МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственное образовательное учреждение
высшего профессионального образования
Алтайский государственный технический
университет им. И.И. Ползунова

Загинайлов Ю.Н.

ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Курс визуальных лекций

Специальность 090104
«Комплексная защита объектов информатизации»

Барнаул 2010

УДК 621.38.067 (075.8)

Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: курс визуальных лекций / Ю.Н. Загинайлов; Барнаул: АлтГТУ.-2010- -104с.

Изложены теоретические основы информационной безопасности на уровне Российской Федерации, организации, технической системы.

Приведены объекты обеспечения информационной безопасности, угрозы объектам, политики и структуры систем обеспечения информационной безопасности.

Рассмотрены понятия и классификации защищаемой информации, угроз безопасности информации, объектов, способов, средств и систем защиты информации.

Предназначены для студентов специальности 090104 «Комплексная защита объектов информатизации».

СОДЕРЖАНИЕ

ЧАСТЬ I
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Часть II
МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Тема №1
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЕЁ СОСТАВЛЯЮЩИЕ

ВОПРОСЫ

1.1 БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

1.2 ИНФОРМАЦИЯ В СОВРЕМЕННОМ МИРЕ И ЕЁ СВОЙСТВА

1.3 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПОНЯТИЕ И СОСТАВЛЯЮЩИЕ

Литература: 1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пособие для вузов.-М:Горячая линия-Телеком, 2004.-280с

2. Организационно – правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А.А.Стрельцов [и др.]; под ред.А.А.Стрельцова.- М.: Издательский центр «Академия», 2008.-256с.

1.1 Безопасность в информационном обществе

ИНФОРМАЦИОННОЕ ОБЩЕСТВО КАК НОВЫЙ ЭТАП РАЗВИТИЯ ЦИВИЛИЗАЦИИ

В исторической науке выделяют три основных этапа развития цивилизации: доиндустриальный, индустриальный, постиндустриальный или информационный

ХАРАКТЕРИСТИКА ЭТАПОВ РАЗВИТИЯ ОБЩЕСТВА			
Этап Развития общества	Основной производственный ресурс	Тип производственной деятельности	Характер базовых технологий производства
Доиндустриальный	Сырьё	Добыча	Трудоёмкие
Индустриальный	Энергия	Изготовление	Капиталоёмкие
Постиндустриальный (информационный)	Информация	Обработка	Наукоёмкие

Информационное общество как новый этап развития человеческой цивилизации в XXI веке характеризуется высоким уровнем развития информационных (ИТ) и телекоммуникационных технологий (ИТТ) и их интенсивным использованием гражданами, бизнесом и органами государственной власти

1.1 Безопасность в информационном обществе

ИНФОРМАЦИОННОЕ ОБЩЕСТВО КАК НОВЫЙ ЭТАП РАЗВИТИЯ ЦИВИЛИЗАЦИИ

Переход от индустриального к информационному обществу существенно усиливает роль интеллектуальных факторов производства. Увеличение добавленной стоимости в экономике происходит в значительной мере за счет интеллектуальной деятельности, повышения технологического уровня производства и распространения современных ИТ и ИТТ. В результате возникает новое качество жизни общества, проявляющееся в наибольшей степени в *экономической, социальной, и духовной сферах, а также в сфере государственного управления*. .

В экономической сфере **это проявляется в появлении «Информационной» экономики и электронно-сетевой формы реализации экономических отношений. Информатизация средств производства.**

В социальной сфере **все большее число видов труда требует серьезной профессиональной подготовки, происходит формирование и обособление новой технократической элиты, расширяются возможности социальных институтов государства по предоставлению гражданам социальных услуг**

В Духовной сфере **– революционное повышение интеллектуальной деятельности. Расширение возможностей для доступа к информации, для взаимодействия между людьми**

В сфере государственного управления**: революционное повышение эффективности управления государством, взаимодействия государства и общества, общественного контроля за деятельностью государства.**

1.1 Безопасность в информационном обществе

ИНФОРМАЦИОННОЕ ОБЩЕСТВО КАК НОВЫЙ ЭТАП РАЗВИТИЯ ЦИВИЛИЗАЦИИ

Таким образом, информация и ИТ в современном мире определяют пути и направления развития любого общества и государства, коренным образом влияют на формирование человека как личности. Высокие технологии, в том числе информационные и телекоммуникациионные, становятся локомотивом социально-экономического развития, а обеспечение гарантированного свободного доступа граждан и общества к информации - одной из важнейших задач государства.

Программы развития информационных технологий ведущих мировых держав, государственное финансирование таких программ выходят на первое место, опережая ракетные и космические программы.

В России
Программный документ

Стратегия развития информационного общества в Российской Федерации.
(утв. Президентом РФ 7 февраля 2008 г. N Пр-212)

Являясь основной прогресса современного общества, высокие технологии, в том числе ИТ и ИТТ, становятся фактором общественного развития, что приводит к объективной зависимости развития общества в различных сферах жизни, сферы государственного управления от ИТ и ИТТ

1.1 Безопасность в информационном обществе

ПРОБЛЕМА БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Являясь основной прогресса современного общества, высокие технологии, в том числе ИТ и ИТТ, становятся фактором общественного развития, что приводит к объективной зависимости развития общества в различных сферах жизни, сферы государственного управления от ИТ и ИТТ

Это порождает угрозу использования этой зависимости во вред обществу, поскольку, изменяя социальную организацию общества, ИТ и ИТТ фактически не оказывают влияния на основные законы развития общества, природу человека, биологическую и психологическую основу его жизни. В связи с этим не претерпевают изменений и основные источники угроз интересам человека, общества и государства, свойственные доиндустриальному и индустриальному этапам развития цивилизации (преступления, финансовые махинации войны и военные, а также политические конфликты, террористические действия, криминальные структуры и т.п)

Существенным отличием угроз, возникающих в информационном обществе, от угроз, характерных для индустриального общества, является изменение форм их проявления и способов реализации.

Информация стала фактором, способным привести к крупномасштабным авариям, военным конфликтам и поражению в них, дезорганизовать государственное управление, финансовую систему, работу научных центров.

5

1.1 Безопасность в информационном обществе

ПРОБЛЕМА БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

1. **Традиционные преступления с корыстными целями (мошенничество, хищение и т.п.) стали совершаться с использованием ИТ и ИТТ**

   Так, преступления с корыстными целями, всегда представлявшие собой значительную социальную опасность, все чаще совершаются не только с применением современных ИТ, но и с использованием информации в качестве средства осуществления корыстных посягательств. По мере развития«электронно-сетевой» экономики, информатизации государственных органов тенденция роста этого вида преступлений в ближайшем будущем, видимо, будет нарастать.

2. **Новый вид преступлений с использованием информации в качестве средства осуществления корыстных посягательств (шантаж и т.п.).**

3. **Преступления в сфере компьютерной информации (вредоносные программы, НСД к информации, нарушение работы ЭВМ, системы ЭВМ или их сети)**

   Все больший ущерб предпринимательской деятельности граждан и организаций, а также деятельности государственных органов наносят распространение в компьютерных сетях вредоносных программ (вирусов), осуществление несанкционированного доступа к информационным ресурсам, распространение «информационной» макулатуры (спама).

4. **Расширяется использование современных ИТ для совершения преступных деяний в области нарушения конституционных прав и свобод человека и гражданина, ведения экономического и промышленного шпионажа, раскрытия сведений, составляющих личную, семейную, коммерческую, государственную и другие охраняемые законом тайны.**

5. **Опасность использования современных ИТ для информационных (информационно-психологических) войн, террористических действий, дезорганизации управления критически важными объектами инфраструктуры**

   Многие страны активно проводят исследования в области использования ИТ для оказания силового давления на политическое руководство противостоящих государств, совершенствуют методы и способы ведения так называемых информационных войн.

6

1.1 Безопасность в информационном обществе

ПРОБЛЕМА БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Все это выделяет обеспечение безопасности в качестве важнейшего направления деятельности человека, организаций и государственных органов в информационном обществе.

Важная особенность указанной деятельности — многообразие возможных объектов безопасности, проявлений угроз этим объектам и содержания последствий таких проявлений.

Для эффективного обеспечения безопасности важно не только владеть необходимыми знаниями и навыками осуществления тех или иных конкретных мероприятий, использования средств и методов проти-водействия угрозам, но и обладать определенной теоретической подготовкой, позволяющей комплексно рассматривать возникающие в данной области вопросы применительно к любому объекту безопасности.

7

1.2 ИНФОРМАЦИЯ В СОВРЕМЕННОМ МИРЕ И ЕЁ СВОЙСТВА

ОСНОВНЫЕ ФОРМЫ ПРОЯВЛЕНИЯ ИНФОРМАЦИИ

Термин «информация» происходит от латинского *information*, что означает разъяснение, изложение. Однако разные науки сегодня вкладывают в это понятие различное содержание. Диапазон толкований термина «информация» достаточно широк, точно также и широк диапазон рассмотрения её свойств.

С правовой точки зрения, закреплённой в информационном законодательстве России *информация* - это сведения (сообщения, данные) независимо от формы их представления.

сведения -
запечатлённые в организме результаты отражения движения объектов материального мира

сообщения
– *набор знаков*, с помощью которых сведения могут быть *переданы* другому организму и *восприняты* им

«данные»
можно рассматривать как разновидность сообщений, предназначенных для автоматизированной обработки с использованием СВТ.

***В теории ИБ принята органическая точка зрения*, основанная на философском подходе**

Согласно органической точке зрения, информация представляет собой результаты отражения объектов материального мира, запечатлённые в организме или коллективе организмов и используемые ими для адаптации к изменениям окружающего мира.

В отличие от других организмов человек способен не только приспосабливаться к реальной жизни и условиям, но и оказывать воздействие на условия своего существования. Реализация этих способностей человека целиком и полностью основывается на восприятии, накоплении и использовании информации в форме ***сведений***, а также получении и передаче её в форме ***сообщений***. С этой точки зрения информация представляет собой явление жизни и человека и общества, важнейший фактор их существования.

8

1.2 ИНФОРМАЦИЯ В СОВРЕМЕННОМ МИРЕ И ЕЁ СВОЙСТВА

ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

Передача сообщений через естественную среду обитания - воздух - обеспечивает обмен сведениями между индивидами, однако обладает рядом объективных ограничений по дальности и оперативности осуществления информационного обмена, по длительности хранения переданных сообщений и возможности их ретроспективного анализа.

Преодоление выделенного ограничения связано с созданием искусственной среды передачи информации, которая придает процессу информационного взаимодействия новое качество – это информационная инфраструктура.

ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

По содержанию → **Совокупностью используемых обществом ИТ и технических систем, реализующих эти технологии, а также совокупность социальных институтов, обеспечивающих создание, эксплуатацию и модернизацию технических систем обеспечения информационного взаимодействия.**

Ключевым элементом информационной инфраструктуры,являются *информационные технологии.*

По форме → по форме — **это совокупность социально-технических систем, реализующих функции обеспечения информационного взаимодействия, и общественно поддерживаемого порядка использования данных систем в жизни человека и общества.**

9

1.2 ИНФОРМАЦИЯ В СОВРЕМЕННОМ МИРЕ И ЕЁ СВОЙСТВА

СВОЙСТВА ИНФОРМАЦИИ

Информация как предмет защиты имеет свои специфические особенности. К ним можно отнести:

1. Информация в форме сведений всегда связана с человеком (физическим лицом), а в форме сообщений и данных связана с человеком (физическим лицом) и материальным носителем, на котором она фиксируется.

2. Информация может быть товаром и объектом рыночных отношений. Право собственности закреплено гражданским законодательством, включает имущественные права. Для реализации права необходимо документирование информации - фиксация на материальном носителе.

3. Информация как предмет жизнедеятельности и жизнеобеспечения имеет ценность (цену) и (или) важность, которые могут меняться во времени, и приносить доход или другие материальные и нематериальные блага её собственникам, владельцам пользователям. Для сохранения ценности (важности) информации необходимо поддерживать её потребительские свойства: конфиденциальность, целостность, доступность. При нарушении хотя бы одного из этих свойств ценность информации снижается либо теряется вообще.

Конфиденциальность **- свойство (характеристика) информации, указывающая на необходимость ограничения круга субъектов, имеющих доступ к данной информации.**

Целостность информации **- свойство информации существовать в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).**

Доступность информации **- состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно**

10

1.3 ПОНЯТИЕ БЕЗОПАСНОСТИ И ЕЁ СОСТАВЛЯЮЩИЕ

ПОНЯТИЕ БЕЗОПАСНОСТИ

Понятие ***«безопасность»*** в русском языке определяется как:

1. «Отсутствие опасности» (*Даль В.* Толковый словарь живого великорусского языка).

2. «Состояние, при котором не угрожает опасность, есть зашита от опасности», (*Ожегов С. И.,* Словарь русского языка)

понятие ***«опасность»*** означает «**возможность, угрозу чего-нибудь опасного, т.е. способного причинить какой-нибудь вред, несчастье**»

а понятие ***«угроза»*** — «**возможную опасность, запугивание, обещание причинить кому-нибудь неприятность, зло**» (*Ожегов С. И.*)

Таким образом, ***безопасность*** **есть невозможность нанесения вреда кому-нибудь или чему-нибудь вследствие проявления угроз, т.е. их защищенность от угроз.**

11

1.3 ПОНЯТИЕ БЕЗОПАСНОСТИ И ЕЁ СОСТАВЛЯЮЩИЕ

ПОНЯТИЕ БЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ

К О М П О Н Е Н Т Ы

ОБЪЕКТ БЕЗОПАСНОСТИ

– это то чему не должен быть нанесён вред

УГРОЗЫ ОБЪЕКТУ БЕЗОПАСНОСТИ

- проявление взаимодействия объекта безопасности с другими объектами, способными нанести ему вред

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТА

Деятельность по обеспечению безопасности объекта

- формирование политики безопасности, целей и стратегии
- определение и реализация мер безопасности и системы безопасности
- контроль (аудит) и совершенствование мер системы

Средства обеспечения безопасности объекта

-совокупность материальных, духовных, финансовых, правовых, организационных и технических средств осуществления деятельности по обеспечению безопасности

Субъекты обеспечения безопасности объекта

- индивиды, организации, органы государства, осуществляющие деятельность по обеспечению

12

1.3 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПОНЯТИЕ И СОСТАВЛЯЮЩИЕ

СОСТАВЛЯЮЩИЕ (КОМПОНЕНТЫ) ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

объект безопасности	угрозы объекту безопасности	обеспечение безопасности объекта

Концептуальная модель информационной безопасности

1. Объекты ИБ	2. Угрозы объектам ИБ	3. Политика обеспечения ИБ	4.Система обеспечения ИБ

ОРГАНИЗАЦИОННЫЕ УРОВНИ ОБЕСПЕЧЕНИЯ ИБ

Объекты определённые в: Стратегии развития информационного общества в РФ Доктрине информационной безопасности РФ Стратегии национальной безопасности РФ до 2020	ГОСУДАРСТВЕННЫЙ РОССИЙСКАЯ ФЕДЕРАЦИЯ
Объекты определённые в: ГОСТ Р ИСО/МЭК 27001-2006. ГОСТ Р ИСО/МЭК 13335-1-2006. ГОСТ Р 50922-2006. Национальный стандарт РФ. Защита информации. Основные термины и определения.	ОРГАНИЗАЦИЯ (ПРЕДПРИЯТИЕ, УЧРЕЖДЕНИЕ)

13

1.3 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПОНЯТИЕ И СОСТАВЛЯЮЩИЕ

ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УРОВНИ	ПОНЯТИЕ
РОССИЙСКАЯ ФЕДЕРАЦИЯ	Под информационной безопасностью РФ следует понимать состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства от внутренних и внешних угроз способных нанести ущерб этим интересам.
ОРГАНИЗАЦИЯ (ПРЕДПРИЯТИЕ, УЧРЕЖДЕНИЕ)	Информационная безопасность организации - это состояние защищённости объектов (активов) организации, при котором обеспечивается конфиденциальность, целостность, доступность информации.
ТЕХНИЧЕСКАЯ СИСТЕМА хранения, обработки и передачи информации	Информационная безопасность – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой – её функционирование не создаёт информационных угроз для элементов самой системы и внешней среды.

14

Тема №2
МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

ВОПРОСЫ

2.1 ИНФОРМАЦИОННАЯ ВОЙНА КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

2.2 МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

2.3 ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

Литература

1. Методические рекомендации к курсу.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» 2006г. (ПСС Гарант, Интернет)
3. Стратегия национальной безопасности РФ до 2020 года. (ПСС Гарант, Интернет)

2.1 Информационная война как угроза национальной безопасности

ПОНЯТИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ И ЕЁ ОСОБЕННОСТИ

Термин «информационная война» (далее – ИВ) появился в середине 80-х г.г. в связи с новыми задачами Вооруженных Сил США после окончания «холодной войны». Начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г., когда новые информационные технологии впервые были использованы как средства ведения войны.

