АПИБК-2020

МАТЕРИАЛЫ

МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КАЗАХСТАНЕ

Алматы

15 января, 2020 года

Институт информационных и вычислительных технологий МОН РК

«Ғылым ордасы»

МАТЕРИАЛЫ

Международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане»
15 января 2020 года

Алматы 2020

УДК 004
ББК 32.973.202
А35

А35 **Актуальные проблемы информационной безопасности в Казахстане:** Матер. Межд. науч. – практ. конф. (15 января 2020 г.). – Алматы, 2020. – с. 260

ISBN 978-601-332-542-2

В настоящее издание вошли материалы докладов Международной научно – практической конференции «Актуальные проблемы информационной безопасности в Казахстане».

Работа конференции проводилась при участии представителей органов государственной власти, квазигосударственных предприятий, научных сообществ и вузов, руководителей и специалистов компаний – разработчиков средств защиты информации, телекоммуникационных компаний, операторов связи, организации, осуществляющих свою деятельность в области информационной безопасности.

Рассмотрены актуальные вопросы обеспечения информационной безопасности в государственном секторе, состоялся диалог представителей отрасли и регуляторов, проведены обмен опытом и повышение информированности участников конференции о состоянии информационной безопасности в Республике Казахстан.

Материалы сборника предназначены для научных работников и преподавателей вузов соответсвтующего профиля, докторантов и магистрантов, а так же для специалистов, чьей задачей является использование средств обеспечения информационной безопасности.

УДК 004
ББК 32.973.202

ISBN 978-601-332-542-2

Соответственно, после нажатия этой кнопки происходит сразу два события, которые при обычной авторизации проходят поэтапно. А именно аутентификация и вывод из строя насоса.

Таким образом был выявлен инцидент: проведение атаки грубой силы по подбору пароля и отключению насоса.

Выводы. Каждый из приведенных выше международных стандартов с разной степенью пояснения и в различной структуре описывает набор мер построения процесса управления инцидентами информационной безопасности. Необходима разработка стандартов РК путем гармонизации и адаптации международных стандартов в области компьютерной криминалистики. При этом следует учесть обновление международных стандартов и тенденцию к увеличению их количества в области форензики.

Приведенное тестовое расследование полностью моделирует инцидент реальной жизни, так как исследуемые пакеты, предоставленные обучающим центром ENISA, получены с реальной атомной станции. Такое, приближенное к реальным условиям, расследование готовит начинающего специалиста к оперативным действиям и выбору методики сетевой криминалистики.

Литература

1. Casey, E. Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet / E. Casey. – NYC: Academic Press, 2011. – 840 p.
2. Федотов, Н.Н. Форензика – компьютерная криминалистика /Н.Н. Федотов. – Москва: Юридический Мир, 2007. – 432 с.
3. European Union Agency for Cybersecurity. ENISA Collection of CERT. - https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#network_forensics (13.11.2019)

ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ НОВОГО АЛГОРИТМА ШИФРОВАНИЯ QAMAL

Алгазы[2] К.Т, Бабенко[1] Л.К., Бияшев[2] Р.Г., Ищукова[1] Е.А., Капалова[2] Н.А., Нысанбаева[2] С.Е.

e-mail: kunbolat@mail.ru

[1]Институт компьютерный технологий и информационной безопасности Южного федерального университета, Россия

[2]Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В настоящий момент в Республике Казахстан ведутся работы по разработке нового стандарта симметричного шифрования данных. Одним из претендентов на роль стандарты выступает алгоритм шифрования Qamal, разработанный и Институте информационных и вычислительных технологий (г. Алматы, Республика Казахстан). В статье рассмотрены дифференциальные свойства основных операций, составляющих шифр Qamal. Рассмотрены подходы к построению*

многораундовых характеристик для шифра Qamal. Было показано, что для версии шифра со 128-битным блоком данных и таким же размером секретного ключа уже для трех раундов шифрования имеет сложность нахождения правильных пар текстов 2^{-120}, что делает дифференциальный криптоанализ неприменимым к шифру Qamal.

