілгендей 202-аудиторияда контроллер, 2 есептегіштер, құлып орналасқан. Бұл кезеңде жасалған жұмыстар келесі кезең үшін де пайдаланды.



2-сурет. Құрылғылар қойылған мнемосхема

СМС жолдауды бантау. Бұл кезеңде механика-математикалық факультеттің ақпараттық жүйелер кафедрасының мәліметтер қорындағы белгілі бір оқиғалар орын алған жағдайда жұмыс өнімділігін жоғарылату мақсатында берілген номерге СМС жолдау мүмкіндігі қарастырылды.

GSM модемді қолдана отырып SMS-таратуларды (рассылка) орнату. Алғашқыда модем ретінде, USB порт арқылы компьютерге қосыла алатын және де ішкі модеммен жабдықталған ұялы телефон қолданылды. Мұндай ұялы телефон, аз мөлшердегі SMS таратуға жарамды, ал көп мөлшердегі SMS-таратуларды жіберу үшін USB-модем қолданылмақ.

SMS-провайдер арқылы смс-таратуларды орнату. Іске асыру барысында QuickTelecom(<http://sms1.quicktelecom.kz>) компаниясы смс провайдер ретінде

таңдалды. Мұндай программалық модульді орнату барсында SMPP протоколы қолданылады. «SMS» (Short Message Service, қазақша транскрипциясы: «СМС») - бұл байланыстың жылжымалы және жердегі желілері, соның ішінде GSM стандартының ұялы телефондары үшін арналған қысқа мәтінді хабарламалар, олардың мәтіндері әріптерден, сандардан және басқа белгілерден тұруы мүмкін; SMS – хабарлама екі түрлі форматта жасалуы мүмкін: Unicode (соның ішінде орыс тілі) және 7bit (ағылшынша мәтін және көп көлемдегі символдар). Хабарлама бір немесе бірнеше SMS-тен тұруы мүмкін. Бір хабарламадағы SMS санын енгізілген мәтін негізінде есептеу unicode формуласы бойынша жүргізіледі: егер ұзындығы ≤ 70 , онда 1 SMS, басқаша, SMS саны былай анықталады: SMS саны = символдық хабарламаның ұзындығы/67 (мысалы, 135 символдан тұратын ұзындықтағы мәтін 3 SMS хабарлама ретінде саналады). 7bit: егер ұзындығы ≤ 160 , онда 1 SMS, басқаша, SMS саны былай анықталады: SMS саны = символдық хабарламаның ұзындығы/ 153 (мысалы, 310 символдан тұратын ұзындықтағы мәтін 3 SMS хабарлама ретінде саналады).

Аудиторлық қорды визуализациялау. Белгілі-бір іс-шараларды өткізуге аудиторияларды іздеу немесе сабақ кестесі өзгерген кезде мұғалімдер факультет диспетчерлеріне хабарласады. Аудиторияларды іздеу көп уақыт алмайды. Ұсынылып отырған программалық жабдықтама біздің факультет диспетчерлеріне көмек ретінде жасалынып отыр. Сонымен қатар техникалық қауіпсіздігі бар кез келген мекемеде қолданса болады. Сабақтың реттік нөмірін және аудиторияның түрін таңдағанда, нәтижесі экранға шығады. Курсорды сабақ батырмасына апарған кезде, аудитория түрі мен аудиторияның сыйымдылығын көрсетеді. Экранда белгілі бір уақыт кезіндегі аудиторияның бос болмауы қызыл түспен көрсетілінеді. Изделінді уақыт кезінде аудиторияның бос болып, бірақ сыйымдылығы сәйкес келмейтін аудитория сұр түспен көрсетілінеді. Программада лекция өтуге арналған аудитория 25-тен асатын сыйымдылықпен, ал семинар сабақтарға 25-тен кем сыйымдылықпен жасалынған. Сонымен қатар программада, зертханалық аудиторияда семинар

немесе лекция сабақтарын өтуге болмайтынын да көруге болады. Визуализациялау программасы C# тілінде жазылды. Жұмыстың нәтижесін <http://www.studenthelp.kz> сайтынан таба аласыз.

Қолданылған әдебиеттер

1. ХоффманЛ.Дж. Современные методы защиты информации. М.: Сов. Радио, 1980 г.
2. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М., 2001 – 496 с
3. Единая система S-20. Руководство администратора. Доступно на <http://www.perco.ru>
4. Мусиралиева Ш.Ж, Бекбулатов Е. О курсе «Технические системы безопасности», Труды международной конференции "Применение информационно-коммуникационных технологий в образовании и науке" , Алматы, 22-23 ноября 2013 года.

Нурланова Б.М., Жумагулова С.К., Алибиев Д.Б.

АҚПАРАТТЫ ҚОРҒАУДЫҢ КРИПТОГРАФИЯЛЫҚ ӘДІСТЕРІН ҚОЛДАНУДЫҢ КЕЙБІР АСПЕКТІЛЕРІ

Академик Е.А.Бөкетов атындағы Қарағанды мемлекеттік университеті
Қарағанды қаласы, Қазақстан Республикасы

Қазақстан Республикасының Еуразиялық аймаққа кіруі, ХХІ ғасырға аяқ басуы ел Президентінің «Қазақстан-2030» атты стратегиялық бағдарламасына сәйкес жаңа техника мен технология үдерістерінің дамуы, келешекте жоғары оқу орындарында білім беру қандай бағытта өрбуі керек деген өзекті мәселе туғызады. Барлық өркениетті елдерде азаматтардың қауіпсіздік сақшысы ретінде заңдар тұр, барлық есептеуіш техника саласында құқық қолданатын іс-тәжірибе әзірге дамымаған, ал заң шығарушы процесс технология дамуына

ілесе алмайды, сондықтан компьютерлік жүйе жұмысының сенімділігі көбіне өзін-өзі қорғау шараларына сүйенеді.

Қазіргі кезде, ақпараттық жүйелерде криптографиялық әдістерді қолдану мәселесі туындады. Криптографиялық әдістер, ақпаратты қорғаудың ең тиімді құралдары болып табылады.

Кез-келген криптографиялық әдіс қажырлылығы және еңбек сыйымдылығы деген көрсеткіштермен сипатталады [1].

Әдістің қажырлылығы – бұл шифрленген мәтіннің ең кіші көлемі. Оны статистикалық талдау арқылы бастапқы мәтінді ашып көруге болады. Солай, шифрдың қажырлылығы бір кілтті қолданған кезде шифрленетін ақпараттың ықтимал шамасын анықтайды.

Әдістің еңбек сыйымдылығы бастапқы мәтіннің бір символды шифрлеу үшін қажетті элементарлы операциялар санымен анықталады.

Криптоалгоритмдердің классификациясы [2].

Барлық криптоалгоритмдер классификациясының негізгі схемасы болып келесілер саналады:

Жасырып жазу.

Хат жіберуші және хат алушы хабарламамен екеуіне ғана белгілі өзгерістерді жасайды. Бөтен адамдарға шифрлеу өзінің алгоритмі белгісіз. Жасырып жазу криптография болып саналмайды.

Кілтпен криптография.

Берілетін деректерге әсердің алгоритмі барлық бөтен адамдарға белгілі, бірақ ол бір параметрден тәуелді болады (хат жіберуші және хат алушы білетін «кілт»).

Симметриялы криптоалгоритмдер.

Хабарламаны шифрлеу және дешифрлеу үшін ақпараттың бір блогы қолданылады.

Асимметриялы криптоалгоритмдер.

Алгоритмдер хабарламаны шифрлеу үшін бәріне белгілі («ашық») кілт, ал дешифрлеу үшін басқа («жабық») кілт пайдаланады.

Стеганография.

Осы өнердің негізінде құпиялы хабарламасы бар екенін жасыру жатады. Мұнда келесілерді пайдалануға болады: «астар болатын хат», бұл жерде жазба қорғаныстық тыспен жасырылады.

Мәліметтерді криптографиялық түрлендіру арқылы қорғау қауіпсіздік мәселесінің тиімді шешімі болып табылады. Шифрленген мәліметтерді кілті бар қолданушылар ғана дешифрлей алады.

Кілті ашық жүйелер мәліметтерді шифрлеуде болашағы зор криптографиялық стандарт болып табылады. Мұндай жүйелерде шифрлеу үшін бір кілт, ал шифрді ашу үшін екінші кілт қолданылады. Бірінші кілт ашық болып табылады және өз ақпараттарын шифрлеуде кез-келген қолданушының пайдалануы үшін желі бойынша жарияланады. Шифрленген ақпаратты қабылдаушы мәліметтерді дешифрлеу үшін екінші кілтті қолданады. Ал екінші кілт - құпиялы. Сонымен қатар, мынадай шарт орындалуы тиіс: жарияланған бірінші кілттен екінші кілт анықталмауы тиіс.

Кілті ашық криптографиялық жүйелер қайтымсыз немесе бірбағытты функцияларды қолданады, соңғысының қасиеті мынадай: x мәні берілсе, $f(x)$ мәнін есептеу оңай, бірақ кері функцияны есептеу қиын.

Қазіргі уақытта мәліметті қорғауда RSA ашық кілтті криптографиялық әдіс кең таралған. Мұндағы, RSA дегеніміз жасаған адамдардың аттарының бірінші әріптері (Rivest, Shamir, Adleman). Оның криптотұрақтылығы жоғары және қарапайым программалық, аппараттық тәсілдерде іске асыруға болады. Бұл әдістің көмегімен қағазсыз мәлімет алмасу және тасымалдау жағдайындағы жеке қолтаңба мәселесі шешілді [3].

«Орын ауыстыру» класына «Кардано торы» деп аталатын шифр да жатады. Ол - қағаз бетіне қойған кезде кейбір бөліктері ғана ашық қалатын, көбіне квадрат болып келетін, қуысы бар тікбұрышты карточка. Карточканың

жолдары мен бағандарының саны – жұп. Карточка оны тізбектей қозғаған (немесе бұрған) кезде, оның астында жатқан қағаз бетінің әрбір торы бос болмайтындай етіп жасалған.

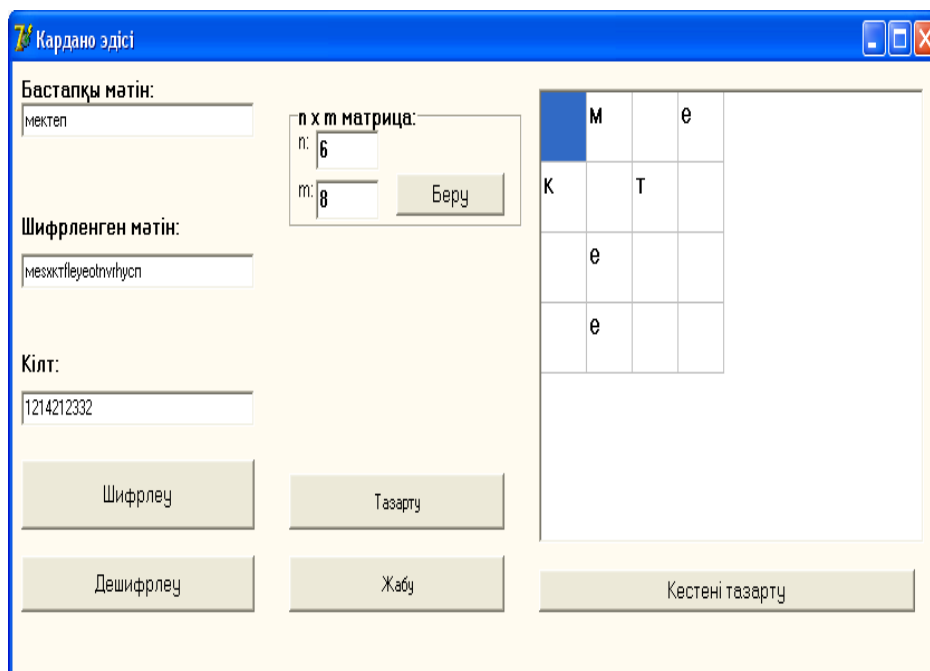
Шифратор торды қағаз бетіне орналастырады және жеке символ, буын немесе толық сөз сиятындай тікбұрышты қуыстарға хабарлама жазады. Берілген хабарлама көптеген кішкентай фрагменттерге бөлінеді екен. Содан кейін тор алынып тасталады да, қағаздағы бос орындар жасырылған мәтін криптомәтіннің бөлігі болатындай бөгде мәтінмен толтырылады. Осылай толтыру белгілі әдеби шеберлікті талап етеді.

Хабарламаны алушыда да осындай тор болуы керек. Тордың көшірмелері алғашқы үлгіден кесіледі, бірақ өзара сәйкестік үшін басқа да көптеген үлгілер жасауға болар еді.

Торды төрт түрлі, яғни тордың мүмкін орналасу санын төрт есе арттыратын жоғары, төмен, тігінен және төңкерілген түрде орналастыруға болады. Егер Кардано торы квадрат болса, онда тордың орналасуының екінші нұсқасы мүмкін болады, яғни квадраттың центрінен 90° бұрылыстар жасау.

Бұл әдіс өте баяу, сол себепті әдеби дағдыларды қажет етеді. Бірақ, ең бастысы кез-келген шифрлейтін аппарат жоғалмайды, ұрланбайды немесе тәркіленбейді. Сондықтан, бір торды жоғалту осы тордың көмегімен шифрленген барлық құпия хабарламаларды жоғалтуды білдіреді.

Delphi ортасында бұл әдіс келесі бағдарламада көрсетілген (сурет 1).



Сурет 1 – Кардано шифрлеу тәсілін іске асыратын бағдарлама

Әдебиеттер

4. Шеннон К. Теория связи в секретных системах/Сб.: «Работы по теории информации и кибернетике»- М.: Иностранная литература, 2003 - С.333-402.
5. Грушо А.А, Тимонина Е.Е. Теоретические основы защиты информации. - М.: Издательство агентства «Яхтсмен», 1996-71с.
6. Пшенин Е.С. Теоретические основы защиты информации. Еч. пос. Алматы; КазНТУ, 2000-452с.

Нысанбаева С.Е., Магзом М.М.

МОДЕЛИРОВАНИЕ НЕТРАДИЦИОННОГО АЛГОРИТМА ШИФРОВАНИЯ С ПРИМЕНЕНИЕМ СХЕМЫ ФЕЙСТЕЛЯ

Институт Информационных и Вычислительных Технологий Комитета
Науки Министерства Образования и Науки Республики Казахстан, Алматы,
Казахстан

Введение

В нетрадиционной системе шифрования криптостойкость алгоритма определяется полным секретным ключом. Он состоит из секретных параметров криптоалгоритма, разработанного на базе непозиционных полиномиальных систем счисления (НПСС). Синонимы НПСС – классическая система счисления остаточных классов (СОК), полиномиальная СОК и модулярная арифметика.

Классическая СОК базируется на китайской теореме об остатках, которая гласит, что любое число может быть представлено своими остатками (вычетами) от деления на систему оснований, которую образуют попарно простые числа [1,2]. В отличие от классических СОК предлагаемые криптографические процедуры рассматриваются в полиномиальных системах счисления в остаточных классах, в которых основаниями служат не простые числа, а неприводимые многочлены над полем $GF(2)$ [3,4]. Криптографические алгоритмы и методы, разработанные на базе НПСС, называют нетрадиционными, модулярными или непозиционными.

Нетрадиционные методы и алгоритмы криптографии, построенные на базе непозиционных полиномиальных систем счисления, позволяют повысить надежность алгоритма шифрования и уменьшить длину ключа. Криптостойкость в этом случае определяется полным ключом, зависящим не только от длины ключа (ключевой последовательности), но и от выбранной системы полиномиальных оснований, а также от количества перестановок оснований в системе. Чем больше длина полного ключа шифрования в НПСС, тем больше вариантов выбора систем рабочих оснований. Поэтому криптостойкость предложенного алгоритма шифрования с использованием НПСС существенно возрастает с увеличением длины электронного сообщения [3].

Использование схемы Фейстеля в криптографическом алгоритме

При разработке симметричных блочных шифров широкую популярность приобрела криптосистема, названная схемой(сетью) Фейстеля. Впервые она

была использована Хорстом Фейстелем в 1973 г. при разработке шифра Lucifer [6], и затем применялась во многих разработках блочных шифров, в том числе и в финалистах AES [7]. Схема Фейстеля является методом смешивания подблоков входного текста в шифре посредством повторяющегося применения зависящих от ключей нелинейных функций, называемых F -функциями и выполнения перестановок подблоков. Раунд блочного шифра является преобразованием, которое соединяет подблоки входного блока посредством F -функций и перестановок подблоков. В стандартной сети Фейстеля открытый текст разбивается на два подблока одинаковой длительности. В общем случае, сеть Фейстеля может разбивать входной блок на $n \geq 2$ подблоков. Далее подразумевается, что все подблоки имеют одинаковую длину, так что каждый подблок может участвовать в транспозиции с любым другим подблоком. Обобщенная схема обмена является перестановкой $n \geq 2$ подблоков в раунде.

Для модификации модели нетрадиционного алгоритма шифрования предполагается использование сети Фейстеля. Целью этих работ является улучшение статистических характеристик непозиционных криптограмм. В связи с этим планируется рассмотреть несколько моделей схемы Фейстеля.

В отличие от традиционной сети Фейстеля, где входными данными является открытый текст сообщения, в разрабатываемой модели на вход подаётся битовая последовательность шифротекста, получаемая в при шифровании нетрадиционным алгоритмом.

Необходимым условием стойкости шифра является достижение полной диффузии. Диффузионный процесс шифра характеризуется результатом распространения влияние одного входного бита на много выходных. Шифр называется полным, если каждый выходной бит зависит от всех входных [5]. В рассматриваемых моделях все F -функции подразумеваются полными.

В большинстве шифров с архитектурой сети Фейстеля используемая функция F в течение каждого раунда зависит только от одного из подключей, вырабатываемых из основного ключа шифра. Сеть с такого рода зависимостью

функции гаммирования называют гетерогенной и гомогенной в противном случае. Применение гетерогенных сетей может значительно улучшить характеристики шифра, поскольку неравномерное изменение внутренних свойств сети в пределах допустимых границ делает изучение свойств шифра достаточно затруднительным занятием.

Для примера рассмотрим модель, в которой блок входных данных F длиной 128 бит разделяется на два подблока равной длины R_i и L_i .

При использовании гомогенной сети на каждом этапе шифрования используется отдельная ключевая последовательность $K^{(i)}$:

$$\begin{aligned} L_i &:= R_{i-1}, \\ R_i &:= L_{i-1} \oplus F(R_{i-1}, K_i) \end{aligned} \quad (8)$$

При использовании гетерогенной сети на каждом этапе функция шифрования F подблока зависит не только от раундового ключа $K^{(i)}$, но и от выбранной системы оснований (1):

$$\begin{aligned} L_i &:= R_{i-1}, \\ R_i &:= L_{i-1} \oplus F(R_{i-1}, K_i, P(x)) \end{aligned} \quad (9)$$

Для проверки эффективности модифицированных алгоритмов был проведен анализ статистических характеристик получаемых шифртекстов. Проверка на удовлетворение модели строгому лавинному критерию проведена путем проверки полученной битовой последовательности статистическими тестами Американского института стандартов NIST для криптографических функций [8]. «NIST Statistical Test Suite» – статистический пакет, состоящий из 16 тестов, разработанных для проверки случайности двоичных последовательностей, производимых как техническими средствами, так и программным обеспечением.

Как показали тесты, применение схемы Фейстеля позволяет скрыть структурные особенности блока исходного текста, что при использовании правильного режима шифрования значительно улучшает статистические характеристики всего шифротекста.

Полученные модели были реализованы программно с использованием языка программирования Java. Использование платформы Java даёт возможность использовать программную реализацию нетрадиционного алгоритма шифрования в широком спектре устройств и систем. Реализация библиотеки криптоалгоритма позволяет внедрять данный алгоритм шифрования в различные клиент-серверные системы, веб-приложения и мобильные устройства.

Заключение

Предлагаемая система шифрования основывается на теории непозиционных полиномиальных систем счисления. Криптостойкость разработанного алгоритма характеризуется полным секретным ключом шифрования, который определяется не только длиной ключевой последовательности, но и выбранной системой полиномиальных оснований.

Разработанная модель модификации криптографического алгоритма на основе сети Фейстеля позволит существенно повысить статистические характеристики получаемых шифротекстов.

Литература

- [1] Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. - 439 с.
- [2] Бияшев Р.Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10. 1985: утв. 28.03.1986. - М., 1985. - 328 с.
- [3] Бияшев Р.Г., Нысанбаева С.Е. Алгоритм формирования электронной цифровой подписи с возможностью обнаружения и исправления ошибки // Кибернетика и системный анализ. – 2012 г. – Т. 48, № 4. – С. 14-23.

- [4] Нысанбаев Р.К. Криптографический метод на основе полиномиальных оснований // Вестник Мин-ва науки и высшего образования и Нац. акад. наук Республики Казахстан – Алматы: Гылым. – 1999. – № 5. – С. 63-65.
- [5] Schneier B., Kelsey J.: Unbalanced Feistel Networks and Block-Cipher Design, Fast Software Encryption, Third International Workshop Proceedings (February 1996), Springer-Verlag, 1996, pp. 121-144.
- [6] Feistel H. Cryptography and Computer Privacy, H. Feistel // Scientific American. – 1973. V. 228, N. 5. P. 15-23.
- [7] Report on the Development of the Advanced Encryption Standard (AES) / J. Nechvatal, E. Barket, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback // Computer Security Division; Information Technology Laboratory; NIST: Technology Administration; U.S. Department of Commerce, 2000, 116 p.
- [8] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto et al. // NIST Special Publication 800.-22, 2001, 154 p.

Полежаев П.Н.

**РЕАЛИЗАЦИЯ АЛГОРИТМА МЕЖСЕТЕВОГО ЭКРАНА ДЛЯ
ОБЛАЧНЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ
ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ**

Оренбургский государственный университет, Оренбург, Российская Федерация

В настоящее время облачные технологии получили большое распространение, они активно используются для организации функционирования ИТ-инфраструктур компаний (модель IaaS, Infrastructure as a Service), а также для предоставления доступа к программному обеспечению в виде сервиса (модель SaaS, Software as a Service).

Одной из актуальных проблем для облачных систем является обеспечение их безопасности [1], в частности решение задачи фильтрации сетевого трафика средствами межсетевых экранов. Эффективность ее решения зависит не только от правильной настройки правил фильтрации, но и от адекватного выбора мест установки межсетевых экранов. Обычно они располагаются на границах сетей, в этом случае они способны проверять входящий и исходящий трафик, однако внутрисетевой трафик остается нефильтрованным. Такой принцип совершенно неприемлем для облачных систем, использующих средства виртуализации ресурсов (виртуальные машины, виртуальные сети и т.п.) для размещения данных и приложений различных пользователей.

С целью контроля изоляции трафика различных пользователей друг от друга, а также для обеспечения безопасности их виртуальных сетей необходима реализация распределенного межсетевого экрана, способного выполнять анализ потоков данных, передаваемых между любой парой узлов (физических и виртуальных), а не только на границах сети.

Вариант архитектуры подобного решения был нами предложен в работе [2]. Он основан на применении технологии программно-конфигурируемых сетей и протокола OpenFlow [3] для решения следующих задач:

а) реализация межсетевого экрана на уровне сети с фильтрацией трафика в каждом коммутаторе OpenFlow, а также на узлах сети с помощью программного коммутатора OpenVSwitch, поддерживающего OpenFlow;

б) эффективная маршрутизация сетевого трафика внутри сети, позволяющая прогонять его через элементы безопасности (служебные виртуальные машины, содержащие: системы обнаружения вторжений, средства глубокого анализа и фильтрации пакетов, средства защиты от утечек данных, антивирусы и т.п.) или ответвлять его на них.

В основе подхода программно-конфигурируемых сетей лежит возможность динамического управления пересылкой данных в сети с помощью

открытого протокола OpenFlow. Все сетевые коммутаторы, поддерживающие OpenFlow, объединяются под управлением контроллера OpenFlow, который обеспечивает приложениям доступ к управлению сетью.

Каждый коммутатор OpenFlow имеет таблицу потоков, содержащую правила обработки пакетов. Каждое правило включает две части – признаки заголовков пакетов и набор действий. При поступлении в коммутатор нового пакета, происходит сопоставление его заголовков с признаками правил в таблице. В случае совпадения выполняются все действия из соответствующего набора. Если подходящее правило в таблице отсутствует, то пакет передается контроллеру OpenFlow. Контроллер принимает решение о дальнейших действиях над пакетом, которые реализуются в виде команды передачи пакета на определенный порт коммутатора и/или в установке для пакета нового правила в таблицу данного и, возможно, других коммутаторов.

Опишем предложенный алгоритм межсетевого экрана, который был реализован в рамках данного исследования (см. рисунки 1 и 2).

Для контроллера OpenFlow должны быть созданы три модуля:

а) Модуль топологии и состояния сети – строит текущее представление сети в виде мультиграфа, информация для весов вершин и дуг собирается из разных источников, к которым относятся протоколы SNMP, LLDP и ARP.

б) Модуль межсетевого экрана – обслуживает базу правил фильтрации пакетов, кэшированную в его памяти, и применяет ее.

в) Модуль маршрутизации и QoS – вычисляет и прокладывает маршруты передачи потоков данных в соответствии с текущим состоянием сети, требованиями к QoS, а также требованиями к используемым элементам безопасности.

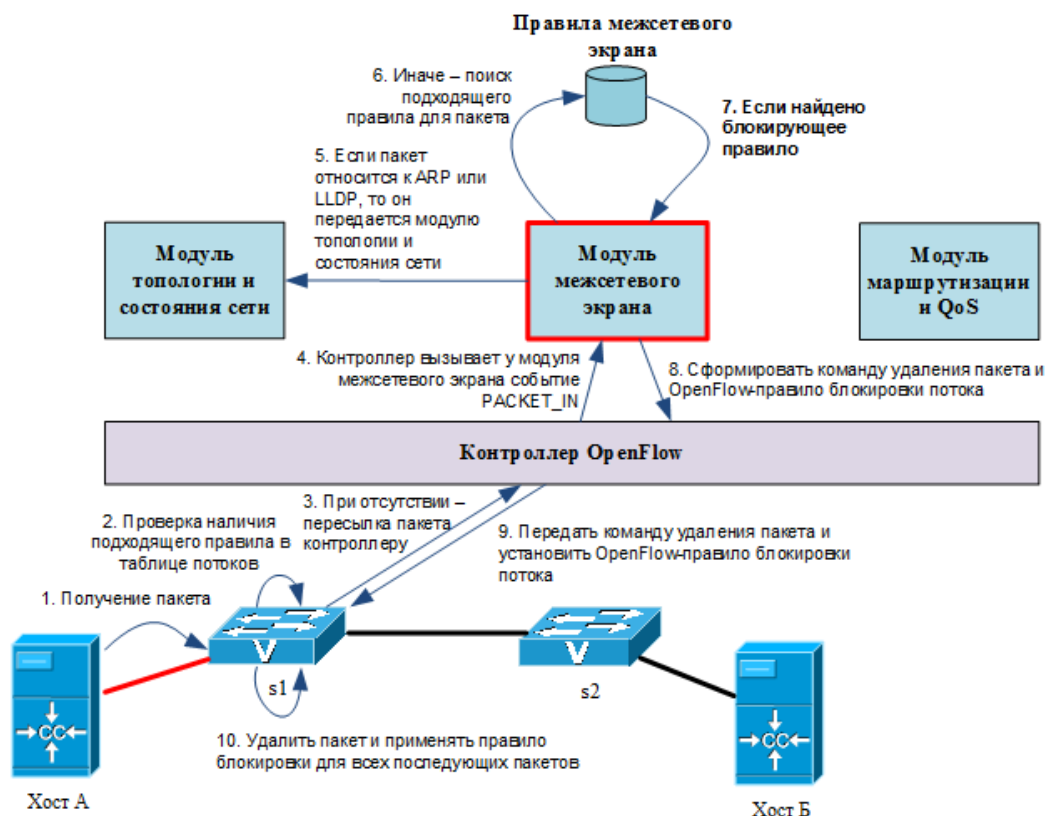


Рисунок 1 – Алгоритм работы межсетевого экрана в случае, когда для пакета найдено блокирующее правило

Когда коммутатор OpenFlow получает первый пакет нового потока данных, он проверяет наличие подходящего для пакета правила в его таблице потоков. При его отсутствии коммутатор пересылает пакет контроллеру OpenFlow, который в модуле межсетевого экрана вызывает событие PACKET_IN (появление нового необработанного пакета). Модуль межсетевого экрана по заголовкам пакета определяет тип его протокола, если это ARP или LLDP, то он пересылает его модулю топологии и состояния сети. Иначе – он производит просмотр правил межсетевого экрана в порядке их приоритета и выбирает первое подходящее из них.

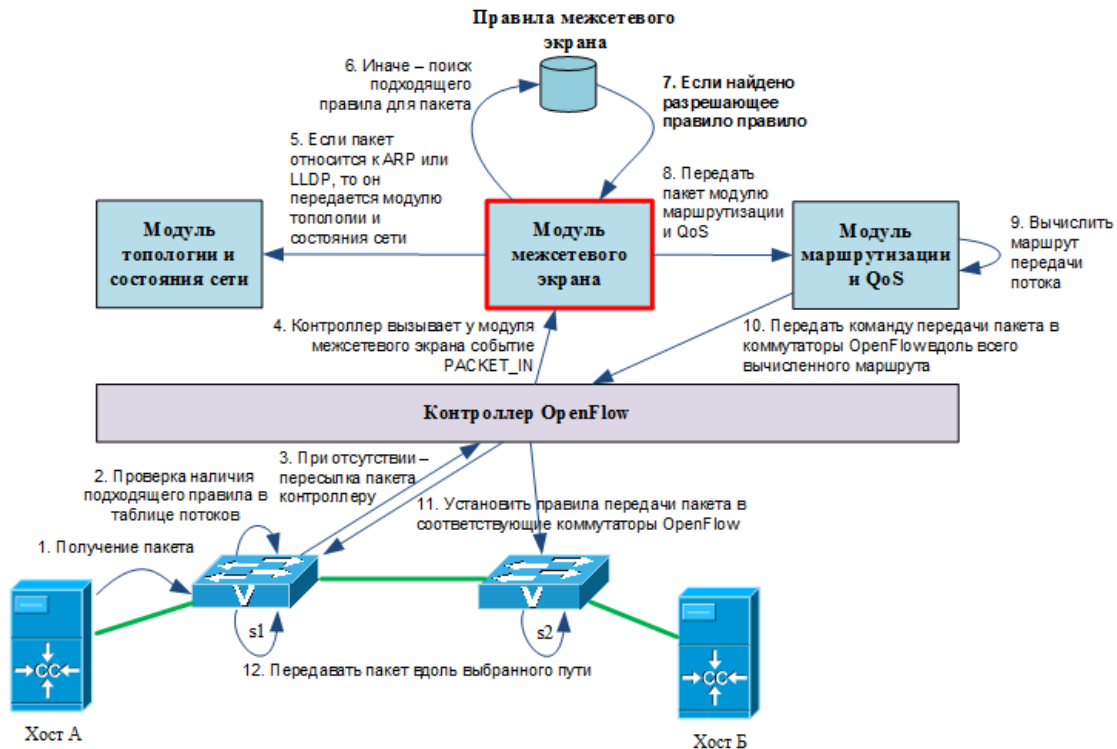


Рисунок 2 – Алгоритм работы межсетевого экрана в случае, когда для пакета найдено разрешающее правило

Если выбрано блокирующее правило (рисунок 1), то модуль межсетевого экрана формирует команду на удаление пакета, а также правило OpenFlow для удаления всех последующих пакетов данного потока. Команда и правило устанавливаются контроллером в коммутатор-источник пакета. В результате коммутатор удаляет текущий пакет (применяется команда), а также все последующие пакеты текущего потока (применяется правило OpenFlow в таблице потоков).

В случае, когда выбрано разрешающее правило (рисунок 2), модуль межсетевого экрана пересылает пакет модулю маршрутизации и QoS, который вычисляет оптимальный маршрут передачи данных, конвертирует его в набор правил OpenFlow для пересылки пакетов вдоль этого маршрута. Затем эти правила устанавливаются в таблицы потоков всех коммутаторов вдоль маршрута. В результате все пакеты будут передаваться по вычисленному маршруту.

Предложенный алгоритм межсетевого экрана был реализован и верифицирован на симуляторе программно-конфигурируемых сетей Mininet. В результате была подтверждена корректность и адекватность предлагаемого решения. В будущем планируется реализация принципа контроля состояния для межсетевого экрана.

Исследования выполнены при поддержке РФФИ (проект № 14-07-97034), Президента Российской Федерации, стипендии для молодых ученых и аспирантов (СП-2179.2015.5).

Литература

1. Адлова Л.С., Полежаев П.Н. Безопасность образовательных ресурсных облачных центров // "Информационная безопасность в свете Стратегии Казахстан-2050": Сборник трудов I Международной научно-практической конференции (12 сентября 2013 г., Астана). - Астана, 2013. - С. 86-91.
2. Полежаев П.Н., Адлова Л.С. Разработка архитектуры системы защиты информации в корпоративных программно-конфигурируемых сетях // Перспективные информационные технологии (ПИТ 2015), Том 1: труды Международной научно-технической конференции / под ред. С.А. Прохорова. - Самара: Издательство Самарского научного центра РАН, 2015. - С. 289-293.
3. Полежаев П.Н. Математическая модель распределенного вычислительного центра обработки данных с программно-конфигурируемыми сетями его сегментов // Вестник "Оренбургского государственного университета", 2013. - №5(154) - С. 198-204.

Рогов П. Д., Ворович Б.А., Белокур Н.А.

**СТРАТАГЕМНОЕ МЫШЛЕНИЕ КАК ОСНОВА ДОСТИЖЕНИЯ
ЦЕЛЕЙ В БОРЬБЕ ЗА НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ**

Центральный научно-исследовательский институт вооружения и военной техники Вооруженных Сил Украины, г. Киев, Украина.

Все люди знают ту форму, посредством которой я победил, но никто не знает той формы, посредством которой я организовал победу... Когда формы нет, даже мудрец не сможет о чем-либо судить... У того, кто умеет нападать, противник не знает, где ему обороняться; у того, кто умеет обороняться, противник не знает, где ему нападать. Тончайшее искусство!

Сунь-цзы (VI–V вв. до н.э.)

Главным законом мирового развития с начала XXI века стала глобализация с ее объективными и закономерными процессами – интеграция, глобализация развития, глобальная трансформация. Для всех без исключения стран это открывает новые перспективы и, к тому же, несет и новые большие угрозы. Не может остаться в стороне этих процессов и Украина. Пребывание на грани двух больших пространств цивилизации (европейского и евразийского) является определяющим фактором ее политической судьбы. Выбор внешнеполитического вектора, а соответственно и стратегии национальной безопасности для Украины предопределяет актуальность статьи. Этот вопрос изучали много исследователей [1 - 4, 8]. Процессы глобализации стали вызовом для большинства национальных государств, невзирая на их пространственное размещение, уровень политического и экономического развития. Концепция глобализации в современной политологии является одним из самых популярных инструментов анализа международных процессов.

В процессе проведения глобальной политики нивелируются противоречия международных отношений в военно-политической, экономической и информационной сферах. Среди них – также противоречия, связанные с преодолением экономической отсталости развивающихся стран, закреплением их суверенитета и равноправия. Преодолеваются совместными усилиями негативные последствия деятельности руководителей государств с

целью устранения возможности возникновения глобальных экономических, энергетических и экологических катастроф.

Эволюционируя вместе с общественным развитием, политика и государственное управление в разных культурах породили такой специфический способ освоения социальной действительности как стратагемное мышление, что позволяет разработать непрямой способ победы (достижение желательных целей) в борьбе за национальные интересы.

Присутствуя во всех мировых культурах и находя отображение во всех цивилизациях, наибольшего развития стратагемное мышление (стратагемность) получила в восточной культуре, а именно в культуре Древнего Китая. Стратагемное мышление допускает наличие в действиях отдельных личностей, организаций и даже государств скрытого подтекста, скрытых целей, намерений и действий, которые отличаются от официально провозглашенных и декларируемых [5 - 7].