Под **информационной войной** понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии, посредством воздействия на информацию и ИС противника при одновременном обеспечении безопасности и защиты собственной информации и ИС. **(Понятие сформированное в военных кругах США)**

Особенности информационной войны:

1. Охватывает **в качестве самостоятельных объектов все виды информации и информационных систем, отделяя информацию от среды использования;**

2. Объекты **могут выступать и как оружие, и как объект защиты;**

3. Расширяет **территорию и пространство ведения (традиционной войны), ведется как при объявлении войны, так и в кризисных ситуациях в различных сферах жизнедеятельности.**

4. Ведется как специализированными военными, так и гражданскими структурами.

2.1 Информационная война как угроза национальной безопасности

ПОНЯТИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ И ЕЁ ОСОБЕННОСТИ

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ ПО ОЦЕНКАМ РОССИЙСКИХ СПЕЦСЛУЖБ, (ПРЕДУСМАТРИВАЕТ):

1. Подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);

2. Радиоэлектронная борьба (электромагнитное воздействие на элементы ИС и ИТКС, системы связи)

3. Радиоэлектронная разведка (получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счет специально внедренных в помещения и технические средства электронных устройств перехвата информации).

4 «Хакерная война» (осуществление НСД к ИР путем использования программно-аппаратных средств прорыва систем защиты ИС и ИТКС противника, с последующим их искажением, уничтожением или хищением либо нарушением нормального функционирования этих систем).

5. Психологическая война (формирование и массовое распространение по информационным каналам противника или глобальным сетям информационного взаимодействия дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения).

6. Получение интересующей информации путем перехвата и обработки открытой информации, передаваемой по незащищенным каналам связи, циркулирующей в ИС, а также публикуемой в СМИ.

2.1 Информационная война как угроза национальной безопасности

ИНФОРМАЦИОННОЕ ОРУЖИЕ

ИНФОРМАЦИОННОЕ ОРУЖИЕ – это средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всех средств высокотехнологичного обеспечения жизни общества и функционирования государства.**(Российскими экспертами и учёными)**

Информационное оружие от обычных средств поражения отличает:

1. Скрытность – возможность достигать цели без видимой подготовки и объявления войны;

2. Масштабность – возможность наносить невосполнимый ущерб, не признавая национальных границ и суверенитетов, без привычного ограничения пространства во всех сферах жизнедеятельности человека;

3.Универсальность – возможность многовариантного использования как военными, так и гражданскими структурами страны нападения против военных и гражданских объектов страны поражения.

Основные объекты применения ИО (как в мирное, так и в военное время) :

1. Компьютерные системы и системы связи, используемые государственными организациями при выполнении своих управленческих функций;

2. Военная информационная инфраструктура, решающая задачи управления войсками и боевыми средствами, сбора и обработки информации в интересах вооруженных сил;

4. Информационные и управленческие структуры банков, транспортных и промышленных предприятий;

5. СМИ, в первую очередь электронные (радио, телевидение и т.д.).

2.1 Информационная война как угроза национальной безопасности

ИНФОРМАЦИОННОЕ ОРУЖИЕ

***Сфера применения ИО** (включает как военную, так и экономическую, банковскую, социальную и иные области потенциального использования в целях):*

1. Дезорганизации деятельности управленческих структур, транспортных потоков и средств коммуникации;

2. Блокирования деятельности отдельных предприятий и банков, а также базовых отраслей промышленности (путем нарушения многозвенных технологических связей и системы взаиморасчетов, проведения валютно-финансовых махинаций и т.п.);

3. Инициирования крупных техногенных катастроф на территории противника в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии;

4. Массового распространения и внедрения в сознание людей определенных представлений, привычек и поведенческих стереотипов;

5. Вызова недовольства или паники среди населения, а также провоцирования деструктивных действий различных социальных групп.

С появлением новых информационных технологий и организацией международного информационного обмена на новом уровне информационная составляющая в стратегии обеспечения информационной безопасности, (по оценкам Совета Безопасности РФ, руководителей российских спецслужб и Минобороны России), **вышла на первый план.**

2.2 Место информационной безопасности в системе национальной безопасности

ПОНЯТИЕ И СОВРЕМЕННАЯ СТРАТЕГИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Необходимым условием нормального существования и развития каждого общества является защищенность от внешних и внутренних угроз, устойчивость к попыткам внешнего давления, способность как парировать такие попытки и нейтрализовать возникающие угрозы, так и обеспечивать такие внутренние и внешние условия существования страны, которые гарантируют возможность стабильного и всестороннего прогресса общества и его граждан. **Для характеристики этого состояния используется понятие Национальной безопасности.**

Понятие национальной безопасности

"НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ" - состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства

Стратегия национальной безопасности РФ

Стратегия национальной безопасности Российской Федерации (до 2020 года) - официально признанная система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу.

Стратегия национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента РФ от 12 мая 2009 г. N 537)

Стратегия является базовым документом по планированию развития системы обеспечения национальной безопасности РФ, в котором излагаются порядок действий и меры по обеспечению национальной безопасности.

Основными направлениями обеспечения национальной безопасности РФ являются *стратегические национальные приоритеты*, которыми определяются задачи важнейших социальных, политических и экономических преобразований для создания безопасных условий реализации конституционных прав и свобод граждан РФ, осуществления устойчивого развития страны, сохранения территориальной целостности и суверенитета государства.

2.2 Место информационной безопасности в системе национальной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РФ

"система обеспечения национальной безопасности" - силы и средства обеспечения национальной безопасности.

Сферы обеспечения национальной безопасности

(в соответствии со Стратегией национальной безопасности РФ)

Система документов стратегического планирования
Федеральные (ведомственные) целевые программы, государственный оборонный заказ, концепции, доктрины и основы государственной политики в сферах обеспечения национальной безопасности и по отдельным направлениям внутренней и внешней политики государства) формируется Правительством РФ и заинтересованными федеральными органами исполнительной власти на основании Конституции РФ, федеральных законов и иных нормативных правовых актов РФ.

Основными приоритетами национальной безопасности Российской Федерации являются национальная оборона, государственная и общественная безопасность.

- Внутриполитическая сфера
- Экономическая сфера
- Социальная сфера
- Сфера науки и образования
- Международная сфера
- Информационная сфера
- Экологическая сфера
- Военная сфера
- Сфера общественной безопасности
- Оборонно-промышленная сфера
- Духовная сфера

Государственная политика РФ в области НБ обеспечивается согласованными действиями всех элементов системы обеспечения НБ при координирующей роли Совета Безопасности РФ за счет реализации комплекса мер организационного, нормативно-правового и информационного характера.

Информационная безопасность

Информационная безопасность является одним из видов обеспечения национальной безопасности

Доктрина информационной безопасности

2.2 Место информационной безопасности в системе национальной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РФ

Место ИБ в системе НБ определяется важностью объектов обеспечения ИБ, угроз объектам ИБ и её влиянием на состояние национальной безопасности.

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ, поскольку объекты ИБ находятся во всех сферах жизнедеятельности.

Национальная безопасность РФ существенным образом зависит от обеспечения ИБ, и в ходе технического прогресса эта зависимость будет возрастать.

Наиболее важными мерами являются:

1. **Создание Межведомственной комиссии Совета Безопасности РФ по ИБ (1997г);**
2. **Разработка и принятие Доктрины информационной безопасности РФ (2000г);**
3. **Создание (1995г.,). и совершенствование системы подготовки кадров в области ИБ**
4. **Создание системы защиты государственной тайны, системы ПДТР и ТЗИ и других систем;**
5. **Разработка концепции правового обеспечения информационной безопасности.**
6. **Разработка и реализация мер по противодействию информационному оружию и информационной войне.**

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ СОДЕРЖИТ

Доктрина информационной безопасности РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ. Доктрина информационной безопасности РФ принята в 2000 году и утверждена Президентом РФ.

Доктрина ИБ РФ содержит

- Национальные интересы РФ в информационной сфере, виды и источники угроз ИБ РФ
- Методы обеспечения информационной безопасности
- Основные положения государственной политики
- Организационную основу и функции системы обеспечения ИБ РФ

2.2 Значение информационной безопасности для субъектов информационных отношений

ИНФОРМАЦИОННЫЕ ПРАВООТНОШЕНИЯ

Информационные отношения – это отношения, возникающие между субъектами в информационной сфере. Информационные отношения, регулируемые правом – информационные правоотношения. Нормы права, регулирующие информационные правоотношения содержаться в Федеральных законах России, основным из которых является Федеральный закон «Об информации, информационных технологиях и о защите информации».

***Правоотношение* - обусловленное правовой нормой отношение между субъектами, которые имеют субъективные права и юридические обязанности.**

Структура информационного правоотношения

субъекты - носители права и обязанностей	**субъективные права и юридические обязанности,** определяющие содержание правоотношения	**объекты права**
Обладатели информации - гражданин (физическое лицо), - юридическое лицо, - Российская Федерация, - субъект Российской Федерации, -муниципальное образование. От имени РФ, субъекта РФ, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления	**Субъективные права** определяют возможность субъекта права действовать дозволенным образом и требовать определенного поведения от других субъектов (лиц) в связи с реализацией данного права. **Юридические обязанности** однозначны по их содержанию, императивны, непререкаемы, обеспечены юридическими механизмами, а также правом требования со стороны другого лица исполнения обязанности (право притязания).	- Информация - Информационные ресурсы - Информационные технологии (ИТ) - Информационные системы (ИС) - Информационно-телекоммуникационные сети (ИТКС) - другие

Информационные отношения – это отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации.

2.2 Значение информационной безопасности для субъектов информационных отношений

ЗНАЧЕНИЕ ИБ ДЛЯ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

Значение информационной безопасности для субъектов информационных отношений связано с реализацией их прав и выполнения обязанностей в рамках информационных правоотношений:

С правами:

1) с правом собственности на ИР, ИТ, ИС, ИТКС, включением их в состав имущества и использованием в качестве товара (в соответствии с Гражданским кодексом РФ);

2) с правом (информационными правами определёнными в Конституции РФ и информационном законодательстве):

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
2) использовать информацию, в том числе распространять ее, по своему усмотрению;
3) передавать информацию другим лицам по договору или на ином установленном законом основании;
4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

3) с реализацией права на доступ к информации;

С обязанностями

1) с выполнением обязанностей при осуществлении своих информационных прав:

1) соблюдать права и законные интересы иных субъектов права (лиц);
2) принимать меры по защите информации;
3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

2) с соблюдением конфиденциальности информации ограниченного доступа;

3) с обеспечением защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

2.2 Значение информационной безопасности для субъектов информационных отношений

ОСОБЕННОСТИ ПРАВ СОБСТВЕННОСТИ НА ИНФОРМАЦИЮ (ИР)

Отношения по поводу права собственности на ИР регулируются гражданским законодательством РФ, и имеют ряд особенностей:

1. ИР являются объектами отношений физических, юридических лиц, государства, составляют ИР России и защищаются законом наряду с другими ресурсами.
2. ИР могут быть товаром, за исключением случаев, предусмотренных законодательством РФ.
3. Право собственности на средства обработки информации не создает права собственности на ИР, принадлежащие другим собственникам.
4. ИР, являющиеся собственностью организаций, включаются в состав их имущества в соответствии с гражданским законодательством РФ.
5. ИР, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.
6. ИР могут быть и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений.
7. На ИР распространяется право интеллектуальной собственности.
7. На ИС, ИТ, ИТКС распространяются право «вещной» собственности – имущественные права, а на содержащиеся в их составе объекты интеллектуальной собственности – право интеллектуальной собственности в т.ч. авторские права..

11

2.3 Значение информационной безопасности для субъектов информационных отношений

1. Информационные технологии –
процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных Федеральным законом «Об информации... .»;

2) развитие ИС различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в РФ ИТКС, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей.

2. Информационная система –
совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Право собственности на информационные системы принадлежит субъекту решением и на средства которого они созданы.
1) государственные ИС (федеральные и региональные - собственник государство)
2) **муниципальные ИС**, созданные на основании решения органа местного самоуправления (собственники - муниципальные органы);
3) **иные информационные системы** (собственники юридические и физические лица).
Субъекты, осуществляющие эксплуатацию ИС, являются операторами.

12

2.3 Значение информационной безопасности для субъектов информационных отношений

3. Информационно-телекоммуникационная сеть
- технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием СВТ

Использование информационно-телекоммуникационных сетей

1. На территории РФ использование ИТКС осуществляется с соблюдением требований законодательства РФ в области связи, Федерального закона «Об информации ..» и иных нормативных правовых актов РФ.

2. Регулирование использования ИТКС, доступ к которым не ограничен определенным кругом лиц, осуществляется в РФ с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области (Интернет). Порядок использования иных ИТКС определяется владельцами таких сетей с учетом требований, установленных Федеральным законом «Об информации».

3. Использование ИТКС в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений этой деятельности.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности.

5. Передача информации посредством использования ИТКС осуществляется без ограничений. Ограничения могут быть установлены только законом.

6. Особенности подключения государственных ИС к ИТКС могут быть установлены нормативным правовым актом Президента или Правительства РФ.

13

Тема №3
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВОПРОСЫ

3.1 КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИБ РФ И ОСНОВНЫЕ ПОНЯТИЯ

3.2 ОБЪЕКТЫ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

3.3 ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

3.4 СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Литература

1. Методические рекомендации к курсу.
2. **Доктрина информационной безопасности РФ.**

1

3.1 Концептуальная модель ИБ РФ и основные понятия

ПОНЯТИЕ И КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИБ РФ

Теоретические основы информационной безопасности Российской Федерации, призваны в форме научного знания, дать целостное представление об объектах и субъектах обеспечения информационной безопасности, угрозах этим объектам и интересам Российской Федерации, политике и системе обеспечения информационной безопасности, о принципах, закономерностях и существенных связях между ними.

Под информационной безопасностью РФ следует понимать состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства от внутренних и внешних угроз способных нанести ущерб этим интересам.

ГОСУДАРСТВО – основной субъект обеспечения ИБ РФ

Осуществление деятельности по обеспечению ИБ РФ возложено на государство, которое в соответствии с законодательством является основным субъектом обеспечения безопасности.

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ РФ отражается в специальном нормативно-методическом документе, утверждаемом Президентом РФ - *доктрине* информационной безопасности Российской Федерации.

Кроме этого вопросы обеспечения информационной безопасности отражаются в документах раскрывающих стратегию и обеспечение национальной безопасности, программы информатизации, развития информационной и информационно-телекоммуникационной инфраструктуры и построения информационного общества в РФ.

1. Доктрина информационной безопасности РФ
2. Стратегия развития информационного общества в РФ
3. Стратегия национальной безопасности

Определяют содержание компонентов ИБ РФ

Концептуальная модель информационной безопасности Российской Федерации

Информационная безопасность Российской Федерации

К О М П О Н Е Н Т Ы

Объекты ИБ РФ	**Угрозы объектам ИБ РФ**	**Государственная политика обеспечения ИБ РФ**	**Система обеспечения ИБ РФ**

3.2 Объекты и угрозы информационной безопасности России

ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

Основными объектами обеспечения информационной безопасности Российской Федерации являются ее национальные интересы в информационной сфере

В соответствии с Доктриной ИБ РФ национальные интересы в информационной сфере включают следующие основные составляющие

Объектами обеспечения ИБ являются (группы объектов)

1. **Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею,** обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны

2. **Информационное обеспечение государственной политики Российской Федерации**

3. **Развитие современных ИТ, отечественной индустрии информации,** обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок; обеспечение накопления, сохранности и эффективного использования отечественных ИР

4. **Защита национальных информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных (ИС) и телекоммуникационных систем (ИТКС)**

1. **Интересы в области информационных прав и свобод**
   - правовой статус субъектов информационной сферы РФ (совокупность реальных прав и обязанностей субъектов).

2. **Информация в форме сведений и сообщений (ИР)** в ИС, ИТКС и др. ТСОИ

3. **Объекты информационной инфраструктуры РФ** (ИТ, ИС, ИТКС, помещения)

3

3.2 Объекты и угрозы информационной безопасности России

ГРУППЫ ОБЪЕКТОВ	НЕПОСРЕДСТВЕННЫЕ ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИБ РФ
1. Интересы в области информационных прав и свобод	**- информационные права и свободы человека и гражданина** закреплённые в Конституции и информационном законодательстве **- достоинство личности, свобода совести, свобода мысли и слова**, а также свобода лит., худ., научного, технического и других видов творчества, преподавания; **- свобода массовой информации;** **- неприкосновенность частной жизни, личная и семейная тайна.**
2. Информация в форме сведений и сообщений (ИР) в ИС, ИТКС и др.ТСОИ	**- общедоступные ИР в ИС** федеральных органов исполнительной власти и СМИ; **- ИР государственных органов, предприятий оборонного комплекса, правоохранительных органов, содержащие информацию ограниченного доступа** (сведения, отнесенные к государственной тайне, и конфиденциальную информацию); **- результаты фундаментальных, поисковых и прикладных научных исследований,** потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу РФ; **- незапатентованные изобретения, промышленные образцы, полезные модели** и экспериментальное оборудование (объекты интеллектуальной собственности) ;
3. Объекты информационной инфраструктуры РФ (ИТ, ИС, ИТКС, помещения)	**- ИС и ИТКС (их информативные физические поля)** обеспечения нужд государственного управления, обороны страны, национальной безопасности и правопорядка; **- ИС и ИТКС ключевых объектов инфраструктуры РФ** , в том числе критических важных объектов, и объектов повышенной опасности; **- корпоративные и индивидуальные ИС и ИТКС**; **- ИТ и ИТТ, АСУ, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу ИОД**, их информативные физические поля; **- помещения, предназначенные для ведения закрытых переговоров**, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа;

ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

I. ВИДЫ УГРОЗ ИБ РФ ОБЩЕЙ НАПРАВЛЕННОСТИ

1. **Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности**
2. Угрозы информационному обеспечению государственной политики РФ
3. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи
4. **Угрозы безопасности информационных и телекоммуникационных средств и систем,** как уже развернутых, так и создаваемых на территории России.