Актуальность исследования

Первым из известных государственных стандартов шифрования данных стал стандарт DES, принятый в США в начале 70-х годов. Это было то время, когда первые ЭВМ (электронные вычислительные машины) постепенно переставали быть экзотикой и начали входить в жизнь и работу небольших фирм и исследовательских лабораторий. Это привело к тому, что проблема защиты данных, хранимых и обрабатываемых на них, осознавалась все большим числом специалистов. Многие крупные корпорации, не говоря уже о государственных службах, проводили собственные исследования в данной области. В результате стали появляться различные алгоритмы шифрования. Одним из самых известных исследовательских центров такого рода в те времена являлась научная лаборатория фирмы IBM, возглавляемая доктором Хорстом Фейстелем [1]. В результате была создана система шифрования под названием Люцифер. Для этой системы шифрования Хорстом Фейстелем была предложена математическая модель, которая в настоящее время носит название «схема Фейстеля». Принцип схемы Фейстеля заключается в том, что за один раунд зашифровывается только половина или часть текста. Блок текста разделяется на части. Одна часть проходит через некоторое математическое преобразование. И результат этого преобразования складывается по модулю два со второй частью текста. После этого части текста меняются местами. Еще одним плюсом схемы оказался тот факт, что за счет использования операции «Исключающее-ИЛИ» или как ее еще называют операция сложения по модулю два становится возможным использовать одну и ту же схему как для зашифрования данных, так и для расшифрования данных, достаточно только изменить порядок следования раундовых подключей. Изначально стандарт DES принимался сроком на 5 лет, но впоследствии его срок в статусе стандарта был неоднократно продлен [2]. К концу 20 века компьютеры уже получили широкое распространение и вычислительные мощности выросли в разы. Поэтому правительство США задумалось о смене стандарта. В результате был объявлен конкурс на принятие нового стандарта шифрования данных – конкурс AES (Advanced Encryption Standard). Конкурс был объявлен в 1997 году Национальным институтом стандартов и технологий США (NIST – National Institute of Standards and Technologies) [3]. Для участия в конкурсе было заявлено 15 алгоритмов шифрования, созданных учеными разных стран. В результате пятилетнего исследования в качестве нового стандарта США был выбран алгоритм шифрования Rijndael, разработанный двумя учеными-математиками из Бельгии — Винсентом Риджменом (V. Rijmen) и Джоан Дейменом (J. Daemen). Алгоритм Rijndael построен по схеме сети на основе подстановок и перестановок (SPN) и имеет архитектуру «Квадрат» (Squre). На тот момент архитектура «Квадрат» и SP-сеть представляли собой инновационное решение. Сейчас же многие алгоритмы являются AES-подобными и повторяют структуру шифра Rijndael.

Параллельно с конкурсом AES в январе 2000 года начался весьма похожий конкурс в Европе, предполагающий выбор криптостандартов Евросоюза. Этот конкурс назывался NESSIE (New European Schemes for Signature, Integrity and Encryption — «новые европейские алгоритмы электронной подписи, обеспечения целостности и

шифрования») [3]. В результате работы над конкурсом NESSIE учеными-криптографами был написан большой труд под названием «NESSIEsecurityreport»[3], однако европейский стандарт так и не был выбран.

Под влиянием настроений США и Европы в Японии был создан проект CRYPTREC. CRYPTREC – это аббревиатура от Cryptography Research and Evaluation Committee [4]. Проект был создан с целью исследования криптоалгоритмов и последующей рекомендации конкретных алгоритмов для использования в государственных и частных организациях. В результате проекта CRYPTREC был выделен ряд алгоритмов шифрования, рекомендованных к использованию. Для 64-битных шифров были рекомендованы: CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, трехключевой вариант алгоритма Triple DES. Для 128-битных: AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000.