Термин “стратагема” имеет европейское происхождение, его возникновение связывают с древнегреческим словом *strategema*, служащим для обозначения военного дела и военных хитростей. В настоящее время термин “стратагема” может быть использован в нескольких значениях. В непосредственно прикладном варианте он обозначает военную хитрость или хитрость, уловку в политической, экономической, преступной деятельности, частной жизни [6, 7].

Китайские стратагемы не просто дают рецепты возможных действий. Они определяют ту сферу, в которой ты находишься, те моральные и социальные нормы, которым ты следуешь или которыми ты пренебрегаешь во имя достижения цели. Китайские стратагемы признают единственный критерий истинности — эффективность твоих действий в борьбе за власть и ресурсы. Для них не существует понятий нравственности, духовности, морали как необходимых элементов твоей личности или деятельности. Существует единственный критерий — эффективность. Нет друзей и союзников, все —

враги. Некоторые враги — явные, некоторые — тайные или потенциальные. Нравственность и прочие духовные атрибуты рассматриваются как инструменты, которыми ты должен пользоваться в своих целях, но отнюдь не как нормы, которым ты обязан следовать. Общий принцип китайских стратагем — “Цель оправдывает средства” [7].

Подобная практика была выработана в условиях бесконечных войн, когда вопросы нравственности и морали стояли далеко не на первом месте. На первом месте стоял вопрос о выживании. Выжить можно было, экономя и приумножая собственные ресурсы, заключая выгодные союзы, покоряя более слабых, избегая войн с более сильными. Согласно Х. Зенгера стратагемы могут относиться к разным категориям: камуфляж (чем-то правдоподобным); введение в заблуждение (чем-то ошибочным); увлечение добычи; блокада; получение преимущества; соращение и побег [6].

Под стратагемным мышлением понимается разновидность умственной деятельности человека, направленной на специфическое освоение социальной действительности в условиях противостояния, ради достижения интереса (выигрыша) с помощью выработки теории, правил, технических и конкретных приемов достижения стратегического преимущества в борьбе и противостоянии за счет планирования скрытой ловушки, маневра, приема, хитрости и т.п.

В более широком смысле, стратагемное мышление представляет собой совокупность умственных операций, направленных на освоение общественно-политической действительности с помощью планирования стратегических приемов и системы “непрямых ходов”, которые применяются для достижения скрытой цели, получения преимущества или перехвата инициативы в борьбе.

В современном обществе остро появляется проблема манипулирования человеческим сознанием и влияния на человеческое поведение, а применения разнообразных маневров и приемов во всех сферах общественной практики требует этико-моральной и ценностной регуляции. Противоречие между распространенным использованием, силой влиянию, которое имеет

стратагемное мышление в политической деятельности, с одной стороны, и тотальной теоретической неразработанностью, отсутствием осмысления этого явления, а с другой стороны – и создает научную проблему, которую необходимо оперативно решить.

Наиболее перспективными методами ведения информационной войны являются именно методы влияния на индивидуальное, групповое и общественное сознание (подсознание). Реализация подобных методов в информационную эпоху требует пересмотра на государственном уровне ключевых подходов к проведению внешней и внутренней политики.

После детального анализа американскими военными экспертами результатов вооруженных конфликтов с участием США (операций против Югославии, Афганистана, Ирака) была доказана необходимость достижения информационного преимущества над противником и совершенствования существующей системы проведения информационных и психологических операций.

В ходе этих кампаний американские военные еще раз убедились в огромном потенциале средств манипулирования информацией.

Предотвращение возможных угроз и противоправных действий могут быть обеспечены самими разными мероприятиями и средствами, начиная от внедрения философии глубоко осознанного отношения сотрудников к проблеме информационной безопасности и защиты информации, к созданию глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Учитывая изложенное, необходимо констатировать, что вследствие целеустремленной информационной деятельности стран друг на / против друга и недостаточному вниманию к формированию и реализации собственной государственной информационной политики (продвижению позитивного имиджа страны за рубежом, противодействию негативным внешним информационно-психологическим воздействиям и т.п.), в настоящее время

защита информационного пространства, защита индивидуального сознания ее граждан, массового сознания народа, являются одними из наиболее острых вопросов национальной безопасности любого государства.

Литература

1. Надольный И. Трансформация культурного потенциала личности в контексте глобализационных парадигм / Эффективность государственного управления в контексте глобализации и евроинтеграции: Материалы научно-практической конференции / Под общ. редакцией В. И. Лугового, В. М. Князева. - К.: Изд-во НАГУ, 2003. – С. 61.

2. Кравчук М. Концептуальная эволюция теорий глобализации // Политический менеджмент. - 2003. - № 2. – С. 122.

3. Ю. Нишанбаев. Восточные стратагемы, библия стратега. - М.: Амрита-Русь, 2007.

4. Стратагемы - оружие информационных атак. В. Боршевич, В. Тудос. E-mail: owl@dekart.com

5. Тридцать шесть стратагем. Китайские секреты успеха (Перевод с китайского В. В. Малявина. - М.: Белые альвы, 2000.

6. Х. фон Зенгер. Стратагемы. О китайском искусстве жить и выживать. - М.: Эксмо, 2004. – Т. 1-2.

7. А.И. Воеводин. Стратагемы - стратегии войны, манипуляции, обмана. - М.: Изд. группа “Эт Сеттера”, 2004.

8. В. Тарасов. Искусство управленческой борьбы. Технологии перехвата и удержания управления. - М.: Добрая книга, 2006.

Сарычев Ю.А., Сницаренко П.Н.

**УСЛОВИЯ ВНЕДРЕНИЯ ГОСУДАРСТВЕННОЙ СИСТЕМЫ
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНЫ
В ВОЕННОЙ СФЕРЕ**

Национальный университет обороны Украины имени Ивана Черняховского,
г. Киев, Украина

Надлежащее выполнение функций и задач Министерством обороны (МО) Украины и Вооруженными Силами (ВС) Украины, как основными субъектами обеспечения обороноспособности государства, которые определены законодательством, без достижения необходимого состояния информационной безопасности в военной сфере является невозможным. Ведь все процессы управления (осуществляющиеся исключительно информационными методами) по любой из определенных задач могут быть реализованы полностью только в состоянии информационной безопасности, когда созданы, доступны и защищены необходимые информационные ресурсы. Создать такие условия без привлечения инфраструктуры государства, лишь путем использования только собственных возможностей, МО и ВС Украины принципиально не в состоянии. Поэтому это обстоятельство обуславливает необходимость интеграции усилий разных ведомств и учреждений государства для создания и использования единого информационного пространства в интересах обеспечения информационной безопасности в военной сфере.

Таким образом, существует неотложная потребность внедрения общегосударственного механизма управления процессом обеспечения информационной безопасности Украины в военной сфере. Этот процесс является сложным и многогранным, поскольку он может включать целевые программы, проекты и отдельные действия (мероприятия, работы), которые направлены на реализацию определенного порядка обеспечения информационной безопасности государства в военной сфере. Исполнителями этого процесса должны быть как профильные структуры в составе МО Украины и ВС Украины, так и других субъектов Сектора безопасности и обороны государства, а также задействованные предприятия и учреждения Украины, которые не относятся к названным субъектам.

Для того, чтобы такой механизм управления мог быть внедрен в Украине и стал дееспособным (эффективным), необходимо создать систему обеспечения

информационной безопасности государства в военной сфере. При этом создание системы требует выполнения следующих главных условий.

Условие 1. Принятие единой терминологии относительно информационной безопасности государства в военной сфере. Необходимость этого условия является очевидной и чуть ли не самой главной, выходя из того, что все участники процесса обеспечения информационной безопасности государства в военной сфере должны однозначно понимать друг друга в ходе общения и проведения практических мероприятий. Наиболее важными и основополагающими для создания общегосударственной системы понятиями целесообразно считать такие.

Информационная безопасность государства в военной сфере – состояние защищенности информационного пространства военной сферы в условиях влияния внутренних и внешних информационных угроз.

Состояние защищенности информационного пространства военной сферы достигается способностью информационной инфраструктуры военной сферы своевременно образовать и постоянно поддерживать это пространство с необходимым уровнем полноты (достаточности) и защищенности и регламентированным доступом к информационным ресурсам для осуществления информационного обеспечения управления процессами военного строительства, подготовки и применения вооруженных формирований государства.

Объекты информационной безопасности государства в военной сфере – носители данных и информации в составе информационной инфраструктуры военной сферы.

Носителями данных и информации являются материальные объекты, которые обеспечивают получение, запись, хранение и передачу информации (данных) в пространстве и времени.

Субъекты обеспечения информационной безопасности государства в военной сфере – определенные и наделенные полномочиями организационные структуры, целью и заданием которых является построение, развитие, применение и защита составляющих информационной инфраструктуры военной сферы, которые

образуют (формируют) информационное пространство военной сферы.

Система обеспечения информационной безопасности государства в военной сфере – организованная совокупность органов государственного и военного управления, информационной инфраструктуры военной сферы, а также правовых, организационных и технических норм для формирования и реализации государственной информационной политики с целью создания и эффективного использования информационного пространства военной сферы и его всесторонней защиты от внешних и внутренних угроз.

Информационное пространство военной сферы – часть информационного пространства государства: среда, в которой происходят информационные процессы и информационные отношения относительно создания, сбора, получения, хранения, использования, распространения, охраны и защиты информации (информационных продуктов, информационных ресурсов) военного характера.

Условие 2. Наличие концептуальных основ обеспечения информационной безопасности Украины в военной сфере, которые утверждает Президент Украины. Главное направление принципов – определение основных ориентиров усовершенствования информационной инфраструктуры в интересах создания, развития и защиты единого информационного пространства военной сферы как базового элемента обеспечения информационной безопасности в этой сфере. Концептуальные основы должны базироваться на понятной всеми заинтересованными субъектами единой терминологии (выполнении условия 1). Такой документ должен стать нормативно-правовым фундаментом как всего процесса обеспечения информационной безопасности Украины в военной сфере, так и его государственного управления через внедрение соответствующей системы.

Условие 3. Внесение изменений в законодательное поле Украины ради возможности выполнения концептуальных положений. Это условие является важным ввиду того, что общегосударственное управление информационными процессами в военной сфере нуждается во “вторжении” в функциональную

деятельность разных ведомств, учреждений и организаций Украины, а потому эта потребность должна быть нормирована законодательством государства.

Условие 4. Принятие законодательного решения относительно создания организационной структуры государственной системы обеспечения информационной безопасности Украины в военной сфере. Утверждение концептуальных принципов обеспечения информационной безопасности Украины в военной сфере, а также выполнение условия 3 закладывает правовой фундамент для внедрения единой государственной политики и образования административно упорядоченной системы обеспечения информационной безопасности в этой сфере.

После выполнения приведенных условий может быть создана соответствующая организационная структура общегосударственной системы, обладающая следующими характерными особенностями.

Организационное обеспечение заключается в проведении общегосударственной и ведомственной координации мероприятий, направленных на достижение информационной безопасности Украины в военной сфере с контролем их выполнения, а также осуществлении взаимодействия всех привлекаемых субъектов для проведения таких мероприятий, и сегодня нуждается в следующем:

повышение роли Совета национальной безопасности и обороны Украины (СНБОУ) по вопросам информационной политики и информационной безопасности за счет создания при нем постоянно действующего рабочего органа по информационной безопасности Украины в военной сфере;

скорейшее общественно-политическое признание роли и повышение активности созданного Министерства информационной политики Украины как главного координатора деятельности субъектов по обеспечению информационного суверенитета Украины, в основе чего – обеспечение информационной безопасности государства, в том числе в военной сфере;

образование всеми министерствами (ведомствами) Украины структурных подразделений по вопросам отраслевой информационной безопасности, а в МО Украины – структурных подразделений по вопросам обеспечения

информационной безопасности в соответствии с уровнем их компетенции.

Организационное обеспечение нуждается также в усовершенствовании системы подготовки военных специалистов в области информационной безопасности, прежде всего, на основе новейшей теории информационной операции в военной сфере.

Неотъемлемой функцией организационной структуры также является методическое руководство, заключающееся в проведении мероприятий по конкретным видам деятельности (целевые программы, проекты, планы, действия, и тому подобное) относительно обеспечения информационной безопасности Украины в военной сфере в форме отдельных директив, распоряжений, инструкций, указаний, а также совещаний, научно-практических конференций и семинаров. При этом общее методическое руководство процессом обеспечения информационной безопасности Украины в военной сфере осуществляет Президент Украины – Верховный Главнокомандующий ВС Украины при участии рабочих органов СНБОУ. Методическое руководство отдельными направлениями деятельности в этой сфере должно осуществляться через профильные структурные подразделения задействованных субъектов в соответствии с уровнем их компетенции.

Обязательным элементом в реализации политики информационной безопасности государства в военной сфере является научное обеспечение, которое заключается в научном обосновании и осуществлении научного сопровождения мероприятий, направленных на развитие информационной инфраструктуры военной сферы, обеспечение достаточности информационного пространства военной сферы и его всестороннюю защиту от деструктивного информационного влияния.

Таким образом, выполнение указанных условий открывает путь к реализации системы обеспечения информационной безопасности Украины в военной сфере, эффективного государственного управления этим процессом,

причем не только в военной сфере, но аналогичным образом и в других сферах жизнедеятельности государства.

Сарычев Ю.А., Ткаченко В.А.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЙСК В СОВРЕМЕННЫХ УСЛОВИЯХ

Национальный университет обороны Украины имени Ивана Черняховского,
г. Киев, Украина

Опыт локальных войн и вооруженных конфликтов конца XX – начала XXI ст. свидетельствует, что неизменным атрибутом победы в современных условиях является обеспечение информационного преимущества в военной сфере, в частности преимущества в морально-психологическом состоянии собственных войск над войсками противника. Это достигается благодаря эффективным мероприятиям осуществления информационно-психологического влияния на собственные войска и войска противника. Такие мероприятия могут проводиться как в мирное время, так и в особый период.

Основной целью деструктивного информационно-психологического влияния, которое имеет негативные последствия для объекта влияния, следующее:

в мирное время - дестабилизация общественно-политической обстановки в государстве; деморализация мирного населения и армии; внесение раздора между политическими силами; создание предпосылок социального взрыва;

в военное время: подрыв морально-психологического состояния войск противника; внесение раздора между армией, народом и властью; дискредитация военного и государственного руководства; подстрекательство к неповиновению власти.

Информационно-психологическое влияние по характеру может быть:

наступательным – целью является распространение у противника

(правительства страны или блока стран, населения, военного командования и личного состава воинских частей и соединений) сомнений в правоте его собственных действий, деморализация и дезорганизация деятельности противника;

оборонным – целью является укрепление морально-психологического состояния своих войск, населения, а также защита от деструктивного информационно-психологического влияния противника и нейтрализация последствий такого влияния.

При этом под морально-психологическим состоянием личного состава понимают степень моральной готовности, военно-профессиональной и психологической способности личного состава выполнить определенные задания при любых условиях обстановки.

Информационно-психологическое влияние осуществляется в форме кампаний, операций, акций, атак и отдельных актов, которые могут реализовываться как самостоятельные мероприятия (действия), так и быть составляющими более масштабных военных или информационных кампаний, операций или акций. В интересах объединений, соединений и воинских частей, информационно-психологические мероприятия (действия) проводятся на стратегическом, оперативном и тактическом уровнях.

На стратегическом уровне для информационно-психологических мероприятий (действий) характерна глобальность, то есть системное применение возможностей не только вооруженных сил, но и других государственных и негосударственных учреждений.

На оперативном уровне информационно-психологические мероприятия (действия) проводятся в интересах достижения среднесрочных целей, поддержки военных кампаний и операций. При этом объектом влияния обычно являются войска противника и население в определенном регионе.

Как правило, информационно-психологические мероприятия (действия) стратегического и оперативного уровней проводят при участии военно-

политического руководства государств, которое определяет порядок их организации и проведения, регламентирует деятельность всех органов, которые принимают у них участие. Решение относительно осуществления информационно-психологического влияния принимает военное руководство, а само влияние осуществляют преимущественно штатные воинские подразделения, которые чаще всего называют силами психологических операций.

На тактическом уровне информационно-психологические мероприятия (действия) проводятся в пределах плановых мероприятий (действий) оперативного и стратегического уровней руководства и осуществляются в интересах выполнения боевых заданий воинскими соединениями, частями и подразделениями, в их зоне ответственности.

Относительно деструктивного информационно-психологического влияния на личный состав войск следует заметить, что он может осуществляться как общий (на военнослужащего как человека в обществе) – преимущественно в мирное время, так и как специальный (на воина и защитника) – преимущественно в особый период.

Как в мирное время, так и в особый период, цель деструктивного информационно-психологического влияния на личный состав войск достигается, в частности, путем:

возбуждение у солдат и офицеров страха и неуверенности в будущем;

формирование недоверия к командирам;

убеждение военнослужащих к разочарованию в собственных силах, невыполнению своих обязанностей, отказа от сопротивления противнику и сдаче в плен.

Такие результаты обеспечиваются реализацией мероприятий (действий) информационно-психологического влияния как на лиц, которые принимают решение (ЛПР) и олицетворяют органы военного управления, так и на подчиненных военнослужащих.

Мероприятия, которые проводятся против ЛПР, могут быть направленными на дезорганизацию их управленческой деятельности, на скрытое или открытое подталкивание их до принятия “необходимого” решения, на побуждение ЛПР к сознательному сотрудничеству с противником. Основная цель информационно-психологических мероприятий (действий) против ЛПР – подрыв его авторитета в глазах подчиненного личного состава вооруженных сил, собственного населения, мирового сообщества.

В отличие от информационно-психологического влияния на органы военного управления, в частности ЛПР, который должен быть избирательным с точки зрения его реализации, такое влияние на массовое сознание военнослужащих во время ведения “гибридной” войны выглядит более прямолинейным и агрессивным и имеет такую направленность:

акции запугивания противника (демонстрация военного могущества, политического давления, экономической блокады, свертывания культурных и научных контактов, и тому подобное);

критика и зарождение сомнений среди военнослужащих в правильности внешней и внутренней политики страны (коалиции стран);

осуждение моральных и военных взглядов политического, военного руководства и лидеров государства, подрыв их авторитета, а также доверия к ним в глазах военнослужащих;

дискредитация военно-политической теории, военной доктрины, военных концепций;

формирование у личного состава вооруженных сил негативного отношения до войны;

разжигание политической, национальной, религиозной, этнической вражды между разными группами личного состава вооруженных сил;

пропаганда политического, военного, экономического, технологического, информационного преимущества государства - противника и его союзников;

побуждение военнослужащих к антиобщественным поступкам, которые дестабилизировали бы нормальную повседневную жизнь армии;

распространение среди военнослужащих религиозных и националистических суеверий;

инициализация сомнений среди личного состава в целесообразности ведения боевых действий;

дезинформация военнослужащих относительно реального состояния дел на поле боя;

побуждение военнослужащих к симуляции, дезертирству и самовольному оставлению района боевых действий;

создание паники, массовых психозов, настроения поражения среди военнослужащих.

Базовыми методами информационно-психологического влияния, которые применяются среди военнослужащих, является убеждение и внушение. Информационно-психологическое влияние со стороны противодействующих сил на личный состав войск (сил) во время выполнения ими заданий может осуществляться в различных условиях обстановки.

Информация такого направления распространяется с помощью открыток, радио- и телевещания, Интернета, средств мобильной и громкоговорящей связи, а также другими каналами распространения информации. Техника передачи таких сообщений в ходе боевых действий может изменяться, но информационный смысл остается неизменным – прекратить боевые действия (сопротивление) противнику.

Таким образом, в данной статье приведены основные особенности осуществления информационно-психологического влияния на ЛППР и личный состав воинских формирований, который наиболее эффективно проявляется в условиях “гибридной” войны и требует реагирования на его проявления путем адекватного противодействия.

Сейлова Н.А., Алимсеитова Ж.К., Оган А., Балтабай А.

ПРИМЕНЕНИЕ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО ОТПЕЧАТКУ ПАЛЬЦА В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева, Алматы, Республика Казахстан

Информация является одним из наиболее ценных ресурсов любой компании, поэтому обеспечение защиты информации является одной из важнейших и приоритетных задач.

На сегодняшний день существуют множество аппаратных и программных средств биометрической защиты информации, такие как сканеры отпечатков пальцев, сканеры сетчатки глаза и многие другие.

Биометрия – уникальная, измеримая характеристика человека для автоматической идентификации или верификации. Термин «автоматически» означает, что биометрические технологии должны распознавать или верифицировать человека быстро и автоматически, в режиме реального времени. Идентификация с помощью биометрических технологий предполагает сравнение ранее внесенного биометрического образца с вновь поступившими биометрическими данными [1].

Все биометрические системы работают практически по одинаковой схеме. Во-первых, система запоминает образец биометрической характеристики (это и называется процессом записи). Во время записи некоторые биометрические системы могут попросить сделать несколько образцов для того, чтобы составить наиболее точное изображение биометрической характеристики. Затем полученная информация обрабатывается и преобразовывается в математический код.

Кроме того, система может попросить произвести еще некоторые действия для того, чтобы «приписать» биометрический образец к определенному человеку. Например, персональный идентификационный номер

(PIN) прикрепляется к определенному образцу, либо смарт-карта, содержащая образец, вставляется в считывающее устройство. В таком случае, снова делается образец биометрической характеристики и сравнивается с представленным образцом [2].

Идентификация по любой биометрической системе проходит четыре стадии: запись, выделение, сравнение, совпадение/несовпадение.

Отпечатки пальцев каждого человека уникальны по своему рисунку. Отпечатки пальцев не совпадают у одного человека на разных пальцах, даже у близнецов. Это одна из самых популярных технологий, которая применяется для обеспечения безопасности доступа к компьютеру и сети. У этой технологии, на сегодняшний день, наверное, больше всего применений.

Рассмотрим работу оптического USB 2.0 сканера отпечатков пальцев U.are.U 4500, который применяется в учебном процессе для изучения работы биометрической технологии по отпечаткам пальцев.

Вопрос быстрой и в тоже время защищенной идентификации пользователя выходит на первый план в современном обществе. U.are. U 4500 оптический USB 2.0 сканер отпечатков пальцев, который способен отказаться от скрытых или подмены отпечатков пальцев [3]. Модель U.are. U 4500 HD также оснащен датчиком высокого долговечного покрытия.



Рисунок 1. – USB 2.0 сканера отпечатков пальцев U.are. U 4500

Считыватель окончательных отпечатков пальцев USB U.are.U 4500 Fingerprint USB - это сканер предназначенный, как и для опытных пользователей, так и для использования в общих средах. Сканер U.are. U 4500 является естественным выбором для тех, кто выбирает самое лучшее. Считыватель U.are.U 4500 использует оптические технологии сканирования отпечатков пальцев для превосходного качества изображения и надежности продукта. Сочетание U.are. U 4500 отпечатков пальцев с FingerJet соответствие двигателя производит непревзойденную способность распознавать даже самые трудно распознаваемые отпечатки пальцев.

Применение устройства:

- наркологический диспансер;
- доступ в оздоровительный клуб членам клуба;
- выполнение рецепта;
- время и посещаемости;
- финансы и банковские реквизиты доступа;
- точка обслуживания (розничная торговля и ресторан);
- государственное и местное управление.

После установки драйверов устройства, у нас открывается окно программы, который имеет интерфейс, как показан на рисунке 2.



Рисунок 2. – Интерфейс программы

В окне мы выбираем сканер отпечатка пальцев (рисунок 3).

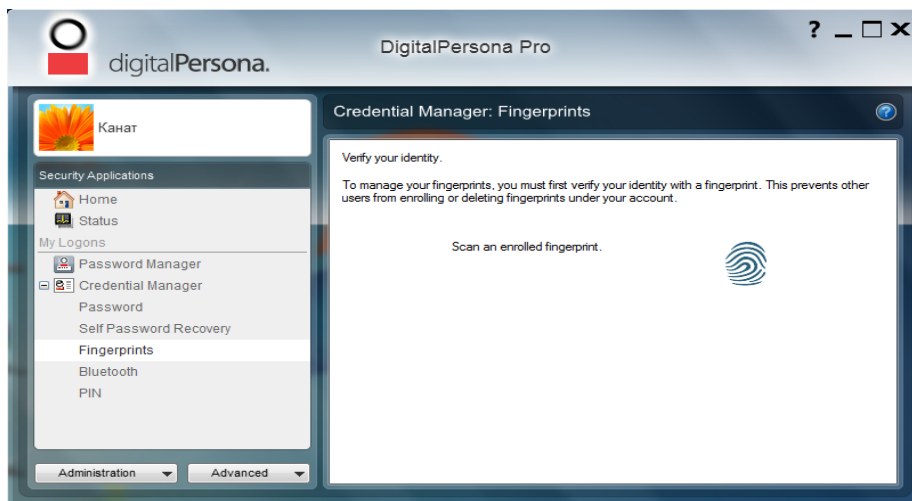


Рисунок 3. – Выбор сканера отпечатка пальцев

Следующим шагом, определяем какой из пальцев мы будем сканировать (рисунок 4), затем программой нам даётся 4 попытки отсканирования отпечатка пальцев, после завершения сканирования мы сохраняем сделанную нами работу.



Рисунок 4. – Сканирование отпечатков пальцев

После сканирования и сохранения отпечатка пальца, чтобы зайти в эту область мы должны правильно поставить палец для входа, если по каким-то

причинам вы неправильно поставили свой палец, программа выдаст ошибку, как показано ниже на рисунке 5.

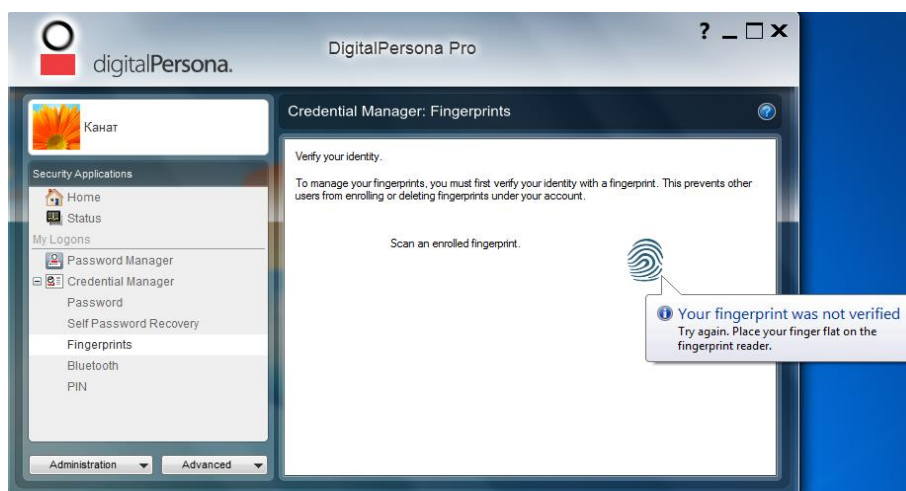


Рисунок 5. – Ошибка при сканировании

Теперь после завершения работы и перед включением компьютера у нас на рабочем столе выходит следующая информация (рисунок 6), т.е. вход в систему будет осуществляться по паролю пользователя системы и по сохраненным отпечаткам пальцев пользователя.



Рисунок 6. – Вход систему по сканированным отпечаткам пальцев

Для входа в систему мы выбираем сканер отпечатка пальцев (рисунок 7), программа проверяет соответствие сохраненного отпечатка пальцев вашему и

если он распознал, что это «Свой» вы смело входите в систему, а если же это «Чужой», то, увы система для вас недоступна.

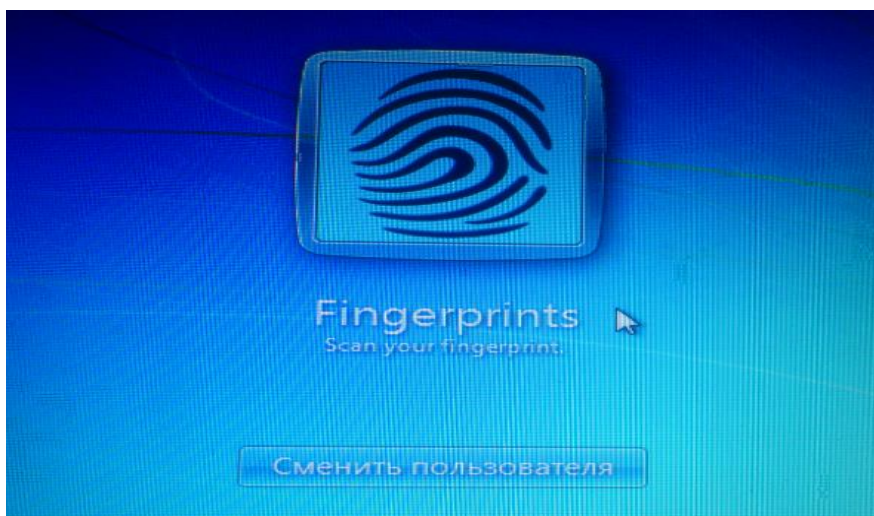


Рисунок 7. – Окно входа в систему

Использование биометрии для идентификации открывает ряд уникальных возможностей. Биометрия позволяет идентифицировать вас с помощью вас самих же [4]. Биометрия предлагает быстрый, удобный, точный, надежный и не очень дорогой способ идентификации с огромным количеством самых разнообразных применений.

Литература

- 1.Ахметов Б.С., Алибиева Ж.М., Бекетова Г.С. Биометрия, биометриялық идентификаторлар мен технологиялар. Вестник НАН РК2014. - № 6. - С. 3
2. Сейлова Н. А., Каныбек К., Жандыбаева М.А.Биометрические средства идентификации личности. Труды международных Сатпаевских чтений «Роль и место молодых ученых в реализации новой экономической политики Казахстана». Т.4. –2015. С. 911.
4. Балтабай А.Г., Айтхожаева Е. Ж., Сейлова н.А. Проектирование и обеспечение целостности биометрической базы данных. Труды международных

Сатпаевских чтений «Роль и место молодых ученых в реализации новой экономической политики Казахстана». Т.4. –2015. С. 547.

Сейткулов Е.Н., Боранбаев С.Н., Давыдов Г.В.

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТИ ПОЯВЛЕНИЯ БУКВ В ТЕКСТАХ НА КАЗАХСКОМ ЯЗЫКЕ

Евразийский национальный университет им. Л.Н.Гумилева

Белорусский государственный университет информатики и радиоэлектроники

Для формирования речеподобных сигналов определенного диктора на заданном языке необходимо иметь статистические характеристики текстов для заданного языка, чтобы речеподобные сигналы по формальным требованиям соответствовали статистическим характеристикам заданного языка.

Казахский кириллический алфавит, разработанный С.А. Аманжоловым и принятый в 1940 году, содержит 42 буквы: 33 буквы русского алфавита и 9 букв казахского алфавита Ә, Ғ, Қ, Ң, Ө, Ү, Ұ, Һ, І (таблица 1).

Таблица 1 –Алфавит казахского языка

1 А а	2 Ә ә	3 Б б	4 В в	5 Г г	6 Ғ ғ	7 Д д
8 Е е	9 Ё ё	10 Ж ж	11 З з	12 И и	13 Й й	14 К к
15 Қ қ	16 Л л	17 М м	18 Н н	19 Ң ң	20 О о	21 Ө ө
22 П п	23 Р р	24 С с	25 Т т	26 У у	27 Ү ү	28 Ұ ұ
29 Ф ф	30 Х х	31 Һ һ	32 Ц ц	33 Ч ч	34 Ш ш	35 Щ щ
36 Ъ	37 Ы ы	38 І і	39 Ы	40 Э э	41 Ю ю	42 Я я

Исследования вероятности появления букв казахского алфавита были выполнены с использованием текстов из средств массовой информации, художественной и технической литературы. Общее число выборки составило 435 тысяч знаков.

Частотность употребления букв казахского алфавита в текстах приведена в таблице 1.

Таблица 1. Частотность употребления букв казахского алфавита.

Буква	Частота употребления, %	Буква	Частота употребления, %	Буква	Частота употребления, %
А	12,52	О	2,45	Ь	0,04
Б	2,48	П	1,58	Э	0,05
В	0,29	Р	5,85	Ю	0,03
Г	1,23	С	3,51	Я	0,33
Д	4,52	Т	5,52	І	5,42
Е	8,02	У	1,52	Ғ	1,98
Ж	1,75	Ф	0,09	Қ	2,76
З	1,81	Х	0,28	Ң	1,71
И	1,31	Ц	0,06	Ү	0,81
Й	1,61	Ч	0,01	Ұ	1,01
К	2,68	Ш	1,44	Ё	0,01
Л	4,92	Щ	0,01	Һ	0,01
М	3,56	Ъ	0,01	Ә	0,96
Н	6,92	Ы	7,75	Ө	1,18

Статистические данные по длине слов (число букв в слове) представлены в таблице 2.

Таблица 2 Статистика числа букв в слове для казахского языка.

Число букв	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Частота, %	3,8	7,0	8,6	14,1	8,1	14,7	9,7	6,0	5,9	6,7	6,5	3,8	2,3	1,2	1,6

Слова с одной буквой в слове в казахском языке отсутствуют. Образование сложных слов в казахском языке может быть осуществлено двумя основными способами: путем сложения основ; путем перевода словосочетаний в сложные слова. Представленные данные по статистике длины слов в казахском языке являются усредненными, так как существенное влияние оказывает стиль изложения текста. Следует отметить, что буквы В, Ф, Ц, Ч, Ы, Ъ, Е, Э используются в казахском языке только для написания слов иностранного происхождения.

Частотность употребления букв казахского алфавита в начале слова отличается от общей частотности букв казахского алфавита в текстах. В таблице 3 приведена частотность появления букв в начале слова.

Таблица 3 – Частотность употребления букв казахского алфавита в начале слова

Буква	Частотность употребления, %		
	Словарь (50 000 слов)	Техническая литература (10 000 слов)	Выборка текстов средств массовой информации (10 000 слов)
Қ	14,5	12	11
Т	10,6	10	9,4
Ж	9,6	10	9,3
Б	8,7	10,6	12,3
А	8,5	8,5	8,2
К	7,4	6,3	7,3
С	6,4	8	7,5
Ш	4,8	1,5	2,3
М	3,7	5	4,4
Е	3,5	5	4,8

Д	3,2	3,7	4,3
О	1,9	3,5	3,8
Ұ	1,6	1,7	1,6
Ө	1,3	2,6	2,5
Ү	1,2	1,6	1,4
Ә	1,2	1,3	1
П	1,2	0,8	1
И	1,2	0,7	0,8
Н	1,2	1	1
Ы	1,1	0,2	0,3
З	1	0,7	0,8
Ф	1	0,01	0,1
І	0,8	0,8	0,8
Л	0,6	0,3	0,3
Р	0,6	0,9	0,9
Х	0,6	1,3	1,1
Э	0,6	0,6	0,6
У	0,6	0,6	0,5
В	0,3	0,1	0,1
Ғ	0,3	0,5	0,3
Ц	0,1	0,03	0,04
Ч	0,04	0,01	0,04
Щ	0,02	0,01	0,04
Ю	0,02	0,01	0,02
Я	0,02	0,03	0,06

Представленные статистические данные о частотности длины слов в казахском языке, частотности появления букв в начале слова и частотности появления букв в текстах на казахском языке являются достаточными для формирования

текстов, по которым можно формировать по базе аллофонов речеподобные сигналы на казахском языке.

Разработка и обоснование требований к базе аллофонов на казахском языке

Синтез речеподобных сигналов также как и синтез речи может быть выполнен двумя основными методами. Первый метод - это синтез речи с использованием фонемного синтезатора, суть которого заключается в генерации фонем и дальнейшей компиляции из них слов и фраз.