УГРОЗЫ КОНСТИТУЦИОННЫМ ПРАВАМ И СВОБОДАМ ЧЕЛОВЕКА И ГРАЖДАНИНА В ОБЛАСТИ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ	
1	**Принятие органами государственной власти, нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области и информационной деятельности;**
3	**Противодействие в реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;**
4	**Нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;**

5

3.2 Объекты и угрозы информационной безопасности России

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СРЕДСТВ И СИСТЕМ	
1	**Противоправные сбор и использование информации;**
2	**Нарушения технологии обработки информации;**
3	**Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;**
4	**Разработка и распространение программ, нарушающих нормальное функционирование ИС ИТКС, в том числе систем защиты информации (Программные вирусы и закладки);**
5	**Уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;**
6	**Воздействие на парольно - ключевые системы защиты АС обработки и передачи информации;**
7	**Компрометация ключей и средств криптографической защиты информации;**
8	**Утечка информации по техническим каналам**;
9	**Внедрение электронных устройств для перехвата информации в технические средства** обработки, хранения и передачи информации по каналам связи, **а также в служебные помещения** органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
10	**Уничтожение, повреждение, разрушение** или **хищение** машинных и других **носителей информации**;
11	**Перехват информации в сетях** передачи данных и на линиях связи, дешифрование этой информации и **навязывание ложной информации**;
12	**Использование несертифицированных** отечественных и зарубежных **информационных технологий, средств защиты информации**, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
13	**Несанкционированный доступ к информации**, находящейся в банках и базах данных;
14	**Нарушение законных ограничений на распространение информации** (разглашение, шпионаж).

6

3.2 Объекты и угрозы информационной безопасности России

ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

К внешним источникам относятся:
• **Деятельность иностранных разведывательных и информационных структур**, направленная против интересов РФ в информационной сфере;
• **деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки** иностранных государств;
• **Разработка рядом государств концепций информационных войн**, предусматривающих создание средств опасного воздействия на ИС и ТКС, сохранности ИР, получение несанкционированного доступа к ним.
• Стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информ -ных рынков;
• Технологический отрыв ведущих держав мира в области ИТ, обострение международной конкуренции за обладание ИТ и ресурсами;
• Деятельность международных террористических организаций;
К внутренним источникам относятся:
• Слабое развитие отечественных отраслей промышленности?;
• Неблагоприятная криминогенная обстановка, снижение степени защищенности законных интересов граждан, общества и государства в информационной сфере;
• Недостаточная координация деятельности органов государственной власти по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;
• **Недостаточная разработанность нормативной правовой базы**, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
• Неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
• **Отставание России от ведущих стран мира по уровню информатизации всех сфер деятельности**

3.3 Политика обеспечения информационной безопасности Российской Федерации

ПРИНЦИПЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИБ РФ

1	**Соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению ИБ РФ;**
2	**Открытость в реализации функций федеральных органов государственной власти**, органов государственной власти субъектов РФ и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;
3	**Правовое равенство всех участников процесса информационного взаимодействия** вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
4	**Приоритетное развитие отечественных современных информационных и телекоммуникационных технологий**, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

3.3 Политика обеспечения информационной безопасности Российской Федерации

ФУНКЦИИ ГОСУДАРСТВА ПО ОБЕСПЕЧЕНИЮ ИБ РФ	
1	**Проводит объективный и всесторонний анализ и прогнозирование угроз ИБ РФ, разрабатывает меры по ее обеспечению;**
2	**Организует работу законодательных (представительных) и исполнительных органов государственной власти РФ** по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз ИБ РФ;
3	**Поддерживает деятельность общественных объединений**, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
4	**Осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;**
5	**Проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ**
6	**Способствует предоставлению физическим и юридическим лицам доступа** к мировым информационным ресурсам, **глобальным информационным сетям**;
7	**Организует разработку федеральной программы обеспечения ИБ РФ**, объединяющей усилия государственных и негосударственных организаций в данной области;
8	**Способствует интернационализации глобальных информационных сетей и систем**, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.
9	**Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области ИБ РФ!!!**

9

3.4 Система обеспечения ИБ РФ

СИСТЕМА ОБЕСПЕЧЕНИЯ ИБ РФ (СОСТАВ)

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИБ РФ

Органы законодательной, исполнительной, судебной власти

1. Законы РФ и международные договоры. 2. Подзаконные акты: Президента РФ, Правительства РФ

МВК Совета Безопасности РФ в области ИБ

Координирует деятельность органов и сил по обеспечению ИБ

ОРГАНИЗАЦИОННАЯ ОСНОВА СОИБ РФ

Организационное обеспечение ИБ РФ

Президент РФ, Правительство РФ, Совет федерации, Госдума, Совет безопасности, МВК,
Органы исполнительной, судебной власти, Общественные объединения, граждане,

СИСТЕМА ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ (СЗИ ГТ)

Органы защиты ГТ: 1. МВК ЗГТ, 2.ФСБ РФ, 3. СВР РФ, 4. МО РФ, 5. Организации и их подразд-я по защите ГТ
(МВК по защите ГТ) – координирует деятельность

ГОСУДАРСТВЕННАЯ СИСТЕМА ПДТР и ТЗИ (противодействия техн-ким разведкам и технической защиты информации)

Организует ФСТЭК России

СИСТЕМА ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИБ

Организует Минобрнауки

СИСТЕМА ЗАЩИТЫ ИНТЕЛ-ЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ФОИВИС (Роспатент)

СИСТЕМЫ ЛИЦЕНЗИРОВАНИЯ (3 системы)

1. В области защиты гостайны
2. В области защиты конфид-й информации
3. В области криптографической защиты информации

СИСТЕМЫ СЕРТИФИКАЦИИ СрЗИ (3 системы сертификации)

1. По требованиям безопасности информации
2. Криптографических средств защиты
3. Средств защиты ГТ (СЗИ-ГТ)

СИСТЕМА ЭКСПОРТНОГО КОНТРОЛЯ

ФСТЭК России

СИСТЕМА ЗАЩИТЫ информационных прав субъектов и противодействия преступлениям в информационной сфере

Органы судебной власти, Общественная палата
Уполномоченные по правам человека
Прокуратура, МВД России (Управление К)

10

3.4 Система обеспечения ИБ РФ

ОСНОВНЫЕ ФУНКЦИИ СОИБ РФ:	
1	**Разработка и совершенствование нормативной правовой базы в области обеспечения ИБ РФ;**
2	**Создание условий для реализации прав граждан и общественных объединений в информационной сфере,** определение и поддержание баланса между потребностью субъектов в свободном обмене информацией и необходимыми ограничениями на её распространение;
4	**Оценка состояния, источников угроз ИБ РФ, определение приоритетных направлений противодействия этим угрозам** (предотвращения, отражения и нейтрализации этих угроз);
4	**Координация и контроль деятельности органов, решающих задачи обеспечения ИБ РФ (**федеральных органов государственной власти и других государственных органов)
5	**Защита государственных ИР**, (прежде всего в федеральных органах государственной власти и органах государственной власти субъектов РФ, на предприятиях оборонного комплекса);
6	**Предупреждение, выявление и пресечение правонарушений, в информационной сфере, осуществление судопроизводства по делам о преступлениях в этой области;**
7	**Совершенствование системы подготовки кадров, используемых в области ИБ РФ**;
8	**Обеспечение контроля за созданием и использованием СрЗИ посредством обязательного лицензирования деятельности в данной сфере и сертификации СрЗИ;**
9	**Организация разработки федеральной и региональных программ,** фундаментальных и прикладных научных исследований, проведение единой технической политики **обеспечения ИБ и координация деятельности по их реализации**
10	**Осуществление международного сотрудничества в области обеспечения ИБ**, представление интересов РФ в соответствующих международных организациях.

3.4 Система обеспечения ИБ РФ

Правовое обеспечение ИБ РФ

Правовое обеспечение информационной безопасности является самостоятельным комплексным направлением правового регулирования отношений в области проявления угроз объектам информационной безопасности и противодействия эти угрозам на основе норм и институтов различных отраслей права (конституционного, гражданского, уголовного, и информационного).

Система правового обеспечения ИБ РФ. Включает отдельные нормативные правовые акты, специально предназначенные для регулирования отношений в области обеспечения информационной безопасности, и отдельные нормы в этой области, содержащиеся в нормативных правовых актах различных отраслей законодательства. К нормативным правовым актам относятся:
- федеральные законы РФ и законы субъектов РФ, в том числе технические регламенты;
- Указы Президента РФ;
- Постановления Правительства РФ;
- нормативные правовые акты федеральных органов исполнительной власти уполномоченных осуществлять правовое регулирование в области информационной безопасности и защиты информации.

Правовое обеспечение создаёт правовую основу для функционирования всех других систем в области ИБ и управления ими со стороны Президента РФ и Правительства РФ.

3.4 Система обеспечения ИБ РФ

Организационная основа СОИБ

Правовое обеспечение информационной безопасности является самостоятельным комплексным направлением правового регулирования отношений в области проявления угроз объектам информационной безопасности и противодействия эти угрозам на основе норм и институтов различных отраслей права (конституционного, гражданского, уголовного, и информационного).

Система правового обеспечения ИБ РФ. Включает отдельные нормативные правовые акты, специально предназначенные для регулирования отношений в области обеспечения информационной безопасности, и отдельные нормы в этой области, содержащиеся в нормативных правовых актах различных отраслей законодательства. К нормативным правовым актам относятся:
- федеральные законы РФ и законы субъектов РФ, в том числе технические регламенты;
- Указы Президента РФ;
- Постановления Правительства РФ;
- нормативные правовые акты федеральных органов исполнительной власти уполномоченных осуществлять правовое регулирование в области информационной безопасности и защиты информации.

Правовое обеспечение создаёт правовую основу для функционирования всех других систем в области ИБ и управления ими со стороны Президента РФ и Правительства РФ.

13

3.4 Система обеспечения ИБ РФ

Система защиты государственной тайны

Система защиты государственной тайны - *совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях.* Вся деятельность по защите государственной тайны в России осуществляется в соответствии с законом РФ «О государственной тайне».

Коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства Российской Федерации о государственной тайне, является Межведомственная комиссия по защите государственной тайны. Руководство деятельностью Межведомственной комиссии осуществляет Президент Российской Федерации.

Государственная система противодействия техническим разведкам (ПДТР) и технической защиты информации (ТЗИ).

Государственная система противодействия техническим разведкам (ПДТР) и технической защиты информации (ТЗИ). Организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой возложено законодательством РФ на Федеральную службу по техническому и экспортному контролю (до 2004 года именовалась – Гостехкомиссия России).

14

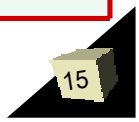
3.4 Система обеспечения ИБ РФ

Система подготовки кадров в области информационной безопасности.

Система подготовки кадров в области информационной безопасности. Она включает:
- учреждения высшего и среднего профессионального образования, ведущие подготовку по направлению Информационная безопасность с уровнем подготовки: техник, бакалавр, специалист, магистр;
- государственные образовательные стандарты высшего (ГОС ВПО) и среднего специального образования в области информационной безопасности;
- научную специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность», для подготовки кадров высшей квалификации (кандидат наук, доктор наук), включающей физико-математические науки, технические науки, юридические науки;
- учебно – методическое объединение (УМО) вузов по образованию в области информационной безопасности и учебно-методический совет (в структуре УМО в области истории и архивоведения).
- курсы переподготовки и повышения квалификации в этой области, действующие на базе вузов и центров информационной безопасности.

Система защиты интеллектуальной собственности

Система защиты интеллектуальной собственности. Образуется совокупностью:
- законодательства РФ в области интеллектуальной собственности, основу которого составляет часть IV Гражданского кодекса РФ;
- федерального органа исполнительной власти уполномоченного в области интеллектуальной собственности (Роспатент);
- органами МВД, осуществляющими борьбу с нарушениями в области интеллектуальной собственности;
- общественными организациями в области коллективного управления авторскими правами (Российское авторское общество и др.).



3.4 Система обеспечения ИБ РФ

Система защиты информационных прав субъектов и противодействия преступлениям в информационной сфере.

Система защиты информационных прав субъектов **и противодействия преступлениям в информационной сфере.** Эта система включает:
- нормы Конституции РФ и нормы федеральных законов, содержащие информационные права;
- суды различных инстанций, органы прокуратуры, осуществляющие защиту информационных прав граждан, общественных организаций;
- общественные институты (общественная палата при Президенте РФ) и специальные институты по правам человека (уполномоченные по правам человека) и др.;
- специальные органы в системе МВД России (Управление «К») по борьбе с преступлениями в сфере высоких технологий.

Система экспортного контроля

Система экспортного контроля. Руководство указанной государственной системой возложено законодательством РФ на Федеральную службу по техническому и экспортному контролю

Система научно-исследовательских институтов (НИИ), научных и научно-исследовательских центров в области ИБ

Система научно-исследовательских институтов (НИИ), научных и научно-исследовательских центров в области ИБ предназначена для осуществления фундаментальных и прикладных научных исследований в области обеспечения ИБ РФ. Она включает:
- специализированные в области ИБ научно-исследовательские институты при Академии наук РФ, вузах, ведомствах и ведомственных вузах (ФСБ России, ФСТЭК России);
- специализированные научные и научно – исследовательские центры в области ИБ, как при государственных учреждениях и органах государственной власти, так и негосударственных;
- учебно-научные центры при ведущих вузах России.

3.4 Система обеспечения ИБ РФ

Системы лицензирования по видам деятельности в области ИБ.

Системы лицензирования по видам деятельности в области ИБ. Для регламентации деятельности в области информационной безопасности в России функционируют три системы лицензирования:

- система лицензирования в области защиты государственной тайны (регламентируется законодательством «О государственной тайне»);
- система лицензирования в области защиты конфиденциальной информации (регламентируется законом «О лицензировании отдельных видов деятельности» и нормативными актами Правительства РФ);
- система лицензирования в области криптографической защиты информации (регламентируется законом «О лицензировании отдельных видов деятельности» и нормативными актами Правительства РФ).

Каждая из систем имеет сеть аккредитованных лицензионных центров в субъектах РФ. Виды деятельности и условия лицензирования по ним в рамках каждой системы определены нормативными актами Правительства РФ.

Системы сертификации средств обеспечения ИБ

Системы сертификации средств обеспечения ИБ. Сертификация средств защиты информации осуществляется в целях подтверждения их соответствия требованиям технических регламентов, стандартов, специальных нормативных документов в области ИБ. К сертификации относится также аттестация объектов информатизации по требованиям безопасности информации. Она проводится в соответствии с нормами Федерального закона «О техническом регулировании».

Системы сертификации:

1.Система сертификации средств защиты информации по требованиям безопасности информации РОСС RU. 0001. 01БИ00;

2. Система сертификации средств криптографической защиты информации РОСС.RU.0001.030001;

3. Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (СЗИ-ГТ).

Тема №4
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ВОПРОСЫ

3.1 КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИБ ОРГАНИЗАЦИИ И ОСНОВНЫЕ ПОНЯТИЯ

3.2 ОБЪЕКТЫ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

3.3 ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

3.4 СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Литература

1

3.1 Концептуальная модель ИБ РФ и основные понятия

ПОНЯТИЕ И КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИБ ОРГАНИЗАЦИИ

Теоретические основы информационной безопасности организации, призваны в форме научного знания, дать целостное представление об объектах информационной безопасности организации, угрозах этим объектам и интересам субъектов, политике и системе обеспечения информационной безопасности организации, их закономерностях и существенных связях между собой и окружающей средой.

В качестве такой формы научных знаний, основанных на практическом опыте следует считать международные стандарты в области информационной безопасности, принятые в России на уровне национальных. Их необходимо рассматривать как основные источники теории ИБ организации:

- **Стандарты одна из форм накопления знаний;**
- **В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами**

ГОСТ Р ИСО/МЭК 27001 -2006 Национальный стандарт РФ. Информационная технология. Методы и средства обеспечения безопасности. **Системы менеджмента ИБ**. Требования.

ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. **Практические правила управления информационной безопасностью**

ГОСТ Р ИСО/МЭК 13335 Национальный стандарт РФ. Информационная технология. Методы и средства обеспечения безопасности. Части 1-5.(2006-2007)

ГОСТ Р ИСО/МЭК 15408-2008 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. **Критерии оценки безопасности информационных технологий**. Части 1-3.

Стандарты предназначены для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями) и содержат концепции и модели по менеджменту ИБ, руководства по управлению безопасностью ИТ и ИТТ на которых основаны бизнес-процессы организации, методы управления рисками в этой области, меры организационного, технического характера по обеспечению безопасности ИТ (ИТТ), меры физической защиты и

2

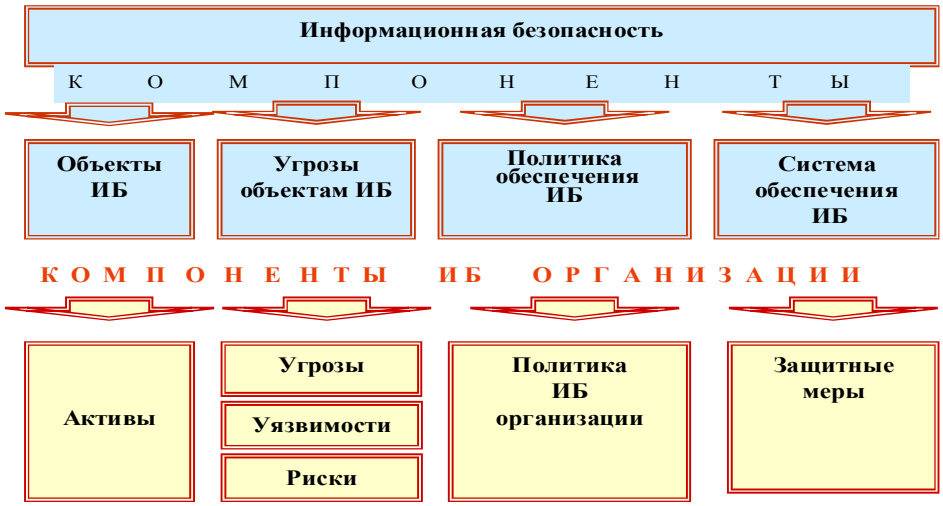
3.1 Концептуальная модель ИБ РФ и основные понятия

ПОНЯТИЕ И КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИБ ОРГАНИЗАЦИИ

Информационная безопасность организации - это состояние защищённости объектов (активов) организации, при котором обеспечивается конфиденциальность, целостность, доступность информации.

Проблемы ИБ организации могут включать в себя потерю:
- **Конфиденциальности;**
- **целостности;**
- **доступности ;**
- **подотчетности;**
- **аутентичности;**
- **Достоверности информации или средств её обработки**

Концептуальная модель информационной безопасности организации



3.1 Концептуальная модель ИБ РФ и основные понятия

ПОНЯТИЕ ИБ ОРГАНИЗАЦИИ

С позиции управления информационной безопасностью организации *информационная безопасность* определяется, как *свойство информации сохранять конфиденциальность, целостность и доступность.*

С позиции безопасности ИТ (ИТТ), на которых основаны бизнес-процессы организации

информационная безопасность
- это все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

3.2 Объекты и угрозы информационной безопасности организации

ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИБ ОРГАНИЗАЦИИ

Основными объектами обеспечения информационной безопасности организации являются ее активы

***Активы (А)* - все, что имеет ценность для организации**

1. Информация /данные:

а) информация в форме сведений (сведения об участниках организации, о состоянии рынка, престиж (имидж) организации и доброе имя участников организации и т.п.);

б) информация в форме сообщений (документы, закрепляющие права собственников организации на материальные и нематериальные активы, документация бухгалтерского учёта, налоговые декларации, договоры на выполнение работ и оказание услуг, документация на выпускаемые изделия и.т.п.);

в) информация (данные) в форме электронных документов (информационные ресурсы в составе ИС);

2. Объекты информационной инфраструктуры

- **ИС и ИТКС (их информативные физические поля)** обеспечивающие бизнес-процессы организации ;
- **ИТ и ИТТ, АСУ, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации**, их информативные физические поля;
- **помещения, предназначенные для ведения закрытых переговоров**, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа;

3. Интересы организации

а) правовой статус организации как объекта информационной сферы – юридического лица (права на объекты интеллектуальной собственности, на коммерческую тайну, на выполнение работ и оказание услуг, на доступ к общедоступной информации государственных органов, и т.п., а также обязанности по предоставлению в уполномоченные государственные органы сведений о результатах экономической деятельности, по предоставлению заинтересованным лицам документов в случае направления заявки на участие в конкурсах и аукционах и т.п.,)

б) персонал организации (его интересы по соблюдению режима персональных данных, права на объекты интеллектуальной собственности и на доступ к информации и т.п.);

4. Продукция и услуги

а). продукция организации;

б) услуги (например, информационные, вычислительные услуги);

в) конфиденциальность и доверие при оказании услуг (например, услуг по совершению платежей);

3.2 Объекты и угрозы информационной безопасности организации

УГРОЗЫ ОБЪЕКТАМ ОБЕСПЕЧЕНИЯ ИБ ОРГАНИЗАЦИИ

С понятием угрозы неразрывно связаны понятия: инцидент информационной безопасности, уязвимость, риск:

Угроза (Т)

потенциальная причина инцидента, который может нанести ущерб системе или организации

Угрозы обладают следующими характеристиками, устанавливающими их взаимосвязь с другими компонентами безопасности:
- источник, внутренний или внешний;
- мотивация, например финансовая выгода, конкурентное преимущество;
- частота возникновения; - правдоподобие; - вредоносное воздействие.

Примеры угроз: целенаправленные угрозы, обусловленные человеческим фактором: подслушивание/перехват, модификация информации, атака хакера на систему, злонамеренный код (вирус), хищение информации или носителя информации.
При оценке уровень угрозы в зависимости от результата ее воздействия может быть определен как высокий, средний или низкий.

инцидент информационной безопасности (I)

- любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

Результатом воздействия могут стать разрушение конкретного актива, повреждение ИТТ, нарушение их конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности. Непрямое воздействие может включать в себя финансовые потери, потерю доли рынка или репутации.

Уязвимость (V)

- слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами;

Связанные с активами уязвимости включают в себя слабости физического носителя, организации, процедур, персонала, управления, администрирования, аппаратного/программного обеспечения или информации. Угрозы могут использовать уязвимости для нанесения ущерба ИТТ или целям бизнеса. Уязвимость может существовать и в отсутствие угрозы. При оценке уровень уязвимости может быть определен как высокий, средний или низкий

Риск (R)
*= (V) *(T)*

- потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов.

Обработка риска включает в себя устранение, снижение, перенос и принятие риска.

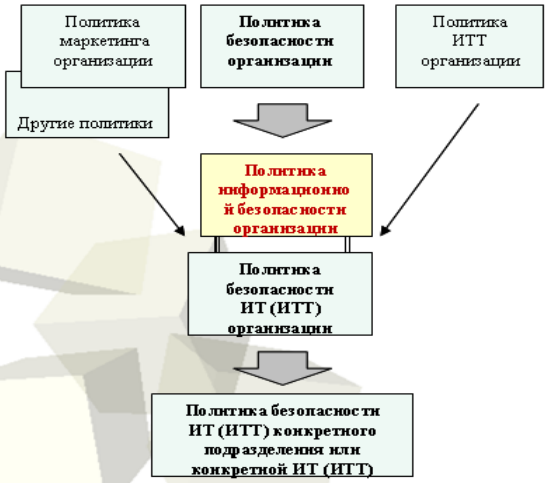
3.2 Политика обеспечения информационной безопасности организации

Политика ИБ организации **– это правила и процедуры (методы), которые следует соблюдать для достижения целей обеспечения информационной безопасности.**

Цель**: Обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами.**

В пределах организации соблюдается иерархия политик безопасности (рис.4.2) от бизнес - политики организации в целом до политики безопасности конкретной ИТ (ИТТ) на которой основаны бизнес процессы.

Иерархия политик безопасности в организации



Политика ИБ организации может состоять из принципов безопасности и директив для организации в целом. Политика безопасности организации должна отражать более широкий круг аспектов политики организации, включая аспекты, которые касаются прав личности, законодательных требований и стандартов.
Должна быть оформлена документально.
Обеспечивает согласованность всех защитных мер.

Политика безопасности информационных (информационно – телекоммуникационных) технологий
- правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационных (информационно-телекоммуникационных) технологий управлять, защищать и распределять активы, в том числе критичную информацию.

Политика безопасности ИТ (ИТТ) должна формироваться, исходя из согласованных целей и стратегий безопасности ИТ (ИТТ) организации. Необходимо выработать и сохранять политику безопасности ИТ (ИТТ), соответствующую ***законодательству, требованиям регулирующих органов, политике в области бизнеса, безопасности и политике ИТ (ИТТ).***

7

4.4 Система обеспечения информационной безопасности организации

Система обеспечения информационной безопасности организации. В логике стандарта ГОСТ Р ИСО/МЭК 13335-2006 *система обеспечения информационной безопасности организации* может быть определена как *совокупность защитных мер направленных на исключение или снижение до приемлемого уровня рисков, связанных с угрозами конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки (ИТ и ИТТ).*

Защитная мера *(S)* - сложившаяся практика, процедура или механизм обработки риска.
Защитные меры - это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов.

СОИБ ОРГАНИЗАЦИИ

Система менеджмента информационной безопасности (СМИБ) организации

– это часть общей системы менеджмента организации, основанная на использовании методов оценки бизнес - рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.
ГОСТ Р ИСО/МЭК 27001-2006 Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2008-48с.

Система менеджмента безопасности ИТ и ИТТ	Субъекты обеспечения ИБ организации	Организационные защитные меры	Физические защитные меры	Специальные защитные меры (технического характера):
Подсистема СМИБ организации ГОСТ Р ИСО/МЭК 13335	**-советы по безопасности ИТ, -специализированные структурные подразделения по вопросам ИБ -(отделы ИБ) или должностные лица (администраторы безопасности), - а также структурные образования, специализирующиеся на оказании услуг в данной области**	*-Политика обеспечения безопасности ИТ организации -Проверка соответствия безопасности установленным требованиям -Обработка инцидента -Персонал -- эксплуатационные вопросы* **-ГОСТ Р ИСО/МЭК 13335**	(должны применяться к зданиям, зонам безопасности, местам размещения ЭВМ и офисным помещениям): **ГОСТ Р ИСО/МЭК 13335**	***-Идентификация и аутентификация -Логическое управление и аудит доступа -Защита от вирусов -Управление сетью - Криптография*** **ГОСТ Р ИСО/МЭК 13335, 15408**

9

4.4 Система обеспечения информационной безопасности организации

Организационные защитные меры. К ним относятся:

- *Политика обеспечения безопасности ИТ организации* (Политика обеспечения безопасности системы ИТ, управление безопасностью ИТ (учреждение комитета по безопасности ИТ и назначения лица (уполномоченного по безопасности ИТ), ответственного за безопасность каждой системы ИТ), Распределение ответственности и полномочий, Организация безопасности ИТ, Идентификация и определение стоимости активов, Одобрение систем ИТ);
- *Проверка соответствия безопасности установленным требованиям* (Соответствие политики обеспечения безопасности ИТ защитным мерам, Соответствие законодательным и обязательным требованиям);
- *Обработка инцидента* (Отчет об инциденте безопасности, Отчет о слабых местах при обеспечении безопасности, Отчет о нарушениях в работе программного обеспечения, Управление в случае возникновения инцидента);
- *Персонал* (обязанности, соглашение о конфиденциальности, обучение, дисциплина, ответственность);
- *эксплуатационные вопросы* (оборудование ИТ и связанных с ним систем) (управление резервами, документация, техобслуживание, Мониторинг изменений, записи аудита и регистрация, Тестирование безопасности, Управление носителями информации. Обеспечение стирания памяти, Распределение ответственности и полномочий Корректное использование программного обеспечения, Управление изменениями программного обеспечения
- *Планирование непрерывности бизнеса* (стратегия непрерывности бизнеса, план непрерывности бизнеса, проверка и актуализация плана непрерывности бизнеса, дублирование)

Физические защитные меры

(должны применяться к зданиям, зонам безопасности, местам размещения ЭВМ и офисным помещениям):

Материальная защита (защитные меры, применяемые для защиты здания, включают в себя заборы, управление физическим доступом (пропускные пункты), прочные стены, двери и окна);

Противопожарная защита (средства обнаружение огня и дыма, охранной сигнализации и подавления очага возгорания);

Защита от воды/других жидкостей *(*защита в случае возникновения угрозы затопления);

Защита от стихийных бедствий *(*защищены от удара молнии и оснащены защитой от грозового разряда);

Защита от хищения (идентификация и инвентаризация ресурсов, проверка охраной и администраторами носителей конфиденциальной информации, выносимого оборудования, (например, съемных и сменных дисках, флэш-накопителях, оптических дисках, гибких дисках и др.)).

Энергоснабжение и вентиляция (альтернативный источник энергоснабжения и бесперебойного питания, поддержание допустимой температуры и влажности);

Прокладка кабелей *(* защищены от перехвата информации, повреждения и перегрузки. Проложенные кабели должны быть защищены от случайного или преднамеренного повреждения).

10

4.4 Система обеспечения информационной безопасности организации

Специальные защитные меры (технического характера):

Идентификация и аутентификация (на основе некоторой информации, известной пользователю (пароли), на основе того, чем владеет пользователь (карточки (жетоны), смарт-карты с запоминающим устройством (ЗУ) или микропроцессором) и персонального идентификационного номера - PIN кода), на основе использования биометрических характеристик пользователя (отпечатки пальцев, геометрия ладони, сетчатка глаз, а также тембр голоса и личная подпись);

Логическое управление и аудит доступа *для:*

- ограничения доступа к информации, компьютерам, сетям, приложениям, системным ресурсам, файлам и программам;

- регистрации подробного описания ошибок и действий пользователя в следе аудита и при анализе записей для обнаружения и исправления нарушений при обеспечении безопасности. (Политика управления доступом, Управление доступом пользователя к ЭВМ, Управление доступом пользователя к данным, услугам и приложениям, Анализ и актуализация прав доступа, Контрольные журналы)

Защита от злонамеренных кодов: (*вирусы; черви; троянские кони (*Сканеры, Проверки целостности, Управление обращением съемных носителей, Процедуры организации по защитным мерам (руководящие указания для пользователей и администраторов)

Управление сетью (Операционные процедуры (документация операционных процедур и установление порядка действий для реагирования на значительные инциденты безопасности), Системное планирование, Конфигурация сети (документирование, межсетевая защита), Разделение сетей (физическое и логическое), Мониторинг сети, Обнаружение вторжения.

Криптография (математический способ преобразования данных для обеспечения безопасности - помогает обеспечивать конфиденциальность и/или целостность данных, неотказуемость) Защита конфиденциальности данных (с учётом законодательных и обязательных требований), Защита целостности данных (хэш-функции, цифровые подписи и/или другие), Неотказуемость, Аутентичность данных, Управление ключами (генерирование, регистрацию, сертификацию, распределение, установку, хранение, архивирование, отмену, извлечение и уничтожение ключей).

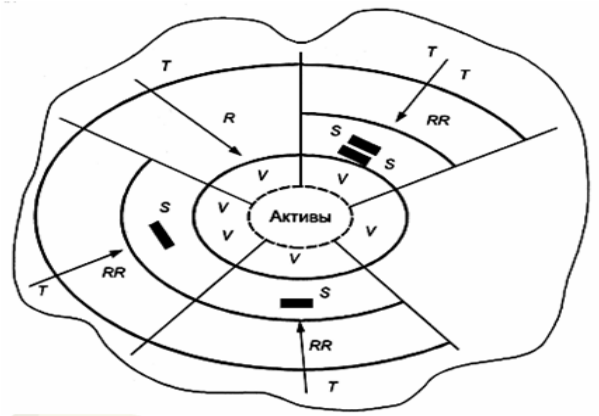
Порядок выбора защитных мер очень важен для правильного планирования и реализации программы информационной безопасности.

- согласно типу и характеристикам системы ИТ;
- согласно общим оценкам проблем и угроз безопасности;
- в соответствии с результатами детального анализа рисков.

11

4.5 Модель безопасности ИТ (ИТТ) организации

МОДЕЛЬ БЕЗОПАСНОСТИ ИТ (ИТТ) ОРГАНИЗАЦИИ



R - риск; RR - остаточный риск; S - защитная мера; T - угроза; V - уязвимость актива; N- сценарий.