В России стандарт симметричного шифрования ГОСТ 28147-89 был принят в 1989 году. Однако до 1994 года он оставался засекреченным. ГОСТ 28147-89 представляет собой 64-битный блочный шифр, построенный по схеме Фейстеля. Разработчики заложили в шифр избыточную стойкость за счет большого количества раундов шифрования (32 раунда) и наложения секретного ключа с использованием операции сложения по модулю 2^{32}. 1 января 2016 года в России был принят новый стандарт шифрования данных – ГОСТ Р 34.12 – 2015 [6]. В новый стандарт шифрования входят два алгоритма шифрования: Магма и Кузнечик. Магма представляет собой бывший стандарт ГОСТ 28147-89 с одним исключением. В стандарте ГОСТ 28147-89 S-блоки замены не были зафиксированы и могли выбираться произвольным образом. В алгоритме Магма S-блоки регламентированы стандартом. Алгоритм Кузнечик представляет собой 128-битный симметричный блочный шифр, построенный по принципу SP-сети.

Государства, которые раньше составляли СССР, получили в наследство и стандарт шифрования ГОСТ28147-89. В настоящий момент наблюдается тенденция данных государств к развитию собственной государственной системы безопасности, которая в том числе включает и развитие собственных стандартов шифрования данных. Так, в Республике Беларусь был разработан стандарт СТБ 34.101.31-2007 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности» [7]. Сначала в 2007 году стандарт СТБ 34.101.31-2007 был принят в качестве предварительного стандарта в 2007 году. В 2011 году СТБ 34.101.31-2007 был введен в действие в качестве окончательного стандарта. В июле 2015 года стандарт симметричного шифрования был принят в Украине [8]. Стандарт ДСТУ 7624:2014 описывает работу алгоритма шифрования Калина, который является AES-подобным алгоритмом шифрования.

В Республике Казахстан в настоящий момент также ведется работа по созданию государственного стандарта симметричного шифрования данных в рамках проекта программы целевого финансирования «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» от Комитета науки Министерства образования и науки Республики Казахстан (№ гос. регистрации 0118РК01064).Одним из проектных алгоритмов шифрования выступает шифр Qamal, предложенный для исследования в настоящей работе. Подробное описание шифра Qamal можно найти в работе [9].

Основные этапы дифференциального анализа

Прежде чем приступить к дифференциальному анализу алгоритма шифрования KazCrypt, необходимо рассмотреть дифференциальные свойства каждого из его операций по отдельности. Подробное описание метода дифференциального анализа можно найти в работах [10 – 13]. Отметим, что всего можно выделить четыре основных этапа применения метода дифференциального анализа.

Этап 1. Анализ дифференциальных свойств всех составляющих преобразований в алгоритме шифрования.

Этап 2. Поиск наиболее вероятного значения дифференциала, то есть такой пары входная разность – выходная разность, появление которой наиболее вероятно.

Этап 3. Поиск правильных пар текстов. То есть таких текстов, для которых сумма по модулю два на входе в алгоритм шифрования совпадает со входной разностью, а сумма значений на выходе алгоритма шифрования совпадает с выходной разностью.

Этап 4. Анализ правильных пар текстов с целью определения битов секретного ключа.

Основная сложность дифференциального криптоанализа заключается в сложности нахождения правильных пар текстов, которая в свою очередь напрямую зависит от значения вероятности рассматриваемого дифференциала. Именно поэтому нахождение дифференциала, имеющего наибольшую вероятность, имеет первоочередное значение. Зная разность самого вероятного дифференциала, можно прогнозировать насколько успешным будет анализ самого шифра, либо его сокращенной версии. Имеется ввиду определение количества раундов шифра, для которых еще возможно применение дифференциального криптоанализа.

Дифференциальные свойства операции сложения по модулю 2

В дифференциальном криптоанализе преобразуемые тексты рассматриваются не по отдельности, а совместно. Вернее рассматривается их разность, которая определяется как результат сложения этих текстов по модулю два: $\Delta X = X \oplus X1$.

В этом случае значение разности ΔX будет содержать нули в тех позициях, в которых исходные сообщения были равны и единицы там, где биты различались.