Второй метод синтеза речеподобных сигналов - это компиляционный синтез, который основан на формировании речевого сигнала путем последовательного акустического воспроизведения единиц речевого сигнала, которые подготовлены заранее и сохраняются в памяти. К структурным единицам речи относятся аллофоны, дифоны, трифоны, полифонны, слоги, отдельные слова и словосочетания из которых могут формироваться речеподобные сигналы.. Выбор структурной единицы речи для синтеза речи, с одной стороны, более просто вести по коротким сегментам с общим незначительным объемом памяти. Однако, при этом имеет место большое количество переходов от одного фрагмента речи к другому, что может сказаться на качестве синтезируемой речи, если не применять сплайны. С другой стороны, при выборе в качестве структурных единиц речи более длинных по звучанию фрагментов, речь становится более естественной, однако необходимы при этом большие объемы памяти и большие базы структурных единиц речи, создание которых является трудоемким процессом. Поэтому для синтеза речеподобных сигналов предлагается использовать аллофоны в качестве структурной единицы речи, а по речевой базе аллофонов можно будет формировать речеподобные сигналы голосом определенного диктора. Хотя качественные показатели речеподобных сигналов, сформированным таким методом, не совсем высокие, они никаким образом не могут оказать влияние на степень защиты речевой информации с помощью комбинированных маскирующих сигналов.

В базу аллофонов были включены все гласные и согласные буквы казахского алфавита, кроме **Ь** и **Ъ**. Для каждой буквы казахского алфавита было сформировано 8 аллофонов с учетом из окружения в тексте (в слове):

- окружение слева отсутствует, а справа расположена гласная буква;
- окружение слева отсутствует, а справа расположена согласная буква;
- слева расположена гласная буква, а справа окружение отсутствует;
- слева расположена согласная буква, а справа окружение отсутствует;
- слева расположена гласная буква и справа расположена также гласная;
- слева расположена согласная буква и справа расположена также согласная;
- слева расположена согласная буква, а справа расположена гласная;
- слева расположена гласная буква, а справа расположена согласная.

Индексы для разделения гласных аллофонов на твердые и мягкие как это делается для русского и белорусского языков, в казахском языке нет необходимости вводить. В казахском языке гласные **А, О, Ұ, Ы** всегда твердые, а гласные **Ә, Ө, Ү, І, Е** всегда мягкие.

Кроме того в базу аллофонов включены наиболее часто встречающиеся сочетания букв с мягким и твердым знаком характерных для типовых форм слов заимствованных с русского языка, что часто встречается в казахском языке. Это следующие сочетания **БЬ, ЗЬ, ТЬ, ЛЬ, НЬ, СЬ, СЬ, ДЬ, БЬ**.

В базе аллофоны имеют обозначения из цифр. Первая цифра обозначает окружение аллофона слева, а вторая цифра – окружение аллофона справа. Цифра **0** означает, что в данном положении окружение отсутствует. Цифра **1** означает, что в указанном положении находится гласная буква. Цифра **2** означает, что в указанном положении находится согласная буква. Так, например, аллофон имеет обозначение **Б12**. Это обозначает, что сформирован звуковой файл взятый из слитного текста с аллофоном **Б**, перед которым расположена гласная буква, а после указанного аллофона расположена согласная буква.

Для разделения гласных аллофонов на ударные и безударные может использоваться их обозначение из трех цифр. При этом, если первая цифра **1**, то гласный аллофон ударный. Если первая цифра **0**, то гласный аллофон безударный. Таким образом должна формироваться база аллофонов для синтеза речеподобных сигналов на казахском языке.

Перечень аллофонов для формирования речеподобных сигналов на казахском языке приведен в таблице 4.

Таблица 4 – Перечень аллофонов казахского языка

а001	ғ12	и001	м12	р01	ү022	ш10	ю022
а002	ғ20	и002	м21	р02	ү102	ш11	ю102
а012	ғ21	и012	м22	р10	ү110	ш12	ю110
а021	ғ22	и021	м20	р11	ү112	ш21	ю112
а022	д01	и022	н01	р12	ү120	ш22	ю120
а102	д02	и102	н02	р21	ү122	ш20	ю122
а110	д10	и110	н10	р22	ф01	щ01	я001
а112	д11	и112	н11	р20	ф02	щ02	я002
а120	д12	и120	н12	с01	ф10	щ10	я012
а122	д20	и122	н21	с02	ф11	щ11	я021
ә001	д21	й001	н22	с10	ф12	щ12	я022
ә002	д22	й002	н20	с11	ф21	щ21	я102
ә012	е001	й012	ң01	с12	ф22	щ22	я110
ә021	е002	й021	ң02	с21	ф20	щ20	я112
ә022	е012	й022	ң10	с22	х01	ы001	я120
ә102	е021	й102	ң11	с20	х02	ы002	я122
ә110	е022	й110	ң12	т01	х10	ы012	бь
ә112	е102	й112	ң21	т02	х11	ы021	зь
ә120	е110	й120	ң22	т10	х12	ы022	ть
ә122	е112	й122	ң20	т11	х21	ы102	ль
б01	е120	к01	о001	т12	х22	ы110	нь

б02	е122	к02	о002	т21	х20	ы112	сь
б10	ë001	к10	о012	т22	h01	ы120	сь
б11	ë002	к11	о021	т20	h02	ы122	дь
б12	ë012	к12	о022	у001	h10	і001	бъ
б21	ë021	к21	о102	у002	h11	і002	
б22	ë022	к22	о110	у012	h12	і012	
б20	ë102	к20	о112	у021	h21	і021	
в01	ë110	к01	о120	у022	h22	і022	
в02	ë112	к02	о122	у102	h20	і102	
в10	ë120	к10	о001	у110	ц01	і110	
в11	ë122	к11	о002	у112	ц02	і112	
в12	ж01	к12	о012	у120	ц10	і120	
в20	ж02	к21	о021	у122	ц11	і122	
в21	ж10	к22	о022	ұ001	ц12	э001	
в22	ж11	к20	о102	ұ002	ц21	э002	
г01	ж12	л01	о110	ұ012	ц22	э012	
г02	ж20	л02	о112	ұ021	ц20	э021	
г10	ж21	л10	о120	ұ022	ч01	э022	
г11	ж22	л11	о122	ұ102	ч02	э102	
г12	з01	л12	п01	ұ110	ч10	э110	
г20	з02	л21	п02	ұ112	ч11	э112	
г21	з10	л22	п10	ұ120	ч12	э120	
г22	з11	л20	п11	ұ122	ч21	э122	
ғ01	з12	м01	п12	ұ001	ч22	ю001	
ғ02	з20	м02	п21	ұ002	ч20	ю002	
ғ10	з21	м10	п22	ұ012	ш01	ю012	
ғ11	з22	м11	п20	ұ021	ш02	ю021	

Буквы **В, Ё, Ф, Х, һ, Ц, Ч, Щ, Ъ, Ь, Э** в исконно казахских словах не употребляются. Из них буквы **Ё, Ц, Ч, Щ, Ъ, Ь, Э** используются для произношения слов заимствованных из русского языка. Буква **һ** используется в словах заимствованных с арабо-персидских языков, и произносится как глухая **Х**. Общее количество аллофонов казахского языка для синтеза речеподобных сигналов составляет 361. Аллофоны, выделенные в таблице цветом не относятся к чисто казахским и являются заимствованными из других языков, поэтому их количество может быть сокращено, как редко встречающиеся в казахском языке.

Список литературы

1. Киселев, В.В. Система синтеза русской речи на основе компиляционного метода / В.В. Киселев, Б.М. Лобанов // Доклады БГУИР, 2004, №4, С.138 – 142.
2. Давыдов Г.В. Защита речевой информации шумовым речеподобным сигналом / Г.В. Давыдов, В.А. Попов, А.В. Потапович // Известия Белорусской инженерной академии. – 2000. – №1 (9) 71. – С. 146–148.
3. Хорев, А.А. Техническая защита информации: учеб. пособие для студ. вузов. В 3 т. Т. 1. Технические каналы утечки информации / А.А. Корев. – М.: НПЦ «Аналитика», 2008. – 436 с.
4. <http://www.dialog-21.ru/digests/dialog2006/materials/html/Lobanov.htm>, Лобанов Б.М. Фонетико-акустическая база данных для многоязычного синтеза речи по тексту на славянских языках / Б.М. Лобанов, Л.И. Цирульник, Б. Пьорковская, Я. Рафалко, Э. Шпилевский.
5. Давыдов, Г.В. Аппаратный генератор случайных чисел / Г.В. Давыдов, А.И. Кухаренко, В.А. Попов, А.А. Тереня // Тезисы докладов X Белорусско-Российской научно-технической конференции «Технические средства защиты информации», Минск, 29-30 мая 2012 г. – С.32.
6. Сучасная беларуская мова: Уводзіны. Фанетыка. Фаналогія. Арфаэпія. Графіка. Арфаграфія. Лексікалогія. Лексікаграфія. Фразеалогія. Фразеаграфія.

Вучэб. дапам. / Я.М. Камароускі, В.П. Красней, У.М. Лазоускі і інш. – 2-е выд. дапрац. і дап. – Мн.: Выш. школа, 1995. – 334 с.

7. Соломенник, А.И. Автоматизация процедуры подготовки нового голоса для систем синтеза русской речи / А.И. Соломенник, П.Г. Чистиков, С.В. Рыбин, А.О. Таланов, Н.А. Томашенко // Изв. вузов, Приборостроение, 2013, т. 56, №2, С. 29 – 32.

8. Литературный энциклопедический словарь/Под общ. ред. В.М. Кожевникова, П.А. Николаева. – М.: Сов. энциклопедия, 1987. –752 с. –(С.96-97: ст. Диалог; Диалогическая и монологическая речь.).

9. Ястрежембский, В.Р. Методологические аспекты лингвистического анализа диалога // Диалог. - М.: ИНИОН, 1991. - С. 82-110.

10. Сорокин, В.Н. Сегментация и распознавание гласных / В.Н. Сорокин, А.И. Цыплихин // Информационные процессы, 2004, т.4, №2, С. 202–220.

11. Рылов, А.С. Анализ речи в распознающих системах / А.С. Рылов – Мн.: Бестпринт, 2003. – 264 с.

12. Дегтярев, Н.П. Параметрическое и информационное описание речевых сигналов / Н.П. Дегтярев. – Минск: Объединенный институт проблем информатики Национальной академии наук Беларуси, 2003. – 216 с.

13. Ермоленко Т., Шевчук В. Алгоритмы сегментации с применением быстрого вейвлет–преобразования. // Диалог'2003. www.dialog-21.ru

14. Медведев, М.С. Фонемная сегментация речевого сигнала с использованием вейвлет–преобразования. // V Всероссийская конференция молодых ученых по математическому моделированию и информационным технологиям с участием иностранных ученых – 1-3 ноября, г. Новосибирск, Россия.

15. Лобанов, Б.М. Автоматизация клонирования персонального голоса и дикции для систем синтеза речи по тексту. Б.М. Лобанов, В.В. Киселёв. // Труды Международной конференции Диалог-2003, Москва, 2003, С. 417-424.

16. Bradley, J.S. ; Gover, B.N. Designing and Assessing the Architectural Speech Security of Meeting Rooms and Offices. Canada. 2006.

Сейткулов Е.Н., Боранбаев С.Н., Давыдов Г.В.

РАЗРАБОТКА АЛГОРИТМА СИНТЕЗА РЕЧЕПОДОБНЫХ СИГНАЛОВ НА КАЗАХСКОМ ЯЗЫКЕ

Евразийский национальный университет им. Л.Н.Гумилева

Белорусский государственный университет информатики и радиоэлектроники

Трудности синтеза речеподобных сигналов на казахском языке связаны с особенностями казахского языка в отличие от русского и белорусского языков: фонетический закон сингармонизма; мягкость и твердость слов; четкость произношения гласных и согласных, отсутствие смазывания; более быстрый темп речи по сравнению с белорусским и русским языками; падение ударения всегда на последний слог в слове; безударные гласные не подвергаются редукции, а звучат несколько короче, чем ударные; соединение нескольких слов в одно большое.

Фонетические закономерности казахского языка:

- звуки **п, к, қ** между гласными переходят в **б, г, ғ**;

- звуки **п, к, қ** в начале слова переходят в **б, г, ғ**, если предыдущее слово окончилось на гласную букву;

- звук **с** переходит в звук **ш**, если после **с** следовала согласная **ш** или **ж**;

- звук **а** произносится мягко между **ш-ш, ж-й, ш-й**.

На рисунке 4 представлен алгоритм синтеза речеподобных сигналов на казахском языке.

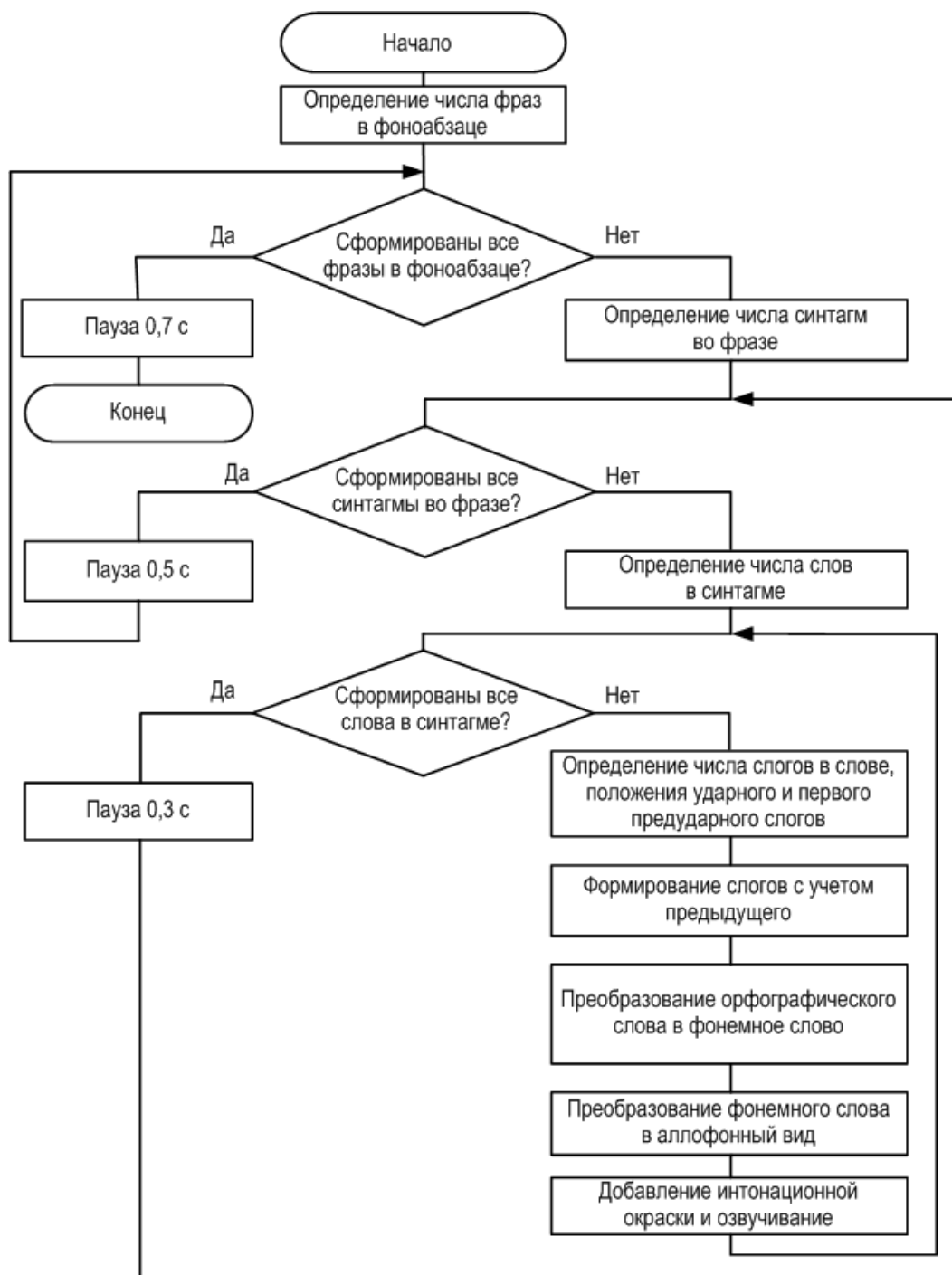


Рисунок 4 - Алгоритм синтеза речеподобных сигналов на казахском языке.

Работа алгоритма синтеза речеподобных сигналов на казахском языке . Генератор случайных чисел формирует целое случайное число в заданном числовом диапазоне. По значению этого случайного числа, согласно таблице вероятностей числа фраз в фоноабзаце и соответствующего им делению диапазона случайных чисел на поддиапазоны, определяется поддиапазон в который попадает это случайное число и соответствующее этому поддиапазону

значение числа фраз для заданного фоноабзаца. Далее для каждой фразы необходимо определить число синтагм из которых она состоит. Для этого формируется генератором случайных чисел новое случайное число. По значению случайного числа в соответствии с таблицей вероятностей числа синтагм во фразе и соответствующего им делению диапазона случайных чисел на поддиапазоны, определяется поддиапазон в который попадает это случайное число и соответствующее этому поддиапазону значение число синтагм во фразе. По значению следующего случайного числа определяется аналогичным образом число синтагм во второй фразе. Процесс продлается пока не будет определено число синтагм для каждой фразы фоноабзаца.

После этого формируется новое случайное число, по значению которого определяется число слов в первой синтагме согласно таблицы вероятностей числа слов в синтагме и соответствующего им делению диапазона случайных чисел на поддиапазоны. Так определяется число слов в первой синтагме. Аналогично определяется число слов для каждой синтагмы.

После этого генератором случайных чисел формируется следующее случайное число, по значению которого определяется число букв в первом слове согласно таблицы вероятностей числа букв в слове и соответствующего им делению диапазона случайных чисел на поддиапазоны. Аналогично определяется число букв для каждого слова всех синтагм.

После этого генератором случайных чисел формируется следующее случайное число, по значению которого определяется первая букв в первом слове согласно таблицы вероятностей букв в слове и соответствующего им делению диапазона случайных чисел на поддиапазоны. Аналогично определяются последующие буквы для каждого слова. При этом необходимо учитывать особенности казахского языка указанные выше. Если выбранная буква в слове противоречит особенностям казахского языка, то формируется генератором случайных чисел новое случайное число для выбора другой буквы не вступающей в противоречие с особенностями казахского языка.

Особенности казахского языка учтены в алгоритме синтеза речеподобных сигналов на казахском языке. В блоке **"Формирование слогов с учетом предыдущего"** происходит выбор гласных в слове по первой гласной в этом слове. Если первая гласная в слове мягкая, то и остальные гласные в слове должны быть мягкими.

Таким образом, формируется текст речеподобных сигналов. Акустическое воспроизведение текста выполняется по базе аллофонов путем последовательного воспроизведения аллофона в виде wav файла, записанного в базе аллофонов.

Список литературы

1. Киселев, В.В. Система синтеза русской речи на основе компиляционного метода / В.В. Киселев, Б.М. Лобанов // Доклады БГУИР, 2004, №4, С.138 – 142.
2. Давыдов Г.В. Защита речевой информации шумовым речеподобным сигналом / Г.В. Давыдов, В.А. Попов, А.В. Потапович // Известия Белорусской инженерной академии. – 2000. – №1 (9) 71. – С. 146–148.
3. Хорев, А.А. Техническая защита информации: учеб. пособие для студ. вузов. В 3 т. Т. 1. Технические каналы утечки информации / А.А. Корев. – М.: НПЦ «Аналитика», 2008. – 436 с.
4. <http://www.dialog-21.ru/digests/dialog2006/materials/html/Lobanov.htm>, Лобанов Б.М. Фонетико-акустическая база данных для многоязычного синтеза речи по тексту на славянских языках / Б.М. Лобанов, Л.И. Цирульник, Б. Пьорковская, Я. Рафалко, Э. Шпилевский.
5. Давыдов, Г.В. Аппаратный генератор случайных чисел / Г.В. Давыдов, А.И. Кухаренко, В.А. Попов, А.А. Тереня // Тезисы докладов X Белорусско-Российской научно-технической конференции «Технические средства защиты информации», Минск, 29-30 мая 2012 г. – С.32.

6. Сучасная беларуская мова: Уводзіны. Фанетыка. Фаналогія. Арфаэпія. Графіка. Арфаграфія. Лексікалогія. Лексікаграфія. Фразеалогія. Фразеаграфія. Вучэб. дапам. / Я.М. Камароускі, В.П. Красней, У.М. Лазоускі і інш. – 2-е выд. дапрац. і дап. – Мн.: Выш. школа, 1995. – 334 с.

7. Соломенник, А.И. Автоматизация процедуры подготовки нового голоса для систем синтеза русской речи / А.И. Соломенник, П.Г. Чистиков, С.В. Рыбин, А.О. Таланов, Н.А. Томашенко // Изв. вузов, Приборостроение, 2013, т. 56, №2, С. 29 – 32.

8. Литературный энциклопедический словарь / Под общ. ред. В.М. Кожевникова, П.А. Николаева. – М.: Сов. энциклопедия, 1987. – 752 с. – (С.96-97: ст. Диалог; Диалогическая и монологическая речь.).

9. Ястрежембский, В.Р. Методологические аспекты лингвистического анализа диалога // Диалог. - М.: ИНИОН, 1991. - С. 82-110.

10. Сорокин, В.Н. Сегментация и распознавание гласных / В.Н. Сорокин, А.И. Цыплихин // Информационные процессы, 2004, т.4, №2, С. 202–220.

11. Рылов, А.С. Анализ речи в распознающих системах / А.С. Рылов – Мн.: Бестпринт, 2003. – 264 с.

12. Дегтярев, Н.П. Параметрическое и информационное описание речевых сигналов / Н.П. Дегтярев. – Минск: Объединенный институт проблем информатики Национальной академии наук Беларуси, 2003. – 216 с.

13. Ермоленко Т., Шевчук В. Алгоритмы сегментации с применением быстрого вейвлет–преобразования. // Диалог'2003. www.dialog-21.ru

14. Медведев, М.С. Фонемная сегментация речевого сигнала с использованием вейвлет–преобразования. // V Всероссийская конференция молодых ученых по математическому моделированию и информационным

технологиям с участием иностранных ученых – 1-3 ноября, г. Новосибирск, Россия.

15. Лобанов, Б.М. Автоматизация клонирования персонального голоса и дикции для систем синтеза речи по тексту. Б.М. Лобанов, В.В. Киселёв. // Труды Международной конференции Диалог-2003, Москва, 2003, С. 417-424.

16. Bradley, J.S. ; Gover, B.N. Designing and Assessing the Architectural Speech Security of Meeting Rooms and Offices. Canada. 2006.

Сейткулов Е.Н., Оспанов Р.М., Майманов Е.М.

СЕРВИС ШИФРОВАНИЯ ДАННЫХ НА ЗАДАННОЕ ВРЕМЯ

Факультет информационных технологий ЕНУ им. Л.Н. Гумилева,
НИИ информационной безопасности и криптологии ЕНУ им. Л.Н. Гумилева,
ТОО «Information Services Group»,
Астана, Республика Казахстан

Введение. В 1994 году в [1, chapter 14.5] Тимоти Мэй (Timothy С. May) впервые предложил рассмотреть задачу отправки секретного сообщения в будущее, т.е. задачу шифрования сообщений, расшифрование которых возможно только лишь по истечении заданного времени в будущем.

Решение этой задачи имеет ряд интересных практических приложений, например:

- 1) “запечатывание” дневников и записей на определенный срок, причем таким образом, что даже их автор не мог бы их “распечатать” раньше срока,
- 2) защита данных, полученных в результате научных исследований или экспериментов, до момента их завершения и опубликования с

целью предотвращения утечки информации или давления со стороны заинтересованных лиц,

- 3) сокрытие предложения цены участниками торгов до завершения торговой сессии,
- 4) защита промежуточных данных голосования до их завершения с целью исключения влияния на ход голосования.

Область применения может быть весьма обширна и включает в себя не только аукционы и голосование, а также финансовые рынки и их регулирование, электронная коммерция, право.

Необходимость в таком криптографическом приложении имеется и в Республике Казахстан. В частности, в 2015 году Веб-портал государственных закупок Республики Казахстан выразил свою потребность в средстве, обеспечивающем шифрование данных пользователей портала (поставщиков), с возможностью расшифрования не ранее заданного времени.

С 1994 года исследователи описали ряд интересных подходов к решению задачи шифрования в будущем. В 1996 году в [2] Ривест, Шамир и Вагнер (R. L. Rivest, A. Shamir, D. A. Wagner) применили “шарады” с временным замком (“time-lock puzzles”). В 1997 году в [3] Беллар и Голдвассер (M. Bellare, S. Goldwasser) описали схему шифрования с частичным условным депонированием ключей (partial key escrow protocol). В 2005 году в [4] Блейк и Чан (I. F. Blake, A. C.-F. Chan) использовали билинейные отображения на GDH группах (Gap Diffie-Hellman groups). Существует ряд других работ в этом направлении.

Отдельного внимания заслуживает следующий подход. В 2006 году в [5] Рабин и Торп (M.O. Rabin and C. Thorpe) построили криптографический протокол, обеспечивающий зашифрование сообщений, расшифрование которых будет гарантированно не ранее заданного точного времени, даже если

это расшифрование окажется нежелательным для отправителя. Свое решение авторы назвали Time-Lapse Cryptography (TLC), отмечая различие между протоколами, подобным их, в которых время с момента зашифрования до момента расшифрования фиксировано, и другими протоколами, в которых дается лишь оценка этого времени или находится нижний предел оценки. На свое изобретение авторы получили патент [6]. В 2009 году в [7] была представлена реализация TLC на языке Erlang 5.6.5 на серверах под управлением Debian 4.0 Linux на четырехъядерных процессорах Intel Xeon, 2.0 ГГц.

В 2015 году нами была разработана на языке Java программная реализация протокола на основе TLC с целью создания программного комплекса, обеспечивающего шифрование данных пользователей портала государственных закупок Республики Казахстан, с возможностью расшифрования не ранее заданного времени. В данной работе мы представляем новый протокол, основанный на TLC, с применением криптографии на эллиптических кривых над конечными полями.

Протокол TLC. Рассмотрим описание протокола TLC, опубликованного в [5]. Его авторы использовали протокол распределенной генерации ключей Педерсена (Pedersen distributed key generation), протокол проверяемого порогового разделения секрета Фельдмана (Feldman verifiable threshold secret sharing) и алгоритм шифрования Эль-Гамала. Протокол осуществляется при помощи Сервиса (Time-Lapse Cryptography Service), состоящего из n участников P_1, \dots, P_n . Каждый участник Сервиса P_i может быть представлен автономным компьютером (сервером), безошибочно и секретно выполняющим вычисления, предусмотренные протоколом, надежно хранящим все свои секретные данные, имеющим безопасный способ резервного копирования данных для аварийного восстановления. Все участники Сервиса могут приватно и секретно обмениваться информацией между собой, образуя сеть. Предполагается пороговое значение t такое, что самое большее $t - 1$ участников

могут нарушить протокол, и самое меньшее t участников являются надежными. Должно выполняться условие $n \geq 2t - 1$ ($t \leq (n+1)/2$), например, если $n = 3$, то $t \leq 2$). Для дальнейшей эффективности, надежности и устойчивости к атакам, используется небольшая сеть M из K менеджеров, которые действуют как “команда управления” Сервисом. Эта управляющая команда должна создавать расписание открытых и соответствующих закрытых ключей, создаваемых Сервисом; вести внутреннюю доску объявлений для использования участниками Сервиса; вести открытую доску объявлений для пользователей Сервиса. Целостность этих досок объявлений достигается каждым менеджером, ведущим собственные копии этих двух досок объявлений. Участники и пользователи Сервиса будут смотреть на сообщения, размещенные на каждом из копий досок объявлений, и определять правильные значения большинством записей. Каждое сообщение Сервиса сопровождается цифровым подписью. Действия всех участников протокола синхронизируются при помощи общедоступных и надежных часов таких, как предоставляемых NIST. Протокол предусматривает использование согласованных параметров алгоритма шифрования Эль-Гамала: простое число p , порождающий элемент g простого порядка q . Эти параметры можно найти, например, в документах RFC 3526 [8] и RFC 5114 [9].

Пусть в некоторый момент времени T Алиса хочет отправить Бобу зашифрованное сообщение m так, чтобы Боб смог расшифровать его не раньше установленного будущего момента времени $T+\delta$, причем без дальнейшего участия Алисы.

1) Алиса запрашивает или выбирает у Сервиса подходящую ключевую структуру K_{ID} . Ключевая структура $K_{ID} = (ID, T_{ID}, \delta_{ID}, PK_{ID})$ состоит из уникального идентификатора ID , времени публикации T_{ID} , промежутка времени δ_{ID} и открытого ключа PK_{ID} .

2) Сервис может генерировать ключевые структуры на периодической основе; например, каждый день он может создавать ключи со сроком службы 1

неделю, или каждые 30 минут создавать ключи со сроком службы 2 часа. Такое расписание размещается менеджерами на открытой доске объявлений. Кроме того, Сервис может принимать запросы от пользователей генерировать новые ключи с заданным сроком службы; менеджеры принимают эти запросы и размещают их на открытой доске объявлений. Участники Сервиса создают ключи согласно протокола, подписывают их и опубликовывают подписанные ключевые структуры на открытой доске объявлений.

Генерация ключевых структур происходит следующим образом:

Каждый участник P_i должен сгенерировать случайный многочлен степени $t-1$ $f_i(z)=x_i+a_{1i}z+a_{2i}z^2+\dots+a_{t-1i}z^{t-1}$ из $F_q[z]$ (т.е. сгенерировать случайную последовательность $t-1$ значений $x_i, a_{1i}, a_{2i}, \dots, a_{t-1i}$). Составляющей частью секретного ключа является $f_i(0)=x_i$. Каждый участник P_i должен вычислить доли секрета $x_{ij}=f_i(j)$ ($f_i(j)=x_i+a_{1i}j+a_{2i}j^2+\dots+a_{t-1i}j^{t-1}$) и проверочные значения $c_0 = h_i = g^{x_i} \pmod{p}$, $c_1 = g^{a_{1i}} \pmod{p}$, ..., $c_{t-1} = g^{a_{t-1i}} \pmod{p}$. Затем каждый участник P_i отправляет всем участникам P_j, j из $[1, n]$, $(j, x_{ij}, \text{SIGN}_i(j, x_{ij}))$ и публикует на внутренней доске объявлений $(c_0, \text{SIGN}_i(c_0)), \dots, (c_{t-1}, \text{SIGN}_i(c_{t-1}))$. Теперь каждый P_j, j из $[1, n]$, может проверить, что x_{ij} правильная доля секрета, сравнивая $g^{x_{ij}} \equiv c_0 c_1^j c_2^{j^2} \dots c_{t-1}^{j^{t-1}} \pmod{p}$ (*). Если равенство (*) не выполняется, то участник P_j выражает жалобу против P_i . Если участник P_i получает жалобу против себя, то он опубликовывает значение x_{ij} , удовлетворяющее равенству (*). Каждый участник P_i отмечает дисквалифицированным каждого участника, который получил более k жалоб или ответил на жалобу значениями, не удовлетворяющими равенству (*). Каждый участник P_i создает множество Q всех не дисквалифицированных участников. Каждый участник P_j, j из Q , вычисляет $h = \prod_{i \text{ из } Q} h_i \pmod{p}$, формирует ключевую структуру $K_{ID}=(ID, T_{ID}, \delta_{ID}, PK_{ID}=h)$ и публикует $(K_{ID}, \text{SIGN}_j(K_{ID}))$ на внутренней и открытой досках объявлений.

3) Алиса проверяет соответствие цифровых подписей $\text{SIGN}_i(K_{ID})$ опубликованным ключевым структурам K_{ID} минимум для t участников и их

идентичность.

4) Алиса генерирует случайное значение y , вычисляет $c_1 = g^y \pmod p$ и $c_2 = m PK_{ID}^y \pmod p$ и отправляет пару $c = (c_1, c_2)$ Бобу.

5) Боб получает пару $c = (c_1, c_2)$ и ожидает либо значение y от Алисы, либо наступления момента времени $T_{ID} + \delta_{ID}$.

6) При наступлении момента времени $T_{ID} + \delta_{ID}$ каждый участник P_i должен опубликовать свою составляющую часть закрытого ключа $x = DK_{ID}$ на внутренней доске объявлений. Каждый участник проверяет, что у каждого P_i из Q опубликованная составляющая часть x_i удовлетворяет уравнению $g^{x_i} \equiv h_i \pmod p$. Каждый участник P_j должен опубликовать x_{ij} . Каждый участник P_j вычисляет сумму $DK_{ID} = x = \sum_{i \text{ из } Q} x_i \pmod q$ и публикует $(ID, DK_{ID}, SIGN_j(ID, DK_{ID}))$ на открытой доске объявлений.

7) Если Алиса отправляет Бобу значение y , то Боб расшифровывает сообщение m и без закрытого ключа, либо при наступлении момента времени $T_{ID} + \delta_{ID}$ Боб получает DK_{ID} от Сервиса и расшифровывает сообщение m : $m = c_2 c_1^{p-1-DK_{ID}} \pmod p$.

Протокол ECTLС. В основе нашего протокола лежит протокол TLC, описанный выше. Но вместо протокола распределенной генерации ключей Педерсена, протокола проверяемого порогового разделения секрета Фельдмана и алгоритма шифрования Эль-Гамала используются, соответственно, протокол распределенной генерации ключей, основанный на дискретном логарифмировании на эллиптических кривых [10], протокол проверяемого порогового разделения секрета Педерсена и алгоритм шифрования Эль-Гамала на эллиптических кривых. Таким образом, мы называем протокол Elliptic Curve Time-Lapse Cryptography (ECTLC). Протокол также осуществляется при помощи Сервиса (Time-Lapse Cryptography Service), описанного выше. Протокол предусматривает использование согласованных параметров используемой эллиптической кривой: модуль эллиптической кривой простое число p , уравнение эллиптической кривой, коэффициенты уравнения a и b из

поля F_p , точка эллиптической кривой G простого порядка q . Эти параметры можно найти, например, на сайте проекта SafeCurves [11].

Основные этапы нашего протокола осуществляются следующим образом:

1) Генерация ключей. При наступлении времени T_{ID} каждый участник P_i выбирает случайные значения $a_{i0}, a_{i1}, \dots, a_{ik}, b_{i0}, b_{i1}, \dots, b_{ik}$, где $k = t-1$, из поля F_p (т.е. $0 \leq a_{ir} < p, 0 \leq b_{ir} < p$). a_{i0} является частью закрытого ключа. Затем каждый участник P_i вычисляет $s_{ij} = a_{i0} + a_{i1}j + a_{i2}j^2 \dots + a_{ik}j^k \pmod{q}$ и $s'_{ij} = b_{i0} + b_{i1}j + b_{i2}j^2 \dots + b_{ik}j^k \pmod{q}$, где $j \neq i$ - номер сервера $P_j, 1 \leq j \leq n$. Затем каждый участник P_i вычисляет $C_{ir} = a_{ir} G + b_{ir} G', 0 \leq r \leq k$ (здесь применяются операция сложения точек эллиптической кривой и умножение точки на число). Затем каждый участник P_i отправляет s_{ij} и s'_{ij} серверам P_j по закрытым каналам связи между P_i и P_j , а $C_{ir} (0 \leq r \leq k)$ открыто публикует. Каждый участник P_i получив s_{ji} и s'_{ji} от участников $P_j, 1 \leq j \leq n, j \neq i$, проверяет равенство $s_{ji} G + s'_{ji} G' = \sum_{r=0}^k i^{r*} C_{jr} (**)$. Если равенство (***) не выполняется для значений s_{ji} и s'_{ji} , полученных от участника P_j , то участник P_i выражает жалобу против P_j . Если участник P_i получает жалобу против себя, то он публикует значения s_{ij} и s'_{ij} , удовлетворяющие равенству (**). Каждый участник P_i отмечает дисквалифицированным каждого участника, который получил более k жалоб или ответил на жалобу значениями, не удовлетворяющими равенству (**). Каждый участник P_i создает множество Q всех не дисквалифицированных участников. Каждый участник P_i из множества Q вычисляет $A_{i0} = a_{i0}G$ и публикует A_{i0} . Каждый участник P_i из множества Q получает A_{j0} и вычисляет открытый ключ $Pk_i = \sum_{j \text{ из } Q} A_{j0}$.