Модель безопасности отображает:

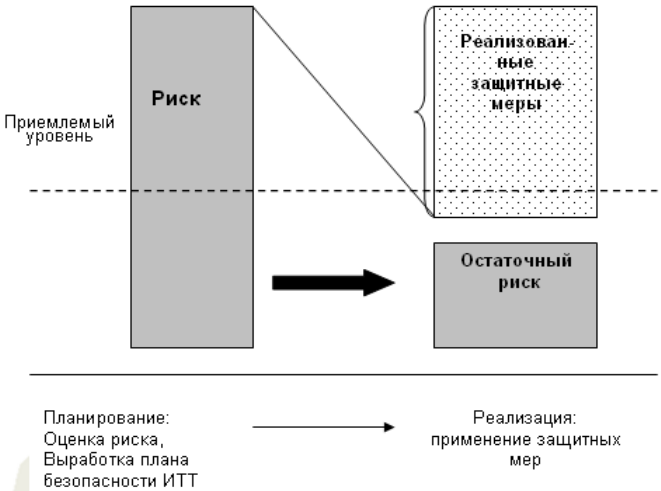
- окружающую среду, содержащую ограничения и угрозы, которые постоянно меняются и известны лишь частично;
- активы организации (A);
- уязвимости, присущие данным активам (V);
- меры для защиты активов (S);
- приемлемые для организации остаточные риски (RR);
- угрозы безопасности активам (T);
- возможные сценарии (N).

Сценарии	Описание сценария
№1	Защитная мера S может быть эффективна для снижения рисков R, связанных с угрозой T, способной использовать уязвимость актива V. Угроза может достичь цели, только если активы уязвимы для данной угрозы
№2	Защитная мера может быть эффективной для снижения риска, связанного с угрозой, использующей группу уязвимостей актива;
№3	Группа защитных мер может быть эффективна в снижении рисков, связанных с группой угроз, использующих уязвимость актива. Иногда требуется несколько защитных мер для снижения риска до приемлемого уровня для получения допустимого остаточного риска RR
№4	Риск считают приемлемым и никакие меры не реализуются даже в присутствии угроз и при наличии уязвимостей актива
№5	Существует уязвимость актива, но не известны угрозы, которые могли бы ее использовать.

12

4.5 Модель информационной безопасности организации

ВЗАИМОСВЯЗЬ ЗАЩИТНЫХ МЕР И РИСКА



Часто требуется применение нескольких защитных мер для снижения риска до приемлемого уровня. Если риск считается приемлемым, то реализация защитных мер не требуется.

Существуют следующие возможности снижения уровня риска:

- избегать риска;
- уступить риск (например, путем страховки);
- снизить уровень угроз;
- снизить степень уязвимости системы ИТ;
- снизить возможность воздействия нежелательных событий;
- отслеживать появление нежелательных событий, реагировать на их появление и устранять их последствия.

Выбор защитных мер должен всегда включать в себя комбинацию организационных (не технических) и технических мер защиты. В качестве организационных рассматриваются меры, обеспечивающие физическую, персональную и административную безопасность.

Для выбора соответствующих эффективных защитных мер организация должна исследовать и оценить проблемы безопасности, связанные с коммерческой деятельностью, которую обслуживает рассматриваемая система ИТ. После идентификации проблем безопасности и с учетом соответствующих угроз можно выбирать защитные меры

Проблемы безопасности могут включать в себя потерю:

- конфиденциальности;
- целостности;
- доступности;
- подотчетности;
- аутентичности;
- достоверности.

13

СТАНДАРТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2008-48с.

ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М.: Стандартинформ, 2007 -19с.

ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий. М.: Стандартинформ, 2007-46с.

ГОСТ Р ИСО/МЭК ТО 13335-4-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер. М.: Стандартинформ, 2007 -63с.

ГОСТ Р ИСО/МЭК ТО 13335-5-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. М.: Стандартинформ, 2007 -24с.

ГОСТ Р ИСО/МЭК ТО 18044-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М: Стандартинформ, 2009 -47с.

Раздел 2 Основы защиты информации

Тема 5

ПОНЯТИЕ, СУЩНОСТЬ И ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

Вопросы:

5.1 ОБЩИЙ КОНТЕКСТ ЗАЩИТЫ ИНФОРМАЦИИ

5.2 ПОНЯТИЕ И СУЩНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ КАК ВИДА ДЕЯТЕЛЬНОСТИ

5. 3 ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

5.4 КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .- Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Закон «Об информации, информационных технологиях и о защите информации.
3. Источники указанные в Методических рекомендациях к курсу.

1

ОБЩИЙ КОНТЕКСТ ЗАЩИТЫ ИНФОРМАЦИИ

1. В связи с тем, что информация является предметом собственности (государства, коллектива, отдельного лица (субъекта)), то неизбежно возникает проблема угрозы безопасности этой информации, заключающейся: в неконтролируемом ее распространении, в хищении, несанкционированном уничтожении, искажении, передаче, копировании, блокировании доступа к информации **т.е нарушении её основных свойств: конфиденциальности, целостности, доступности.**

Следовательно, **возникает проблема защиты информации** от утечки и несанкционированных воздействий на информацию и ее носители, а также предотвращения других форм незаконного вмешательства в информационные ресурсы и информационные системы.

В связи с этим, понятие «**Защита информации**» становится основополагающим (ключевым) понятием и рассматривается как **процесс или деятельность,** направленная на предотвращение утечки защищаемой информации, а также по предотвращению различного рода несанкционированных и непреднамеренных воздействий на неё и ее носители.

2. Значимость защиты информации увеличивается в связи с возрастанием возможностей разведок за счет совершенствования технических средств разведки, создания совместных предприятий и производств с зарубежными партнёрами, сокращения закрытых для иностранцев зон и городов.

3. Важность и значение защиты информации в обеспечении национальной безопасности страны в целом и в обеспечении информационной безопасности в частности, раскрываются в нормативно –методических документах: - стратегии национальной безопасности России и доктрине информационной безопасности России, в которых сформулирована политика государства в этой области.

2

СИСТЕМЫ ПОНЯТИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Система понятий	Источники, содержащие понятия
Понятия, связанные с правовым регулированием защиты информации	Федеральные законы: 1. «Об информации, информационных технологиях и о защите информации» . 2. «О государственной тайне» 3. «О коммерческой тайне» 4. « О персональных данных».
Понятия, определяющие предметную область защиты информации	1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2. ГОСТ Р 51275-99. Объект информатизации. Факторы, воздействующие на информацию.
Понятия, связанные с защитой информации от НСД в СВТ и АС	Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. 1992.
Понятия в области безопасности информационных технологий	ГОСТ Р ИСО/МЭК 13335 Национальный стандарт РФ. Информационная технология. Методы и средства обеспечения безопасности. Части 1-5.(2006-2007) ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

РОЛЬ НОРМАТИВНЫХ ДОКУМЕНТОВ (СТАНДАРТОВ) В ЗАЩИТЕ ИНФОРМАЦИИ

Основными нормативными документами являются:
- НД утверждённые постановлениями Правительства РФ;
- НД принимаемые ФСТЭК РФ;
-НД принимаемые ФСБ РФ

1. Необходимость следования техническим регламентам и некоторым стандартам и нормативным документам закреплена законодательно;

2. Они создают основу для взаимодействия между производителями, потребителями и экспертами средств защиты информации;

3. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами;

4. Стандарты одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях защиты ИС;

5. Роль технических регламентов, стандартов и нормативных документов зафиксирована в основных положениях закона РФ «О техническом регулировании».

ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ

ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ
по ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, **несанкционированных и непреднамеренных воздействий на защищаемую информацию**.

ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ
По закону «Об информации…»

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на реализацию целей защиты информации.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на неё и включающая правовые, организационные и технические меры обеспечивающие конфиденциальность, доступность и целостность защищаемой информации.

5

СУЩНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ

Сущность защиты информации раскрывается через её предметную область включающую: виды, направления и соответствующие им способы, цели и задачи защиты информации.

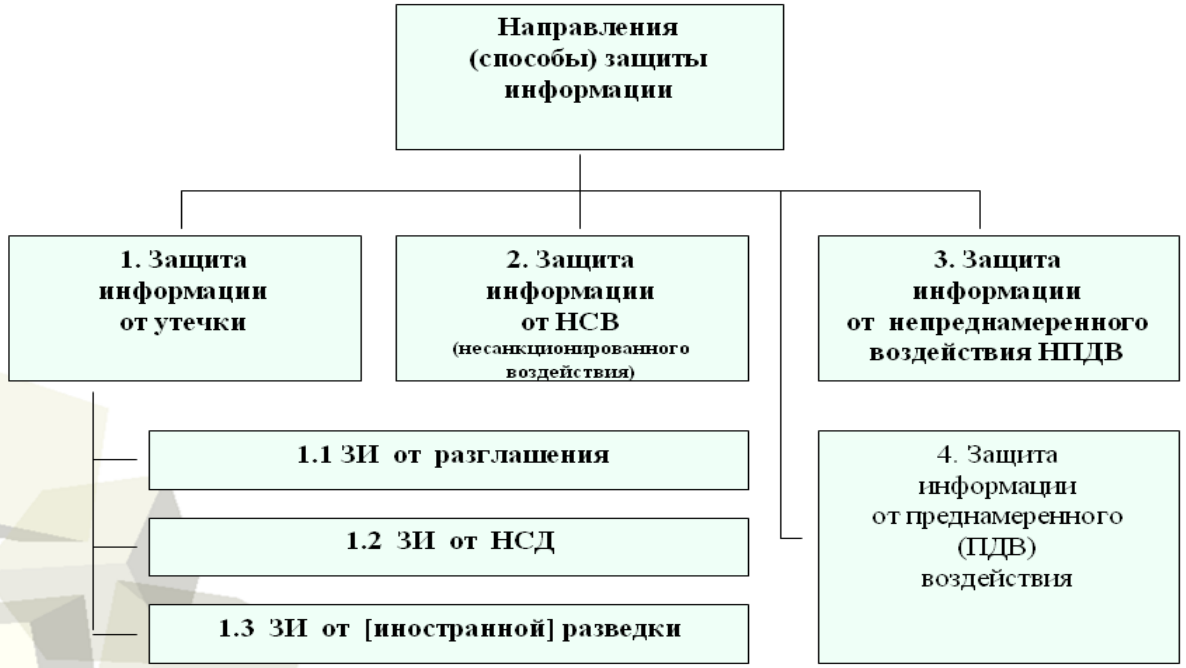
ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ	
Термины	**Определения**
правовая защита информации	Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.
техническая защита информации	Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.
криптографическая защита информации	Защита информации с помощью ее криптографического преобразования.
физическая защита информации	Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты. (Организационная защита)

6

5.2 ПОНЯТИЕ И СУЩНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ КАК ВИДА ДЕЯТЕЛЬНОСТИ

7

НАПРАВЛЕНИЯ И ОТНОСЯЩИЕСЯ К НИМ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ



7

5.2 ПОНЯТИЕ И СУЩНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ КАК ВИДА ДЕЯТЕЛЬНОСТИ

8

НАПРАВЛЕНИЯ И ОТНОСЯЩИЕСЯ К НИМ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.Защита информации от утечки: защита информации, направленная на предотвращение неконтролируемого распространения ЗИ в результате ее разглашения и НСД к ней, а также на исключение (затруднение) получения ЗИ [иностранными] разведками и другими заинтересованными субъектами. Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

1.1 Защита информации от разглашения: защита информации, направленная на предотвращение несанкционированного доведения ЗИ до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

1.2 Защита информации от несанкционированного доступа *(ЗИ от НСД):* защита информации, направленная на предотвращение получения ЗИ заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации. Заинтересованными субъектами, осуществляющими НСД к ЗИ, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

1.3 Защита информации от [иностранной] разведки: защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой. Защита информации от разведки разделяется на защиту от агентурной разведки и технической разведки.

2 Защита информации от несанкционированного воздействия *(ЗИ от НСВ):* защита информации, направленная на предотвращение НСД и воздействия на ЗИ с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

8

5.3 ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

9

ЦЕЛЯМИ ЗАЩИТЫ ИНФОРМАЦИИ ЯВЛЯЮТСЯ:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.

Требования о защите ОДИ могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3

ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ:

1) предотвращение НСД к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов НСД к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

9

5.4 КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ

10

Раздел 2 Основы защиты информации

Тема 6
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И МЕТОДОЛОГИЧЕСКИЙ БАЗИС ЗАЩИТЫ ИНФОРМАЦИИ

Вопросы:

6.1 ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

6.2 МЕТОДОЛОГИЧЕСКИЙ БАЗИС ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

6.3 МОДЕЛИ СИСТЕМ И ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

6. 4 КОНЦЕПЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

Литература

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пособие для вузов.-М:Горячая линия-Телеком, 2004.-280с. (стр.45-68,79-92).
2. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. - Барнаул: АлтГТУ, 2009 –[элетр. с диск.]. (т.8).
3. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: 000 "Инком-бук", 1997. (стр.55-117).
Электронные источники
4. Официальный сайт ВСТЭК http://fstec.ru

6.1 ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

ПОНЯТИЕ, ЗАДАЧИ И СОСТАВНЫЕ ЧАСТИ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ.

ТЕОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ

СИСТЕМА ОСНОВНЫХ ИДЕЙ, ОТНОСЯЩИХСЯ К ЗАЩИТЕ ИНФОРМАЦИИ В СОВРЕМЕННЫХ СИСТЕМАХ ЕЕ ОБРАБОТКИ И НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся и развивающаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

ЗАДАЧИ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

1. ***Предоставлять*** полные и адекватные сведения о происхождении, сущности и развитии проблем защиты информации;

2. ***Полно и адекватно отображать*** структуру и содержание взаимосвязей с родственными и смежными областями знаний;

3. ***Аккумулировать опыт*** предшествующего развития исследований, разработок и практического решения задач защиты информации;

4. ***Ориентировать*** в направлении наиболее эффективного решения основных задач защиты и предоставлять необходимые для этого научно-методологические и инструментальные средства

5. ***Формировать*** научно обоснованные перспективные направления развития теории и практики защиты информации.

6.1 ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

СОСТАВНЫЕ ЧАСТИ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

В качестве составных частей теории защиты информации, в настоящее время, определяют:

1. Полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты информации;

2. Систематизированные результаты ретроспективного анализа развития **теоретических исследований и разработок**, а также **опыта практического решения задач защиты**, полно и адекватно отображающие наиболее устойчивые тенденции в этом развитии;

3. Научно обоснованная постановка задачи защиты информации в современных системах ее обработки, полно и адекватно учитывающая текущие и перспективные концепции построения систем и технологии обработки, потребности в защите информации и объективные предпосылки их удовлетворения;

4 Общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;

5. Методы, необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные прикладные методы решения;

6. Методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;

7. Научно обоснованные предложения по организации и обеспечению работ по защите информации;

8. Научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

6.1 ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

ОСОБЕННОСТИ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ.

Безусловно, что в настоящее время, многие фундаментальные науки, как гуманитарные: философия, история, экономика и другие, так и естественно – нучные: математика, физика, информатика и другие, имеют очень важное значение как базовые науки для всех сфер деятельности человека. Защита информации сегодня рассматривается как прикладная наука информационной сферы жизнедеятельности и как составляющая безопасности государства. Она достаточно глубоко включается в систему общественных отношений, поскольку информация является предметом и объектом собственности, что определяет в качестве первооснов теории защиты правовой базис информационных отношений.

Защита информации носит с одной стороны ярко выраженный правовой характер. С другой стороны, конкретные системы защиты информации на различных объектах её использования имеют техническую основу. Всё это обуславливает ряд особенностей теории защиты информации, её отличие от фундаментальных и некоторых прикладных наук.

ТАКИМИ ОСОБЕННОСТЯМИ ЯВЛЯЮТСЯ:

1) Объективная необходимость и общественная потребность в защите информации;

2) Включенность её в систему общественных отношений;

3) зависимость защиты информации от политико-правовых, социально-экономических, военно-политических реальностей;

4) тесная взаимосвязь с процессами информатизации общества;

5) необходимость обеспечения баланса интересов личности, общества и государства при защите информации через правовое регулирование и взаимный контроль субъектов информационных отношений в сфере защиты информации.

6.1 ОСНОВНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

ОБЩЕМЕТОДОЛОГИЧЕСКИЕ ПРИНЦИПЫ ФОРМИРОВАНИЯ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

1 группа - ОБЩЕТЕОРЕТИЧЕСКИЕ

1) четкая целевая направленность исследований и разработок, причем цели должны быть сформулированы настолько конкретно, чтобы на любом этапе работ можно было предметно оценить степень их достижения.

2) неукоснительное следование главной задаче науки, которая заключается в том, чтобы видимое, лишь выступающее в явлении движение свести к действительному внутреннему движению, которое, как правило, скрыто.

3) упреждающая разработка общих концепций, на базе которых могли бы решаться все частные вопросы. Нетрудно видеть, что данный принцип является дальнейшим развитием предыдущего, его требования заключаются в том, что все получаемые научно обоснованные решения должны образовывать единую систему.

4) формирование концепций на основе реальных фактов, а не абстрактных умозаключений.