Известно, что операция сложения данных с секретным ключом не влияет на изменение разности текстов. Это связано с тем, что при шифровании используется один и тот же секретный ключ шифрования. Таким образом, тексты будут складываться с одним и тем же значением К, которые в свою очередь сложившись друг с другом образуют значение равное нулю: $\Delta X = X \oplus K_i \oplus X1 \oplus K_i = X \oplus X1$.

Дифференциальные свойства операции замены битов с использованием S-блока

Так как S-блок шифра меняет 8 битов на 8 битов, то возможный диапазон входных разностей совпадает с диапазоном выходных разностей и находится в пределах от 0 до 255. Мы построили таблицу зависимости выходных разностей ΔC S-блока от значения входной разности ΔA и выявили следующие свойства:

Свойство 1. Значение $\Delta C = 0$ на выходе преобразования может быть получено только в том случае, когда $\Delta A = 0$. В этом случае вероятность появления разности на выходе равна 1.

Свойство 2. В построенной таблице анализа максимальным значением вероятности является значение 6/256 = 3/128.

Свойство 3. Существуют значения входных разностей ΔA, которые после прохождения через S-блок замены остаются неизменными. Это, например, такие значения (в 10-ной форме) как ΔA = 2, 3, 4, 6, 15, 16, 17, 18 и другие.

Свойство 4. Значение входной разности ΔA= 254 (ΔA = 0xfe) преобразуется в значение разности ΔC = 128 (ΔC = 0x80) с вероятностью p=4/256 = 1/64.

Дифференциальные свойства преобразования Mixer1

Несмотря на то, что преобразование Mixer1 является линейным преобразованием, необходимо определить как будут изменяться значения разностей при применении операции сложения по модулю 256. Известно, что при выполнении операции сложения по модулю 2^n разность остается неизменной с вероятностью p=1 только в том случае, если входная разность содержит всего один ненулевой бит в самом старшем разряде. Таким образом, если в преобразовании Mixer1 будет задействовано значение разности, равное 0x80, то какие бы преобразования мы с ним ни делали, вероятность всегда будет оставаться равной 1. Преобразование Mixer1 зависит от четырех байтов одного столбца. Поэтому важно рассмотреть, как будут меняться выходные значения. При этом с точки зрения дифференциального криптоанализа нас интересуют те варианты, которые затрагивают наименьшее количество активных байтов. Так как в операции Mixer1 сложение выполняется по модулю 256, то значение разности0x80 всегда будет оставаться неизменным. Так, сложение двух одинаковых разностей 0x80 и 0x80 по модулю 256 (0x100) будет приводить к нулю. Таким образом, мы можем рассмотреть 15 вариантов заполнения исходного столбца преобразования Mixer1, где значения байтов могут быть равны только 0x00 или 0x80. Пример одного такого преобразования приведен в таблице 1.

Таблица 1 – Результат преобразования разностей в преобразовании Mixer1. Вариант 1

Исходное состояние	Первое изменение	Второе изменение	Третье изменение	Четвертое изменение
0x80	0x80	0	0	0
0	0x80	0x80	0	0
0	0	0x80	0x80	0
0	0	0	0x80	0x80

Дифференциальные свойства преобразования Mixer2

Преобразование Mixer2 является линейным преобразованием. Оно не оказывает влияния на изменение вероятности преобразования разности. Однако для построения многораундовых характеристик важно определить, как именно будет преобразовано значение строк, содержащих в одном из байтов значение 0x80, которое будет получено после преобразования Mixer1. При этом важно помнить, что каждая строка использует свой полином m для умножения. В каждой строке содержится 4 байта. Если учесть, что каждый байт может содержать или значение разности, равное 0, или значение разности, равное 0x80, то всего получается 15 возможных заполнений для каждой строки от 0x00000080 до 0x80808080. Рассмотрим, как будут преобразованы данные разности с использованием полиномов m (для версии блока в 128 битов получается всего 60 вариантов: 15 вариантов заполнения и 4 полинома m). Нас интересуют те случаи, когда байты на выходе преобразования Mixer 2 после прохождения через блок замены S могут

быть преобразованы к значениям 0x80. То есть в таблице зависимостей ΔA и ΔC на пересечении ΔA, образованного из байта выхода преобразования Mixer2, и ΔC=0x80, должно стоять значение, отличное от 0. Мы разработали программу, с помощью которой просчитали все возможные вариант.