2) Зашифрование. Сообщение m помещается в точку эллиптической кривой:

выбирается точка $M=(x, y)$ такая, что часть вектора x фиксирована и соответствует сообщению m , а вектор y удовлетворяет уравнению эллиптической кривой при выбранном x , т.е. y – квадратный корень по модулю

p (алгоритм Шенкса). Выбирается случайное число r , $0 < r < q$. Вычисляется $C1 = rG$: $rG = G + G + \dots + G$ (r раз) ($+$ - операция сложения точек эллиптической кривой). Вычисляется $C2 = M + rPk$, где Pk - открытый ключ (точка эллиптической кривой). Пара $(C1, C2)$ – шифртекст.

3) Расшифрование. Вычисляется $DkC1$, где Dk – закрытый ключ. Вычисляется $-DkC1$ (обратный элемент для $DkC1$). Вычисляется $(-DkC1) + C2 = M$.

Заключение. В данной работе представлен протокол, обеспечивающий зашифрование сообщений, расшифрование которых будет возможно не ранее заданного времени. В основе его лежит один из подходов к решению задачи отправки секретных сообщений в будущее, известный как Time-Lapse Cryptography (TLC), описанный в [5], [6]. Однако вместо алгоритмов распределенной генерации ключей, проверяемого порогового разделения секрета и шифрования, используемых в TLC, применяются алгоритмы на основе криптографии на эллиптических кривых, что предполагает большую эффективность. В тоже время предполагается, что эти изменения не влияют устойчивость к известным атакам, обоснованную в [5]. Конечной целью наших исследований является разработка и внедрение практического сервиса шифрования данных на заданное время. Для этого предстоит решить целый ряд задач. Во-первых, нами ведется работа над программной реализацией протокола. Во-вторых, необходимо решить задачу развертывания безопасной и надежной распределенной сети участников сервиса, обеспечивающих генерацию ключей. В-третьих, в перспективе разработать аппаратно-программную реализацию сервиса. В-четвертых, в перспективе рассмотреть возможность использования новых более эффективных алгоритмов и алгоритмов, расширяющих функциональные возможности сервиса. В-пятых, необходимо подробное исследование криптографической стойкости протокола.

Литература

1. T. C. May. The Cyphernomicon: Cypherpunks FAQ and More, v. 0.666, September 10, 1994.
2. R. L. Rivest, A. Shamir, and D. A. Wagner. Time-lock puzzles and timed-release crypto. Technical Report MIT/LCS/TR-684, MIT, 1996.
3. M. Bellare and S. Goldwasser. Verifiable partial key escrow. In ACM Conference on Computer and Communications Security, pages 78–91, 1997.
4. I. F. Blake and A. C.-F. Chan. Scalable, server-passive, user-anonymous timed release public key encryption from bilinear pairing. Proceedings of 25th IEEE International Conference on Distributed Computing Systems, pages 504 – 513, 2005.
5. M.O. Rabin and C. Thorpe. Time-lapse cryptography. Technical report TR-22-06, Harvard University School of Engineering and Computer Science, 2006.
6. M.O. Rabin and C.A. Thorpe, Method and apparatus for time-lapse cryptography U.S. Patent 8,526,621.
7. C. Thorpe, M. Barrientos, and M.O. Rabin. Implementation of A Time-Lapse Cryptography Service. IEEE Symposium on Security and Privacy, Oakland, 2009
8. T. Kivinen, M. Kojo. More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). RFC 3526 (2003)
9. M. Lepinski, S. Kent. Additional Diffie-Hellman Groups for Use with IETF Standards. RFC 5114 (2008)
10. C. Tang, A. T. Chronopoulos. An Efficient Distributed Key Generation Protocol for Secure Communications with Causal Ordering. Proceedings of IEEE ICPADS 2005, The 11th International Conference on Parallel and Distributed Systems, Volume 2, Fukuoka, Japan, pp. 285 - 289, 20-22 July 2005.

11. Daniel J. Bernstein and Tanja Lange. SafeCurves: choosing safe curves for elliptic-curve cryptography. <http://safecurves.cr.yyp.to>, accessed 1 December 2014.

**Спирина Е.А., Самойлова И.А., Смирнова М.А., Мирзабаева В.Д.
ПОДГОТОВКА СТУДЕНТОВ ИТ-СПЕЦИАЛЬНОСТЕЙ В СФЕРЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КАРАГАНДИНСКОМ
ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ**

Карагандинский государственный университет имени академика Е.А.Букетова,
Республика Казахстан, г.Караганда

Отрасль информационной безопасности является одной из наиболее динамично развивающихся во всем мире. Казахстан не является исключением – в последнее время рынок средств обеспечения информационной безопасности показывает уверенный рост. Эксперты говорят, что сегодня наиболее значимыми трендами являются увеличения количества угроз, связанных с мобильными устройствами, и активное использование приемов социальной инженерии. «Традиционные» угрозы, такие, как вирусы и утечки информации, также не теряют своей актуальности.

В среднем, рынок информационной безопасности в Казахстане должен вырасти за год на 35%. Это несколько ниже, чем общемировые темпы (около 40%), и обусловлено это во многом тем, что информационные системы всё еще недостаточно активно используются казахстанскими компаниями. Предпосылки роста рынка информационной безопасности – это, прежде всего, увеличение количество информационных угроз, с которыми сталкиваются организации, а также такие факторы, как рост электронного документооборота, увеличение количества компьютеров и смартфонов в организациях [1].

Необходимость комплексной подготовки специалистов в сфере информационной безопасности и защиты информации в нашей стране

очевидна. В Республике Казахстан к IT-специальностям бакалавриата можно отнести специальности 5B060200 - Информатика, 5B070200 - Автоматизация и управление, 5B070300 - Информационные системы, 5B070400 - Вычислительная техника и программное обеспечение, 5B070500 - Математическое и компьютерное моделирование, 5B100200 - Системы информационной безопасности. В КарГУ имени Е.А. Букетова подготовка бакалавров IT-специальностей осуществляется на протяжении 20 лет по специальностям 5B060200 - Информатика, 5B070300 - Информационные системы. В 2011 году открыта специальность 5B070500 - Математическое и компьютерное моделирование.

В системе подготовки бакалавров по этим специальностям большое внимание уделяется формированию знаний и компетенций студентов в области информационной безопасности и защиты информации.

Учебный план обучающихся предполагает изучение элективных курсов «Информационная безопасность», «Защита информации». Целью изучения дисциплины «Информационная безопасность» является формирование базовых понятий в области информационной безопасности и защиты информации, виды и состав угроз информационной безопасности, принципы и общие методы обеспечения информационной безопасности, основные положения государственной политики обеспечения информационной безопасности, виды уязвимости защищаемой информации и формы ее проявления; каналы и методы несанкционированного доступа к конфиденциальной информации. Данные вопросы рассматриваются относительно требований к функциям системы защиты национальной информационной инфраструктуры Республики Казахстан.

Дисциплина «Защита информации» нацелена на изучение теоретических основ построения и практического использования систем защиты информации в информационных системах, формирование у студентов систематизированных представлений о принципах, методах и средствах реализации защиты данных

по приобретению практических навыков по защите информации в информационных системах, необходимых для их проектирования и эксплуатации. Изучаются основные понятия и направления в защите компьютерной информации, принципы защиты информации, классификации и примеры угроз безопасности компьютерным системам, современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах IT-безопасности, основные инструменты обеспечения многоуровневой безопасности в информационных системах

В элективных дисциплинах «Программирование на C++», «Программирование на Ассемблере», «Разработка клиент-серверных приложений», «Теория кодирования», «Параллельные вычисления» рассматриваются такие темы как: теория современных компьютерных вирусов; методы защиты данных и компьютерных программ от нелегального использования; методы идентификации программных продуктов; алгоритмы, системы и стандарты криптографической защиты информации; методы взлома механизмов защиты; современные технологии лицензирования локального и сетевого программного обеспечения; юридические аспекты защиты программных продуктов от нелегального использования; технологии защиты интеллектуальной собственности в Интернет и т.п.

При изучении дисциплин «Архитектура компьютерных систем» и «Операционные системы» особое внимание уделено изучению методов программно-аппаратной защиты данных в компьютерных системах.

Таким образом, выпускники IT-специальностей обладают базовыми профессиональными компетенциями в сфере информационной безопасности, способны использовать современные технологии программирования для разработки защищенного программного обеспечения; проводить анализ программного кода с целью поиска потенциальных уязвимостей; учитывать требования современных стандартов по безопасности компьютерных систем.

Однако имеется ряд проблем, а именно: в области информационных технологий, в том числе защиты информации, знания устаревают достаточно быстро и часто конкретные знания по дисциплинам, полученные в университете, оказываются недостаточными.

В таких условиях при подготовке IT-специалистов для сферы информационной безопасности необходимо сконцентрировать основное внимание на предоставлении базовых и фундаментальных знаний по дисциплинам, разнообразить круг практических умений, а также сформировать навыки у студентов к самостоятельному обучению. Это позволит выпускникам быстро адаптироваться на рынке труда.

Литература

1. <http://kapital.kz/tehnology/10299/rynok-informacionnoj-bezopasnosti-v-rk-vyrastet-na-35.html>

Стюгин М.А., Паротькин Н.Ю., Золотарев В.В.

ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ ДВИЖУЩЕЙСЯ ЦЕЛИ В ЗАДАЧАХ БЕЗОПАСНОЙ АДРЕСАЦИИ УЗЛОВ КОМПЬЮТЕРНОЙ СЕТИ

Сибирский государственный аэрокосмический университет, Красноярск,
Россия

Сложность современных информационных систем не дает возможности быть уверенным в отсутствии возможности их компрометации. Ситуацию усугубляет то, что защитник имеет всегда крайне ограниченный ресурс времени при проектировании системы. Злоумышленник же, наоборот, имеет большой ресурс времени на исследование уязвимостей, а также информацию относительно вновь найденных уязвимостей программного обеспечения не известных на этапе проектирования системы. Данный факт создает

информационную асимметрию между злоумышленником и защитником. Для решения проблемы такой асимметрии в задачах информационной безопасности была разработана технология MTD. Наиболее подробный обзор данной технологии приведен в статье [1]. Для затруднения этапа рекогносцировки перед реализацией сетевой атаки технология MTD применяется для перемешивания адресов узлов компьютерной сети. Существует несколько практических реализаций такого перемешивания [2, 3]. Разделяется физический и виртуальный (используемый для текущей маршрутизации) адрес хоста, а также модель проверки нарушения политики безопасности, в результате которой пакеты могут проходить через узлы, не имеющие доступа к данной информации [4].

Модель перемешивания адресов

В результате изменения адресации в сети не должна нарушаться работа легальных сервисов. Для этого каждый из узлов сети должен знать, куда направлять пакеты в определенный момент времени. Таким образом, каждый из узлов сети должен обладать достаточной информацией для работы сервисов и функционирования в качестве одного из хостов компании. Для распределения динамики в системе и оповещения хостов относительно таблиц маршрутизации мы можем выделить централизованную схему, частично централизованную схему и децентрализованную схему управления динамикой маршрутизации в локальной сети. Рассмотрим далее последовательно каждую из них.

Централизованная и децентрализованная схемы перемешивания адресов

В централизованной схеме все управление динамикой маршрутизации управляется одним приложением. При этом данное приложение может быть размещено как на одном хосте, так и распределено на нескольких хостах. Но при этом расположенное на каждом из хостов приложение не является самостоятельным в определении адресов и таблиц маршрутизации, а

руководствуется информацией из единого центра или заранее заложенными алгоритмами динамики системы. Если понимать централизованную схему перемешивания адресов в столь широком смысле, то, так или иначе все примеры реализации MTD, описанные в [1-4] можно отнести к централизованным схемам. Централизованная схема MTD приведена на рис.1а.

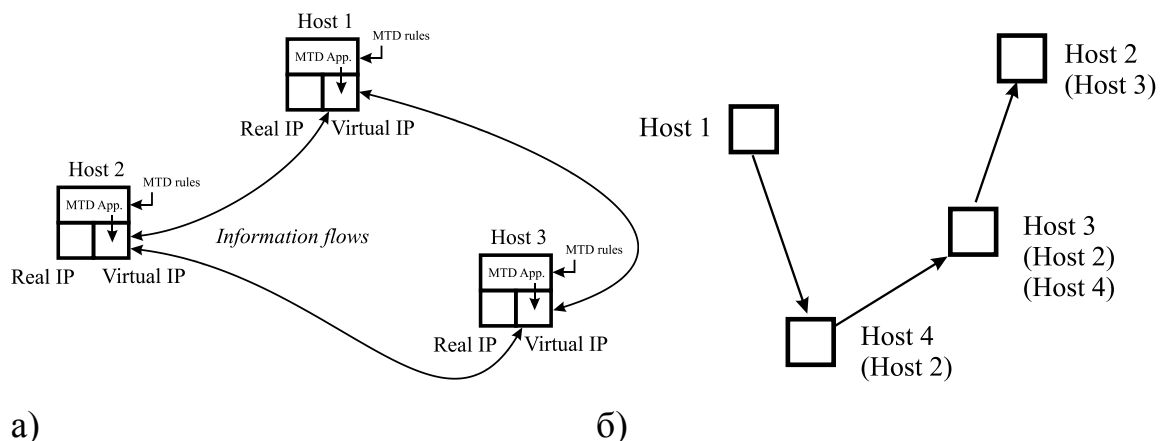


Рис.1. Централизованная и децентрализованная схема MTD.

Пример реализации централизованной схемы может заключаться в следующем. Виртуальные IP адреса меняются по заранее заданному алгоритму, параметром для которого является время и дата. Таким образом, каждый из хостов в определенный момент времени знает, под каким виртуальным адресом находится интересующий его сервис. Реализация вычисления и подмены виртуальных адресов происходит на низких уровнях и является прозрачным для вышестоящих приложений и сервисов.

В полностью децентрализованной схеме каждый из хостов сети участвует в изменении адресации и таблиц маршрутизации без согласования этого с другими хостами и с неким центром. Таблица виртуальных адресов является общеизвестной информацией в сети и каждый из хостов участвует в ее корректировке (рис. 1б). Предложенный вариант децентрализованной схемы является самым безопасным из всех методов перемешивания адресов в сети. В данном случае никто из участников обмена не может сказать, какому реальному хосту в сети предназначается тот или иной пакет, каждый из хостов видит только конечную таблицу адресов, но не маршрут и конечный узел

передачи. Данная модель перемешивания адресов на сегодняшний день еще не была рассмотрена в публикациях по теме MTD. Для решения задачи защиты адресации узла с защищаемой информацией в пределах ЛВС необходимо обеспечить сегментацию сети на канальном уровне при помощи динамических VLAN. Их идентификатор, а соответственно и метка кадра, будут определены текущей записью, под которой произошла авторизация узла на RADIUS-сервере. Динамическое изменение месторасположения узла относительно других VLAN делает атаку на конкретный узел в период до смены принадлежности сложной, поскольку злоумышленнику необходимо выполнить одно из трех действий: получить тегированный кадр, поступивший от искомого узла, что возможно только при подключении к порту коммутатора, входящего в данную сеть с заменой собой его функциональности; получить доступ к БД RADIUS-сервера, зная с алгоритмом ротации используемых учетных записей; получить доступ к конфигурации коммутатора, обслуживающего данную сеть.

Организация защиты на сетевом и транспортных уровнях будет осуществляться путем n -кратной ретрансляции защищаемой информации через групповую рассылку UDP сообщений с данными, зашифрованными на ключе узла назначения. Количество пересылок, порядок смен используемых адресов групп и динамическая принадлежность узла к вещанию в определенной мультикаст группе будет определяться тем же алгоритмом, что будет изменять принадлежность к определенной VLAN. Количество ретрансляций определяется текущим положением узла в циклической очереди. Вывод информации из данной сети будет производиться путем такой же отправки UDP сообщения через последовательность узлов, но в итоге он будет адресован клиентской группе, в которую входят авторы первоначального запроса и последовательно каждый из узлов динамической сети. Использование групповой рассылки с динамических мультикаст группах позволит сохранить работоспособность узлов относительно других сетевых протоколов.

Работа поддержана Минобрнауки России в рамках контракта № 14.574.21.0126 от 27.11.2014 г., уникальный идентификатор проекта RFMEFI57414X0126.

Литература

1. Jajodia, S. Moving Target Defense II. Application of Game Theory and Adversarial Modeling. Series: Advances in Information Security, 2013 / S. Jajodia, A.K. Ghosh, V. Swarup, C. Wang, X.S. Wang. - 203 p.

2. Carroll, T.E., Crouse, M., Fulp, E.W., Berenhaut, K.S. Analysis of network address shuffling as a moving target defense. 2014 IEEE International Conference on Communications, ICC 2014, Pages 701-706.

3. DeLoach, S.A., Ou, X., Zhuang, R., Zhang, S. Model-driven, moving-target defense for enterprise network security. Dagstuhl Seminar 11481 on Models@run.time. LNCS, 2014, Pages 137-161

4. Al-Shaer, E., Duan, Q., Jafarian, J.H. Random host mutation for moving target defense. 8th International ICST Conference on Security and Privacy in Communication Networks, SecureComm 2012; Volume 106 LNICS, 2013, Pages 310-327.

Султанов Т.Т., Бельгибеков Н.А.

**АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ВООРУЖЕННЫХ СИЛАХ
РЕСПУБЛИКИ КАЗАХСТАН**

Национальный университет обороны имени Первого Президента Республики
Казахстан-Лидера Нации, г. Астана

На протяжении 40 лет интерес к автоматизированным системам управления войсками (АСУВ) в мире и в нашей стране остается высоким. Так по некоторым оценкам, одно воинское тактическое формирование, оснащенное

эффективными средствами АСУВ, равноценно трем аналогичным, не оснащенным ими. Иными словами, одна автоматизированная бригада может успешно противостоять трем неавтоматизированным. Это достигается за счет повышения эффективности управления и информационного превосходства над противником, в том числе, благодаря созданию единого информационного пространства театра военных действий.

Внедрение автоматизированных систем управления в войсках рассматривается, как основной инструмент повышения эффективности управления силами и средствами в боевых условиях. Это обеспечивает возможность сокращения армии без снижения ее боеспособности. Сегодня АСУВ и оружием технологически представляют собой глубокую интеграцию в единую систему различных передовых разработок военной индустрии, включая современные высокопроизводительные и отказоустойчивые вычислительные комплексы, широкополосные средства радиосвязи, средства видеонаблюдения и целеуказания, средства ориентирования на местности и электронную картографию, системы поддержки принятия решения и другие системы, как информационного обеспечения и реализации «цифрового поля боя», так и комплексов управления огнем[1].

Задачами АСУВ являются информационное взаимодействие и управление входящими в нее подсистемами, а также предоставление интерфейса для взаимодействующих систем. Насколько эффективны такие механизмы, как раз и определяет качество АСУВ. Причем важна не только массовость структурного включения систем в состав АСУВ, но и уровень их интеграции в составе единого информационно-ударного комплекса. Это определяет качественный переход «железной массы» (бронетехники, авиации) и живой силы, разбросанных по полю боя и легко уничтожаемых поодиночке, в высокоманевренный единый механизм с высокой живучестью и увеличенным боевым потенциалом за счет резкого повышения эффективности управления.

Вне зависимости, кто дает целеуказания для нанесения огневого удара: передовой авианаводчик, оператор беспилотного летательного аппарата, вне зависимости, какие средства нанесения удара при этом будут задействованы: ракетные системы залпового огня или системы высокоточного оружия, в любом случае, система управления обеспечит эффективное поражение сил и средств противника, причем оптимальным образом с исключением удара по своим подразделениям. Интеллектуальная система перепроверит, проанализирует всю имеющуюся информацию иногда, на первый взгляд, напрямую не связанную с решением, но косвенно дающую дополнительные основания при оценке обстановки. Критерии эффективности включают не только вероятность поражения объектов противника, но и такие как минимизацию демаскирующих признаков средств разведки или огневого поражения. Все новейшие технологии ведения вооруженной борьбы, сетцентрические, войны шестого поколения, бесконтактные и прочие, используют концепцию АСУВ.

Все более широкое внедрение информационных технологий является сегодня общемировым явлением. Оно наблюдается практически во всех сферах человеческой деятельности, в том числе - и в военной. Деятельность вооруженных сил характеризуется специфичными, особо жесткими требованиями к работе с информацией и к средствам, эту работу реализующим. Пожалуй, ни в одной другой сфере деятельности, кроме военной, информация с древних времен не воспринималась как ключевой фактор обеспечения самого существования, сохранения жизни государства, с одной стороны, и подавления, уничтожения противника - с другой.

Анализ современного мирового опыта показывает, что успешное проведение военных операций требует своевременного комплексного информационного обеспечения боевых действий, что уже невозможно без современных информационных технологий. Сегодня последствия неэффективной работы с информацией - это потери личного состава,

вооружения, военной техники, которые в значительной мере определяют победу или поражение. Причем очень быстро и бесспорно.

Многие военные аналитики считают, что широкое применение современных информационных технологий привело к революции в военном деле. Обычно в качестве примера рассматривают войны последних лет, которые проводили США. Например, за счет применения информационных технологий войска США в Ираке в 1991 приобрели боевой потенциал, втрое превышающий боевой потенциал обычных частей. Информационные технологии обеспечили сокращение среднего времени подлета и подготовки к атаке ударных вертолетов с 26 до 18 минут и увеличение процента поражения целей противотанковыми управляемыми ракетами с 55% до 93%. Обработка и передача донесений в вышестоящие штабы в звене «рота-батальон» сократилась с 9 до 5 минут, вероятность дублирования телеграмм снизилась с 30% до 4%, передачи подтверждающей информации по телефонным линиям - с 98% до 22% [2].

Современные цифровые устройства позволяют успешно реализовывать тенденцию максимального сжатия цикла управления в цепочке «обнаружение - распознавание - наведение - поражение». Пространство боя насыщается «умными» боевыми системами, роботами, высокоточным оружием, системами спутниковой связи, электронными картами, средствами позиционирования и навигации. Сегодня существуют образцы вооружения, которые в принципе не способны функционировать без контроля компьютеров.

Вместо ставки на огневую мощь на первое место выйдет ставка на своевременную, точную и качественную информацию. Вместо массирования сил и средств - сосредоточение результатов, когда несколько разнесенных в пространстве средств поражения обеспечивают синхронизированное воздействие на противника. Девизом армии вместо «Самые большие пушки» должен стать «Самые умные системы».

Разведка, анализ, принятие решения, доведение его до средств поражения должны выполняться в реальном времени с минимальными временными затратами. Вероятно, на смену большим скоплениям техники и солдат, пробкам на дорогах и неповоротливой логистике должны прийти малочисленные, маневренные, оснащенные передовыми информационными технологиями подразделения, способные дистанционно управлять роботизированными огневыми средствами. В обязательном порядке - надежные защищенные бесшовные коммуникации, абсолютно прозрачные для всех абонентов, способные качественно функционировать в широком диапазоне внешних условий. С другой стороны, реалиями нашего времени стало возникновение виртуальных сетевых организаций, в том числе - террористических. Это новые вызовы, с которыми современному обществу еще только предстоит научиться бороться. В том числе - и в кибернетической сфере [3].

В 2014 году группой ведущих ученых РОО «Академия военных наук» - создан Военно-технический Консорциум, который объединил более 20 научных, образовательных, научно-технических учреждений и производственных предприятий. Среди которых: Национальный университет обороны имени Первого Президента Республики Казахстан - Лидера Нации, КазНУ им. аль-Фараби, Казахская авиационная индустрия, Национальный центр космических информационных технологий, Институт информационных и вычислительных технологий и другие. На сегодняшний день обозначен круг актуальнейших научных задач прикладного характера - это такие направления, как, информационная безопасность, высокоточное оружие и автоматизированные системы управления. В этом направлении и должна двигаться научная мысль казахстанских ученых. Эти и другие аналогичные исследования позволят готовить не только научно-технический резерв для оборонно-промышленного комплекса, но и создавать свои отечественные научно-технические школы, способные поднять военную науку Казахстана на качественно новый уровень. Главной задачей является объединение гражданского и военного секторов

науки, тем самым способствовать развитию передовой научной мысли и ее использованию в обеспечении безопасности государства.

Информатизация военной сферы, широкое внедрение ИТ на сегодня рассматриваются, как одно из важнейших направлений повышения боеспособности вооруженных сил. Применение информационных технологий вызывает революционные преобразования, приводит к смене системы ценностей и приоритетов, которые еще только предстоит осознать и сформировать. Кибернетическое виртуальное пространство начинает рассматриваться, как дополнительное измерение боевого пространства, и здесь РК имеет хорошие шансы достойно выглядеть на мировом рынке военных информационных технологий.

Литература

1. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности. М.: Изд-во КРАСАНД, 2011. 96 с.;
2. Бородакий Ю.В., Лободинский Ю.Г. Эволюция информационных систем - М.: Горячая линия – Телеком, 2011. 368 с.;
3. Медин А., Маринин А. Особенности применения киберсредств в межгосударственных военных и во внутренних конфликтах // Зарубежное военное обозрение. 2013. № 3. С.

Ташатов Н.Н., Сатыбалдина Д.Ж., Мишин В.А., Исайнова А.Н.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ РАБОТЫ КАСКАДНЫХ СХЕМ НА ОСНОВЕ МНОГОПороГОВЫХ ДЕКОДЕРОВ НЕДВОИЧНЫХ СВЕРТОЧНЫХ КОДОВ

Евразийский национальный университет, Астана, РК

Сверточные коды получили широкое распространение во многих радиосистемах передачи информации, таких как системы спутниковой и

сотовой связи, системы цифрового телевидения и радиовещания (в том числе и спутниковые), системы радиосвязи с подвижными объектами и другие системы, основной особенностью которых является работа в каналах связи с низкими энергетическими характеристиками и энергетическими характеристиками, непостоянными во времени [1].

Большое многообразие систем передачи информации, использующих сверточные коды, ставит вопрос о разработке методов их декодирования, обеспечивающих высокие характеристики по помехоустойчивости, быстродействию и сложности реализации.

Алгоритм многопорогового декодирования (МПД) для сверточных кодов [2,3] является развитием простейшего порогового декодера Мессе [4]. В основе алгоритма МПД лежит итеративное декодирование, что позволяет вплотную приблизиться к решению оптимального декодера в достаточно широком диапазоне кодовых скоростей и уровней шума в канале. Высокие характеристики МПД способствуют его широкому применению в составе различных каскадных конструкций, поскольку эффективность последних непосредственно связана с эффективностью их составных элементов [5-9].

В настоящее время специалисты в области помехоустойчивого кодирования проявляют большой интерес к недвоичным кодам, работающим с цифровыми данными на уровне символов, например, с байтами информации. Недвоичные коды применяются в каналах с группирующимися ошибками, в качестве составляющих элементов различных каскадных кодов, для защиты от ошибок информации на различного рода носителях (CD, DVD, Blu-ray и др.), для коррекции ошибок беспроводных каналах связи и в электронных массивах данных [3].

Целью настоящей работы является разработка алгоритмов и программная реализация новых каскадных схем многопорогового декодирования недвоичных сверточных кодов с возможностью анализа эффективности существующих и разработанных методов исправления ошибок.

Для достижения поставленной цели реализован программный комплекс (ПК), который позволяет моделировать каскады недвоичных кодеров и декодеров.

Разработанный ПК удовлетворяет нескольким требованиям:

- возможность использования неограниченного количества элементов каскада;
- возможность задания настроек алгоритмов, используемых в системе (длина регистра, точки съема);
- возможность повторного использования созданных схем;
- хранение и воспроизведение результатов работы схем для анализа эффективности;
- анализ и сравнение эффективности каскадных схем, их скорости работы.

ПК был реализован как многофункциональная информационная система, обеспечивающая автоматизацию процесса кодирования недвоичных данных, генерирование и внесение ошибок в пакет данных и декодирования сверточных самоортогональных кодов .

Целевыми показателями ПК по производительности являются:

- скорость кодирования данных;
- скорость декодирования данных;
- производительность системы не должна уменьшаться при различных входных данных, но одинаковых настройках (параметрах) системы.
- программный продукт должен поддерживать возможность распараллеливания обработки данных;
- локализация программы на два языка в целях создания публикаций в иностранных изданиях.

ПК является модульным, чтобы обеспечить определенную стартовую конфигурацию и иметь дальнейшую возможность поэтапного развития на более поздних этапах. Также должна быть возможность настраивать ПК под новые данные, редактировать число порогов и менять прочие настройки, влияющие как на эффективность, так и скорость обработки данных.

Архитектурно ПК реализован в десктопном варианте с возможностью портативного использования на флеш-носителях. Для хранения расчетных данных применяется no-sql вариант базы данных в виде файлов структурированных данных для возможности быстрого портирования настроек и очистки имеющихся неактуальных результатов.

Для повышения производительности каскадной схемы на основе многопорогового декодера недвоичных кодов необходимо подобрать оптимальные параметры. Основные параметры, доступные для настройки:

- количество кодеров в каскаде;
- длины регистра кодеров;
- точки съема регистров.

Для достижения высоких характеристик декодирования была избрана следующая тактика моделирования:

- выявление оптимальных параметров отдельных сверточных кодеров, так как декодер сверточного кода содержит кодер, необходимый для вычисления синдрома кода;

- конкатенация нескольких кодеров из числа оптимизированных на первом этапе;

- определение оптимального числа кодеров в каскаде в интересах повышения достоверности информации без потери быстродействия.

Для решения первой задачи был разработан программный модуль, реализующий перебор возможных комбинаций длины регистра сверточного кодера и вариации точек съема в регистре, процессы кодирования, внесения искажений и декодирования с целью коррекции ошибок, анализ эффективности разработанных методов исправления с автоматическим построением графиков. Для создания приложения использовалась технология визуального и объектно-ориентированного программирования на платформе .NET Framework (Microsoft Visual Studio Professional 2012). Исходный код написан на языке высокого уровня C#. Реализованы возможности изменения параметров оптимизации

(начальное количество ошибок, веса проверок разностного регистра на каждом пороговом элементе, величины порогов и т.д.).

На рисунках 1 и 2 представлена результаты имитационного моделирования для двух сверточных кодеров в виде зависимости вероятности ошибки на бит $P_b(e)$ алгоритмов декодирования в традиционном виде как функции от уровня битовой энергетике канала, т. е. его уровня шума. Кривая 1 для вероятности ошибки (P_0) в канале без декодирования, кривая 2 отображает результаты работы МПД, для сверточного кодера с оптимизированными параметрами. Если сравнить результаты на рисунке 1, то можно сделать вывод, что данный кодер обеспечивает одинаковую вероятность ошибки без декодирования на уровне мощности канала связи в 10Дб, в то время как декодер обеспечивает снижение вероятности ошибки до этого же уровня уже на мощности канала в 8 Дб.

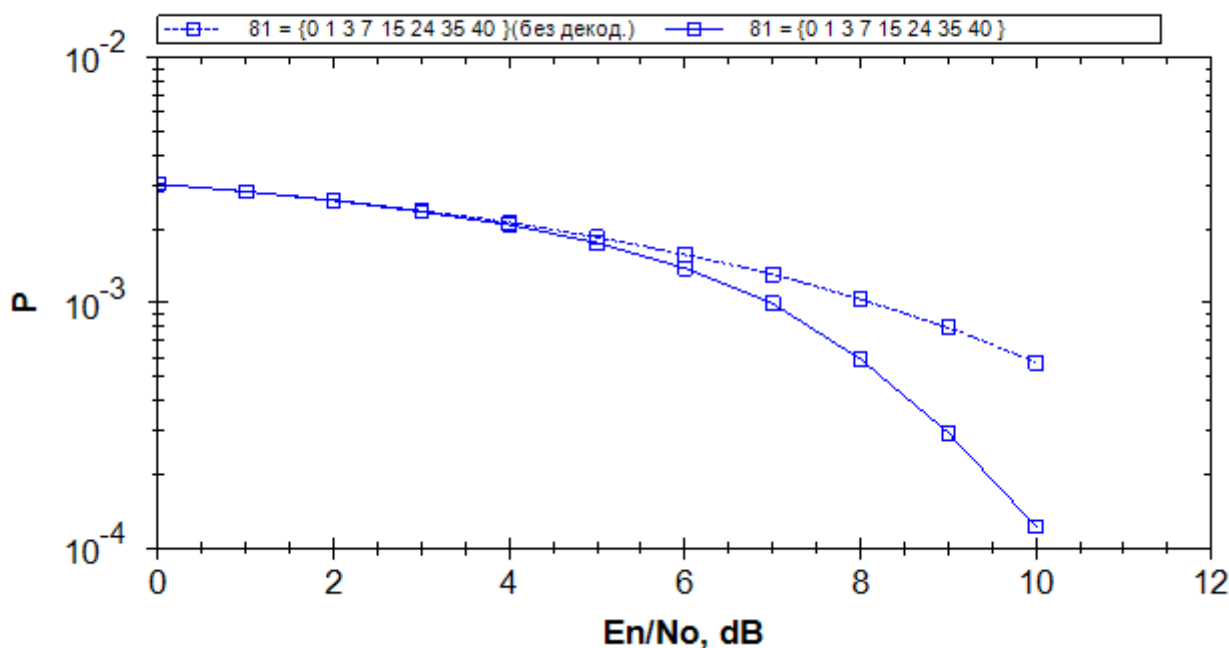


Рисунок 1 – Характеристики МПД на основе кодера с длиной регистра 81 и точками съема $\{0, 1, 3, 7, 15, 24, 35, 40\}$

На рисунке 2 показаны результаты декодирования для двух кодеров (с длинами регистра 81 и 223, точками съема $\{0, 1, 3, 7, 15, 24, 35, 40\}$ и $\{0, 1, 3, 7,$

12, 25, 35, 51, 65, 82, 103, 111}, соответственно), что позволяет сопоставить и сравнить их характеристики. Как видно, характеристики по эффективности декодирования для второго кодера во многом сходятся, значения энергетического выигрыша кодирования и вероятности появления ошибки двух этих кодеров практически идентичны.

Скорость обработки данных у первого декодера значительно выше и составляет 366 Мб/сек, а скорость декодирования во втором случае – 255 Мб/сек. Объясняется это тем, что оба они имеют разную длину регистров, соответственно в регистрах с большей длиной происходит больше проверок в пороговом элементе. Таким образом, показано, что для ускорения процесса каскадного кодирования следует выбирать кодеры с минимальной длиной, но без потери эффективности кодирования.