5) учет всех существенно значимых связей, относящихся к изучаемой проблеме.

6) своевременное видоизменение постановки изучаемой или разрабатываемой задачи. Сущность данного принципа заключается в том, что назревшие качественные изменения, подготовленные изменениями количественными в процессе предшествующего развития изучаемого явления, должны быть актуализированы путем видоизменения самой постановки решаемой задачи.

2 группа ТЕОРЕТИКО-ПРИКЛАДНЫЕ

1) построение адекватных моделей изучаемых систем и процессов;

2) унификация разрабатываемых решений;

3) максимальная структуризация изучаемых систем и разрабатываемых решений;

4) радикальная эволюция в реализации разработанных концепций.

5

6.2 МЕТОДОЛОГИЧЕСКИЙ БАЗИС ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

Методологический базис, как второй компонент теории защиты, составляют совокупности методов и моделей, необходимых и достаточных для исследований проблемы защиты и решения практических задач соответствующего назначения.

МЕТОДЫ	Характеристика
методы классической теории систем	Разрабатывались применительно к потребностям создания, организации и обеспечения функционирования технических, т.е. в основе своей **формальных систем**, формальные модели которых позволяют привлечь строгие математические методы (статистические и др.) оказались недостаточны для решения задач защиты информации поскольку процессы носят случайный характер. (Неформальные модели – описывают процесс в какой либо системе средствами языка)
методы нечетких множеств	Могут использоваться для исследования формальных систем
методы лингвистических переменных (нестрогой математики);	совокупность приемов построения и использования моделей больших систем, основывающихся на неформальных суждениях и умозаключениях человека, формируемых им исходя из жизненного опыта и здравого смысла.
методы неформального оценивания	Наиболее распространённые - методы экспертных оценок.
методы неформального поиска оптимальных решений.	**1) сведение сложной неформальной задачи к формальной постановке в целях использования уже реализованных формальных методов;** **2) неформальный поиск оптимального решения**, т.е. непосредственная реализация процедуры поиска: *экспертные оценки* (количественные, лингвистические); *неформально-эвристическое программирование* (эргатические модели, неформальные аналогии); *управление продуктивным мышлением* (мозговой штурм, психо - интеллектуальная генерация, логический анализ).

6

6.2 МЕТОДОЛОГИЧЕСКИЙ БАЗИС ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДЫ НЕСТРОГОЙ МАТЕМАТИКИ.

Нестрогой математикой или математикой здравого смысла (называемой еще теорией лингвистических переменных) называют совокупность приемов построения и использования моделей больших систем, основывающихся на неформальных суждениях и умозаключениях человека, формируемых им исходя из жизненного опыта и здравого смысла.

Исходным базисом нестрогой математики служит совокупность трех посылок:

1) **в качестве меры характеристик изучаемых систем вместо число-вых переменных или в дополнение к ним используются лингвистические переменные.** Если, например, нас интересует такая характеристика, как вероятность доступа нарушителя к защищаемой информации, то в линг-вистическом измерении значениями этой характеристики могут быть: «крайне незначительная», «существенная», «достаточно высокая», «весь-ма высокая» и т.п.;

2) простые отношения между переменными в лингвистическом измерении описываются с помощью нечетких высказываний, которые имеют следующую структуру: «из А следует В», где А и В - переменные в лингвистическом измерении. Примером такого отношения может быть следующее: если в системе охранной сигнализации вероятность отказов датчиков «значительная», то для предупреждения проникновения на контролируемую территорию посторонних лиц интенсивность организационного контроля за этой территорией должна быть «повышенной». Переменными здесь являются - «вероятность отказов датчиков» и «интенсивность организационного контроля», а лингвистическими значениями - «значительная» и «повышенная» соответственно. Примером также может служить принятые в международном стандарте безопасности информационных технологий «Общие критерии» (ГОСТ Р ИСО/МЭК – 15408) уровни безопасности – «базовый», «средний», «высокий» условно соответствующие уровням возможностей нарушителей компьютерной системы соответственно – «низкий», «умеренный», «высокий».

3) сложные отношения между переменными в лингвистическом измерении описываются нечеткими алгоритмами.

7

6.2 МЕТОДОЛОГИЧЕСКИЙ БАЗИС ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДЫ НЕФОРМАЛЬНОГО ОЦЕНИВАНИЯ.

МЕТОДЫ ЭКСПЕРТНЫХ ОЦЕНОК

экспертными оценками называются такие методы поиска решений сложных, не поддающихся формализации задач, которые основаны на суждениях (оценках, высказываниях) специально выбираемых (назначаемых) экспертов.

Последовательность и содержание решения задач методами экспертных оценок в самом общем виде могут быть представлены следующим образом:

1) разработка постановки задачи;
2) обоснование перечня и содержания тех параметров задачи, для определения значений которых целесообразно использовать экспертные оценки;
3) обоснование форм и способов экспертных оценок;
4) разработка реквизитов (бланков, инструкций и т.п.), необходимых для проведения экспертных оценок;
5) подбор и подготовка (обучение, инструктаж) экспертов, привлекаемых для реше-ния задачи;
6) организация и обеспечение работы экспертов;
7) контроль и первичная обработка экспертных оценок;
8) базовая обработка экспертных оценок.

По способам привлечения экспертов к решению задач различают:
- простые суждения,
- интервьюирование
- анкетирование.

8

6.3 МОДЕЛИ СИСТЕМ И ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

МОДЕЛИРОВАНИЕ И КЛАССИФИКАЦИЯ МОДЕЛЕЙ

МОДЕЛИРОВАНИЕ СИСТЕМЫ

заключается в построении некоторого её образа, адекватного (с точностью до целей моделирования) исследуемой системе, и имитации на ней процессов функционирования реальной системы с целью получения характеристик реальной системы.

КЛАССИФИКАЦИЯ МОДЕЛЕЙ

В общем случае классификацию моделей по масштабу, способам моделирования, характеру моделируемых систем можно представить следующим образом:

Масштаб моделей:	способ моделирования	характер моделируемых систем
- частные, - общие;	-аналитический, -статистический	детерминированные, стохастические (вероятностные).

6.3 МОДЕЛИ СИСТЕМ И ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

МОДЕЛИРОВАНИЕ И КЛАССИФИКАЦИЯ МОДЕЛЕЙ

Поскольку на процессы защиты информации подавляющее влияние оказывают случайные факторы, то, очевидно, все основные модели систем защиты информации неизбежно должны быть стохастическими. Хотя не следует исключать и детерминированный характер моделей хотя бы применительно к частным моделям.

Стохастические (вероятностные) модели

ВЕРОЯТНОСТНАЯ (СТОХАСТИЧЕСКАЯ) МОДЕЛЬ

— *модель*, которая в отличие от детерминированной модели содержит случайные элементы (случайные величины). Таким образом, при задании на входе модели некоторой совокупности значений, на ее выходе могут получаться различающиеся между собой результаты в зависимости от действия случайного фактора (помехи). Другое название В. м. — стохастические модели.

Для описания процессов функционирования стохастических систем необходимы средства отображения влияния случайных факторов. Такие средства содержатся в целом ряде достаточно хорошо разработанных к настоящему времени методов:

(методы описания процессов функционирования стохастических систем):
- статистических испытаний или Монте-Карло;
- теории массового обслуживания;
- теории вероятностных автоматов (машина Тьюринга) и др.

Детерминированные модели

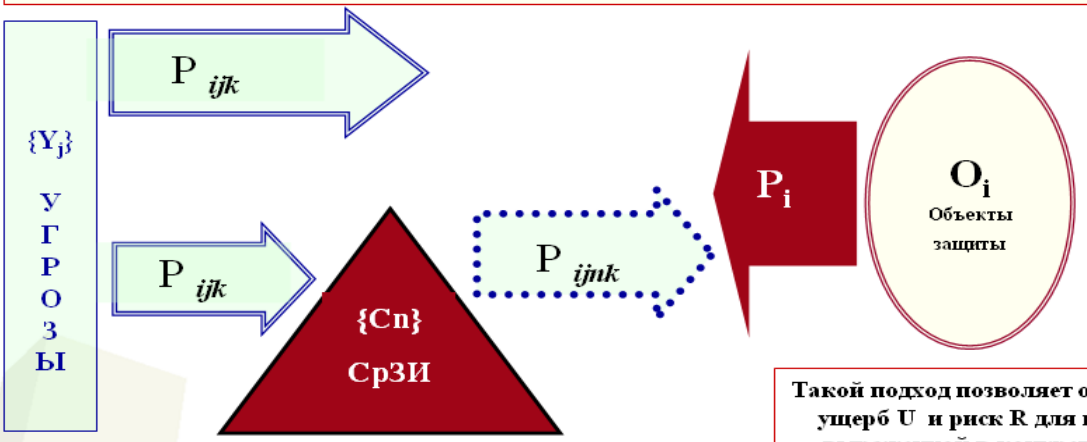
ДЕТЕРМИНИРОВАННАЯ МОДЕЛЬ — аналитическое представление закономерности, операции и т. п., при которых для данной совокупности входных значений на выходе системы может быть получен единственный результат. Такая модель может отображать как вероятностную систему (тогда она является некоторым ее упрощением), так и детерминированную систему.

ДЕТЕРМИНИРОВАННАЯ СИСТЕМА — систем, выходы которой (результаты действия, конечные состояния и т. п.) однозначно определяются оказанными на нее управляющими воздействиями. Такие системы, согласно классификации систем Ст. Бира, могут быть простыми (напр., оконная задвижка) и сложными (напр., компьютер). Д. с. противопоставляется вероятностной, выходы которой лишь случайным образом, а не однозначно зависят от входов.

6.3 МОДЕЛИ СИСТЕМ И ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

ОБЩАЯ МОДЕЛЬ ПРОЦЕССА ЗАЩИТЫ ИНФОРМАЦИИ.

Общая модель процесса защиты информации может быть рассмотрена применительно к объекту информатизации, на котором информация в различных формах хранится, обрабатывается и передаётся с использованием технических систем.



Вероятность надежной защиты информации в группе объектов определяется зависимостью:

$$P = \prod_{\forall i} P_i$$

$$P_i = 1 - \prod_{\forall k} (1 - P_{ik}) \cdot \alpha_k$$

Такой подход позволяет определить возможный ущерб U и риск R для ценной информации, выраженной в конкретной сумме (цене) G.

$$U(R) = (1 - P) * G$$

Oi - i - й объект защиты;
Yj - j –я угроза воздействия на объект защиты (информацию);
{Cn}- n – е средство защиты информации (объекта защиты);
P *ijk* - вероятность негативного воздействия j-й угрозы на i - й объект в k-м его состоянии (без применения средств защиты);
P *ijnk* - вероятность негативного воздействия с учётом нейтрализации воздействия j-й угрозы на i - й объект в k-м его состоянии применением n–го средства защиты;
Pi - вероятность надёжной защиты i –го объекта.

Так, при ценности информации выраженной в цене G=100000руб. и P = 0,8, ущерб U составит 20000 руб. (U= (1-08)*100000=20000руб.), что означает то, что в случае реализации каких-либо угроз потери организации (собственника) в финансовом выражении составят 20000 руб. При этом предотвращённый ущерб составит 80000руб.

11

6.3 МОДЕЛИ СИСТЕМ И ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

ЧАСТНЫЕ МОДЕЛИ ЗАЩИТЫ

Частные модели используются для исследования безопасности отдельных компонентов или процессов.

К ним можно отнести:

- **модели потоков информации на объекте информатизации**
- **частные модели для моделирования угроз безопасности (моделирование конкретной угрозы или некоторой совокупности),**
- **модели нарушителя,**
- **модель безопасности компьютерной системы,**

При моделировании угроз используются как стохастические (вероятностные) модели, методы статистического анализа так и методы неформального анализа.

Современные модели нарушителя характеризуются неформальным описанием, т.е все нарушители распределяются по уровню возможностей, для каждого уровня возможностей определяются возможные способы НСД и т.д. – **неформальная модель нарушителя.** Преимуществом формального описания является возможность привлечь в теорию защиты точные математические методы. То есть доказывать, что данная система в заданных условиях поддерживает политику безопасности. Формальные модели используются для моделирования подсистем безопасности компьютерных систем которые предназначены для защиты наиболее ценной информации (государственной тайны).

ЭКСТРЕМАЛЬНЫЕ ПОКАЗАТЕЛИ ОПРЕДЕЛЯЕМЫЕ ЧАСТНЫМ МОДЕЛИРОВАНИЕМ

- **наиболее ценная (важная) информация;**
- **наиболее уязвимые элементы систем обработки информации;**
- **наиболее опасная угроза;**
- **наиболее опасный злоумышленник;**
- **наименее надёжный механизм защиты;**
- **наиболее надёжная политика безопасности компьютерной системы (ОС, СУБД)**

12

Раздел 2 Основы защиты информации

Тема №7

ОСНОВНЫЕ СВОЙСТВА И СОСТАВ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Вопросы

7.1 ОСНОВНЫЕ СВОЙСТВА ИНФОРМАЦИИ С ТОЧКИ ЗРЕНИЯ ЕЁ БЕЗОПАСНОСТИ

7.2 ПОНЯТИЕ И СОСТАВ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ. ПРИНЦИПЫ ОТНЕСЕНИЯ ИНФОРМАЦИИ К ЗАЩИЩАЕМОЙ

7.3 НОСИТЕЛИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

7.4 УЯЗВИМОСТЬ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ И ФОРМЫ ЕЁ ПРОЯВЛЕНИЯ

Литература

1. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие/Барнаул: АлтГТУ, 2009.- [электр. ресурс].
2. Загинайлов Ю.Н. Методические рекомендации к семинарским занятиям и указания к СРС по дисциплине «Теория информационной безопасности и методология защиты информации»/ Алт.гос.техн.ун-т им.И.И.Ползунова.- Барнаул: Изд-во АлтГТУ.-2005-73с.
3. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008 -10с
4. Закон «Об информации, информационных технологиях и о защите информации.

1

7.1 ОСНОВНЫЕ СВОЙСТВА ИНФОРМАЦИИ С ТОЧКИ ЗРЕНИЯ ЕЁ БЕЗОПАСНОСТИ

ПОНЯТИЕ ИНФОРМАЦИИ

Органическая точка зрения, основанная на философском подходе

с этой точки зрения информация проявляется в двух основных формах:

сведения - запечатлённые в организме (живом организме) результаты отражения движения объектов материального мира;

сообщения – *набор знаков*, с помощью которых сведения могут быть *переданы* другому организму и *восприняты* им.

С позиции права (законодательства РФ)

ИНФОРМАЦИЯ - сведения (сообщения, данные) независимо от формы их представления. (Федеральный закон 2006г. «Об информации, информационных технологиях и о защите информации»)

Понятия и термины, применяемые в праве и законодательстве для обозначения информации (производные формы)

«информация», «документированная информация» «документ», «массив документов», «общедоступная информация», «информация ограниченного доступа», «компьютерная информация», «массовая информация», «правовая информация», «информационные ресурсы», «данные», «банки данных», «файл», «сайт», «электронное сообщение», «электронный документ», «страница», «электронно-цифровая подпись»; и т. д.

2

7.1 ОСНОВНЫЕ СВОЙСТВА ИНФОРМАЦИИ С ТОЧКИ ЗРЕНИЯ ЕЁ БЕЗОПАСНОСТИ

ОСНОВОПОЛАГАЮЩИЕ ФОРМЫ ИНФОРМАЦИИ В ПРАВЕ И ЗАКОНОДАТЕЛЬСТВЕ РФ

основополагающими формами И в праве являются:

1. документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель.

2. информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

ВЫВОД:

Информация (сообщения, данные) связана с материальным носителем и для правовой защиты должна быть документирована, иметь реквизиты.

Основными реквизитами являются:

-наименование документа;
-регистрационный номер;
-дата создания и регистрации;
-автор и (или) исполнитель (Ф.И.О);
-атрибуты учреждения;
- гриф секретности или конфиденциальности, если документ относится к таковым.

3

7.1 ОСНОВНЫЕ СВОЙСТВА ИНФОРМАЦИИ С ТОЧКИ ЗРЕНИЯ ЕЁ БЕЗОПАСНОСТИ

ИНФОРМАЦИЯ КАК ТОВАР

1. С развитием производства и ускорением темпов развития общества информация приобрела *свойства товара* и стала объектом *рыночных отношений* и объектом гражданских прав (прав собственности) закреплённых в Гражданском кодексе, в том числе и исключительных (имущественных) прав на объекты интеллектуальной собственности.

2. Информационные ресурсы включаются в состав имущества государства, юридических и физических лиц, и как любой другой ресурс, обладающий свойством товара, имеет свою товарную или потребительскую стоимость – ценность (цену). Свойствами товара обладает документированная информация на материальном носителе.

Ценность информации

Ценность (цена) информации (информационного ресурса) в общем случае будет складываться из стоимости затрат на его создание, а в случае включения в его состав объектов интеллектуальной собственности ещё и затрат необходимых для оплаты авторам и потребности в нём на рынке, если он создаётся для коммерческих целей.