В результате применения данной программы было выявлено, что из 60 рассмотренных комбинаций заданному условию удовлетворяет всего одно значение. Входная разность, равная 0x80808000 преобразуется к разности 0xbbc868cf и после прохождения через S-блок замены может быть преобразована к значению разности 0x80808080. Именно эту комбинацию мы будем в дальнейшем использовать для построения многораундовых характеристик.

Построение многораундовых характеристик

Опираясь на дифференциальные свойства основных операций шифра Qamal, построим многораундовую характеристику и определим ее вероятность. Наша задача построить характеристику так, чтобы было затронуто как можно меньше активных S-блоков. От этого напрямую зависит вероятность нахождения правильной пары текстов по заданной характеристики. Наша задача определить какое количество раундов для шифра Qamal может быть проанализировано быстрее, чем методом полного перебора. Для блока данных в 128 битов используется секретный ключ длиной 128 битов, а значит сложность полного перебора составляет 2^{128}.

Рассмотрим первый раунд шифрования. Операцию сложения с раундовым подключом мы опускаем, так как она не влияет на изменение разности текстов. Нам необходимо, чтобы на входе преобразования Mixer1 появилось значение байтов 0x80. В соответствии со свойством 4 из подраздела 4.3, значение 0xfe будет преобразовано в значение 0x80 с вероятностью $4/256=1/64=2^{-6}$. При этом мы должны сформировать вход первого раунда таким образом, чтобы после преобразования Mixer1 ненулевая разность оказалась в третьей строке массива состояния. Если входная разность будет затрагивать первый и четвертый байты для первых трех столбцов состояния, то после S-блоков замены все ненулевые байты преобразуются в байты 0x80 с вероятностью $(2^{-6})^6 = 2^{-36}$. Можно видеть, что уже с первого раунда шифрования вероятность получения раундовой характеристики достаточно мала. Преобразование Mixer1 изменит массив состояния, не влияя на общую вероятность. В результате ненулевые байты окажутся только в первых трех позициях третьей строк. Все остальные значения будут нулевыми. Подробно схема преобразования для первого раунда представлена в таблице 2.

Таблица 2. Преобразование разности для первого раунда шифра Qamal

Вход первого раунда				Вход преобразования Mixer 1				Вход преобразования Mixer 2			
0xfe	0xfe	0xfe	0	0x80	0x80	0x80	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0x80	0x80	0x80	0
0xfe	0xfe	0xfe	0	0x80	0x80	0x80	0	0	0	0	0

Выше было показано, что, если на вход третьей строки в преобразовании Mixer2 поступает значение 0x80808000, то на выходе будет получено значение 0xbbc868cf. При этом каждый байт разности 0xbbc868cf может быть преобразован к байту 0x80. Вероятность того, что все четыре байта будут преобразованы в значения 0x80 составит

$(2^{-7})^4 = 2^{-28}$. Таким образом, итоговая вероятность для двух раундов шифрования составит 2^{-64}. После функции Mixer1 будут заполнены вторая и четвертая строки байтами 0x80,как это показано в таблице 3.

Таблица 3. Преобразование разности для второго раунда шифра Qamal

Вход в S-блок				Вход в преобразование Mixer1				Вход в преобразование Mixer2			
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0x80	0x80	0x80	0x80
0xbb	0xc8	0x68	0xcf	0x80	0x80	0x80	0x80	0	0	0	0
0	0	0	0	0	0	0	0	0x80	0x80	0x80	0x80