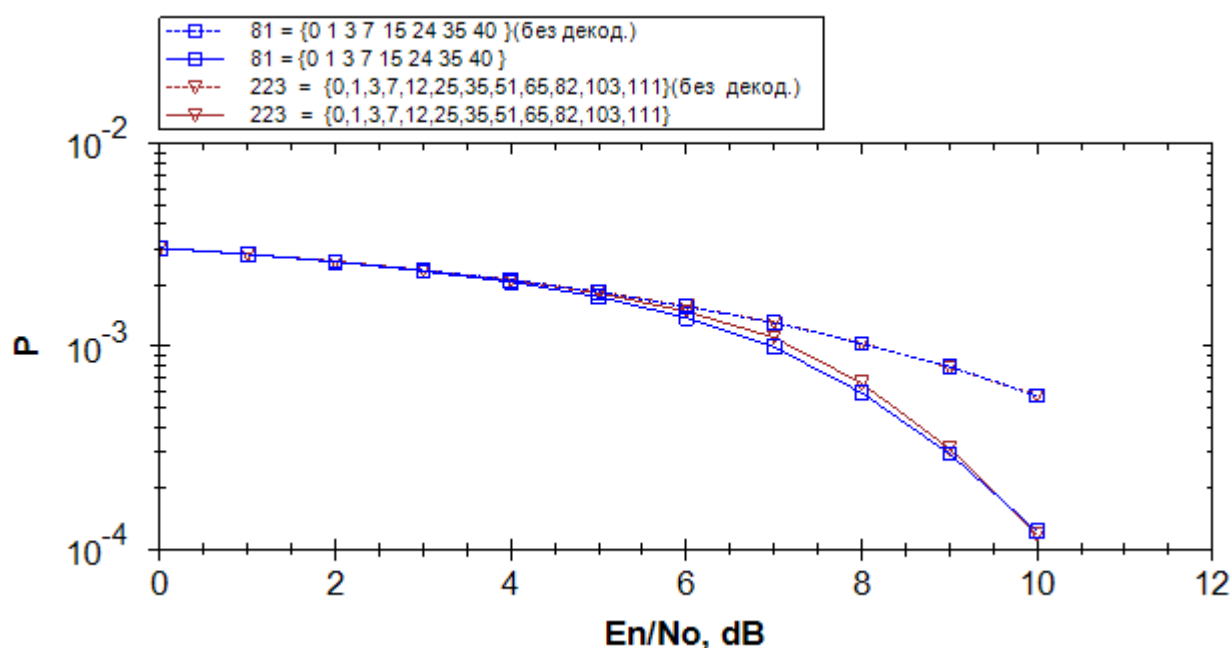


Рисунок 2 – Характеристики МПД на основе кодера с длиной регистра 223 и точками съема {0, 1, 3, 7, 12, 25, 35, 51, 65, 82, 103, 111}

На втором этапе были исследованы характеристики каскадной кодовой конструкции, состоящей из последовательности двух выбранных недвоичных сверточных декодеров.

На рисунке 3 представлены данные имитационного моделирования и все параметры предложенной схемы.

Как видно из рисунка 3, за счет конкатенации двух кодеров и двух декодеров энергетический выигрыш кодирования составляет около 3Дб. Полученный энергетический выигрыш кодирования доказывает, что использование кодеров подобного рода позволит добиться максимальной достоверности информации при передаче по каналу с шумом, а также экономию энергии при передаче на 40%.

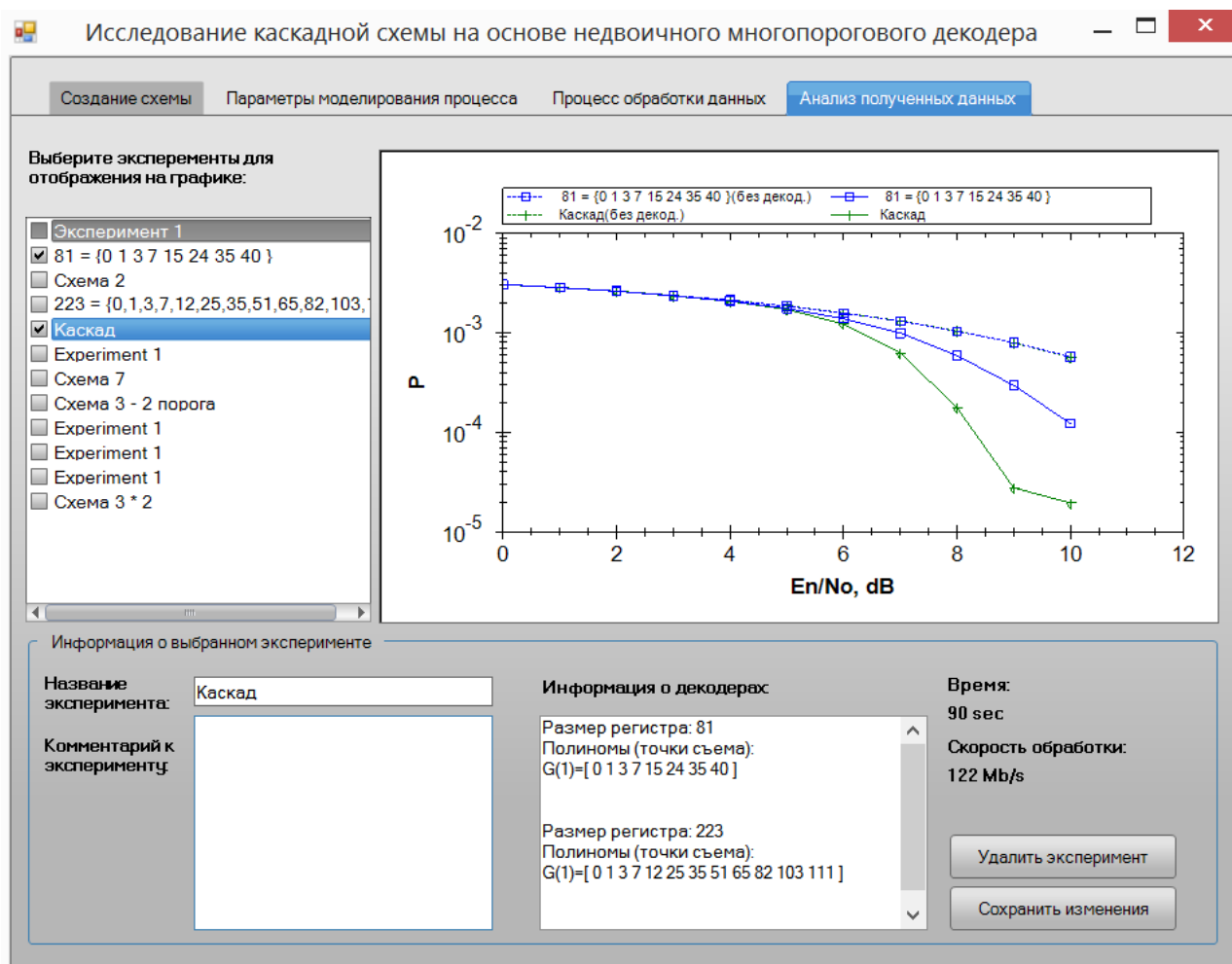


Рисунок 3 – Параметры каскадной конструкции и характеристики декодирования

Разработанный программный комплекс применяется в Евразийском национальном университете им. Л.Н. Гумилева для научно-исследовательских и учебных целей.

Работа выполнена при финансовой поддержке Комитета науки МОН Республики Казахстан (договор №534 от 7 апреля 2015г., приоритет «Информационные и телекоммуникационные технологии»).

Литература

1 Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник / под редакцией чл.-кор. РАН Зубарева Ю. Б. – М.: Горячая линия-Телеком, 2004. – 126 с.

2 Золотарев В.В. Теория и алгоритмы многопорогового декодирования. //Под ред. академика РАН Ю.Б. Зубарева // М.: Радио и связь, Горячая линия – Телеком, 2006. – 276 с.

3 Золотарев В.В., Зубарев Ю.Б., Овечкин Г.В. Многопороговые декодеры и оптимизационная теория кодирования / Под ред. член-корресподента РАН В.К. Левина.- М.: Горячая линия – Телеком, 2012.

4 Месси Дж. Пороговое декодирование.// Пер. с англ.; под ред. Э.Л. Блоха. – М.: Мир, 1966.

5 Золотарев В.В., Сатыбалдина Д.Ж., Овечкин Г.В., Ташатов Н.Н., Мишин В.А. Применение многопороговых алгоритмов в схемах параллельного каскадирования. // Цифровая обработка сигналов и ее применение: доклады 16-й Международной конференции (DSPA-2014). – Москва, т.1 – 2014. – С.101-105.

6 Золотарев В.В., Овечкин Г.В., Сатыбалдина Д.Ж., Андасова Б.З., Ташатов Н.Н, Мишин В.А. Параллель каскадтау сулбарарында копшекті алгоритемдерді колдану. // Вестник ЕНУ им. Л.Н. Гумилева. – 2014. – №2, часть 1. – с.125 – 131

7 Zolotarev V., Ovechkin G., Satybaldina D., Adamova A., Tashatov N., Mishin V. Effective multithreshold decoder for optical and other data transmission systems. // Latest trends on Communications: Proceedings of the 18th International Conference on Communications (part of CSCC'14). – Santorini Island, Greece. – 2014. – Pp. 152-156.

8 Zolotarev V., Ovechkin G., Satybaldina D., Adamova A., Tashatov N., Mishin V. Efficiency multithreshold decoders for self-orthogonal block codes for optical channels. // International Journal of Circuits, Systems and Signal Processing – 2014. – Volume 8. – Pp.487-495.

9 Zolotarev V, Ovechkin G., Seitkulov E., Satybaldina D., Tashatov N. Mishin V. Algorithm of multithreshold decoding for non-binary self-orthogonal concatenated codes. // Application of information and communication technologies-AICT 2014: 8th IEEE International Conference. – Astana, Kazakhstan. – 15-17 October 2014. – Pp. 27-31.

Ташатов Н.Н., Тургинбаева А.С., Серикова Н.С.

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ В РК

Евразийский национальный университет, Астана, РК

Выбор необходимой степени защиты информации и средств ее обеспечения является важной задачей и должен учитывать ряд параметров: уровень секретности информации; ее стоимость; время, в течение которого она должна оставаться в тайне и т.д. Проблема защиты информационных ресурсов в настоящее время приобретает все более важное значение. Так, по данным отчета CSI/FBI Computer Crime and Security Survey, приведены ежегодные ущербы компаний, которые с каждым годом растут. По некоторым оценкам, экономические потери от злонамеренных атак на банковские системы по всему миру составляют ежегодно около 130 млрд. долларов.

Как известно, далеко не все присутствующие на рынке криптографические средства обеспечивают обещанный уровень защиты. Системы и средства криптографической защиты информации (СКЗИ) характеризуются тем, что для них не существует простых и однозначных тестов, позволяющих убедиться в надежной защите информации. В связи с этим, были исследованы протоколы современных казахстанских криптографических систем и выявлены следующие обстоятельства:

- отсутствует доказательство самодостаточного криптографического протокола;
- некоторые организации, предоставляющие официальные государственные услуги на основе открытых ключей, не следуют строго правилам криптографических протоколов;
- не имеется открытого доступа к исходным кодам для их анализа.

Эти обстоятельства приводят к тому, что на рынке появляются средства криптографической защиты информации, про которые никто не может сказать ничего определенного. При этом нередко разработчики держат криптоалгоритм (как показывает практика, с возможными люками для взлома) в секрете. Однако задача точного определения используемого криптоалгоритма не может быть гарантированно сложной хотя бы потому, что он известен разработчикам (получается протокол с использованием доверительного арбитра «Трента»). Кроме того, если нарушитель нашел способ преодоления защиты, то не в его интересах об этом заявлять. В результате пользователи таких СКЗИ попадают в зависимость как минимум от разработчика. Поэтому обществу должно быть выгодно открытое обсуждение безопасности СКЗИ массового применения, а сокрытие разработчиками криптоалгоритмов должно быть недопустимым.

В связи с вышесказанным основными задачами по обеспечению информационной безопасности Республики Казахстан являются [1-5]:

- совершенствование национального законодательства в области информационной безопасности;

- выявление, оценка, прогнозирование источников угроз информационной безопасности;
- разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и методов ее реализации;
- координация деятельности государственных органов и организаций в области обеспечения информационной безопасности;
- развитие системы обеспечения информационной безопасности, совершенствование ее организации, форм, методов и средств нейтрализации угроз информационной безопасности, ликвидации последствий ее нарушений;
- обеспечение активного участия Казахстана в процессах создания и использования глобальных информационных сетей и систем.

Теперь давайте, исследуем вопрос открытого доступа к исходным кодам для их анализа.

Утверждение криптографии использующий открытый ключ предложили Уитфилд Диффи и Мартин Хеллман. Новизна, которую они ввели, заключается в использовании ключа попарно – ключи шифрования и дешифрования и невозможность взять из одного другого. Первый раз, 1976 году, свою идею Диффи и Хеллман показали в Национальной компьютерной конференции и спустя несколько месяцев опубликовали “New Directions in Cryptography” («Новое направление в криптографии») как основу своей работы. И после 1976 года были представлены много разных криптографических алгоритмов использующие открытые ключи. Многие из них не безопасны, а которые безопасны в многих случаях не могут быть разработаны [6].

Алгоритмов, являющихся и продуктивными и безопасными, мало. Обычно такие алгоритмы основаны на сложных задачах факторизации или проблеме логарифмирования в конечном поле. Сама стойкость базового алгоритма Диффи-Хеллмана строится на принципе образующего элемента конечной

группы. При факторизации составного числа на простые множители необходимо учитывать, такие нюансы как свойства простых чисел. Далее характер научных исследований проводимых в мире изменился после появления в 1985 году алгоритмов на эллиптических кривых. Эти алгоритмы взяли к себе на вооружение ряд таких стран как США, Россия, Украина, Казахстан. А многие другие страны переходят от теоретико-числовых методов к конечным группам на эллиптических кривых. Алгоритмы шифрования на эллиптических кривых позволяют заметно экономить время вычислений. Но эллиптическими кривыми, используя теорему Лагранжа, которая гласит, что «порядок любого элемента конечной группы можно однозначно делить порядок группы», можно варьировать криптостойкостью эллиптической кривой при выборе базовой точки P на кривой [7-8].

В заключении можно сказать, что основными целями обеспечения информационной безопасности являются:

–создание и укрепление национальной системы защиты информации, в том числе в государственных информационных ресурсах;

–защита государственных информационных ресурсов, а также прав человека и интересов общества в информационной сфере;

–недопущение информационной зависимости Казахстана, информационной экспансии или блокады со стороны других государств, информационной изоляции Президента, Парламента, Правительства и других государственных органов и организаций;

–ведение политики информационной безопасности РК.

Литература

- 1 СТ РК 34.022-2006. Требования к проектированию, установке, наладке, эксплуатации и обеспечению безопасности информационных систем.
- 2 СТ РК 34.027-2006. Классификация программных средств.

- 3 СТ РК 1695-2007. Аттестация объектов информатизации и средств вычислительной техники.
- 4 СТ РК 34.023-2006. Методика оценки соответствия информационных систем требованиям безопасности.
- 5 Указ президента Республики Казахстан о концепции информационной безопасности до 2016 года, № 174 от 14 ноября 2011 года.
- 6 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. –М.: Триумф, 2002. -595 с.
- 7 Коблиц Н. Введение в эллиптические кривые и модулярные формы. – М.: Мир, 1988. –313 с.
- 8 А.О.Воробьев, А.Г. Коробейников, В.В. Пылин и др. Анализ криптографической стойкости алгоритмов асимметричного шифрования информации // Известия вузов. Приборостроение. – 2007. –Т.50, №8. – С. 28-32.

Тельный А.В.

**О ВОЗМОЖНОСТИ ПОВЫШЕНИЯ ТОЧНОСТИ
ПОЗИЦИОНИРОВАНИЯ ПОДВИЖНОГО ОБЪЕКТА ПРИ
НАВИГАЦИОННЫХ ИЗМЕРЕНИЯХ**

Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, город Владимир, Российская Федерация

При навигационных измерениях движущихся объектов можно использовать ограничения динамических свойств объекта, прогнозируя область пространства возможного местоположения объекта в момент последующих навигационных измерений. При последующих навигационных измерениях, скорректированным местоположением объекта считается пересечение областей пространства последующих навигационных измерений с прогнозируемыми областями.

Пусть $x; y; z$ - истинные координаты объекта в базовой системе координат, связанной с центром масс объекта, а $\bar{x}; \bar{y}; \bar{z}$ - результаты навигационного измерения его местоположения в какой-то момент t .

Пусть по данным результатов навигационных измерений в момент времени t задана область пространства Φ . Ее можно представить в дискретном виде как

$$\Phi = \{(\bar{x} - h_x) + m\Delta x; (\bar{y} - h_y) + n\Delta y; (\bar{z} - h_z) + k\Delta z\}, \quad \text{где } m=0\dots M=2h_x/\Delta x;$$

$$n=0\dots N=2h_y/\Delta y; k=0\dots K=2h_z/\Delta z; m; n; k \text{ - целые числа (индексы разбиения по}$$

координатам). Значения $h_x; h_y; h_z$ - максимальная погрешность измерения

координат движущегося тела с вероятностью не менее $p(0,95)$, т.е.

$$|\bar{x} - x_1| < h_x; |\bar{y} - y_1| < h_y; |\bar{z} - z_1| < h_z \text{ с вероятностью } p(0,95); \Delta x; \Delta y; \Delta z -$$

интервалы разбиения. Пусть имеются последовательные навигационные

измерения в моменты времени $t_1 - t_n$ определяющие области пространства

$\Phi_1 - \Phi_n$ местоположения объекта в моменты времени $t_1 - t_n$:

$$\Phi_1 = \left\{ \begin{array}{l} (\bar{x}_1 - h_x) + m\Delta x; \\ (\bar{y}_1 - h_y) + n\Delta y; \\ (\bar{z}_1 - h_z) + k\Delta z; \end{array} \right\} \dots \Phi_n = \left\{ \begin{array}{l} (\bar{x}_n - h_x) + m\Delta x; \\ (\bar{y}_n - h_y) + n\Delta y; \\ (\bar{z}_n - h_z) + k\Delta z; \end{array} \right\}$$

$\bar{x}_1 \dots \bar{x}_n; \bar{y}_1 \dots \bar{y}_n; \bar{z}_1 \dots \bar{z}_n$ - данные навигационных измерений в моменты времени $t_1 - t_n$. Для прогнозирования области каждого последующего

навигационного измерения Φ_{iD} выбираются параметры ограничения

местоположения объекта из-за его динамических свойств, в качестве которых

могут выступать, например, линейные и угловые скорости и ускорения и

отклонение по углам (рыскания, крена) или прочие параметры. Обобщенные

условия ограничения местоположения объекта по данным навигационных

измерений и динамических свойств объекта для скоростей и ускорений можно

записать так:

$$\left\{ \begin{array}{l}
\frac{\int_{t_1}^{t_2} \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2 + \left(\frac{dz}{dt}\right)^2} dt}{\Delta t} \leq V_{k \max} |_{t=t_2}; \\
\frac{\int_{t_2}^{t_3} \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2 + \left(\frac{dz}{dt}\right)^2} dt}{\Delta t} \leq V_{k \max} |_{t=t_2}; \\
d \left[\frac{\int_{t_2}^{t_3} \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2 + \left(\frac{dz}{dt}\right)^2} dt / \Delta t - \int_{t_1}^{t_2} \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2 + \left(\frac{dz}{dt}\right)^2} dt / \Delta t}{dt} \right] \leq a_{k \max} |_{t=t_3}; \\
\frac{\int_{t_1}^{t_2} \left(\frac{dz}{dt}\right) dt}{\Delta t} \leq V_{\hat{A} \max} |_{t=t_2}; \\
\frac{\int_{t_2}^{t_3} \left(\frac{dz}{dt}\right) dt}{\Delta t} \leq V_{\hat{A} \max} |_{t=t_3}; \\
d \left[\frac{\int_{t_2}^{t_3} \left(\frac{dz}{dt}\right) dt / \Delta t - \int_{t_1}^{t_2} \left(\frac{dz}{dt}\right) dt / \Delta t}{dt} \right] \leq a_{\hat{A} \max} |_{t=t_3}
\end{array} \right. \quad (1)$$

Для угловых отклонений:

$$\begin{aligned}
& \arctg \left[\frac{\int_{t_1}^{t_2} \left(\frac{dz}{dt} \right) dt}{\int_{t_1}^{t_2} \left(\sqrt{\left(\frac{dx}{dt} \right)^2 + \left(\frac{dy}{dt} \right)^2 + \left(\frac{dz}{dt} \right)^2} dt \right)} \right] \leq \Theta_{\max} |_{t=t_2}; \\
& \arctg \left[\frac{\int_{t_2}^{t_3} \left(\frac{dz}{dt} \right) dt}{\int_{t_2}^{t_3} \left(\sqrt{\left(\frac{dx}{dt} \right)^2 + \left(\frac{dy}{dt} \right)^2 + \left(\frac{dz}{dt} \right)^2} dt \right)} \right] \leq \Theta_{\max} |_{t=t_3}; \\
& \arctg \left[\frac{\int_{t_1}^{t_2} \left(\sqrt{\left(\frac{dx}{dt} \right)^2 + \left(\frac{dy}{dt} \right)^2} \right) dt \cos(\Theta_{\max} |_{t=t_2})}{\int_{t_1}^{t_2} \left(\sqrt{\left(\frac{dx}{dt} \right)^2 + \left(\frac{dy}{dt} \right)^2 + \left(\frac{dz}{dt} \right)^2} dt \right)} \right] \leq \Psi_{\max} |_{t=t_2}
\end{aligned} \tag{2}$$

при этом :

$$\begin{aligned}
x_1 \dots x_3 &= (\bar{x}_1 \dots \bar{x}_3 - h_x) + m \Delta x \quad (\text{ïò } m = 0 \text{ äî } m = 2h_x / \Delta x); \\
y_1 \dots y_3 &= (\bar{y}_1 \dots \bar{y}_3 - h_y) + n \Delta y \quad (\text{ïò } n = 0 \text{ äî } n = 2h_y / \Delta y); \\
z_1 \dots z_3 &= (\bar{z}_1 \dots \bar{z}_3 - h_z) + k \Delta z \quad (\text{ïò } k = 0 \text{ äî } k = 2h_z / \Delta z).
\end{aligned} \tag{3}$$

$t_1 - t_3$ моменты времени трех последовательных навигационных измерений.

Данные неравенства следует трактовать следующим образом: - первое неравенство – скорость прохождения объектом пути за время Δt между первым и вторым измерением не может превышать максимально возможную курсовую скорость; - второе неравенство – аналогично, но между вторым и третьим измерением; - третье-неравенство – курсовое ускорение объекта не должно превышать максимально возможное; - четвертое - шестое неравенство аналогично 1-3 неравенству для вертикальной скорости и ускорения; - седьмое-восьмое неравенство определяет максимально возможный угол наклона объекта от вертикали (что фактически определяет угол тангажа) для второго и третьего измерения; - девятое-десятое неравенство определяет максимально возможный угол отклонения от курса для второго и третьего измерения.

Для повышения точности местоположения объекта в пространстве

возможно использование не предельных значений скоростей, ускорений и изменения угловых положений объекта, а текущих реальных данных бортовых измерителей (БИ) параметров движения объекта (скоростей, углов, ускорений). Максимальные параметры определяются текущими показаниями бортовых измерителей, их погрешностями, показаниями датчиков ветра и направлением ветра, а также приращением измеряемых параметров за время между навигационным измерением и ближайшим после него поступлением информации от бортового измерителя.

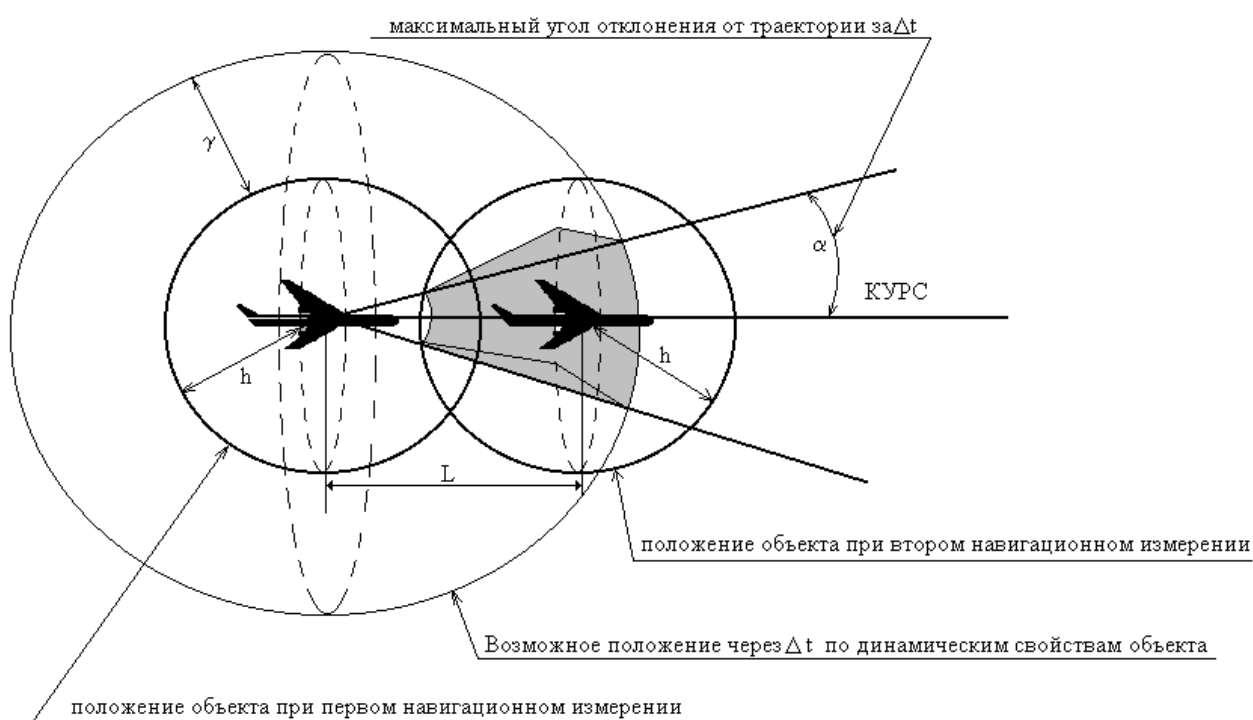


Рис.1. Выигрыш в определении положения объекта в пространстве (закрашенный сегмент). Здесь L - пройденное расстояние за Δt ; h - погрешность измерения; -прогнозируемое максимально возможное положение объекта через Δt , исходя из его потенциальных динамических возможностей.

Возможность повышения точности позиционирования объекта в пространстве, уточняя навигационные данные за счет наложения ограничений, связанных с динамическими свойствами движущегося объекта можно назвать

методом динамической рекуррентной коррекции, и он описан в [1].

Данный способ может обладать следующими преимуществами: - при определенных соотношениях между параметрами движения объекта, точностью их определения, частотой обновления навигационной информации и данных бортовых измерителей можно повысить точность определения местоположения объекта в пространстве; - не требуется проведения дополнительных навигационных измерений или заранее известной траектории движения объекта; - способ позволяет осуществлять комплексирование оборудования бортовых измерителей параметров движения объекта с навигационным оборудованием.

Литература

1. «Способ определения местоположения подвижного объекта при навигационных измерениях» патент РФ на изобретение №2529016RU G01S19/45 (2010.01) заявка №2012149512 от 21.11.2012г. /Тельный А.В. опубл. 27.09.2014г. Бюл. № 27 33с. М. : ФИПС.

Токсоналиева Р.М.

СОВРЕМЕННЫЕ УГРОЗЫ ИНФОРМАЦИОННО - ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ - ЧЛЕНОВ ОДКБ

Институт стратегического анализа и прогноза Кыргызско-Российского славянского университета, г. Бишкек, Кыргызская Республика

В современном мире значимость обеспечения информационно - психологической безопасности общества как составной части региональной безопасности в рамках государств - членов ОДКБ с каждым годом повышается. XXI век характеризуется развитием и применением современной технологии информационно - психологического воздействия ведущими мировыми

державами для вмешательства во внутригосударственные процессы различных стран мира в целях реализации собственных геополитических задач. В условиях глобализации увеличение интенсивного воздействия современной информационно - коммуникативной технологии на человека приводит к изменению его идеологического мировоззрения и поведения. В информационно - психологическом пространстве в основной группе риска остаётся современная молодёжь, у которой отсутствует целостная система ценностных ориентаций и происходит нравственно - культурное переформатирование. Подверженность молодёжи к информационно - психологическому воздействию в настоящее время превращается в серьёзную угрозу информационно - психологической безопасности государств коллективной безопасности.

В современных условиях для стран ОДКБ угрозу представляет информационно - психологическая война нового поколения с применением современных подрывных информационно - коммуникационных технологий, которая оказывает определенное влияние на безопасность государств - участников. Сегодня атрибутом молодёжи стали мобильный телефон, ноутбуки, планшеты и игровые приставки. Интернет стал для молодых людей удобным средством коммуникации, что привело к увеличению роли современных технологий по оказанию информационно - психологического воздействия, проведения различных акций и агитационных работ. Доступность глобальной компьютерной сети позволяет каждому человеку, независимо от места нахождения, общаться с другими и получать доступ к информации. Проведение различных массовых акций с помощью информационно - коммуникационной технологии становится выгодным, эффективным и политически результативным, о чём свидетельствуют антиобщественные акции, происходящие в государствах коллективной безопасности. Осуществление психологических и пропагандистских мероприятий путём модификации открытой информации, прежде всего - сетевых информационных ресурсов, привело к разжиганию национальной вражды, усилению

сепаратистских настроений, формированию иных негативных социальных явлений. Открытость информационного пространства порождает реальную угрозу негативного информационного влияния на общественное сознание населения и представляет социальную опасность для общества. «Информационное пространство - эта сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию» [1].

Современная коммуникационно - информационная технология стала эффективным орудием распространения идеологии современного радикального ислама, которая становится одной из самых реальных угроз информационно - психологической безопасности в мировом пространстве, подменившая существующий уклад жизни на религиозную ориентацию населения региона коллективной безопасности. Радикальный ислам превращается в политическую идеологию и серьезным фактором дестабилизации религиозной и социально-политической обстановки, сменив агрессивную тактику на «мягкое воздействие» с помощью современной информационной технологии. В частности, использование современным радикальным исламом глобальных информационно-вычислительных сетей, средств подпорогового психосемантического воздействия и средств создания виртуальной реальности способствовало развитию идеологии религиозного экстремизма. При радикально-террористической организации «Исламское государство» (ИГ) работает специально созданное медийное подразделение «Аль-Фуркан», которое занимается пропагандой идеологии организации, демонстрируя в сетях Интернет, видеоматериалы с участием детей и девушек террористические акты и тренировки в военных лагерях. В современном мире каждый человек погружен в информационную среду, формирование его мировоззрения зависит от информационного потока. Общество, которое переживает глубокие

трансформации в политической, социально - экономической и духовной сферах, не может избежать информационно - психологического воздействия на психоэмоциональное состояние и поведение молодого поколения. Открытость информационного поля, свободный доступ к Интернет-сайтам, социальным сетям, онлайн видеоканалам и чатам, где информационное пространство перенасыщено различной информацией религиозно-экстремистского характера, втягивает молодёжь к идеологии религиозно - экстремистских террористов. В результате это привело к «саморадикализации» молодёжи, в том числе и несовершеннолетних детей. Процесс «саморадикализации» опасен тем, что обуславливает появление у человека определённого эмоционально - психологического состояния для совершения аналогичных действий, увиденных в видеоматериалах. Формирование конкретного интереса и мотивация к идентичному поведению опасно ростом террористических актов на территории любого государства. Выезд отдельных граждан СНГ для участия в боевых действиях в Сирии в составе «Исламского государства», участвовавшие размещению в Интернете видеороликов и видеообращений от лица ИГ, увеличение числа желающих девушек в его ряды, активизация религиозных экстремистов на территории государств – членов ОДКБ являются результатом процесса «саморадикализации». На развитие данного процесса непосредственную помощь оказывает также система мгновенного обмена информацией как WhatsApp, Viber, Mail.ru Agent и т.п. В настоящее время, по различным официальным данным, в рядах ИГ находятся более 4 тысяч граждан стран Центральной Азии и России. Предотвращение радикализации ислама и обеспечение информационно - психологического пространства региона коллективной безопасности становится одной из важнейших задач государств- участников ОДКБ. Стабилизация религиозной обстановки в зоне действия коллективного договора требует комплексного подхода для осуществления противодействия современному радикальному исламу, который включал бы в себя меры институционально-правового, политико-

организационного, социально-экономического и информационно - пропагандистского характера. В формате ОДКБ принимаются нормативно-правовые документы в области информационной безопасности и вырабатываются конкретные мероприятия по выработке скоординированных действий по обеспечению информационной безопасности. Вместе с тем, регион коллективного договора остается открытой ареной для проведения негативного информационного воздействия на индивидуальное и массовое сознание людей, что наносит ущерб психическому и нравственному здоровью населения, приводит к дестабилизации социально - экономической и общественно - политической обстановки в зоне действия коллективного договора. В этой связи необходимы новые подходы к информационной безопасности и новые механизмы обеспечения информационно - психологического пространства.

Литература

1. Протокол о взаимодействии государств-членов ОДКБ по противодействию преступной деятельности в информационной сфере (25.12.2014) // URL: <http://kg.akipress.org/news:608582>.

Толеуханова Р.Ж.

АНАЛИТИЧЕСКИЙ МЕТОД ВОССТАНОВЛЕНИЯ ЦИФРОВЫХ СИГНАЛОВ ИЗОБРАЖЕНИЙ В БАЗИСЕ УОЛША

Карагандинский государственный университет им. Е.А. Букетова,
Караганда, Республика Казахстан

Современные возможности цифровых технологий позволяют решать задачи передачи сигналов по каналам радиосвязи, кодирования сигналов особенно эффективно. При решении, вместе с математическим аппаратом, используются методы синтеза, преобразования и кодирования сигналов.

По аналитической форме описания сигнала составляется математическая модель процесса, который с физической точки зрения может быть охарактеризован законами изменения напряженности электромагнитного поля, звукового давления, напряжения или тока в цепи, отклонения светового луча на экране и т.п. Реальные сигналы всегда являются функциями с ограниченным интервалом определения, поскольку их наблюдение, регистрация и обработка не могут выполняться бесконечно долго (см. [1], [2]). В данной статье рассматриваются плоские сигналы, т.е. задаваемые на плоскости, - сигналы изображений, в частности, полученные сканированием. При восстановлении исходного фрагмента сигнала изображения выявлены некоторые особенности коэффициентов преобразований Уолша.

Введём необходимые определения. Пусть $F(x, y)$ - непрерывный сигнал, x, y - некоторые аргументы. При этом сигнал на заданных интервалах его определения рассматривается как совокупность элементарных сигналов $\Phi_{n,m}(x, y)$, умноженных на коэффициенты $c_{n,m}$.

$$F(x, y) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} c_{n,m} \Phi_{n,m}(x, y) \quad (1)$$

Будем говорить, что система функций $\{\Phi_{n,m}(x, y)\}$ является базисной, а представление сигнала в виде (1) – его разложение по системе базисных функций. Если система функций выбрана, то сигнал полностью характеризуется матрицей спектральных коэффициентов $\{c_{n,m}\}$ - его спектром.

При практических расчётах ряд (1) обычно ограничивают (усекают). В этом случае представление сигнала будет приближенным

$$F(x, y) \approx F^*(x, y) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} c_{n,m} \Phi_{n,m}(x, y) \quad (2)$$

и имеет место аппроксимация сигнала конечным рядом (2).

Сигнал, представляющий собой функцию двух переменных $F(x, y)$ с ограниченной областью определения $(x, y) \in [0, 1]^2$, можно представить рядом Фурье по системе двумерных функций Уолша $\{w_{n,m}(x, y)\}$:

$$F(x, y) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} c_{n,m} W_{n,m}(x, y) \quad (3)$$

При этом спектр и равенство Парсеваля запишутся следующим образом:

$$c_{n,m} = \int_0^1 \int_0^1 F(x, y) W_{n,m}(x, y) dx dy; \quad (4)$$

$$\int_0^1 \int_0^1 F^2(x, y) dx dy = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} c_{n,m}^2 .$$

Усечённые двумерные ряды Уолша

$$F^*(x, y) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} c_{n,m} W_{n,m}(x, y) \quad (5)$$

обладают теми же видами сходимости, что и усечённые одномерные ряды Уолша, и могут быть использованы для аппроксимации двумерных непрерывных сигналов.

Так как каждая двумерная функция Уолша представляет собой произведение одномерных функций, то спектральные коэффициенты в двумерном базисе Уолша определяются из формулы

$$c_{n,m} = \int_0^1 W_n(x) \left[\int_0^1 F(x,y) W_m(y) dy \right] dx \quad (6)$$

Таким образом, двумерный спектр Уолша можно получить следующим образом: сначала вычислить одномерные спектры сигнала по одной переменной для каждого фиксированного значения второй, а затем выполнить одномерное преобразование Уолша полученных спектров по второй переменной. Этот приём применяется при цифровой обработке двумерных сигналов.