Важность информации

Информация во внешнеполитической, военной, разведывательной, контрразведывательной и оперативно-розыскной деятельности, собственником которой является государство, имеет наивысшую важность. Например, информация о деятельности разведывательных служб не имеет цены, однако ущерб от разглашения такой информации общеизвестен – политический (моральный) ущерб для целого государства и его престижа. Критерием ценности здесь выступает важность и тот ущерб, который может быть нанесён в результате разглашения или утраты этой информации.

Для сохранения ценности (важности) информации необходимо ограничить круг лиц допускаемых к ней (конфиденциальность), и (или) обеспечить её неискажённость (целостность) и доступ для того, для кого она предназначена (доступность)

4

7.1 ОСНОВНЫЕ СВОЙСТВА ИНФОРМАЦИИ С ТОЧКИ ЗРЕНИЯ ЕЁ БЕЗОПАСНОСТИ

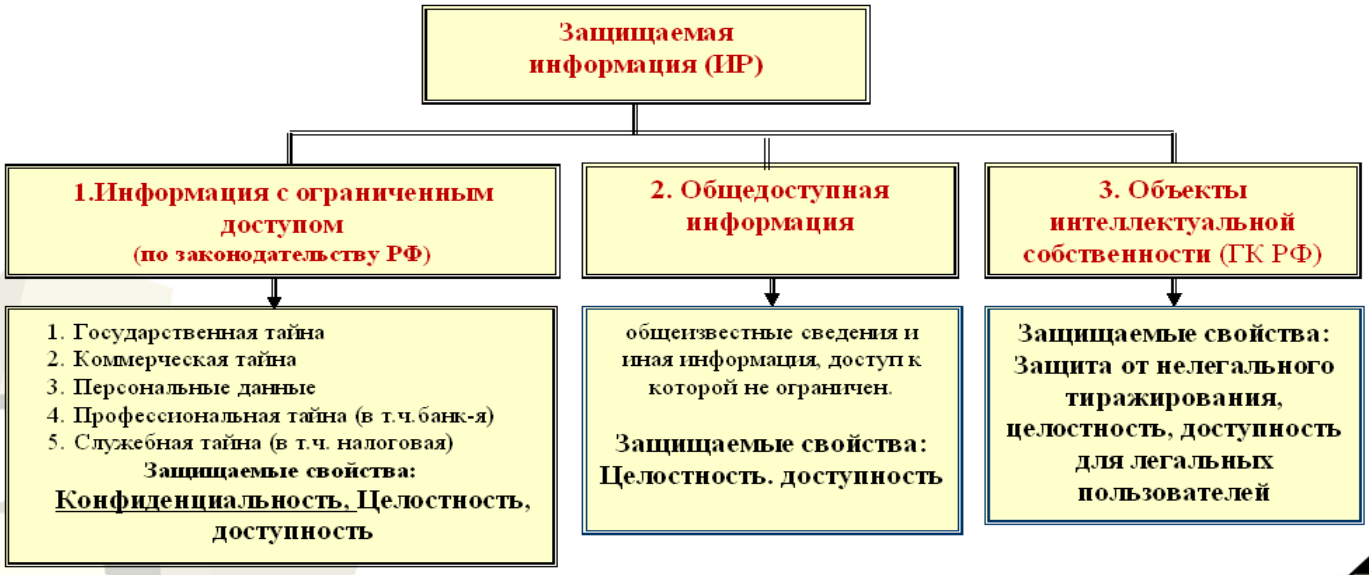
СВОЙСТВА ИНФОРМАЦИИ С ТОЧКИ ЗРЕНИЯ ЕЁ БЕЗОПАСНОСТИ	
1. КОНФИДЕНЦИАЛЬНОСТЬ	**свойство (характеристика) информации, указывающая на необходимость ограничения круга субъектов, имеющих доступ к данной информации.** Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.
2. ЦЕЛОСТНОСТЬ	**свойство информации существовать в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).** Точнее говоря, субъектов интересует обеспечение более широкого свойства - достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее неискаженности.
3. ДОСТУПНОСТЬ	**то есть свойство системы (среды, средств и технологий ее обработки), в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации** и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.
При нарушении хотя бы одного свойства ценность информации снижается или теряется вообще !!!	

5

7.2 ПОНЯТИЕ И СОСТАВ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ. ПРИНЦИПЫ ОТНЕСЕНИЯ ИНФОРМАЦИИ К ЗАЩИЩАЕМОЙ

ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ

- информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.



6

7.2 ПОНЯТИЕ И СОСТАВ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ. ПРИНЦИПЫ ОТНЕСЕНИЯ ИНФОРМАЦИИ К ЗАЩИЩАЕМОЙ

ПРИНЦИПЫ ОТНЕСЕНИЯ ИНФОРМАЦИИ К ЗАЩИЩАЕМОЙ

ПРИНЦИПЫ ОТНЕСЕНИЯ ИНФОРМАЦИИ К ЗАЩИЩАЕМОЙ	
1. ЗАКОННОСТИ	заключается в соответствии информации (ИР) законодательству: 1. Об информации, информационных технологиях и о защите информации, 2. О тайнах (Гос. Тайне, Комм-й тайне, Персональных данных и др.) 3. О собственности и об интеллектуальной собственности (ГК РФ).
2. ОБОСНОВАННОСТИ	заключается в установлении путем экспертной оценки целесообразности отнесения к конфиденциальным конкретных сведений или защищаемых в интересах обеспечения целостности и доступности сведений, вероятных экономических и иных (гражданско - правовых) последствий этого акта исходя из интересов бизнеса и баланса интересов государства, общества и граждан.
3. СВОЕВРЕМЕННОСТИ	заключается в установлении ограничений связанных с доступом к защищаемой информации с момента её получения (разработки сведений, данных) или заблаговременно.

7.3 НОСИТЕЛИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

НОСИТЕЛЬ ИНФОРМАЦИИ

физическое лицо или **материальный объект**, в том числе **физическое поле**, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин. (ГОСТ Р 50922-2006)

КЛАССИФИКАЦИЯ НОСИТЕЛЕЙ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ		
1. Физическое лицо	Человек, с точки зрения гражданских правоотношений - физическое лицо (носитель информации)	
Материальные объекты	**2. Носители** информации, используемые для записи, хранения, обмена, документирования информации	**2.1 На бумажной основе**
		2.2 Фотоплёнка и фотодокументы
		2.3 Машинные (технические) носители (ЭВМ)
		2.4 Другие (те которые могут быть источниками информации – картины, артефакты и т.п)
	3. Физическое поле, в котором информация находит свое отражение	**Электрические, магнитные, электромагнитные поля, акустические, электроакустические, гидроакустические сигналы….(в ТС обработки информации)**
	4. « защищаемые объекты »	специальные, военные, режимные объекты, объекты оборонной промышленности, экономики РФ, войска
	5. « специальные изделия »	вооружение, военная техника, оружие массового поражения, опытные образцы техники или технологий
	6. « вещества» (материалы)	вещества, предназначенные для производства оружия большой поражающей способности, другие

Раздел 2 Основы защиты информации

Тема 8

КЛАССИФИКАЦИЯ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА ПО ВИДАМ ТАЙНЫ И СТЕПЕНЯМ КОНФИДЕНЦИАЛЬНОСТИ

Вопросы

8.1 ПОКАЗАТЕЛИ РАЗДЕЛЕНИЯ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА НА ВИДЫ ТАЙНЫ

8.2 ГОСУДАРСТВЕННАЯ ТАЙНА

8.3 КОММЕРЧЕСКАЯ ТАЙНА

8.4 ПЕРСОНАЛЬНЫЕ ДАННЫЕ

8.5 СЛУЖЕБНАЯ ТАЙНА

8.6 ПРОФЕССИОНАЛЬНАЯ ТАЙНА

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .- Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Закон «Об информации, информационных технологиях и о защите информации.
3. Источники указанные в Методических рекомендациях к курсу.

Понятие тайны

Слово «тайна» имеет древнерусское происхождение.

С одной стороны, это всё то, что на данный момент не осознано человеческим интеллектом (тайна природы).

С другой стороны – это нечто уже известное, но с определённой целью скрытое от других людей (сведения, которые какой-либо субъект считает скрыть от других).

В законодательстве РФ словом тайна обозначают информацию ограниченного доступа

Правовой институт любого вида тайны имеет три составляющие:

(субинституты)

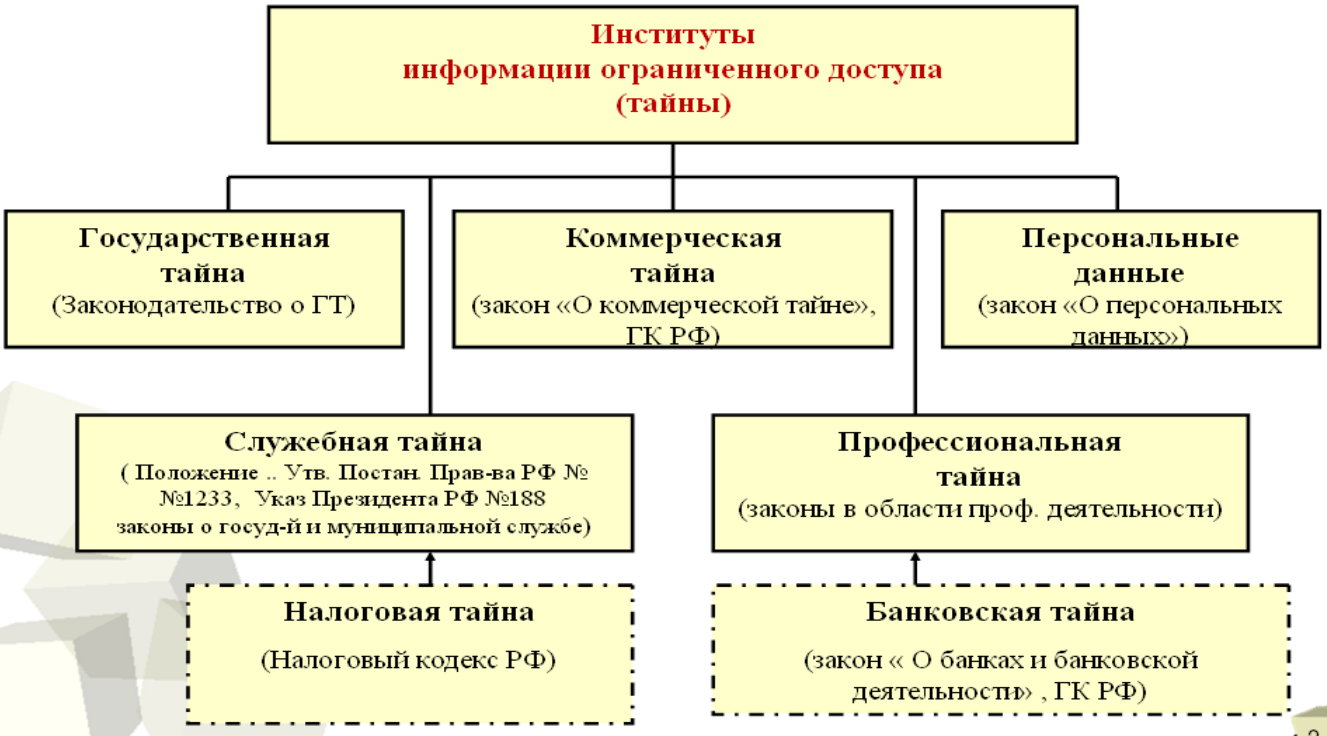
1. Относимые к определённому виду тайны *сведения*, а также научно обоснованные *принципы* и *критерии* отнесения сведений к данному виду.

2. Механизм ограничения доступа к указанным сведениям (механизм защиты);

3. Правовые санкции за неправомерное получение и (или) разглашение указанных сведений.

8.1 ПОКАЗАТЕЛИ РАЗДЕЛЕНИЯ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА НА ВИДЫ ТАЙНЫ

ИНСТИТУТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА



3

8.1 ПОКАЗАТЕЛИ РАЗДЕЛЕНИЯ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА НА ВИДЫ ТАЙНЫ

КЛАССИФИКАЦИЯ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА ПО ВИДАМ ТАЙНЫ

Вид тайны		Показатели разделения на тайны (родовой признак)	
		Собственник	Вид деятельности
Государственная тайна		Государство	*военная, внешнеполитическая, экономическая, разведывательная, контрразведывательная и оперативно-розыскная*
Сведения конфиденциального	Коммерческая тайна	*Юридические лица Физические лица*	Коммерческая деятельность
	Персональные данные	ПЕРСОНА Граждане (физические лица и.т.п) и др. лица	*Любой*
	Служебная тайна	*Органы государственной власти*	Государственная и муниципальная служба
	Профессиональная тайна	*Граждане (физические лица)*	Профессиональная деятельность

4

6.2 ГОСУДАРСТВЕННАЯ ТАЙНА

Закон РФ «О государственной тайне» 1993г.	
ГОСУДАРСТВЕННАЯ ТАЙНА	
-защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, **распространение которых может нанести ущерб безопасности РФ**	
Перечень сведений, составляющих государственную тайну. (ст.5 закона О ГТ)	**представляет собой совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются.** (описывает довольно широкие категории сведений объединенных одним или несколькими признаками в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью)
1. сведения в военной области (6 категорий сведений); 2. сведения в области экономики, науки и техники (5 категорий); 3. сведения в области внешней политики и экономики (2 категории); 4. сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности (7 категорий). **в том числе сведения:** • о методах и средствах защиты секретной информации; • об организации и о фактическом состоянии защиты государственной тайны.	
Не подлежат отнесению к государственной тайне и засекречиванию сведения - (ст.7 Закона «О государственной тайне»)	

ОТНЕСЕНИЕ СВЕДЕНИЙ К ГОСУДАРСТВЕННОЙ ТАЙНЕ И ИХ ЗАСЕКРЕЧИВАНИЕ

Отнесение сведений к государственной тайне и их засекречивание - введение в предусмотренном законом порядке ограничений на их распространение и на доступ к их носителям.

ПРИНЦИПЫ ОТНЕСЕНИЯ ИНФОРМАЦИИ К ГОСУДАРСТВЕННОЙ ТАЙНЕ	
Законность	заключается в соответствии засекречиваемых сведений перечню сведений, составляющих государственную тайну (ст.5 закона «О государственной тайне») и законодательству РФ о государственной тайне, за исключением сведений, не подлежащих отнесению к государственной тайне и засекречиванию (ст.7 закона «О государственной тайне»).
Обоснованность	заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.
Своевременность	заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

8.2ГОСУДАРСТВЕННАЯ ТАЙНА

ПОРЯДОК ОТНЕСЕНИЯ СВЕДЕНИЙ К ГТ (ПЕРЕЧНЕВЫЙ ПОДХОД)

Перечень сведений составляющих ГТ (закон о ГТ ст.5)

Руководители ОГВ, наделённые полномочиями (указом През-та) относят сведения к ГТ и напр. в МВК ЗГТ

Органы госуд-ной власти, предприятия, учреждения, организации обосновывают необходимость отнесения к ГТ разработанных (полученных) сведений

Перечень сведений, отнесённых к ГТ (общероссийский) Утверждается Президентом

Готовится МВК по защите ГТ на основе ведомственных (министерских) перечней. Закрепляет сведения за ведомствами (министерствами) руководители которых наделены полномочиями по распоряжению данными сведениями.

Развёрнутые Перечни сведений, подлежащих засекречиванию в ведомстве (министерстве), организации

Содержит степени секретности для каждых сведений имеют свой гриф

СТЕПЕНИ СЕКРЕТНОСТИ СВЕДЕНИЙ

Степень секретности	Критерии отнесения к степени
Особой важности	***Ущерб интересам России*** (в одной или нескольких областях деятельности: военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной, оперативно-розыскной)
Совершенно секретно	***Ущерб интересам министерства (ведомства)*** или отрасли экономики РФ (в одной или нескольких областях деятельности)
Секретно	***Ущерб интересам предприятия***, учреждения или организации в одной или нескольких областях (все иные сведения)

8.3 КОММЕРЧЕСКАЯ ТАЙНА

ПОНЯТИЕ КОММЕРЧЕСКОЙ ТАЙНЫ

КОММЕРЧЕСКАЯ ТАЙНА

Федеральный закон РФ «О коммерческой тайне» 2004г.

режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

ИНФОРМАЦИЯ, СОСТАВЛЯЮЩАЯ КОММЕРЧЕСКУЮ ТАЙНУ

сведения любого характера

1. **(производственные, технические, экономические, организационные и другие),**
2. **в том числе о результатах интеллектуальной деятельности в научно-технической сфере,**
3. **а также сведения о способах осуществления профессиональной деятельности,**

а) которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам,

б) к которым у третьих лиц нет свободного доступа на законном основании

в) и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

8.3 КОММЕРЧЕСКАЯ ТАЙНА

ОТНЕСЕНИЕ ИНФОРМАЦИИ К КОММЕРЧЕСКОЙ ТАЙНЕ

1. **Право на отнесение** информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации **принадлежит обладателю** такой информации с учетом положений закона о коммерческой тайне.