В результате анализа дифференциальных свойств преобразования Mixer2, было выявлено, что для второй и четвертой строки входная разность 0x80808080 не может быть преобразована таким образом, чтобы в следующем раунде после S-преобразования образовать все байты разности равные 0x80. Поэтому мы рассмотрели другие варианты преобразований. На вход S-блока третьего раунда поступят вторая и четвертая строки состояния, содержащие значение разности 0x95d14821, полученные после преобразования Mixer2 (таблица 4). В соответствии с таблицей дифференциальных свойств, мы определили, что байт 0x95 может быть заменен на байт 0x80. Для остальных байтов был подобран вариант замены, которые после преобразования Mixer1 затронет три ненулевые байта столбца (из четырех). Байт 0xd1 в соответствии с таблицей анализа имеет шансы быть преобразованным в байт 0x40 и в байт 0xc0. В этом случае преобразование Mixer1 будет выполнено в соответствии с таблицей 5. Байты 0x48 и 0x21 не могут быть преобразованы также, как байт 0xd1.Поэтому для них было выявлено, что они имеют возможность преобразования в байты 0x10 и 0xf0. В этом случае преобразование Mixer1 будет выполнено в соответствии с таблицей 6.

Таблица 4. Преобразование разности для третьего раунда шифра Qamal

Вход в S-блок				Вход в преобразование Mixer1				Вход в преобразование Mixer2			
0	0	0	0	0	0	0	0	0x80	0xc0	0x30	0x30
0x95	0xd1	0x48	0x21	0x80	0x40	0x10	0x10	0	0x80	0x20	0x20
0	0	0	0	0	0	0	0	0x80	0x40	0x10	0x10
0x95	0xd1	0x48	0x21	0x80	0xc0	0x1f	0x1f	0	0	0	0

Таблица 5. Преобразование Mixer1 для байтов 0x40 и 0xc0

Входные разности	Первый шаг преобразования	Второй шаг преобразования	Третий шаг преобразования	Выходная разность
0x00	0x00	0x40	0x80	0xc0
0x40	0x00	0x00	0x40	0x80
0x00	0x40	0x00	0x00	0x40
0xc0	0x00	0x40	0x00	0x00

Таблица 6. Преобразование Mixer1 для байтов 0x10 и 0xf0

Входные разности	Первый шаг преобразования	Второй шаг преобразования	Третий шаг преобразования	Выходная разность
0x00	0x00	0x10	0x20	0x30

0x10	0x00	0x00	0x10	0x20
0x00	0x10	0x00	0x00	0x10
0xf0	0x00	0x10	0x00	0x00

Вероятности преобразования каждого байта по S-блоку замены для третьего раунда составляет 2^{-7}. Всего в третьем раунде используется 8 ненулевых блоков. Таким образом, вероятность преобразования в третьем раунде равна $(2^{-7})^8 = 2^{-56}$. Получается, что вероятность для трех раундов шифра будет равна 2^{-120}, что очень близко к значению вероятности полного перебора. Поэтому дальше рассматривать преобразование разности смысла не имеет. Нам необходимо определить значение разности на выходе третьего раунда шифрования. Для этого рассмотрим разности на входе в преобразование Mixer2 третьего раунда. Применив к нему преобразования Mixer1 и Mixer2, получим состояние разностей как показано в таблице 7.

Таблица 7 – Состояние разностей после третьего раунда шифрования

0x4c	0x6b	0x94	0xea
0xad	0xde	0x47	0x5b
0xe1	0xb2	0xd3	0xb1
0x00	0x00	0x00	0x00

Заключение

Нами рассмотрен проектный алгоритм симметричного шифрования Qamal, который рассматривается в качестве претендента на стандарт шифрования данных в Республике Казахстан. Показано, что для версии шифра со 128-битным блоком данных и секретным ключом такой же длины дифференциальный криптоанализ становится неприменимым после трех раундов шифрования. Для полной проверки надежности шифра предстоит еще его тщательное исследование с использованием других криптоаналитических атак.

Работа выполнена в рамках программы целевого финансирования BR05236757 «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» Министерства образования и науки Республики Казахстан.