Выражение

$$F(i, j) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} c_{n,m} W_n\left(\frac{i}{N}\right) W_m\left(\frac{j}{M}\right) \quad (7)$$

определяет двумерный дискретный ряд Фурье-Уолша или двумерное дискретное преобразование Уолша. Коэффициенты этого ряда $c_{n,m}$ - суть двумерный дискретный спектр.

Они, также как и коэффициенты двумерного непрерывного ряда Уолша, могут быть получены двукратным применением одномерного дискретного преобразования Уолша соответственно по координатам i и j :

$$\begin{aligned} c_{n,m} &= \frac{1}{N} \sum_{i=0}^{N-1} \left[\frac{1}{M} \sum_{j=0}^{M-1} F(i,j) W_m \left(\frac{j}{M} \right) \right] W_n \left(\frac{i}{N} \right) = \\ &= \frac{1}{M} \sum_{j=0}^{M-1} \left[\frac{1}{N} \sum_{i=0}^{N-1} F(i,j) W_n \left(\frac{i}{N} \right) \right] W_m \left(\frac{j}{M} \right) \end{aligned} \quad (8)$$

Равенство Парсеваля для двумерных преобразований Уолша имеет вид

$$\frac{1}{NM} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} F^2(i,j) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} c_{n,m}^2$$

и, в свою очередь, может быть использовано для контроля перехода от представления сигнала в области аргументов к спектральной области. В случае использования при обработке сигналов спектральной формы представления сигналов возникает необходимость в операции анализа спектра. В общем случае при анализе спектра непрерывных сигналов в математическом отношении вычисляется зависимость и выполняются операции умножения сигнала на значения базисных функций. Полученные произведения интегрируются на заданном интервале определения.

Следует отметить, что в общем случае при анализе спектра непрерывных сигналов на ЭВМ лучше программировать формулу (4). Операции интегрирования как обычно выполняются с использованием известных численных методов и стандартных подпрограмм. Из соображений экономии машинного времени целесообразно при составлении программы воспользоваться представлением спектра Уолша в виде

$$c_{n,m} = \sum_{i=0}^{N-1} W_n \left(\frac{i}{N} \right) \int_{x_i}^{x_{i+1}} \left[\sum_{j=0}^{M-1} W_m \left(\frac{j}{M} \right) \int_{y_j}^{y_{j+1}} F(x,y) dy \right] dx \quad (9)$$

Достаточно будет вычислить значения интегралов сигнала только на подынтервалах постоянства функции Уолша и спектральные коэффициенты получить путём суммирования этих значений в соответствии с законом изменения знака функции.

Во многих задачах распознавания образов применяются оценки спектральных характеристик. В случае плоского (двумерного) или многомерного сигнала для распознавания используются двумерные или соответственно многомерные спектры [3]. Существование зависимости между ортогональным спектром двумерного сигнала и ортогональным спектром для одномерного массива, полученным из двумерного путём построчного сканирования в одномерный, обнаружено Жуковым Д.М. [4]. Покажем существование этой зависимости для базиса из кусочно-непрерывных функций Уолша. Также, учитывая что при обработке двумерных числовых массивов дискретными преобразованиями Уолша, необходимо выбирать сканирование, при котором в какой-то мере сохраняется «непрерывность» при переходе от точки к точке, имеем следующее утверждение.

Лемма [3]. Для любых $k = 0, 1, \dots, NM - 1$, $l = 0, 1, \dots, NM - 1$

справедливы равенства

$$W\left(\frac{k}{N}, \frac{l}{M}\right) = W_k\left(\frac{l}{NM}\right) = W_l\left(\frac{k}{NM}\right) \quad (10)$$

Теорема. Пусть $\{c_{n,m}\}$ - спектр двумерного сигнала $F(i,j)$ и $\{R_p\}$,

$p = 0, 1, \dots, NM - 1$, - спектр, полученный для одномерного

сигнала $G(k)$, $k = 0, 1, \dots, NM - 1$, в котором при $k = iM + j$,

$0 \leq i \leq N - 1$, $0 \leq j \leq M - 1$, положено $G(k) = G(iM + j) = F(i,j)$.

Тогда при $l = mN + n$, $0 \leq n \leq N - 1$, $0 \leq m \leq M - 1$, справедливы

соотношения $R_p = R_{mN+n} = R_{m,n} = c_{n,m}$.

В теореме показано то, что при переходе от одномерного спектра к двумерному путём расположения по М элементов в каждой строке можно получить транспонированный исходный спектр. Для сокращения объёма вычислений разработаны специальные алгоритмы, учитывающие те или иные особенности СБФ. Из совокупности специализированных алгоритмов анализа спектра наибольшей вычислительной эффективностью обладают итерационные вычислительные процедуры, называемые быстрыми преобразованиями [5].

Анализ точности восстановления отдельных элементов одномерных фрагментов изображений показывает, что если число первой половины коэффициентов трансформанты равно целой степени числа двойки, то в восстановленном фрагменте усреднённым оказывается такое же число элементов. Аналогично, при восстановлении исходного фрагмента сигнала изображения с помощью первой половины коэффициентов преобразований Уолша усреднёнными оказываются по два соседних элемента исходного фрагмента.

Литература

1. Игнатов В.А. Теория информации и передачи сигналов. – М.: Радио и связь, 1991. – 257 с.
2. Смирнов Ю.М. и др. Проектирование специализированных информационно-вычислительных систем. – М.: Высшая школа, 1984. – 359 с.
3. Голубов Б.И., Ефимов А.В., Скворцов В.А. Ряды и преобразования Уолша. Теория и применения. – М.: Наука, 1987. – 343 с.
4. Жуков Д.М. Эквивалентность одномерного и двумерного преобразования Крестенсона-Леви // Методы цифровой обработки изображений. – М.: МИЭТ, 1982. – С.65-70.
5. Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов. – М.: Мир. – 1989. – 341 с.

Tuychiev G.

**THE ENCRYPTION ALGORITHMS GOST28147–89–PES8–4 AND
GOST28147–89–RFWKPES8–4**

National University of Uzbekistan, Uzbekistan, Tashkent

e-mail: blasterjon@gmail.com

Abstract

In the paper a new block encryption algorithm based on networks PES8–4 and RFWKPES8–4, with the use the round function of algorithm GOST 28147–89 is suggested. The block length of created encryption algorithm is 256 bits, the number of rounds is 8, 12 and 16.

Introduction

The encryption algorithm GOST 28147–89 [1] is a standard encryption algorithm of the Russian Federation. It is based on a Feistel network. This encryption algorithm is suitable for hardware and software implementation, meets the necessary cryptographic requirements for resistance and, therefore, does not impose restrictions on the degree of secrecy of the information being protected. The algorithm implements the encryption of 64–bit blocks of data using the 256 bit key. In round functions used eight S–box of size 4x4 and operation of the cyclic shift by 11 bits. To date GOST 28147–89 is resistant to cryptographic attacks.

As the round function networks IDEA4–2, RFWKIDEA4–2, PES4–2 and RFWKPES4–2 [2, 3, 4, 5] using the round function of the encryption algorithm GOST 28147–89 created the encryption algorithm GOST28147–89–IDEA4–2, GOST28147–89–RFWKIDEA4–2, GOST28147–89–PES4–2, GOST28147–89–RFWKPES4–2, [6, 7, 8, 9]. In addition, by using SubBytes(), ShiftRows(), MixColumns() and AddRoundKey() transformations of the encryption algorithm AES as round functions of networks IDEA8–1 [10], RFWKIDEA8–1 [10], PES8–1 [11], RFWKPES8–1 [12], IDEA16–1 [13], RFWKIDEA16–1 [14], PES32–1 [15], RFWKPES32–1 [16], IDEA32–4 [17], RFWKIDEA32–4 [18] created encryption algorithms AES–IDEA8–1 [19], AES–RFWKIDEA8–1 [20], AES–PES8–1 [21], AES–RFWKPES8–1 [22], AES–IDEA16–1 [23], AES–RFWKIDEA16–1 [24], AES–PES32–1 [25], AES–RFWKPES32–1 [25], AES–IDEA32–4 [26], AES–RFWKIDEA32–4 [26]. The networks PES8–4 and RFWKPES8–4 is given in the article [11, 12] and as the Feistel network, when encryption and decryption using the

same algorithm. In the networks PES8–4 and RFWKPES8–4 was used four round functions and as round functions, may be used any transformations.

In this article, applying the round function of the encryption algorithm GOST 28147–89 as round functions of the networks PES8–4 and RFWKPES8–4, developed new encryption algorithms GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4. In the proposed encryption algorithms GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4 block length is 256 bits, the key length is changed from 256 bits to 1024 bits in increments of 128 bits and a number of rounds equal to 8, 12, 16, allowing the user depending on the degree of secrecy of information and speed of encryption to choose the number of rounds and key length. Below will be listed the structure of the proposed encryption algorithm.

The encryption algorithm GOST28147–89–PES8–4

The structure of the encryption algorithm GOST28147–89–PES8–4.

In the encryption algorithm GOST28147–89–PES8–4 length of the subblocks x^0 , x^1 , ..., x^7 , the length of the round keys $K_{12(i-1)}$, $K_{12(i-1)+1}$, ..., $K_{12(i-1)+11}$, $i = \overline{1..n+1}$, K_{12n+8} , K_{4n+5} , ..., K_{4n+11} , as well as the length of the input and output units round function is equal to 32 bits. In this algorithm the encryption round function of GOST 28147–89 is used twice and in each round functions used eight S–box, i.e. the total number of S–box is 16. The structure of the encryption algorithm GOST28147–89–RFWKPES8–4 is shown in Figure 1.

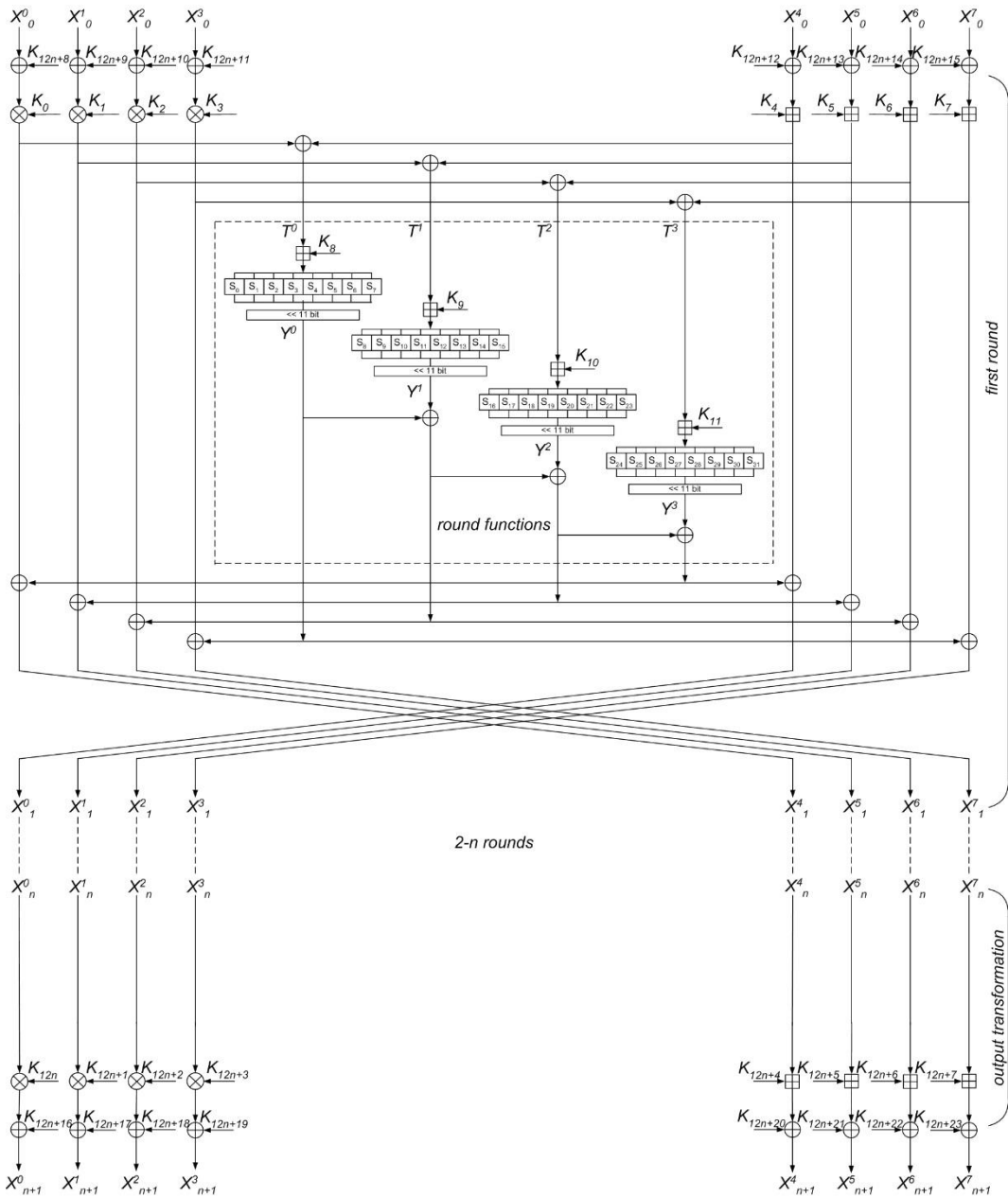


Figure 1. The scheme n -rounded encryption algorithm GOST28147–89–PES8–4

Consider the round function of a encryption algorithm GOST28147–89–PES8–4. First 32 bit subblocks T^0, T^1, T^2, T^3 are summed round keys $K_{12(i-1)+8}, K_{12(i-1)+9}, K_{12(i-1)+10}, K_{12(i-1)+11}, i = \overline{1...n}$, i.e. $S^0 = T^0 + K_{12(i-1)+8}, S^1 = T^1 + K_{12(i-1)+9}, S^2 = T^2 + K_{12(i-1)+10}, S^3 = T^3 + K_{12(i-1)+11}$. 32 bit subblocks S^0, S^1, S^2, S^3 divided into eight four bit subblocks, i.e. $S^0 = s_0^0 \parallel s_1^0 \parallel s_2^0 \parallel s_3^0 \parallel s_4^0 \parallel s_5^0 \parallel s_6^0 \parallel s_7^0, S^1 = s_0^1 \parallel s_1^1 \parallel s_2^1 \parallel s_3^1 \parallel s_4^1 \parallel s_5^1 \parallel s_6^1 \parallel s_7^1, S^2 = s_0^2 \parallel s_1^2 \parallel s_2^2 \parallel s_3^2 \parallel s_4^2 \parallel s_5^2 \parallel s_6^2 \parallel s_7^2, S^3 = s_0^3 \parallel s_1^3 \parallel s_2^3 \parallel s_3^3 \parallel s_4^3 \parallel s_5^3 \parallel s_6^3 \parallel s_7^3$. The four bit subblocks $s_i^0, s_i^1, s_i^2, s_i^3, i = \overline{0...7}$ converted to S–box:

$$R^0 = S_0(s_0^0) \parallel S_1(s_1^0) \parallel S_2(s_2^0) \parallel S_3(s_3^0) \parallel S_4(s_4^0) \parallel S_5(s_5^0) \parallel S_6(s_6^0) \parallel S_7(s_7^0),$$

$$R^1 = S_8(s_0^1) \parallel S_9(s_1^1) \parallel S_{10}(s_2^1) \parallel S_{11}(s_3^1) \parallel S_{12}(s_4^1) \parallel S_{13}(s_5^1) \parallel S_{14}(s_6^1) \parallel S_{15}(s_7^1),$$

$$R^2 = S_{16}(s_0^2) \parallel S_{17}(s_1^2) \parallel S_{18}(s_2^2) \parallel S_{19}(s_3^2) \parallel S_{20}(s_4^2) \parallel S_{21}(s_5^2) \parallel S_{22}(s_6^2) \parallel S_{23}(s_7^2),$$

$$R^3 = S_{24}(s_0^3) \parallel S_{25}(s_1^3) \parallel S_{26}(s_2^3) \parallel S_{27}(s_3^3) \parallel S_{28}(s_4^3) \parallel S_{29}(s_5^3) \parallel S_{30}(s_6^3) \parallel S_{31}(s_7^3).$$

Received 32 bit subblocks R^0, R^1, R^2, R^3 cyclically shifted to the left by 11 bits and get the subblocks $Y^0, Y^1, Y^2, Y^3: Y^0 = R^0 \ll 11, Y^1 = R^1 \ll 11, Y^2 = R^2 \ll 11, Y^3 = R^3 \ll 11$. The S-box of the encryption algorithm are shown in Table 1.

Table 1. The S-box encryption algorithm GOST28147–89–PES8–4

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
S0	0x4	0x5	0xB	0x9	0xE	0x8	0xD	0x0	0x6	0xC	0xF	0x7	0x2	0x1	0x3	0xA
S1	0x5	0x4	0xA	0x8	0xF	0x9	0xC	0x1	0x7	0xD	0xE	0x6	0x3	0x0	0x2	0xB
S2	0xE	0xB	0x4	0x2	0xF	0x7	0xC	0x0	0x8	0x9	0xA	0xD	0x6	0x5	0x3	0x1
S3	0xF	0xA	0x5	0x3	0xE	0x6	0xD	0x1	0x9	0x8	0xB	0xC	0x7	0x4	0x2	0x0
S4	0xD	0xC	0xB	0x1	0x4	0x0	0xF	0x3	0x7	0xE	0x5	0x6	0x9	0x2	0x8	0xA
S5	0xA	0x3	0x4	0x6	0xB	0xF	0x0	0xC	0x8	0x9	0x2	0x1	0xE	0x5	0x7	0xD
S6	0xB	0x2	0x5	0x7	0xA	0xE	0x1	0xD	0x9	0x8	0x3	0x0	0xF	0x4	0x6	0xC
S7	0xC	0x5	0x2	0x0	0xD	0x9	0x6	0xA	0xE	0xF	0x4	0x7	0x8	0x3	0x1	0xB
S8	0xD	0x4	0x3	0x1	0xC	0x8	0x7	0xB	0xF	0xE	0x5	0x6	0x9	0x2	0x0	0xA
S9	0xE	0x7	0x0	0x2	0xF	0xB	0x4	0x8	0xC	0xD	0x6	0x5	0xA	0x1	0x3	0x9
S10	0xF	0x6	0x1	0x3	0xE	0xA	0x5	0x9	0xD	0xC	0x7	0x4	0xB	0x0	0x2	0x8
S11	0x1	0x0	0x7	0x5	0x8	0x4	0xB	0xF	0x3	0xA	0x9	0x2	0xD	0xE	0xC	0x6
S12	0x2	0x3	0x4	0x6	0xB	0x7	0x8	0xC	0x0	0x9	0xA	0x1	0xE	0xD	0xF	0x5
S13	0x3	0x2	0x5	0x7	0xA	0x6	0x9	0xD	0x1	0x8	0xB	0x0	0xF	0xC	0xE	0x4
S14	0x4	0x5	0x2	0x0	0xD	0x1	0xE	0xA	0x6	0xF	0xC	0x7	0x8	0xB	0x9	0x3
S15	0x5	0x4	0x3	0x1	0xC	0x0	0xF	0xB	0x7	0xE	0xD	0x6	0x9	0xA	0x8	0x2
S16	0x6	0x7	0x0	0x2	0xF	0x3	0xC	0x8	0x4	0xD	0xE	0x5	0xA	0x9	0xB	0x1
S17	0x7	0x6	0x1	0x3	0xE	0x2	0xD	0x9	0x5	0xC	0xF	0x4	0xB	0x8	0xA	0x0

S18	0x8	0x9	0xE	0xC	0x1	0xD	0x2	0x6	0xA	0x3	0x0	0xB	0x4	0x7	0x5	0xF
S19	0x9	0x8	0xF	0xD	0x0	0xC	0x3	0x7	0xB	0x2	0x1	0xA	0x5	0x6	0x4	0xE
S20	0x1	0x8	0xF	0x5	0x0	0xC	0x3	0x7	0xB	0xA	0x9	0x2	0xD	0xE	0x4	0x6
S21	0x2	0xB	0xC	0x6	0x3	0xF	0x0	0x4	0x8	0x9	0xA	0x1	0xE	0xD	0x7	0x5
S22	0x3	0xA	0xD	0x7	0x2	0xE	0x1	0x5	0x9	0x8	0xB	0x0	0xF	0xC	0x6	0x4
S23	0x4	0xD	0xA	0x0	0x5	0x9	0x6	0x2	0xE	0xF	0xC	0x7	0x8	0xB	0x1	0x3
S24	0x5	0xC	0xB	0x1	0x4	0x8	0x7	0x3	0xF	0xE	0xD	0x6	0x9	0xA	0x0	0x2
S25	0x6	0xF	0x8	0x2	0x7	0xB	0x4	0x0	0xC	0xD	0xE	0x5	0xA	0x9	0x3	0x1
S26	0x7	0xE	0x9	0x3	0x6	0xA	0x5	0x1	0xD	0xC	0xF	0x4	0xB	0x8	0x2	0x0
S27	0x8	0x1	0x6	0xC	0x9	0x5	0xA	0xE	0x2	0x3	0x0	0xB	0x4	0x7	0xD	0xF
S28	0x9	0x0	0x7	0xD	0x8	0x4	0xB	0xF	0x3	0x2	0x1	0xA	0x5	0x6	0xC	0xE
S29	0xA	0x3	0x4	0xE	0xB	0x7	0x8	0xC	0x0	0x1	0x2	0x9	0x6	0x5	0xF	0xD
S30	0xB	0x2	0x5	0xF	0xA	0x6	0x9	0xD	0x1	0x0	0x3	0x8	0x7	0x4	0xE	0xC
S31	0xC	0x5	0x2	0x8	0xD	0x1	0xE	0xA	0x6	0x7	0x4	0xF	0x0	0x3	0x9	0xB

Consider the process of encryption in the encryption algorithm GOST28147–89–RFWKPE5–2. First 256 bit block of plaintext X is divided into 32 bit subblocks $x_0^0, x_0^1, \dots, x_0^7$ and runs the following steps:

1. subblocks $x_0^0, x_0^1, \dots, x_0^7$ summarized by XOR with the corresponding round keys $K_{12n+8}, K_{12n+9}, K_{12n+10}, \dots, K_{12n+15}$: $X_0^j = x_0^j \oplus K_{12n+8+j}, j = \overline{0 \dots 7}$.

2. subblocks $x_0^0, x_0^1, \dots, x_0^7$ are multiplied and summed accordingly with round keys $K_{12(i-1)}, K_{12(i-1)+1}, K_{12(i-1)+2}, \dots, K_{12(i-1)+7}$ и calculates a 32 bit subblocks T^0, T^1, T^2, T^3 . This step can be represented as follows: $T^0 = (X_{i-1}^0 \cdot K_{12(i-1)}) \oplus (X_{i-1}^4 + K_{12(i-1)+4}),$
 $T^1 = (X_{i-1}^1 \cdot K_{12(i-1)+1}) \oplus (X_{i-1}^5 + K_{12(i-1)+5}), T^2 = (X_{i-1}^2 \cdot K_{12(i-1)+2}) \oplus (X_{i-1}^6 + K_{12(i-1)+6}), T^3 = (X_{i-1}^3 \cdot K_{12(i-1)+3}) \oplus (X_{i-1}^7 + K_{12(i-1)+7}), i = 1$

3. to the T^0, T^1, T^2, T^3 subblocks apply the round function and get the 32 bit subblocks Y^0, Y^1, Y^2, Y^3 .

4. subblocks Y^0, Y^1, Y^2, Y^3 are summed by XOR with subblocks $X_{i-1}^0, X_{i-1}^1, \dots, X_{i-1}^7$, i.e. $X_{i-1}^0 = X_{i-1}^0 \oplus Y^3 \oplus Y^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^1 = X_{i-1}^1 \oplus Y^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^2 = X_{i-1}^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^3 = X_{i-1}^3 \oplus Y^0$, $X_{i-1}^4 = X_{i-1}^4 \oplus Y^3 \oplus Y^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^5 = X_{i-1}^5 \oplus Y^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^6 = X_{i-1}^6 \oplus Y^1 \oplus Y^0$, $X_{i-1}^7 = X_{i-1}^7 \oplus Y^0$, $i=1$.

5. at the end of the round subblocks swapped, i.e. $X_i^0 = X_{i-1}^4$, $X_i^1 = X_{i-1}^5$, $X_i^2 = X_{i-1}^6$, $X_i^3 = X_{i-1}^7$, $X_i^4 = X_{i-1}^0$, $X_i^5 = X_{i-1}^1$, $X_i^6 = X_{i-1}^2$, $X_i^7 = X_{i-1}^3$, $i=1$.

6. repeating the steps 2–5 n time, i.e. $i = \overline{2\dots n}$, obtained the subblocks $X_n^0, X_n^1, \dots, X_n^7$

7. in output transformation round keys $K_{12n}, K_{12n+1}, K_{12n+2}, \dots, K_{12n+7}$ are multiplied and summed into subblocks $X_n^0, X_n^1, \dots, X_n^7$, i.e. $X_{n+1}^0 = X_n^0 \cdot K_{12n}$, $X_{n+1}^1 = X_n^1 \cdot K_{12n+1}$, $X_{n+1}^2 = X_n^2 \cdot K_{12n+2}$, $X_{n+1}^3 = X_n^3 \cdot K_{12n+3}$, $X_{n+1}^4 = X_n^4 + K_{12n+4}$, $X_{n+1}^5 = X_n^5 + K_{12n+5}$, $X_{n+1}^6 = X_n^6 + K_{12n+6}$, $X_{n+1}^7 = X_n^7 + K_{12n+7}$.

8. subblocks $X_{n+1}^0, X_{n+1}^1, \dots, X_{n+1}^7$ are summed by XOR with the round keys $K_{12n+16}, K_{12n+17}, K_{12n+18}, \dots, K_{12n+23}$: $X_{n+1}^j = X_{n+1}^j \oplus K_{12n+16+j}$, $j = \overline{0\dots 7}$. As cipher text receives the combined 32 bit subblocks $X_{n+1}^0 \parallel X_{n+1}^1 \parallel X_{n+1}^2 \parallel \dots \parallel X_{n+1}^7$.

In the encryption algorithm GOST28147–89–PES8–4 when encryption and decryption using the same algorithm, only when decryption calculates the inverse of round keys depending on operations and are applied in reverse order. One important goal of encryption is key generation.

Key generation of the encryption algorithm GOST28147–89–PES8–4

In the n -round encryption algorithm GOST28147–89–PE84–4 used in each round 12 round keys of 32 bits and the output transformation of 8 round keys of 32 bits. In addition, prior to the first round and after the output transformation is applied 8 round keys on 32 bits. The total number of 32 bit round keys is equal to $12n+24$. Hence, if $n=8$ then necessary 120, if $n=12$ then 168 and if $n=16$ then 216 to generate round keys. When encryption in Fig.1 instead of K_i used the round keys K_i^c , and when decryption the round keys K_i^d .

The key length of the encryption algorithm l ($256 \leq l \leq 1024$) bits is divided into 32-bit round keys $K_0^c, K_1^c, \dots, K_{\text{Length}+1}^c$, $\text{Length} = l/32$, here $K = \{k_0, k_1, \dots, k_{l-1}\}$, $K_0^c = \{k_0, k_1, \dots, k_{31}\}$, $K_1^c = \{k_{32}, k_{33}, \dots, k_{63}\}$,

..., $K_{Lenght-1}^c = \{k_{l-32}, k_{l-31}, \dots, k_{l-1}\}$. Then calculated $K_L = K_0^c \oplus K_1^c \oplus \dots \oplus K_{Lenght-1}^c$. If $K_L = 0$ then as K_L selected 0xC5C31537, i.e. $K_L = 0xC5C31537$. Round keys K_i^c , $i = \overline{Lenght..12n+23}$ calculated as follows: $K_i^c = SBox_{32}(K_{i-Lenght}^c) \oplus SBox_{32}(RotWord(K_{i-Lenght}^c)) \oplus K_L$. After each generation of round keys value K_L cyclically shifted left by 1 bit. Here $RotWord32()$ —cyclic shift 32 bit subblock to the left by 1 bit, $SBox32()$ —convert 32-bit subblock in S-box and $SBox(A) = S_0(a_0) \parallel S_1(a_1) \parallel S_2(a_2) \parallel S_3(a_3) \parallel S_4(a_4) \parallel S_5(a_5) \parallel S_6(a_6) \parallel S_7(a_7)$, $SBox(A) = S_7(a_0) \parallel S_8(a_1) \parallel S_9(a_2) \parallel S_{10}(a_3) \parallel S_{11}(a_4) \parallel S_{12}(a_5) \parallel S_{13}(a_6) \parallel S_{14}(a_7)$, $A = a_0 \parallel a_1 \parallel a_2 \parallel a_3 \parallel a_4 \parallel a_5 \parallel a_6 \parallel a_7$ and a_i —the four bit subblock.

Decryption round keys K_i^d calculated on the basis of encryption round keys K_i^c and decryption keys output transformation associated with the encryption keys as follows:

$$(K_{12n}^d, K_{12n+1}^d, K_{12n+2}^d, K_{12n+3}^d, K_{12n+4}^d, K_{12n+5}^d, K_{12n+6}^d, K_{12n+7}^d) = ((K_0^c)^{-1}, (K_1^c)^{-1}, (K_2^c)^{-1}, (K_3^c)^{-1}, -K_4^c, -K_5^c, -K_6^c, -K_7^c). \quad (1)$$

Similarly, the decryption keys of the first, second, third and n-round are associated with the keys of the encoding as follows:

$$\begin{aligned} & (K_{12(i-1)}^d, K_{12(i-1)+1}^d, K_{12(i-1)+2}^d, K_{12(i-1)+3}^d, K_{12(i-1)+4}^d, K_{12(i-1)+5}^d, K_{12(i-1)+6}^d, K_{12(i-1)+7}^d, K_{12(i-1)+8}^d, K_{12(i-1)+9}^d, K_{12(i-1)+10}^d, K_{12(i-1)+11}^d) = \\ & ((K_{12(n-i+1)}^c)^{-1}, (K_{12(n-i+1)+1}^c)^{-1}, (K_{12(n-i+1)+2}^c)^{-1}, (K_{12(n-i+1)+3}^c)^{-1}, -K_{12(n-i+1)+4}^c, -K_{12(n-i+1)+5}^c, -K_{12(n-i+1)+6}^c, -K_{12(n-i+1)+7}^c, K_{12(n-i)+8}^c, \\ & K_{12(n-i)+9}^c, K_{12(n-i)+10}^c, K_{12(n-i)+11}^c), i = \overline{1..n}. \end{aligned} \quad (2)$$

Decryption round keys applied to the first round and after the conversion of the output associated with encryption keys as follows: $K_{12n+8+j}^d = K_{12n+16+j}^c$, $K_{12n+16+j}^d = K_{12n+8+j}^c$, $j = \overline{0..7}$.

For example, if the number of rounds of encryption algorithm is 16, (1) the formula is as follows:

$$(K_{192}^d, K_{193}^d, K_{194}^d, K_{195}^d, K_{196}^d, K_{197}^d, K_{198}^d, K_{199}^d) = ((K_0^c)^{-1}, (K_1^c)^{-1}, (K_2^c)^{-1}, (K_3^c)^{-1}, -K_4^c, -K_5^c, -K_6^c, -K_7^c).$$

In the same way, according to the formula (2) the round keys for the decryption of the first, second and sixteenth round is calculated as follows:

$$(K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d) = ((K_{192}^c)^{-1}, (K_{193}^c)^{-1}, (K_{194}^c)^{-1}, (K_{195}^c)^{-1}, -K_{196}^c, -K_{197}^c, -K_{198}^c, -K_{199}^c, K_{188}^c, K_{189}^c, K_{190}^c, K_{191}^c)$$

$$(K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d, K_{16}^d, K_{17}^d, K_{18}^d, K_{19}^d, K_{20}^d, K_{21}^d, K_{22}^d, K_{23}^d) = ((K_{180}^c)^{-1}, (K_{181}^c)^{-1}, (K_{182}^c)^{-1}, (K_{183}^c)^{-1}, -K_{184}^c, -K_{185}^c, -K_{186}^c, -K_{187}^c, K_{176}^c, K_{177}^c, K_{178}^c, K_{179}^c)$$

$$(K_{180}^d, K_{181}^d, K_{182}^d, K_{183}^d, K_{184}^d, K_{185}^d, K_{186}^d, K_{187}^d, K_{188}^d, K_{189}^d, K_{190}^d, K_{191}^d) = ((K_{12}^c)^{-1}, (K_{13}^c)^{-1}, (K_{14}^c)^{-1}, (K_{15}^c)^{-1}, -K_{16}^c, -K_{17}^c, -K_{18}^c, -K_{19}^c, K_8^c, K_9^c, K_{10}^c, K_{11}^c)$$

Similarly, the round keys are calculated cipher upon number of rounds equal to 8 and 12.

The encryption algorithm GOST28147–89–RFWKPE8–4

The structure of the encryption algorithm GOST28147–89–RFWKPE8–4

In the encryption algorithm GOST28147–89–RFWKPE8–4 length of the subblocks x^0, x^1, \dots, x^7 , the length of the round keys $K_{8(i-1)}, K_{8(i-1)+1}, \dots, K_{8(i-1)+11}, i = \overline{1 \dots n+1}$, $K_{8n+8}, K_{8n+9}, \dots, K_{8n+15}$, as well as the length of the input and output units round function is equal to 32 bits. In this algorithm the encryption round function of GOST 28147–89 is used twice and in each round functions used eight S–box, i.e. the total number of S–box is 16. The structure of the encryption algorithm GOST28147–89–RFWKPE8–4 is shown in Figure 1.

Consider the round function of a encryption algorithm GOST28147–89–PES8–4. First 32 bit subblocks T^0, T^1, T^2, T^3 divided into eight four bit subblocks, i.e.

$$T^0 = t_0^0 \parallel t_1^0 \parallel t_2^0 \parallel t_3^0 \parallel t_4^0 \parallel t_5^0 \parallel t_6^0 \parallel t_7^0, \quad T^1 = t_0^1 \parallel t_1^1 \parallel t_2^1 \parallel t_3^1 \parallel t_4^1 \parallel t_5^1 \parallel t_6^1 \parallel t_7^1, \quad T^2 = t_0^2 \parallel t_1^2 \parallel t_2^2 \parallel t_3^2 \parallel t_4^2 \parallel t_5^2 \parallel t_6^2 \parallel t_7^2,$$

$T^3 = t_0^3 \parallel t_1^3 \parallel t_2^3 \parallel t_3^3 \parallel t_4^3 \parallel t_5^3 \parallel t_6^3 \parallel t_7^3$. The four bit subblocks $t_i^0, t_i^1, t_i^2, t_i^3, i = \overline{0 \dots 7}$ converted to S–box:

$$R^0 = S_0(t_0^0) \parallel S_1(t_1^0) \parallel S_2(t_2^0) \parallel S_3(t_3^0) \parallel S_4(t_4^0) \parallel S_5(t_5^0) \parallel S_6(t_6^0) \parallel S_7(t_7^0),$$

$$R^1 = S_8(t_0^1) \parallel S_9(t_1^1) \parallel S_{10}(t_2^1) \parallel S_{11}(t_3^1) \parallel S_{12}(t_4^1) \parallel S_{13}(t_5^1) \parallel S_{14}(t_6^1) \parallel S_{15}(t_7^1),$$

$$R^2 = S_{16}(t_0^2) \parallel S_{17}(t_1^2) \parallel S_{18}(t_2^2) \parallel S_{19}(t_3^2) \parallel S_{20}(t_4^2) \parallel S_{21}(t_5^2) \parallel S_{22}(t_6^2) \parallel S_{23}(t_7^2),$$

$$R^3 = S_{24}(t_0^3) \parallel S_{25}(t_1^3) \parallel S_{26}(t_2^3) \parallel S_{27}(t_3^3) \parallel S_{28}(t_4^3) \parallel S_{29}(t_5^3) \parallel S_{30}(t_6^3) \parallel S_{31}(t_7^3).$$

Received 32 bit subblocks R^0, R^1, R^2, R^3 cyclically shifted to the left by 11 bits and get the subblocks $Y^0, Y^1, Y^2, Y^3: Y^0 = R^0 \ll 11, Y^1 = R^1 \ll 11, Y^2 = R^2 \ll 11, Y^3 = R^3 \ll 11$. The S–box of the encryption algorithm are shown in Table 1.