Литература

1. History of DES. - http://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/des%20history.html
2. Bruce Shnier Applied Cryptography: Protocols, Algorithms, and Source Code in C. - 1996. - John Wiley & Sons. - 784 P.
3. Панасенко С.П. Конкурсы AES и NESSIE [Электронный ресурс] - https://www.osp.ru/pcworld/2004/12/169401/
4. Specifications of e-Government Recommended Ciphers // https://www.cryptrec.go.jp/en/method.html
5. GOST 28147-89: Encryption, Decryption and Message Authentication Code (MAC) Algorithms // https://tools.ietf.org/html/rfc5830
6. GOST R 34.12–2015 «Information technology. Cryptographic data security. Block ciphers» // https://tc26.ru/en/standards/standards/gost-r/gost-r-34-12-2015-information-technology-cryptographic-data-security-block-ciphers.html

7. Fault-based Attacks on the Bel-T Block Cipher Family // https://zerobyte.io/publications/2015-JP-belt.pdf
8. A New Encryption Standard of Ukraine: The Kalyna Block Cipher - https://pdfs.semanticscholar.org/7771/8fbf6c2044b6f1aa2e66a1eda99121caa4da.pdf
9. Kunbolat Algazy, Ludmila Babenko, Rustem Biyashev, Evgeniya Ishchukova, Nursulu Kapalova, Saule Nyssanbayeva Investigation of the Different Implementations for the New Cipher Qamal // SIN '19 Proceedings of the 12th International Conference on Security of Information and Networks Article No. 8. Sochi, Russia — September 12 - 15, 2019 - doi>10.1145/3357613.3357622
10. E. Biham, A. Shamir: "DifferentialCryptanalysisoftheFull 16-roundDES", Crypto'92, Springer-Velgar, 1998, p.487
11. E. Biham, A. Shamir: "Differential Cryptanalysis of DES-like Cryptosystems", Extended Abstract, Crypto'90, Springer-Velgar, 1998, p.21
12. E.A. Ishchukova, E.A. Tolomanenko, L.K. Babenko Differential analysis of 3 round Kuznyechik // Proceedings of the 10th international conference on Security of information and networks (SIN 2017), ACM, New York, NY, USA.
13. Бабенко Л.К. Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа // Москва, «Гелиос АРВ», 2006 г. – 376 с.

О МОДЕЛИ РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Бегимбаева Е.Е.
e-mail: enlik_89@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Обнаружение конфликтов при информационном взаимодействии возможно только при наличии адекватной модели, которая описывает автоматизированную систему и элементы с потенциально конфликтным взаимодействием. В статье рассмотрен модуль разрешения конфликтных ситуаций в автоматизированной системе защищенного информационного взаимодействия. Приведены недостатки обеспечения бесконфликтного взаимодействия.*

В настоящее время происходит активный процесс информатизации всех сфер деятельности общества и государства. Она направлена, на активное внедрение компьютерной техники и новых информационных технологий в различные сферы, на эффективное формирование и использование национальных информационных ресурсов. При автоматизации информационного взаимодействия важным является обеспечение информационной безопасности. В связи с этим задачи обеспечения защиты информации в автоматизированной системе информационного взаимодействия (АСИВ) выходят на передний план. Для решения этих задач разрабатывается комплекс

Содержание

Amanzholova S. Meer Jaro Khan Sagymbekova A. Nurbala R.	SECURE IDENTITY ACCESS MANAGEMENT	5
Razaque A. Amanzholova S. Sagymbekova A.	PROTECTION OF CONTROL FRAMES FROM DENIAL OF SERVICE ATTACKS DURING HANDOVER PROCESS	13
Razaque A. Amanzholova S. Shevchenko Y. Samburskaya S. Fazylbekova R.	SCHOOL SECURITY SYSTEM USING RFID	23
Zhukabayeva T.K. Abdildayeva A.A. Mardenov E.M. Khu Ven–Tsen	SECURITY ISSUES IN WIRELESS SENSOR NETWORK	33
Абуов Б.Б.	ЭЛЕКТРОНДЫҚ САУДАНЫҢ ИНТЕГРАЦИЯЛАНҒАН АҚПАРАТТЫҚ ЖҮЙЕСІ	37
Бисаринов Б.Ж., Бисаринова А.Т.	ҮЛКЕН ДЕРЕКТЕРДІ (BIG DATA) ЗЕРТТЕУДІҢ МАҢЫЗДЫЛЫҒЫ	41
Капалова Н.А. Абишева А.Ж.	САНДЫҚ СЕРТИФИКАТТАРДЫ ҚОЛДАНУ	46
Қорласбай М.С	ОҚЫТУШЫЛАРДЫҢ ҒЫЛЫМИ БЕЛСЕНДІЛІГІН БАҚЫЛАУҒА АРНАЛҒАН АЖ КОНЦЕПЦИЯСЫ	54
Мусиралиева Ш.Ж. Болатбек М.А.	ӘЛЕУМЕТТІК ЖЕЛІДЕГІ ЭКСТРЕМИСТІК МӘТІНДЕРДІ ЖІКТЕУ ДӘЛДІГІН ГРАММАТИКАЛЫҚ ҚАТЕЛЕРДІ АНЫҚТАУ ЖӘНЕ ТҮЗЕТУ АРҚЫЛЫ АРТТЫРУ	57
Орақ Б.Б.	ISO 9001-2015 ХАЛЫҚАРАЛЫҚ СТАНДАРТЫНДАҒЫ БІРТҰТАС ЖҮЙЕ РЕТІНДЕ ЖАҢАЛЫҚТАР БАҒДАРЛАМАЛАРЫНЫҢ САПА МЕНЕДЖМЕНТІНІҢ МОДЕЛІ	61
Самрат С.М. Сулейменов О.Т.	АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ SOC-ТЫҢ АЛАТЫН ОРНЫ	70

Сейтқали Ғ.Т.	ЭЛЕКТРОНДЫ ҚҰЖАТ АЙНАЛЫМДАҒЫ АҚПАРАТ ҚАУІПСІЗДІГІН ҚАМАТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ	74
Шайкулова А.А. Калижанова А.У.	ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ АҚПАРАТТЫҚ ҚАУІПСІЗДІК АСПЕКТІСІНДЕ	79
Абдикаликов К.А.	СОКРЫТЫЕ ВОДЯНЫЕ ЗНАКИ С ИСПОЛЬЗОВАНИЕМ БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ	83
Айтхожаева Е.Ж. Акатаев Н.Н.	УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ИНФРАСТРУКТУРАХ	86
Айтхожаева Е.Ж. Сырлыбаева А.Н	СТАНДАРТЫ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ И КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА	91
Алгазы К.Т Бабенко Л.К. Бияшев Р.Г. Ищукова Е.А. Капалова Н.А. Нысанбаева С.Е.	ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ НОВОГО АЛГОРИТМА ШИФРОВАНИЯ QAMAL	97
Бегимбаева Е.Е.	О МОДЕЛИ РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ	105
Бияшев Р.Г. Алгазы К.Т. Хомпыш А.	ИССЛЕДОВАНИЕ РАЗРАБОТАННЫХ АЛГОРИТМОВ ПО КРИТЕРИЮ «ЛАВИННОГО ЭФФЕКТА»	107
Дайырбаева Э.Н., Липская М.А.	ОСОБЕННОСТИ ЦИФРОВОЙ СТЕГАНОГРАФИИ КАК МЕТОДА ОБЕСПЕЧЕНИЯ СОКРЫТИЯ ИНФОРМАЦИИ	119
Дюсенбаев Д. Сақан Қ.	КРИПТОГРАФИЧЕСКАЯ АТАКА НА АЛГОРИТМ «QAMAL» МЕТОДОМ БУМЕРАНГА	123
Жаннатова М.Т.	ИГРОВАЯ СИСТЕМА ОБУЧЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБУЧЕНИЯ СТУДЕНТОВ В КУРСЕ СИСТЕМНОГО АНАЛИЗА	130
Жижимов В.В.	УГРОЗЫ ИНФОРМАЦИОННОЙ (КИБЕР) БЕЗОПАСНОСТИ - ТЕРМИНОЛОГИЧЕСКИЙ АСПЕКТ	135