Consider the process of encryption in the encryption algorithm GOST28147–89–RFWKPE8–4–2. First 256 bit block of plaintext is divided into 32 bit subblocks $x_0^0, x_0^1, \dots, x_0^7$ and runs the following steps:

1. subblocks $x_0^0, x_0^1, \dots, x_0^7$ summarized by XOR with the corresponding round keys $K_{8n+8}, K_{8n+9}, K_{8n+10}, \dots, K_{8n+15}$: $X_0^j = X_0^j \oplus K_{8n+8+j}, j = \overline{0 \dots 7}$.

2. subblocks $X_0^0, X_0^1, \dots, X_0^7$ are multiplied and summed accordingly with round keys $K_{8(i-1)}, K_{8(i-1)+1}, K_{8(i-1)+2}, \dots, K_{8(i-1)+7}$ and calculates a 32 bit subblocks T^0, T^1, T^2, T^3 .

This step can be represented as follows: $T^0 = (X_{i-1}^0 \cdot K_{8(i-1)}) \oplus (X_{i-1}^4 + K_{8(i-1)+4})$,
 $T^1 = (X_{i-1}^1 \cdot K_{8(i-1)+1}) \oplus (X_{i-1}^5 + K_{8(i-1)+5})$, $T^2 = (X_{i-1}^2 \cdot K_{8(i-1)+2}) \oplus (X_{i-1}^6 + K_{8(i-1)+6})$, $T^3 = (X_{i-1}^3 \cdot K_{8(i-1)+3}) \oplus (X_{i-1}^7 + K_{8(i-1)+7})$, $i = 1$

3. to the T^0, T^1, T^2, T^3 subblocks apply the round function and get the 32 bit subblocks Y^0, Y^1, Y^2, Y^3 .

4. subblocks Y^0, Y^1, Y^2, Y^3 are summed by XOR with subblocks $X_{i-1}^0, X_{i-1}^1, \dots, X_{i-1}^7$, i.e. $X_{i-1}^0 = X_{i-1}^0 \oplus Y^3 \oplus Y^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^1 = X_{i-1}^1 \oplus Y^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^2 = X_{i-1}^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^3 = X_{i-1}^3 \oplus Y^0$,
 $X_{i-1}^4 = X_{i-1}^4 \oplus Y^3 \oplus Y^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^5 = X_{i-1}^5 \oplus Y^2 \oplus Y^1 \oplus Y^0$, $X_{i-1}^6 = X_{i-1}^6 \oplus Y^1 \oplus Y^0$, $X_{i-1}^7 = X_{i-1}^7 \oplus Y^0$, $i = 1$.

5. at the end of the round subblocks swapped, i.e. $X_i^0 = X_{i-1}^4$, $X_i^1 = X_{i-1}^5$, $X_i^2 = X_{i-1}^6$,
 $X_i^3 = X_{i-1}^7$, $X_i^4 = X_{i-1}^0$, $X_i^5 = X_{i-1}^1$, $X_i^6 = X_{i-1}^2$, $X_i^7 = X_{i-1}^3$, $i = 1$.

6. repeating the steps 2–5 n time, i.e. $i = \overline{2 \dots n}$, obtained the subblocks $X_n^0, X_n^1, \dots, X_n^7$

7. in output transformation round keys $K_{8n}, K_{8n+1}, K_{8n+2}, \dots, K_{8n+7}$ are multiplied and summed into subblocks $X_n^0, X_n^1, \dots, X_n^7$, i.e. $X_{n+1}^0 = X_n^0 \cdot K_{8n}$, $X_{n+1}^1 = X_n^1 \cdot K_{8n+1}$, $X_{n+1}^2 = X_n^2 \cdot K_{8n+2}$,
 $X_{n+1}^3 = X_n^3 \cdot K_{8n+3}$, $X_{n+1}^4 = X_n^4 + K_{8n+4}$, $X_{n+1}^5 = X_n^5 + K_{8n+5}$, $X_{n+1}^6 = X_n^6 + K_{8n+6}$, $X_{n+1}^7 = X_n^7 + K_{8n+7}$.

8. subblocks $X_{n+1}^0, X_{n+1}^1, \dots, X_{n+1}^7$ are summed by XOR with the round keys $K_{8n+16}, K_{8n+17}, K_{8n+18}, \dots, K_{8n+23}$: $X_{n+1}^j = X_{n+1}^j \oplus K_{8n+16+j}$, $j = \overline{0 \dots 7}$. As ciphertext receives the combined 32 bit subblocks $X_{n+1}^0 \parallel X_{n+1}^1 \parallel X_{n+1}^2 \parallel \dots \parallel X_{n+1}^7$.

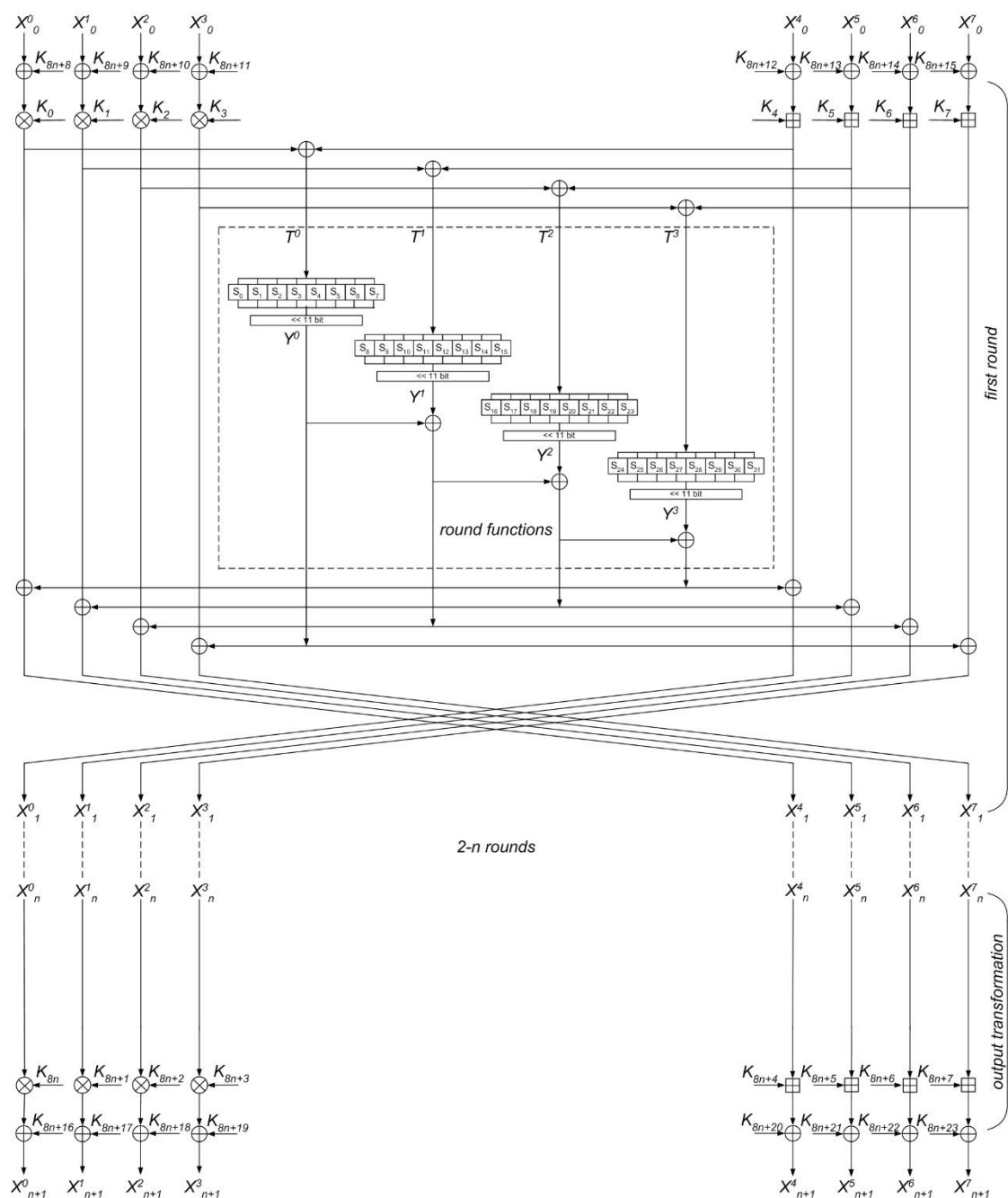


Figure 2. The scheme n -rouned encryption algorithm GOST28147–89–RFWKPES8–4

In the encryption algorithm GOST28147–89–RFWKPES8–4 when encryption and decryption using the same algorithm, only when decryption calculates the inverse of round keys depending on operations and are applied in reverse order. One important goal of encryption is key generation.

Key generation of the encryption algorithm GOST28147–89–RFWKPE8–4.

In the n -round encryption algorithm GOST28147–89–RFWKPE8–4 used in each round 8 round keys of 32 bits and the output transformation of 8 round keys of 32 bits. In addition, prior to the first round and after the output transformation is applied 8 round keys on 32 bits. The total number of 32-bit round keys is equal to $8n+24$. Hence, if $n=8$ then necessary 88, if $n=12$ then 120 and if $n=16$ then 152 to generate round keys. When encryption in Fig.1 instead of K_i used the round keys K_i^c , and when decryption the round keys K_i^d .

The key length of the encryption algorithm l ($256 \leq l \leq 1024$) bits is divided into 32-bit round keys $K_0^c, K_1^c, \dots, K_{Lenght-1}^c$, $Lenght=l/32$, here $K = \{k_0, k_1, \dots, k_{l-1}\}$, $K_0^c = \{k_0, k_1, \dots, k_{31}\}$, $K_1^c = \{k_{32}, k_{33}, \dots, k_{63}\}$, \dots , $K_{Lenght-1}^c = \{k_{l-32}, k_{l-31}, \dots, k_{l-1}\}$. Then calculated $K_L = K_0^c \oplus K_1^c \oplus \dots \oplus K_{Lenght-1}^c$. If $K_L = 0$ then as K_L selected $0xC5C31537$, i.e. $K_L = 0xC5C31537$. Round keys K_i^c , $i = \overline{Lenght..8n+23}$ calculated as follows: $K_i^c = SBox_0(32(K_{i-Lenght}^c)) \oplus SBox_1(32(RotWord(K_{i-Lenght}^c))) \oplus K_L$. After each generation of round keys value K_L cyclically shifted left by 1 bit.

Decryption round keys K_i^d calculated on the basis of encryption round keys K_i^c and decryption keys output transformation associated with the encryption keys as follows:

$$(K_{8n}^d, K_{8n+1}^d, K_{8n+2}^d, K_{8n+3}^d, K_{8n+4}^d, K_{8n+5}^d, K_{8n+6}^d, K_{8n+7}^d) = ((K_0^c)^{-1}, (K_1^c)^{-1}, (K_2^c)^{-1}, (K_3^c)^{-1}, -K_4^c, -K_5^c, -K_6^c, -K_7^c).$$

Similarly, the decryption keys of the first, second, third and n -round are associated with the keys of the encoding as follows:

$$(K_{8(i-1)}^d, K_{8(i-1)+1}^d, K_{8(i-1)+2}^d, K_{8(i-1)+3}^d, K_{8(i-1)+4}^d, K_{8(i-1)+5}^d, K_{8(i-1)+6}^d, K_{8(i-1)+7}^d) = ((K_{8(n-i+1)}^c)^{-1}, (K_{8(n-i+1)+1}^c)^{-1}, (K_{8(n-i+1)+2}^c)^{-1}, (K_{8(n-i+1)+3}^c)^{-1}, -K_{8(n-i+1)+4}^c, -K_{8(n-i+1)+5}^c, -K_{8(n-i+1)+6}^c, -K_{8(n-i+1)+7}^c), i = \overline{1..n}.$$

Decryption round keys applied to the first round and after the conversion of the output associated with encryption keys as follows: $K_{8n+8+j}^d = K_{8n+16+j}^c$, $K_{8n+16+j}^d = K_{8n+8+j}^c$, $j = \overline{0..7}$.

Results

As a result of the present research constructed a new block encryption algorithms called GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4. This algorithm is built on the basis of the network RFWKPES4–2 using the round function of GOST 28147–89. The block length is 128 bits, the number of rounds and key length are variable. This user depending on the degree of secrecy of information and speed of encryption can choose the number of rounds and key length.

It is known that S–box of the block encryption algorithm GOST 28147–89 are confidential and are used as long–term keys. In Table 2 below describes the options openly declared S–box such as: deg –degree of the algebraic nonlinearity; NL –nonlinearity; λ –relative resistance to the linear cryptanalysis; δ –relative resistance to differential cryptanalysis; SAC – criterion strict avalanche effect; the BIC criterion of independence of output bits. For S–box was resistant to crypt attack it is necessary that the values deg and NL were large, and the values λ , δ , SAC and BIC small.

Table 2: Parameters of the S–boxes of the GOST 28147–89

№	Parameters	S1	S2	S3	S4	S5	S6	S7	S8
1	deg	2	3	3	2	3	3	2	2
2	NL	4	2	2	2	2	2	2	2
3	λ	0.5	3/4	3/4	3/4	3/4	3/4	3/4	3/4
4	δ	3/8	3/8	3/8	3/8	1/4	3/8	0.5	0.5
5	SAC	2	2	2	4	2	4	2	2
6	BIC	4	2	4	4	4	4	2	4

In block encryption algorithms GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4 for all S–box the following equality: $\text{deg}=3$, $NL=4$, $\lambda=0.5$, $\delta=3/8$, $\text{SAC}=4$, $\text{BIC}=4$ i.e. resistance not lower than algorithm GOST 28147–89.

Studies show that the speeds of the encryption algorithm block cipher GOST28147–89–RFWKPES4–2 faster than GOST 28147–89. Created on 16–round algorithm 1.25 times faster than 32 round GOST 28147–89 algorithm.

So, we have constructed a new block encryption algorithms called GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4 based on networks PES8–4 and

RFWKPE8–4 using the round function of GOST 28147–89. Installed that the resistance offered by the author of the block encryption algorithm is not lower than the resistance of the GOST 28147–89 algorithm.

References

1. GOST 28147–89. National Standard of the USSR. Information processing systems. Cryptographic protection. Algorithm cryptographic transformation.
2. Aripov M.M. Tuychiev G.N. The network IDEA4–2, consists from two round functions // Infocommunications: Networks–Technologies–Solutions. –Tashkent, 2012, №4 (24), pp. 55–59.
3. Tuychiev G.N. The networks RFWKIDEA4–2, IDEA4–1 and RFWKIDEA4–1 // Acta of Turin polytechnic university in Tashkent, 2013, №3, pp. 71-77
4. Tuychiev G.N. The network PES4–2, consists from two round functions // Uzbek journal of the problems of informatics and energetics. –Tashkent, 2013, №5–6, pp. 107–111
5. Tuychiev G.N. About networks PES4–1 and RFWKPES4–2, RFWKPES4–1 developed on the basis of network PES4–2 // Uzbek journal of the problems of informatics and energetics. –Tashkent, 2015, №1, pp. 97–103.
6. Tuychiev G. Creating a data encryption algorithm based on network IDEA4–2, with the use the round function of the encryption algorithm GOST 28147–89 // Infocommunications: Networks–Technologies–Solutions. –Tashkent, 2014, №4 (32), pp. 49–54.
7. Tuychiev G. Creating a encryption algorithm based on network RFWKIDEA4–2 with the use the round function of the GOST 28147-89 // International Conference on Emerging Trends in Technology, Science and Upcoming Research in Computer Science (ICDAVIM-2015), //printed in International Journal of Advanced Technology in Engineering and Science, 2015, vol. 3, №1, pp. 427-432

8. Tuychiev G. Creating a encryption algorithm based on network PES4-2 with the use the round function of the GOST 28147-89 // TUIT Bulletin, -Tashkent, 2015, №2(34), pp. 132-136
9. Tuychiev G. Creating a encryption algorithm based on network RFWKPES4-2 with the use the round function of the GOST 28147-89 // International Journal of Multidisciplinary in Cryptology and Information Security, 2015, vol.4., №2, pp. 14-17
10. Tuychiev G.N. About networks IDEA8-2, IDEA8-1 and RFWKIDEA8-4, RFWKIDEA8-2, RFWKIDEA8-1 developed on the basis of network IDEA8-4 // Uzbek mathematical journal, -Tashkent, 2014, №3, pp. 104-118
11. Tuychiev G.N. About networks PES8-2 and PES8-1, developed on the basis of network PES8-4 // Transactions of the international scientific conference «Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2012», Volume № II, -Samarkand, 2014, pp. 28-32.
12. Tuychiev G.N. About networks RFWKPES8-4, RFWKPES8-2, RFWKPES8-1, developed on the basis of network PES8-4 // Transactions of the international scientific conference «Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2012», Volume № 2, -Samarkand, 2014, pp. 32-36
13. Tuychiev G.N. About networks IDEA16-4, IDEA16-2, IDEA16-1, created on the basis of network IDEA16-8 // Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions» -Tashkent, 2014
14. Tuychiev G.N. About networks RFWKIDEA16-8, RFWKIDEA16-4, RFWKIDEA16-2, RFWKIDEA16-1, created on the basis network IDEA16-8 // Ukrainian Scientific Journal of Information Security, -Kyev, 2014, vol. 20, issue 3, pp. 259-263
15. Tuychiev G. About networks PES32-8, PES32-4, PES32-2 and PES32-1, created on the basis of network PES32-16 // Ukrainian Scientific Journal of Information Security, -Kyev, 2014, vol. 20, issue 2, pp.164-168

16. Tuychiev G.N. About networks RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 and RFWKPES32–1, created on the basis of network PES32–16 // Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions» –Tashkent, 2014.
17. Tuychiev G.N. About networks IDEA32–8, IDEA32–4, IDEA32–2, IDEA32–1, created on the basis of network IDEA32–16 // Infocommunications: Networks–Technologies–Solutions. –Tashkent, 2014. №2 (30), pp. 45–50.
18. Tuychiev G.N. To the networks RFWKIDEA32–16, RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2 and RFWKIDEA32–1, based on the network IDEA32–16 // International Journal on Cryptography and Information Security (IJCIS), Vol. 5, No. 1, March 2015, pp. 9-20
19. Tuychiev G. New encryption algorithm based on network IDEA8–1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Computer Science, 2015, Volume 3, Issue 1, pp. 1–6
20. Tuychiev G. New encryption algorithm based on network RFWKIDEA8–1 using transformation of AES encryption algorithm // International Journal of Computer Networks and Communications Security, 2015, Vol. 3, №. 2, pp. 43–47
21. Tuychiev G. New encryption algorithm based on network PES8–1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security, 2015, vol.4., №1, pp. 1–5
22. Tuychiev G. New encryption algorithm based on network RFWKPES8–1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security, 2014, vol.3., №6, pp. 31–34
23. Tuychiev G. New encryption algorithm based on network IDEA16–1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Information Technology, 2015, Volume 3, Issue 1, pp. 6–12

24. Tuychiev G.N. The encryption algorithm AES–RFWKIDEA16–1 // Infocommunications: Networks–Technologies–Solutions. –Tashkent, 2015. №2 (34). pp. 48–54.
25. Tuychiev G. Creating a block encryption algorithm based networks PES32-1 and RFWKPES32-1 using transformation of the encryption algorithm AES // Compilation scientific work scientific and practical conference «Current issues of cyber security and information security-CICISIS-2015», -Kyev, 25-28 February 2015, p. 101-112
26. Tuychiev G.N. Creating a block encryption algorithm on the basis of networks IDEA32-4 and RFWKIDEA32-4 using transformation of the encryption algorithm AES // Ukrainian Scientific Journal of Information Security, –Kyev, 2015, vol. 21, issue 1, pp. 148–158

Устинова Л.В.¹, Смирнова М.А.², Самойлова И.А.²

АКТИВНЫЕ МЕТОДЫ ВОЗДЕЙСТВИЯ В СЕТИ

¹Назарбаев Интеллектуальная школа химико-биологического направления
г.Караганды, Казахстан, Караганда

²Карагандинский государственный университет им. академика
Е.А.Букетова, Казахстан, Караганда

Современный квалифицированный специалист, работающий в сфере информационных технологий, должен знать и уметь применить основные положения в области защиты информации в сети, располагать сведениями как о пассивных так и активных методах воздействия в сети.

Сканирование уязвимостей – это автоматизированный процесс, направленный на обнаружение известных уязвимостей в сетевых и программных платформах [1]. В результате сканирования подбираются эксплойты для осуществления непосредственно несанкционированного доступа (НСД) к узлам сети. На рисунке 1 представлены результаты использования

сканера уязвимостей Internet Security Scanner (ISS) [2].

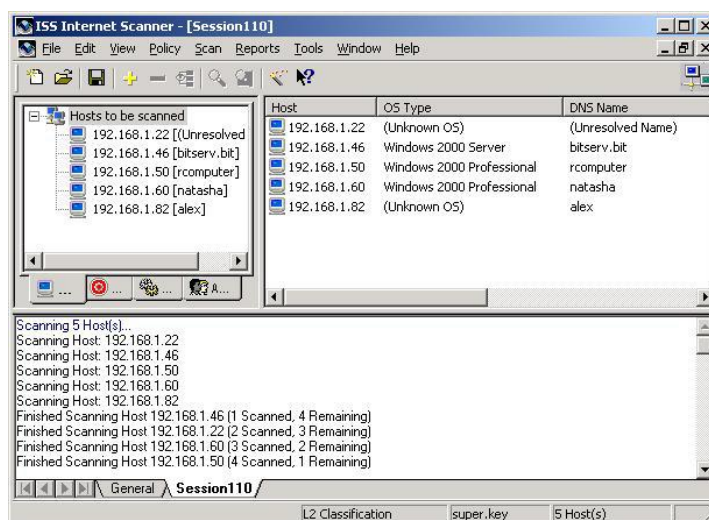


Рис. 1 Результат работы сканера ISS

Для скрытия фактов НСД используют Rootkits. Например, утилита AFX Windows Rootkit позволяет скрыть заданные ключи реестра, процессы, файлы, каталоги, сетевую активность. Поэтому администратор системы не увидит в списке процессов подозрительных программ сетевые соединения (netstat).

Результат работы утилиты для сокрытия определенного процесса представлен на рисунке 2. Для выявления таких процессов (Spyware, Rootkits) можно использовать Security Task Manager.

Рассмотрим методы защиты от активных воздействий на примере противодействия *вирусам, сетевым червям, троянским программам*. Эффективным методом выявления троянских программ, эксплойтов (ошибка ПО) является использование мониторов (например, Tauscan).

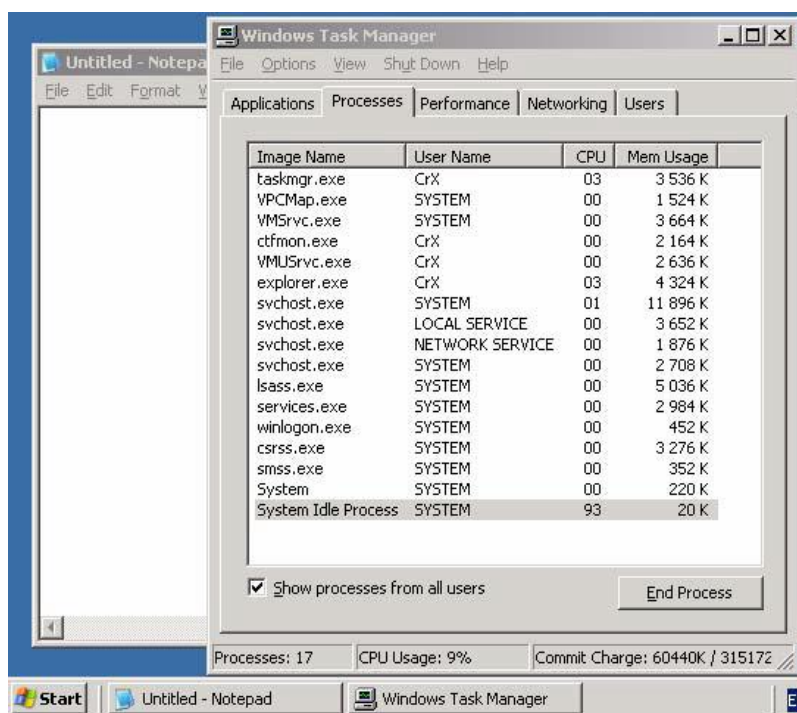


Рис. 2 Скрытие процессов AFX Windows Rootkit

На рисунке 3 показано окно карантина антивируса Symantec Antivirus Server, в результате которого были обнаружены эксплойта kaHt2 и троян Back Orifice 2000 [2].

Дополнительной защитой от внедрения троянских программ является установка брандмауэра. При попытке троянской программы осуществить выход в сеть, брандмауэр блокирует обращение или выводит предупреждение.

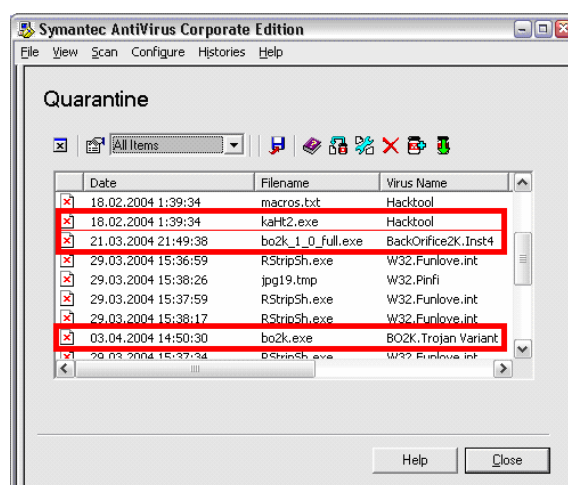


Рис. 3 Обнаружение вредоносного программного обеспечения

Пример данного уведомления приведен на рисунке 4. Брандмауэр Agnitum

Outpost выводит предупреждение о попытке explorer.exe (замаскированный троян Back Orifice) установить соединение с удаленным хостом *192.16.105.75*.

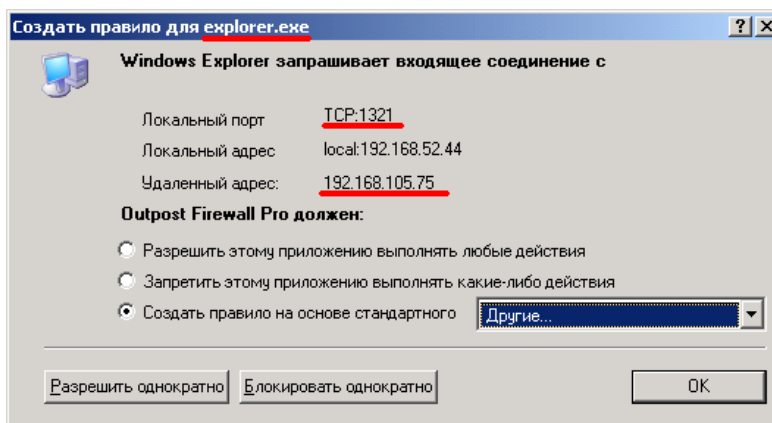


Рис. 4 Вывод предупреждения Agnitum Outpost

Для определения удаленно подключенных (несанкционированно) к системе пользователей, использующих трояны, эксплойты, необходимо придерживаться следующих рекомендаций.

1. Анализ открытых портов в Windows.

Для удаленного управления системой они открывают определенный порт, устанавливая с ним соединение (чаще всего номер порта, больше 1024). Это диапазон портов, не закрепленных за определенными службами.

Для анализа открытых портов в Windows используется команда `netstat -an`. Как показано на рисунке 5, открыт порт 39720, с которым установлено соединение (состояние ESTABLISHED).

```

C:\Command Prompt
Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             0.0.0.0:0              LISTENING
TCP   0.0.0.0:445             0.0.0.0:0              LISTENING
TCP   0.0.0.0:1025            0.0.0.0:0              LISTENING
TCP   0.0.0.0:5000            0.0.0.0:0              LISTENING
TCP   0.0.0.0:39720           0.0.0.0:0              LISTENING
TCP   192.168.120.24:135     192.168.105.75:2076   ESTABLISHED
TCP   192.168.120.24:139     0.0.0.0:0              LISTENING
TCP   192.168.120.24:39720   192.168.105.75:2077   ESTABLISHED
UDP   0.0.0.0:135            *:*                    *:*
UDP   0.0.0.0:445            *:*                    *:*
UDP   0.0.0.0:500            *:*                    *:*
UDP   0.0.0.0:1026           *:*                    *:*
UDP   0.0.0.0:1027           *:*                    *:*
UDP   127.0.0.1:123          *:*                    *:*
UDP   127.0.0.1:1900         *:*                    *:*
UDP   192.168.120.24:123     *:*                    *:*
UDP   192.168.120.24:137     *:*                    *:*
UDP   192.168.120.24:138     *:*                    *:*
UDP   192.168.120.24:1900    *:*                    *:*
C:\Documents and Settings\Administrator>

```

Рис. 5 Анализ портов

2. Анализ консольных приложений.

Для организации удаленного доступа часто используют консоль, запущенную на удаленной системе с правами учетной записи SYSTEM. Так как в нормальном режиме функционирования консоль с правами SYSTEM не может быть запущена, этот факт несложно определить (рис. 6).

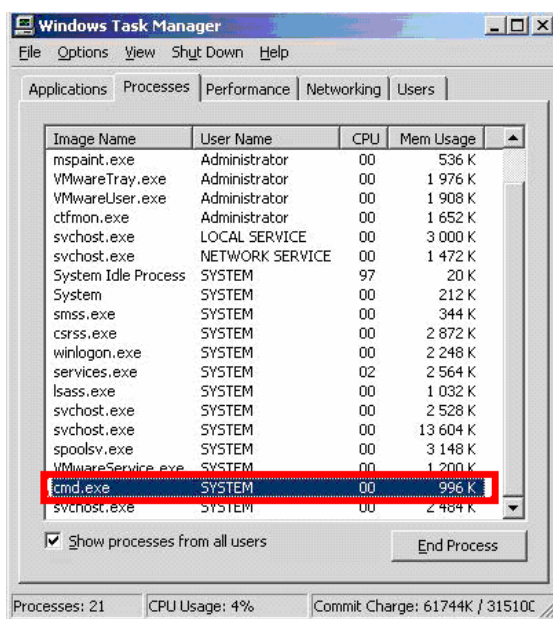


Рис. 6 Выявление нарушения удаленного доступа

Однако обнаружение удаленно подключившихся посредством эксплойта пользователей стандартными способами, а именно в окне "Активные пользователи", не всегда возможно. Во вкладке "Пользователи" отображается только администратор (рис. 7).



Рис. 7 Результат взлома не обнаружен

Поэтому стандартные средства операционных систем не всегда позволяют обнаружить наличие посторонних пользователей. Существуют специальные программы, например, Rootkit Hunter (Linux/Unix) или Patchfinder (Windows)

для их выявления [3].

Таким образом, сведения об активных методах воздействия в сети необходимо учитывать при разработке планов систем защиты информации на различных уровнях обеспечения информационной безопасности.

Литература

1. Пшенин Е.С. Теоретические основы защиты информации. Учебное пособие. Алматы: Каз НТУ, 2000 - 125 с.
2. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004. - 161 с.
3. Карминский А.М. Информатизация бизнеса: концепции, технологии, системы. – М.: Финансы и статистика, 2004. - 282 с.

Червяков Н.И., Шалалыгина И.В.

АНАЛИЗ МЕТОДА И АЛГОРИТМА ОСНОВНОГО МОДУЛЯРНОГО ДЕЛЕНИЯ

Северо-Кавказский федеральный университет, г.Ставрополь, Россия

Аннотация

Основные назначения этой статьи – провести теоретическое обоснование и анализ выполнения метода и алгоритма основного модулярного деления. Будут рассмотрены наиболее важные теоретико-числовые алгоритмы.

Введение

Решение широкого круга задач современных фундаментальных и прикладных исследований в таких областях как ядерная физика, оптика, геофизика, нейрофизика, физика атмосферы, сейсмографии, связи, медицинской электроники и многих других требует формирования и быстрой обработки в реальном масштабе времени и высокой степени достоверности огромных массивов цифровой информации.

Благодаря последним достижениям теории и применения цифровой обработки сигналов (ЦОС), лишь сравнительно недавно удалось решить ряд важных трудоемких задач по обработке многомерных сигналов звуковой локации, космической астрономии, медицинской электроники и другим проблемам.

Основная часть

Различные алгоритмы деления целых чисел $\frac{a}{b}$ можно описать итеративной схемой, используемой так называемый метод спуска Ферма [4]. Конструируется некоторое правило ϕ , которое каждой паре целых положительных чисел a и b ставит в соответствие некоторое целое положительное q такое, что $a - bq = r > 0$. Тогда деление a на b осуществляется по следующему правилу: согласно операции j паре чисел a и b ставится в соответствие число q_1 , такое, что $a - bq_1 = r_1 \geq 0$. Если $r_1 < b$, то деление закончено, если же $r_1 \geq b$, то, согласно ϕ , паре чисел (r_1, b) ставится в соответствие q_2 , такое, что $r_1 - bq_2 = r_2 \geq 0$.

Если $(r_2 < b)$, то деление завершается, если же $(r_2 \geq b)$, то, согласно ϕ , паре (r_2, b) ставится в соответствие q_3 такое, что $r_2 - bq_3 = r_3 \geq 0$ и так далее. Так как последовательное применение операции ϕ приводит к строго убывающей последовательности положительных целых чисел $a \geq r_1 \geq r_2 \geq r_3 \geq \dots \geq 0$, то процесс является конечным и алгоритм реализуется за конечное число шагов [2-4].

В общем случае b может быть и не равным модулю или их произведению. Здесь встает проблема выбора b таким, чтобы оно было равным либо модулю, либо их произведению. Если эта проблема будет решена, тогда итерации могут быть сведены к процессу масштабирования, которые рассмотрены выше [1,5]. Для решения этой проблемы вначале докажем теорему о границах изменения b .

Теорема 2. Если на K -шаге зафиксирован случай $0 \leq r_{k-1} - bq_k = r_k < b$, тогда частное q от деления целых чисел a на b будет равно $\sum_{i=1}^k q_i + r'_k$. Если $r_k < \frac{b}{2}$, то $r'_k = 0$, а если $r_k > \frac{b}{2}$, то $r'_k = 1$.

Проведенные расчеты на ЭВМ приведены на графике рисунком 1.

Из рисунка 1 видно, что в качестве делителя лучшие характеристики получаются при $\lambda = 1, 2, 3, 4$. При $\lambda = 1$ частное представляет собой точное значение, а при $\lambda = 2$ частное при малом числе итераций приближается к точному ее значению. Таким образом, в качестве делителя выбирается величина $b \leq \bar{b} \leq 2b$.

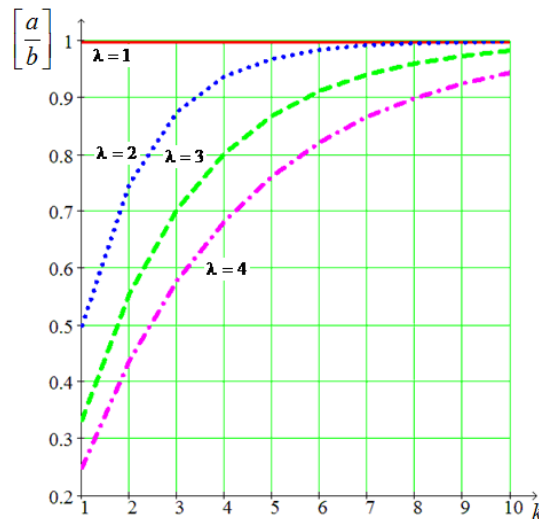


Рисунок 1 – График зависимости точности вычислений от значения величины делителя и числа итераций

Заметим, что при $\lambda = 1$ сумма $\sum_{i=1}^k q_i = \left[\frac{a}{b} \right] = \frac{a}{b}$. Для вычисления частного с точностью 0.9 и выше значение 1 целесообразно выбрать равное двум, то есть $b \leq \bar{b} < 2b$.

Проблема разработки оптимальных вычислительных алгоритмов деления побуждает к разработке таких операций ϕ_i , которые бы минимизировали число шагов спуска Ферма и вместе с тем достаточно просто реализовывались на

заданной вычислительной базе. Кроме того, на способ формирования операции ϕ существенно влияет также принятая система кодирования числовой информации [4,6]. Теперь возникает еще одна проблема, каким образом полученный приблизительный делитель \bar{b} свести либо к величине одного модуля или их произведению?

Предлагается модифицированный модулярный алгоритм деления целых чисел на основе метода спуска Ферма, который направлен на использование деления на приблизительный делитель \bar{b} , в предположении, что \bar{b} либо целое положительное число попарно простое с p_1, p_2, \dots, p_n , либо целое положительное число, представляющее собой произведение чисел, попарно простых с p_1, p_2, \dots, p_n . Этот приблизительный делитель выберем из значения делителя, используемого в применении алгоритма масштабирования. Так как в этом случае b не равно \bar{b} ошибка деления будет представлена в частном, которое при выполнении итерации будет уменьшаться до нуля.

Допустим, что и делимое a и делитель b являются положительными числами, и что значение для \bar{b} найдено в соответствии с условием $b \leq \bar{b} < 2b$, где b – это допустимый делитель для алгоритма масштабирования. Метод нахождения \bar{b} , удовлетворяющий этому условию, рассмотрен выше.

В алгоритме деления первым этапом является этап вычисления частного по алгоритму масштабирования, при котором $q_i = \left[\frac{a}{b} \right]$. Найденный таким образом q_1 далее используется в рекурсивных соотношениях $a_i = a_{i-1} - bq_i$, $a_0 = a$ и $q_i = \left[\frac{a_{i-1}}{b} \right]$ для получения q_2 , q_3 и так далее.

Эта повторяющаяся процедура продолжается до тех пор, пока $q_i = 0$, либо до $a_i = 0$.

Если это возникает на r -ом повторении, то $q = \left[\frac{a}{b} \right] = \sum q_i - q'_r$,

$$\text{где } q'_r = \begin{cases} q_r, & \text{если } q_r \neq 0 \text{ и } a_r = 0; \\ 1, & \text{если } q_r = 0 \text{ и } a_{r-1} \geq b \text{ для любых } \bar{b} \neq b \\ 0, & \text{иначе.} \end{cases}$$

Действительность этого алгоритма зависит от трех предпосылок:

1. Или q_i , или a_i становится нулевым после последнего числа повторений.
2. Ряд $\prod_{i=0}^{r-1} q_i + q'_r$ должен быть равен $\left[\frac{a}{b} \right]$.
3. Для любого b существует подходящий \bar{b} . Причем \bar{b} определяется из условия $b \leq \bar{b} < 2b$ и удовлетворяющий условию алгоритма масштабирования.

Заключение

Приблизительный делитель \bar{b} можно найти путем использования наиболее значимой ненулевой цифры, представленного \bar{b} в полиадической системе счисления. Эту ненулевую цифру заменим ближайшим простым числом или произведением простых чисел. Тогда делитель \bar{b} можно представить в виде простого числа или произведения простых чисел, что позволит использовать для вычисления частного алгоритм масштабирования.

Литература

1. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Ряднов С.А. Модулярные параллельные вычислительные структуры нейропроцессорных систем. – М.: ФИЗМАТЛИТ, 2003. – 288 с.
2. Галушкин А.И., Червяков Н.И., Евдокимов А.А., Лавриенко И.Н., Лавриенко А.В., Шаров Д.А. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. – М.: ФИЗМАТЛИТ, 2012. – 280 с.
3. Червяков Н.И. Организация арифметических расширителей в микропроцессорных системах, базирующихся на множественном представлении информации // Управляющие системы и машины. – 1987. – №1. – С. 26-29.

4. Червяков Н.И. Методы и принципы построения модулярных нейрокомпьютеров // 50 лет модулярной арифметике, сборник трудов Юбилейной Международной научно-технической конференции. Москва, ОАО «Ангстрем», МИЭТ. – 2006. – С. 239-249.

5. Червяков Н.И. Реализация высокоэффективной модулярной цифровой обработки сигналов на основе программируемых логических интегральных схем // Нейрокомпьютеры: разработка, применение. – 2006. – № 10. – С. 24-36.

6. Червяков Н.И., Бабенко М.Г. Системы защиты данных на эллиптической кривой. Модулярная арифметика. Методы и алгоритмы моделирования вычислительных структур на эллиптических кривых с параллелизмом машинных операций. М.: Saarbücken, 2011. - 121 с.

7. Червяков Н.И., Бабенко М.Г., Кучеров Н.Н. Применение корректирующих кодов СОК для диагностики работы модулярных процессоров// Наука. Инновации. Технологии. 2014. № 3. С. 24-39.

Червяков Н.И., Шалалыгин Д.Г.

**АНАЛИЗ МЕТОДОВ КОРРЕКЦИИ ОШИБОК В СИСТЕМЕ
ОСТАТОЧНЫХ КЛАССОВ**

Северо-Кавказский федеральный университет, г.Ставрополь, Россия

Аннотация. В статье рассматриваются теоретические обоснования и анализ выполнения коррекции ошибок в системе остаточных классов (СОК). Также анализируются модификации алгоритма вычисления интервального номера.

Введение

Современные средства цифровой обработки сигналов должны обеспечивать первичную обработку сигнала в реальном масштабе времени. Распараллеливание на уровне арифметических операций позволяет обеспечить

данное требование. При этом использование алгебраических кодов, обладающих свойством кольца, позволяет проводить с высокой эффективностью операции по обнаружения и коррекцию ошибок. Так как данные коды относятся к кодам классов вычетов, то для организации коррекции результата должны быть использованы позиционные характеристики.

Основная часть

При цифровой обработке сигналов (ЦОС) в реальном масштабе применяют параллельно-конвейерные вычисления. Одним из наиболее перспективных направлений обеспечения высокой скорости обработки сигналов является использование модулярных непозиционных кодов. В данных системах позиционные отсчеты сигналов представляются в виде наборов остатков, величины которых определяются значениями оснований кодов классов вычетов [1-4]. Наряду с высоким быстродействием непозиционные модулярные коды позволяют проводить операции по поиску и коррекции ошибок, которые возникают в процессе вычислительных устройств из-за отказов оборудования. Правильный выбор соответствующего алгоритма, позволяющий определить ошибочный остаток, а также глубину ошибки, выполняет поиск и коррекцию ошибок при минимальных схемных и временных затратах.

Известно, что введение двух контрольных оснований в упорядоченное множество оснований СОК, удовлетворяющих условию

$$P_k P_{k-1} < P_{k+1} P_{k+2}, \quad (1)$$

где k - количество рабочих оснований, позволяет осуществлять коррекцию однократных ошибок, возникающих в кодах СОК. Использование контрольных оснований расширяет рабочий диапазон, определяемый согласно

$$P_{\text{раб}} = \prod_{i=1}^k P_i \quad (2)$$

до значения полного диапазона

$$P_{полн} = \prod_{i=1}^{k+2} p_i = P_{раб} \prod_{i=k+1}^{k+2} p_i \quad (3)$$

Комбинация СОК считается разрешенной, если она принадлежит рабочему диапазону. Известно, что ошибка преобразует правильную комбинацию $A = (\alpha_1, \alpha_2, \dots, \alpha_{k+2})$ в комбинацию $A^* = (\alpha_1^*, \dots, \alpha_i^*, \dots, \alpha_{k+2})$, где $\alpha_i^* = \alpha_i + \Delta\alpha_i$ – искаженный остаток, $\Delta\alpha_i$ – глубина ошибки. В этом случае производится перевод искаженного числа из рабочего диапазона, в диапазон полный. Следовательно, зная местоположение искаженной комбинации $A^* = (\alpha_1^*, \dots, \alpha_i^*, \dots, \alpha_{k+2})$, можно однозначно определить основание, по которому произошла ошибка, а также ее глубину.

Данное свойство непозиционных модулярных кодов и предопределило повышенный интерес разработчиков к позиционным характеристикам, с помощью которых можно однозначно определить ошибочное основание и глубину ошибки. В качестве позиционных характеристик могут выступать коэффициенты обобщенной полиадической системы счисления (ОПСС), приведенные в работах [5, 6]. В работах [7, 8] рассматриваются алгоритмы расширения системы оснований модулярного кода с последующим вычислением невязки кода. Особое место среди позиционных характеристик занимает интервальный номер [9]. Это обусловлено тем, что данная позиционная характеристика имеет простой физический смысл. Определение данной характеристики осуществляется согласно

$$l_{инт} = \left[\frac{A}{P_{раб}} \right] \quad (4)$$

Очевидно, что операция деления (4) относится к немодульным, ее сводят к совокупности модульных операций. В работе [9] представлен алгоритм, который позволяет осуществлять поиск и коррекцию ошибки в коде классов вычетов, используя интервальный номер числа.

В основу данного алгоритма положено свойство подобия ортогональных базисов полных и безизбыточных систем класса, согласно которому

$$B_i^* \equiv B_i \pmod{P_{раб}}, \quad (5)$$

где B^* и B – ортогональные базисы безизбыточной и полной системы.

$$\text{Тогда, используя (5), получаем: } B_i = \left[\frac{B_i}{P_{раб}} \right] P_{раб} + B_i^* = K_i P_{раб} + B_j^*. \quad (6)$$

Подставив последнее равенство в выражение (4) получаем

$$l = \left[\sum_{i=1}^{k+2} \alpha_i (K_i P_{раб} + B_i^*) + \frac{RP_{полн}}{P_{раб}} \right], \quad (7)$$

где R – ранг полной системы оснований СОК.

$$\text{Проведя упрощения, имеем: } l = \left(\sum_{i=1}^{k+r} \alpha_i K_i + \left[\sum_{j=1}^k \frac{\alpha_j B_j^*}{P_{раб}} \right] + \frac{RP_{полн}}{P_{раб}} \right) \pmod{P_{конт}}, \quad (8)$$

$$\text{где } P_{конт} = \prod_{i=k+1}^{k+2} p_i.$$

Так как множество значений интервального номера 1 представляет собой кольцо по модулю $P_{конт}$, то выражение (8) можно преобразовать к виду

$$l = \left[\sum_{i=1}^{k+2} \alpha_i K_i + R^* \right]_{P_{полн}}^+, \quad (9)$$

$$\text{где } R^* = \left[\sum_{j=1}^k \frac{\alpha_j B_j^*}{P_{раб}} \right] - \text{ранг в безизбыточной системы.}$$

Если число, представленное в модулярном коде, принадлежит рабочему диапазону, то значение интервального номера равно нулю, т.е. $l = 0$. При возникновении ошибки число A не будет принадлежать рабочему диапазону, а будет размещаться вне его. Следовательно, если номер числа будет отличен от нуля, то это свидетельствует о том, что исходная комбинация модулярного числа содержит ошибку.

Проведенный анализ необходимых схемных затрат на реализацию данного алгоритма вычисления позиционной характеристики показал, что

применение составного модуля $P_{\text{конт}}$, по которому определяется значение интегрального номера 1, с точки зрения аппаратных затрат, является не самым оптимальным. Это обусловлено тем, что одномерные исчисления над кольцом, определяемым значением $P_{\text{конт}} = \prod_{i=k+1}^{k+2} p_i$, требует обработки $\lceil \log_2 P_{\text{конт}} \rceil$ разрядных операндов.

С целью сокращения аппаратных затрат в работе[9] предлагается усовершенствовать данный алгоритм. В основу усовершенствования целесообразно положить изоморфизм, порожденный китайской теоремой об остатках (КТО). Использование этого изоморфизма позволяет перейти от одномерной обработки к многомерной. Приравнивая соответствующие значения $P_{\text{конт}}$ и основания p_{k+1}, p_{k+2} получаем 2 преобразования, которые можно реализовать параллельно

$$\begin{cases} l^{k+1} = \left[\sum_{i=1}^{k+r} \alpha_i K_i + R^* \right]_{P_{k+1}}^+ \\ l^{k+r} = \left[\sum_{i=1}^{k+r} \alpha_i K_i + R^* \right]_{P_{k+r}}^+ \end{cases} \quad (10)$$

Несмотря на то, что выражения (9) и (10) позволяют получить одинаковый результат, тем не менее, использование изоморфизма КТО позволяет сократить схемные затраты, которые необходимы на реализацию алгоритма вычисления интервала. Проведенный анализ [9] показал, что реализация вычисления интервала согласно (10) потребовала на 14,3% меньше схемных затрат по сравнению с алгоритмом (9). При этом при увеличении размерности контрольных оснований выигрыш в схемных затратах увеличивается.

Заключение

Использование избыточных модулярных кодов позволяет осуществлять поиск и коррекцию ошибок, которые могут возникать в процессе

функционирования непозиционного спецпроцессора. Проанализирован алгоритм, позволяющий определить местоположение ошибки и ее глубину с использованием позиционной характеристики интервала. Был рассмотрен алгоритм, в основу которого был положен изоморфизм КТО. Переход к параллельному алгоритму позволил сократить схемные затраты, необходимые для вычисления позиционной характеристики при обработке 16-разрядных данных на 14,3% по сравнению с классическим методом вычисления интервала числа. При этом при увеличении размерности контрольных оснований возрастает выигрыш от использования разработанного алгоритма.

Литература

1.Бережной В.В., Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А. Нейросетевая реализация в полиномиальной системе классов вычетов операции ЦОС повышенной разрядности // Нейрокомпьютеры: разработка и применение. 2004. - № 5-6. - С. 94.

3.Калмыков И.А., Оленев А.А., Бережной В.В. Систолический процессор дискретного преобразования Фурье с коррекцией ошибки // Патент на изобретениеRUS 2018950

4.Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А., Бережной В.В. Архитектура отказоустойчивой нейронной сети для цифровой обработки сигналов // Нейрокомпьютеры: разработка и применение. 2004. - №12. -С. 51-57.

5.Калмыков И.А., Ханватов А.Б., Сагдеев А.К. Разработка методов обнаружения и коррекции ошибок в коде полиномиальной системы классов вычетов, базирующихся на вычислении синдрома ошибки // Фундаментальные исследования. - 2006. - №2. - С. 13.

Червяков Н.И., Шалалыгин Д.Г., Шалалыгина И.В.

КРАТКАЯ ХАРАКТЕРИСТИКА СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Северо-Кавказский федеральный университет, г.Ставрополь, Россия

Ключевые слова: Система остаточных классов (СОК), класс вычетов, китайская теорема об остатках (КТО), модульные операции.

Аннотация

Основные назначения этой статьи – провести теоретическое обоснование и анализ выполнения арифметических операций над числами, представленными в СОК. Будут рассмотрены наиболее важные теоретико-числовые алгоритмы, являющиеся основой арифметики в остаточных классах.

Введение

Основной теоретико-числовой базой системы остаточных классов является теория сравнений. Полной системой вычетов по модулю p называется совокупность p целых чисел, содержащая точно по одному представителю из каждого класса вычетов по модулю p . Каждый класс вычетов по модулю p содержит в точности одно из чисел совокупности всех возможных остатков от деления на p : $\{0, 1, \dots, p-1\}$. Множество $\{0, 1, \dots, p-1\}$ также называется полной системой наименьших неотрицательных вычетов по модулю p .

Основная часть

Один из методов выполнения арифметических операций над длинными целыми числами основан на простых положениях теории чисел. Представление чисел в СОК позволяет заменить операции с большими числами на операции с малыми числами, которые представлены в виде остатков от деления больших чисел на заранее выбранные взаимно-простые модули p_1, p_2, \dots, p_n . Пусть

$$A \equiv \alpha_1 \pmod{p_1}, A \equiv \alpha_2 \pmod{p_2}, \dots, A \equiv \alpha_n \pmod{p_n}. \quad (1)$$

Тогда целому числу A можно поставить в соответствие кортеж $(\alpha_1, \alpha_2, \dots, \alpha_n)$ наименьших неотрицательных вычетов по одному из

соответствующих классов. Данное соответствие будет взаимно однозначным, пока $A < p_1 p_2 \dots p_n$, в силу Китайской Теоремы об Остатках (КТО). Кортеж $(\alpha_1, \alpha_2, \dots, \alpha_n)$ можно рассматривать как один из способов представления целого числа A в ЭВМ – модулярное представление или представление в СОК.

Основным преимуществом такого представления является тот факт, что выполнение операций сложения, вычитания и умножения реализуется очень просто, по формулам:

$$\begin{aligned} A \pm B &= (\alpha_1, \alpha_2, \dots, \alpha_n) \pm (\beta_1, \beta_2, \dots, \beta_n) = \\ &= ((\alpha_1 \pm \beta_1) \bmod p_1, (\alpha_2 \pm \beta_2) \bmod p_2, \dots, (\alpha_n \pm \beta_n) \bmod p_n); \end{aligned} \quad (2)$$

$$\begin{aligned} A \times B &= (\alpha_1, \alpha_2, \dots, \alpha_n) \times (\beta_1, \beta_2, \dots, \beta_n) = \\ &= ((\alpha_1 \times \beta_1) \bmod p_1, (\alpha_2 \times \beta_2) \bmod p_2, \dots, (\alpha_n \times \beta_n) \bmod p_n). \end{aligned} \quad (3)$$

Эти операции носят название модульных, так как для их выполнения в СОК достаточно одного такта обработки численных значений, причем эта обработка происходит параллельно и значения информации в каждом разряде не зависит от других разрядов.

Основной недостаток модулярного представления чисел состоит в том, что трудно упорядочить множество всех целочисленных кортежей длины n так, чтобы этот порядок соответствовал естественному порядку на множестве целых чисел. Как следствие этого факта, трудно установить, является ли кортеж $(\alpha_1, \alpha_2, \dots, \alpha_n)$ большим (меньшим), чем $(\beta_1, \beta_2, \dots, \beta_n)$. Трудно также проверить, возникло ли переполнение допустимого диапазона чисел $P = p_1 p_2 \dots p_n$ в результате выполнения операций сложения или умножения, но еще труднее выполнить операцию деления. Эти, и некоторые другие операции, носят название немодульных, так как для их выполнения требуется знание о величине числа в целом, которое называется позиционной характеристикой числа.

Модель целочисленной модулярной арифметики можно задать следующей сигнатурой $\langle |P|, |\bullet|_{p_i}^+, MO, NO \rangle$, где: $|P|$ - полная система вычетов по модулю

полного динамического диапазона, $|\bullet|_{p_i}^+$ - вычет чисел по модулю p_i , МО – множество модульных операций, к которым относятся арифметические операции сложения, вычитания, умножения и деления нацело или умножение на обратный элемент, НО – множество немодульных операций, к которым относятся расширения база СОК, деления, масштабирования и другие.

Немодульные операции обусловлены знанием числового значения модулярной величины, которая определенным образом связана со значениями компонент модулярного представления. Эти операции являются медленными, что снижает эффективность применения модулярной алгебры. Для реализации немодульных операций используются специальные функционалы, которые определяют количественные характеристики отношения порядка над множеством модулярных векторов. Одно из устоявшихся названий функционалов – позиционная характеристика (ПХ) модулярной величины или числовой величины в модулярном коде. В основе алгоритмов выполнения немодульных операций лежат методы вычисления ПХ, сложность которых непосредственно влияет на скорость выполнения немодульных операций в модулярной алгебре. Поиск эффективных и универсальных ПХ важен для теоретических основ модулярных вычислительных структур и вычислительных средств на их основе.

Заключение

В настоящее время известны следующие методы определения позиционных характеристик модулярного представления чисел [1-4]: метод ортогональных базисов, метод функции Эйлера, метод интервальных оценок, метод с использованием коэффициентов обобщенной позиционной системы счисления (ОПСС) и другие.

Анализ позиционных характеристик показал, что коэффициенты ОПСС представляют собой универсальную позиционную характеристику на основе которой можно эффективно выполнить основные проблемные операции системы остаточных классов.

Литература

1. Машинная арифметика в остаточных классах / И. Я. Акушский, Д. И. Юдицкий. – М.: «Советское радио», 1968. – 440 с.
2. Модулярные параллельные вычислительные структуры нейропроцессорных систем / Н. И. Червяков, П. А. Сахнюк, А. В. Шапошников, С. А. Ряднов; под ред. Н. И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 288 с.
3. Нейрокомпьютеры в остаточных классах / Н. И. Червяков, П. А. Сахнюк, А. В. Шапошников, А. Н. Макоха; под ред. А. И. Галушкина. – М.; Радиотехника, 2003. – 272 с.
4. A. Omondi, Premkumar. Residue Number Systems. Theory and Implementation. London. Imperial College Press 2007. – 295 p.
5. Дерябин М.А., Зайцев А.А. Использование модулярной арифметики для ускорения выполнения операций над числами большой разрядности// Вестник Уфимского государственного авиационного технического университета. 2013. Т. 17. № 5 (58). С. 245-251.

Черногорова Ю.В.

**ИССЛЕДОВАНИЕ АЛГОРИТМОВ ПЕРЕВОДА ЧИСЕЛ ИЗ СИСТЕМЫ
ОСТАТОЧНЫХ КЛАССОВ В
ПОЗИЦИОННУЮ СИСТЕМУ СЧИСЛЕНИЯ**

ФГАОУ ВПО «Северо-Кавказский федеральный университет», Ставрополь,
Российская Федерация

1 Введение. Постановка задачи

Для решения широкого круга задач объем математических расчетов растет по экспоненциальному закону. Анализ известных подходов [1] показывает, что при разработке высокоскоростных вычислений требуется использование распределенных вычислений. Одним из подходов к построению

высокопроизводительных вычислений является использование системы остаточных классов (СОК), которая обеспечивает параллелизм на уровне выполнения элементарных операций [2]. Системой остаточных классов называется система, в которой целое положительное число A представляется в виде набора остатков (вычетов) $(\alpha_1, \alpha_2, \dots, \alpha_n)$ по выбранным взаимно простым основаниям p_1, p_2, \dots, p_n .

Развитие современной вычислительной базы делает СОК удобным для многих приложений: цифровой обработки данных, криптографии, систем передачи данных и др. Преимуществом СОК является переход от работы с числами большой длины к проекциям числа меньшей размерности, что позволяет проводить арифметические операции без переноса между проекциями числа и способствует уменьшению аппаратных и временных затрат. Одной из проблемных операций является перевод числа из СОК в позиционную систему счисления. Из всего вышесказанного особую актуальность приобретает следующая научная задача: исследование методов перевода числа из СОК в позиционную систему счисления (ПСС).

2 Методы перевода из СОК в ПСС

2.1 Метод ортогональных базисов

С выбором системы определяются ее основные константы – базисы B_i , $i = \overline{1, n}$. Задача перевода числа $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ в ПСС заключается в определении таких чисел M_i , $i = \overline{1, n}$, для которых $A = \sum_{i=1}^n M_i B_i$. Тогда ортогональные базисы определяются по формуле

$$B_i = \frac{m_i P}{p_i} = m_i P_i, \quad i = \overline{1, n},$$

где $P_i = \frac{P}{p_i} = p_1 \cdot p_2 \cdot \dots \cdot p_{i-1} \cdot p_{i+1} \cdot \dots \cdot p_n$, m_i – целые положительные числа, которые

определяются из сравнений $P_i m_i \equiv 1 \pmod{p_i}$.

Тогда, по Китайской теореме об остатках (КТО), число

$$A = (\alpha_1, \alpha_2, \dots, \alpha_n) \equiv \sum_{i=1}^n \alpha_i B_i \pmod{P}.$$

Так как ортогональные базисы B_i полностью определяются выбором оснований системы, то они могут быть заранее вычислены, что сводит к минимуму количество элементарных операций, необходимых для перевода числа из СОК в ПСС. Очевидным минусом данного метода является необходимость нахождения остатка по модулю P большой разрядности.

2.2 Метод перевода с помощью обобщенной позиционной системы

Другой метод определения величины числа связан с переводом числа из системы остаточных классов в ОПС. Пусть p_1, p_2, \dots, p_n – также основания ОПС, тогда число A можно представить в виде

$$A = \alpha_n p_1 p_2 \dots p_{n-1} + a_{n-1} p_1 p_2 \dots p_{n-2} + \dots + a_3 p_1 p_2 + a_2 p_1 + a_1 \quad (1)$$

где $0 \leq a_k < \prod_{i=1}^{k-1} p_i$ ($i = \overline{1, n}$) – коэффициенты ОПС.

Цифры ОПС могут быть получены из соотношений:

$$a_1 \equiv \alpha_1 \pmod{p_1}$$

$$a_2 \equiv (\alpha_2 - a_1) \tau_{12} \pmod{p_2}$$

$$a_3 \equiv ((\alpha_3 - a_1) \tau_{13} - a_2) \tau_{23} \pmod{p_3}$$

...

$$a_n \equiv (((\dots(\alpha_n - a_1) \tau_{1n} - a_2) \tau_{2n} - \dots - a_{n-1}) \tau_{(n-1)n}) \pmod{p_n}.$$

где $\tau_{kj} = \left| \frac{1}{p_k} \right|_{p_j}$ – обратный элемент по умножению для чисел p_k по модулю p_j .

Преимущество рассмотренного метода перед методом ортогональных базисов состоит в том, что все вычисления выполняются по модулям меньшей разрядности, причем в отдельных каналах, соответствующих модулям p_i , правда, к сожалению, не параллельно [3].

2.3 Интервальный метод

Достаточно эффективными методами перевода чисел из СОК в ПСС являются интервальные методы, основанные на интервальных характеристиках чисел. Одна из таких характеристик – номер интервала.

Выберем дробящий модуль p_i и проведем дробление заданного диапазона на интервалы путем деления P на модуль p_i . Тогда количество интервалов $m = P_i = \frac{P}{p_i}$, а длина интервала определяется величиной модуля. В

результате величину любого числа A можно найти как $A = p_i l_A + \alpha_i$, где

$l_A = \left\lfloor \sum_{i=1}^n \left\lfloor l_{A_i} \alpha_i \right\rfloor_{p_i} \right\rfloor_{p_i}^+$. Причем $l_{A_j} = \frac{P_j^{\varphi(p_j)}}{p_i}$, если $i \neq j$, и $l_{A_i} = \frac{P_i^{\varphi(p_i)} - 1}{p_i}$ – постоянные

коэффициенты, определенные системой оснований, а $\varphi(p_i)$ – функция Эйлера.

Тогда $A = \left(\left\lfloor \sum_{i=1}^n \left\lfloor l_{A_i} \alpha_i \right\rfloor_{p_i} \right\rfloor_{p_i}^+ \right) p_i + \alpha_i$.

Данный метод перевода из СОК в ПСС требует большего числа элементарных операций, чем метод ортогональных базисов, но существенно меньше чем перевод с помощью ОПС. Максимальный размер модуля, по которому берется остаток, меньше чем в методе ортогональных базисов, но существенно больше чем при переводе с помощью ОПС. Таким образом, интервальный метод отличается более оптимальным сочетанием количества элементарных операций и максимальной разрядности модуля, по сравнению с рассмотренными выше.

2.4 Диагональная функция

Для набора взаимно простых модулей p_1, p_2, \dots, p_n определим параметр

$SQ = P_1 + P_2 + \dots + P_n$, называемый суммой частных, где $P_i = \frac{P}{p_i}$ и $P = \prod_{i=1}^n p_i$ это

динамический диапазон СОК. Определим также константы

$$k_i = \left| -\frac{1}{m_i} \right|_{SQ} \text{ для } i = 1, 2, \dots, n.$$

Диагональная функция, соответствующая данному числу A , представленному в СОК как $(\alpha_1, \alpha_2, \dots, \alpha_n)$ определяется как

$$D(A) = |\alpha_1 k_1 + \alpha_2 k_2 + \dots + \alpha_n k_n|_{SQ}.$$

Заметим, что $D(A)$ является монотонной функцией [4]. В соответствии с КТО, исходное число в ПСС равно:

$$A = \frac{P \cdot D(A) + \alpha_1 P_1 + \alpha_2 P_2 + \dots + \alpha_n P_n}{SQ}.$$

Перевод из СОК в ПСС при помощи диагональной функции не является наилучшим ни с точки зрения количества элементарных операций, ни с точки зрения максимального размера модуля, кроме того на финальном шаге используется операция деления, являющаяся одной из наиболее затратных с точки зрения аппаратных ресурсов и времени выполнения.

3 Сравнительный анализ методов перевода из СОК в ПСС

Составим таблицу, отражающую количество элементарных операций необходимых для перевода тем или иным методом (без учета предвычислений и с учетом возможности параллельного выполнения операций) и максимальную длину модуля, по которому берется остаток. Заметим, что операции по каждому модулю выполняются параллельно, а суммирование на финальном этапе можно оптимизировать с помощью билинейного спаривания. Пусть каждое из оснований СОК имеет длину b бит, а их количество равно n , тогда:

Таблица 1. Сравнительный анализ различных методов перевода из СОК в ПСС

	Количество умножений	Количество сложений	Максимальная длина модуля
Метод ортогональных базисов	1	$\lceil \log_2 n \rceil$	nb
Метод перевода в ОПС	n	$n + 1 + \lceil \log_2 n \rceil$	b

Интервальный метод	2	$\lceil \log_2 n \rceil + 1$	$(n - 1)b$
Диагональная функция	2	$\lceil \log_2 n \rceil + \lceil \log_2(n + 1) \rceil$	$(n - 1)(b - 1)$

Таким образом, при работе с СОК, имеющей малоразрядные модули, не требующие больших аппаратных ресурсов для обработки, целесообразно применять для перевода из СОК в ПСС метод ортогональных базисов. В том случае, если разрядность оснований СОК достаточно велика, оптимальным будет метод перевода с помощью обобщенной системы счисления. Для интервального метода характерно оптимальное сочетание аппаратных ресурсов необходимых для перевода и времени на его выполнение.

Литература

1. Червяков Н.И. Реализация высокоэффективной модулярной цифровой обработки сигналов на основе программируемых логических интегральных схем // Нейрокомпьютеры: разработка, применение №10, 2006. – с. 24-35.
2. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Ряднов С.А. Модулярные параллельные вычислительные структуры нейропроцессорных систем. – М.: Физматлит, 2003. – 288 с.
3. Червяков Н.И. Преобразование цифровых позиционных и непозиционных кодов в системах управления и связи. – Ставрополь: СВВиУС, 1985. – 63 с.
4. P.V. Ananda Mohan. RNS to Binary Conversion Using Diagonal Function and Pirlo and Impedovo Monotonic Function. Circuits Syst Signal Process, 2015. – 14 с.

Баймолдина С.М.

КОМПЬЮТЕРНАЯ ИНФОРМАТИЗАЦИЯ В РЕСПУБЛИКЕ КАЗАХСТАН: ВОПРОСЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Евразийского национального университета им. Л.Н. Гумилева

Глобализация преступности, проблемы миграционных процессов в мире, ускорение обмена информацией через информационные сети, интернет ресурсы, иные виды мобильной связи, усиливают особую актуальность и значимость вопросов, связанных с соблюдением индивидуальных прав человека и интересов государственной безопасности в информационных системах и информационных ресурсах, а также в процессе коммуникации и связи.

Вопросы, связанные с обеспечением защиты компьютерной информации и информационных систем сейчас является одной из самых актуальных во всем мире.

Необходимость установления уголовной ответственности за причинение вреда в связи с использованием именно компьютерной информации (т.е. информации на машинном носителе, в электронно-вычислительной машине - далее ЭВМ, - системе ЭВМ или их сети) вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации по сравнению, например, с информацией, зафиксированной на бумаге и хранящейся в сейфе. О повышенной уязвимости компьютерной информации свидетельствует и то, что в силу специфичности данного вида информации достаточно сложно в короткие сроки определить был ли осуществлен неправомерный доступ, какая именно часть компьютерной информации была объектом изучения, определенные трудности существуют и в связи с необходимостью ограничения неправомерного доступа. Революция, произошедшая в области создания и использования компьютерной техники, предоставила преступникам широкие возможности доступа к новым техническим средствам и технологиям.¹

¹-Карпов, В. С. Уголовная ответственность за преступления в сфере компьютерной информации. Автореферат диссертации на соискание ученой степени кандидата юридических наук. Красноярск, 2002.

Большое значение на развитие научного направления в сфере уголовной ответственности за преступления в сфере компьютерной информации оказали научные исследования ведущих российских ученых. В рамках данной проблемы защищено ряд диссертаций: Р. М. Айсановым, Д. В. Добровольским, А. М. Дорониным, К. Н. Евдокимовым, У. В. Зининой, А. Ж. Кабановой, В.С. Карповым, А. Н. Копырюлиным, И.А. Сало, Т. Г. Смирновой, С. Г. Спириной, В. Г. Степановым-Егиянцем, А. В. Суслопаровым, Т. Л. Тропиной, С. И. Ушаковым, С. С. Шахраем, В. Н. Щепетильниковым и др.

Новое Уголовное законодательство Республики Казахстан, вступившее в действие с 1 января 2015 года, предусматривает ответственность за правонарушения в сфере компьютерной информации в Главе 7, именуемой как "Уголовные правонарушения в сфере компьютерной информатизации и связи". Данная Глава включает следующие виды правонарушений: Ст.205 "Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть", Ст. 206 "Неправомерные уничтожение или модификация информации", Ст. 207 "Нарушение работы информационной системы или информационно-коммуникационной сети", Ст.208 "Неправомерное завладение информацией", Ст. 209 "Принуждение к передаче информации", Ст. 210 "Создание, использование или распространение вредоносных компьютерных программ и программных продуктов", Ст. 211 "Неправомерное распространение электронных информационных ресурсов ограниченного доступа", Ст. 212 "Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели", Ст.213 "Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства".²

² - Уголовный кодекс Республики Казахстан, вступивший в действие с 1 января 2015 г.

Некоторые нормы рассмотрим более детально. Немаловажной частью нормальной деятельности электронных носителей имеет правильная работа информационных систем. Нарушение работы информационной системы или информационно-коммуникационной сети, в соответствии с новым уголовным кодексом Казахстана подлежит уголовной ответственности (ст. 207 УК РК). Так, например, умышленные действия (бездействие), направленные на нарушение работы информационной системы или информационно-коммуникационной сети, наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

Эти же деяния, совершенные в отношении национальных электронных информационных ресурсов или национальной информационной системы, или группой лиц по предварительному сговору, наказываются штрафом в размере до четырех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до четырех лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. Вышеуказанные деяния, совершенные преступной группой, а также повлекшие тяжкие последствия, наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Также, карается и неправомерное завладение информацией (ст. 208 УК РК). Умышленное неправомерное копирование или иное неправомерное завладение охраняемой законом информацией, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети, если это повлекло существенное

нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста восьмидесяти часов, либо арестом на срок до шестидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового. Это же деяние, совершенное в отношении национальных электронных информационных ресурсов или национальной информационной системы, а также группой лиц по предварительному сговору, наказывается штрафом в размере до двух тысяч месячных расчетных показателей, либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Все перечисленные деяния, предусмотренные частями первой или второй настоящей статьи совершенные преступной группой, повлекшие тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Уголовной ответственности подлежит также и принуждение к передаче информации (ст. 209 УК РК), в которой говорится о том, что принуждение к передаче охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети, под угрозой применения насилия либо уничтожения или повреждения имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, оглашение которых может причинить существенный вред

интересам потерпевшего или его близких, наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

Если было совершено то же деяние, сопряженное с применением физического насилия над лицом или его близкими, группой лиц по предварительному сговору, совершенное с целью получения информации из национальных электронных информационных ресурсов или национальной информационной системы, наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет. Данные деяния, совершенные преступной группой, а также повлекшие тяжкие последствия, наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Таким образом, введение уголовной ответственности за данные виды преступлений создают правовые условия для более полного соблюдения декларируемых прав человека и государственных интересов, связанных с компьютерной информатизацией и связью.