2. Права обладателя ИСКТ, возникают с момента установления им в отношении такой информации **режима коммерческой тайны.**

3. Правовой статус коммерческой тайны закрепляется в **«Перечне информации, составляющей коммерческую тайну организации».**
Перечень информации, составляющей коммерческую тайну, утверждается руководителем организации.

4. Сведения, которые не могут составлять коммерческую тайну приводятся в законе «О коммерческой тайне» (ст.5) .

5. На материальные носители (документы), содержащие ИСКТ наносится **гриф "Коммерческая тайна"** с указанием обладателя этой информации.

9

8.4 ПЕРСОНАЛЬНЫЕ ДАННЫЕ

ПОНЯТИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральный закон РФ от 27.07.06 №152-ФЗ О персональных данных

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПД)	Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД): ФИО, дата и место рождения, адрес, семейное и социальное положения, образование, доходы и др. информация
СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПД	Расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояния здоровья и интимной жизни.
БИОМЕТРИЧЕСКИЕ ПД	Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность.
ОБЩЕДОСТУПНЫЕ ПД	ПД, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПД или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.Персональные данные охраняются в режиме информации ограниченного доступа (конфиденциальной информации). Грифа конфиденциальности для персональных данных законодательством не установлено.

2. Правовой статус персональных данных как информации ограниченного доступа обязан установить оператор. Этот статус закрепляется перечнем персональных данных подлежащих защите. Категорирование персональных данных осуществляется на основе нормативно-методических документов утверждаемых Правительством РФ. Контроль за состоянием безопасности ИСПДн осуществляется ФСБ РФ, ФСТЭК РФ. Контроль за выполнением условий обработки Министерством связи и массовых коммуникаций.

8.5 СЛУЖЕБНАЯ ТАЙНА

СЛУЖЕБНАЯ ТАЙНА

защищаемая по закону конфиденциальная информация, (а) ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также (б) служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или (в) в силу служебной необходимости.

«Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» утверждённом Постановлением Правительства РФ от 3 ноября 1994 г. № 1233.

ОТНЕСЕНИЕ ИНФОРМАЦИИ К СЛУЖЕБНОЙ ТАЙНЕ

К служебной тайне отнесена:

(а) защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления (в соответствии с указом Президента РФ №188 1997г., коммерческая, персональные данные, профессиональная, банковская, налоговая);

(б) служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом (тайна следствия, судебная тайна, тайна о мерах безопасности (судьи, и т.п), тайна усыновления, военная тайна).

(в) В силу служебной необходимости относится

в соответствии с с постановлением Правительства РФ № 1233. Правовой статус для этой информации закрепляется в «Перечне информации ограниченного доступа» Который утверждается руководителем органа государственной власти, государственной (муниципальной) организации, предприятия, учреждения. Для СТ используется гриф «Для служебного пользования» -ДСП.

8.6 ПРОФЕССИОНАЛЬНАЯ ТАЙНА

ПРОФЕССИОНАЛЬНАЯ ТАЙНА

защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ К ПРОФЕССИОНАЛЬНОЙ ТАЙНЕ ОТНЕСЕНЫ:

1. Врачебная тайна (Основы законодательства РФ об охране здоровья граждан).

2. Тайна связи (законы "О связи" "О почтовой связи" УК РФ ст.139 — тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений).

3. Нотариальная тайна («Основы законодательства РФ о нотариате» (ст. 5, 14, 16))

4. Адвокатская тайна.

5.Аудиторская тайна ("Об аудиторской деятельности" ст.8);

6. Тайна усыновления (УК РФ ст. 155).

7. Тайна страхования (ГК РФ).

8. Тайна исповеди («О свободе совести и о религиозных объединениях» п. 7 ст. 3).

К профессиональной тайне относится также банковская тайна – она имеет собственный институт-институт банковской тайны.

Тема 9

ПОНЯТИЕ, КЛАССИФИКАЦИЯ И ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Вопросы:

9.1 ПОНЯТИЕ УГРОЗЫ И ЕЁ ВЗАИМОСВЯЗЬ С УЯЗВИМОСТЬЮ И РИСКАМИ

9.2 ОБЩАЯ КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

9.3 ЦЕЛИ И ЗАДАЧИ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .- Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Источники указанные в Методических рекомендациях к курсу.

ПОНЯТИЕ УГРОЗЫ И ЕЁ ВЗАИМОСВЯЗЬ С УЯЗВИМОСТЬЮ И РИСКАМИ

угроза безопасности информации - совокупность ***условий*** **и** ***факторов***, создающих потенциальную или реально существующую опасность нарушения безопасности информации, или (что равнозначно)?

Уязвимость (информационной системы); *брешь* - свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Если уязвимость соответствует угрозе, то существует риск.

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Риск - ожидаемые потери или возможный результат реализации угрозы при наличии уязвимости и определенных обстоятельств или событий, приводящих к реализации угрозы. Возможность того, что определенная угроза реализуется вследствие наличия определенной уязвимости системы.

(9.1) $R = Руг * Руязв * G$

где: R – степень (уровень) риска; Руг – вероятность реализации угрозы, при наличии уязвимости ; Руязв – вероятность наличия уязвимости; G – цена информации (стоимость активов);

СТРУКТУРНО-ЛОГИЧЕСКАЯ СХЕМА УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.

Профиль субъективной преднамеренной угрозы (источник – способ -канал-уязвимость-риск)

9.1 ПОНЯТИЕ УГРОЗЫ И ЕЁ ВЗАИМОСВЯЗЬ С УЯЗВИМОСТЬЮ И РИСКАМИ

ОСНОВНЫЕ УЯЗВИМОСТИ ИНФОРМАЦИИ И СИСТЕМ ЕЁ ОБРАБОТКИ

Уязвимости носителей	Уязвимости систем обработки	Уязвимости (слабости) систем защиты
Утрата -Хищение -Уничтожение -сбой функционирования	-подверженность программного обеспечения сбоям и отказам -излучения технических средств обработки и обеспечения объекта информатизации, создающие информативные физические поля	-наличие не выявленных «дыр» и «люков» в сертифицированных ОС и БД (системном и прикладном ПО) - слабость парольных систем в АС -подверженность зашифрованной информации криптоанализу - некорректная политика безопасности АС

9.2 ОБЩАЯ КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Признак класса	Вид угрозы	Характеристика
1. По источнику угрозы	***Объективные*** *(Естественные)*	угрозы, вызванные воздействиями на системы обработки информации и ее компоненты объективных физических ***процессов*** или стихийных при-родных **явлений**, независящих от человека.
	Субъективные *(Искусственные)*	угрозы, вызванные умышленными или неумышленными действия ми человека
2. По отношению к объекту защиты	***Внутренние***	источник которых, расположен в пределах контролируемой зоны (территории, помещения)
	Внешние	источник которых, расположен вне контролируемой зоны (территории , помещения)
3. По степени преднамеренности (для субъективных)	***Случайные***	вызванные ошибками или халатностью персонала (непреднамеренные воздействия)
	Преднамеренные	вызванные целенаправленными действиями людей

5

9.2 ОБЩАЯ КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Признак класса	Вид угрозы	Характеристика
4. По цели действия	***Угроза конфиденциальности***	разглашение, НСД, получение разведками
	Угроза целостности	искажение (модификация), уничтожение, копирование
	Угроза доступности	блокирование доступа к информации или носителю
	Угроза праву собственности на информацию	несанкционированное тиражирование и распространение объектов интеллектуальной собственности
5. По характеру воздействия	***Активные (атаки)***	которые, при воздействии, вносят изменения в структуру и содержание АС («троянский конь» и др.)
	Пассивные	которые при реализации ничего не меняют в структуре и содержании АС (угроза копирования секретных данных)
6. По характеру нанесённого ущерба	***Материальный***	потеря упущенной выгоды в результате разглашения коммерческой тайны, утраты интернет - ресурса.
	Моральный	(политический, личный, общественный)

6

9.3 ЦЕЛИ И ЗАДАЧИ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

оценка угроз защищаемой информации и системам её обработки представляет собой анализ рисков - процесс определения угроз, уязвимостей, возможного ущерба, а также контрмер.

целью оценки угроз является определение значения тех показателей, которые необходимы для определения требований к системе защиты

Частными задачами при моделировании и оценке угроз являются:

1) **обоснование (выбор) системы показателей**, необходимых для оценки уязвимости информации

2) **выбор (разработка) методики** для проведения исследований и определения состава угроз;

3) **определение и анализ множества видов уязвимости** информации, носителей и систем её обработки;

4) **определение и анализ источников угроз** и дестабилизирующих факторов;

5) **определение и анализ множества каналов** несанкционированного воздействия на информацию и системы её обработки (каналов утечки информации и несанкционированного доступа);

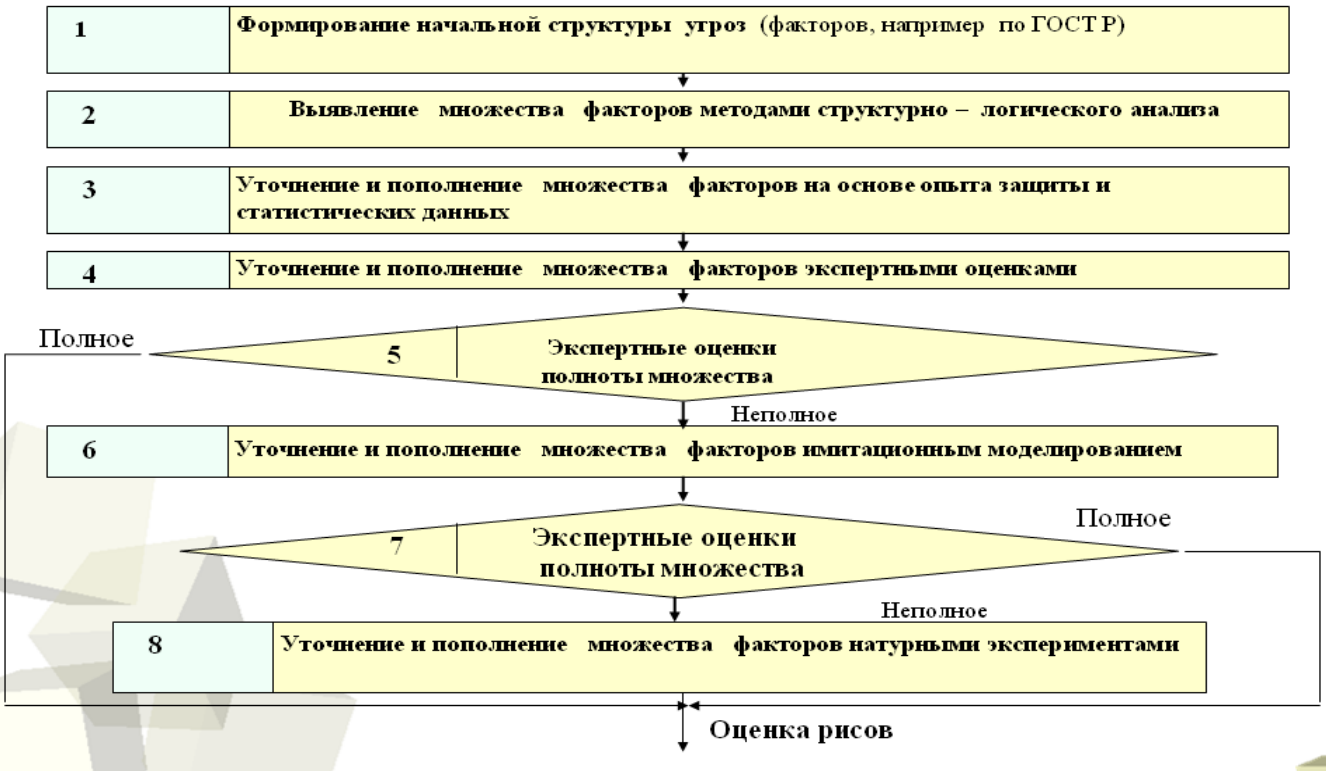
6) **определение возможных способов реализации угроз** и способов атак на системы обработки (АС);

7) **определение относительно полного множества реальных угроз и рисков**, которые будут положены в основу для определения требований к системе защиты информации, с целью уменьшить или исключить риски.

7

9.3 ЦЕЛИ И ЗАДАЧИ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

АЛГОРИТМ ОЦЕНКИ УГРОЗ



8

Тема 10

ИСТОЧНИКИ И СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

ВОПРОСЫ:

10.1 ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

10.2 ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ СО СТОРОНЫ СУБЪЕКТИВНЫХ ИСТОЧНИКОВ

10.3 УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .- Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Источники указанные в Методических рекомендациях к курсу.

1

10.1 ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Классификация источников угроз безопасности информации

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

2

10.1 ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ОБЪЕКТИВНЫЕ ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Под класс	Группа	Источники угроз
внутренние	**Техногенные** (явления техногенного характера – дефекты, сбои, отказы, аварии)	1) некачественные технические средства обработки информации (ИС) 2) некачественное программное обеспечение 3) некачественные системы обеспечения ОИ (охраны, сигнализации, телефонии) 4) другие технические средства применяемые на ОИ
внешние	**Техногенные** (явления техногенного характера - дефекты, сбои, отказы, аварии)	*1) Некачественные системы обеспечения* ОИ (средства связи, инженерные коммуникации системы водоснабжения, канализации) и т.п. 2) непреднамеренные электромагнитные облучения ОИ 3) радиационные облучения ОИ
	Стихийные (природные явления, стихийные бедствия)	1) термические факторы (пожары и т. д.). 2) климатические факторы (наводнения и т. д.). 3) механические факторы (землетрясения и т. д.). 4) электромагнитные факторы (грозовые разряды и т. д.). 5) биологические факторы (микробы, грызуны и т. д.).

3

10.1 ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

СУБЪЕКТИВНЫЕ ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Под класс	Группа	Подгруппа
Внутренние	**Персонал допущенный к защищаемой информации** (обиженные, уволенные сотрудники и т.п., нарушители порядка и правил обращения с информацией. злоумышленники)	1) основной персонал (пользователи, программисты, разработчики) 2) представители службы защиты информации
	Лица, допущенные на ОИ, обслуживанию систем и средств обеспечения ОИ (злоумышленники)	1) вспомогательный персонал (уборщики, охрана) 2) технический персонал (жизнеобеспечение, эксплуатация)
Внешние	**Нарушители и злоумышленники** (преднамеренные действия)	1) иностранные разведки 2) конкуренты и их службы разведки (недобросовестные партнеры) 3) криминальные элементы (сруктуры) 4) потенциальные преступники и хакеры (компьютерные взломщики) и т.д. 5) технический персонал поставщиков телематических услуг 6) представители надзорных организаций и аварийных служб 7) представители силовых структур. 8) самоутверждающиеся личности

4

10.2 ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ СО СТОРОНЫ СУБЪЕКТИВНЫХ ИСТОЧНИКОВ

СУБЪЕКТИВНЫЕ, ВНУТРЕННИЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ (классификация)

Виды внутренних, субъективных угроз БИ	Способы реализации внутренних, субъективных угроз
1. Разглашение конфиденциальной информации лицами, имеющими к ней право доступа	1.1 Разглашение информации лицам, не имеющим права доступа к ЗИ 1.2 Передача информации по открытым линиям связи 1.3 Обработка информации на незащищенных ТС обработки информации 1.4 Опубликование информации в открытой печати и других СМИ 1.5 Копирование информации на незарегистрированный носитель информации. 1.6 Передача носителя информации лицу, не имеющему права доступа к ней. 1.7 Утрата носителя с защищаемой информацией.
2. Неправомерные действия со стороны лиц, имеющих право доступа к ЗИ	2.1 Несанкционированное изменение информации (модификация). 2.2 Несанкционированное копирование информации
3.Несанкционированный доступ к ЗИ	3.1 Подключение к техническим средствам и системам ОИ. 3.2 Использование закладочных устройств 3.3 Использование программного обеспечения технических средств ОИ 3.4 Нарушение функционирования технических средств обработки информации 3.5 Хищение носителя с защищаемой информацией
4. Блокирование доступа к ЗИ	4.1 Блокирование доступа путём установки специального программного обеспечения

10.2 ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ СО СТОРОНЫ СУБЪЕКТИВНЫХ ИСТОЧНИКОВ

СУБЪЕКТИВНЫЕ, ВНУТРЕННИЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ (классификация)

Несанкционированный доступ к защищаемой информации. ***Несанкционированный доступ к ЗИ*** **- получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации *прав* или *правил* доступа к защищаемой информации.**

Подключение к техническим средствам и системам ОИ

может быть осуществлено с использованием штатного оборудования имеющегося на объекте информатизации с нарушением правил его использования или негласно внесённого и неучтённого типового оборудования.

Использование закладочных средств (устройств).

Закладочное средство (устройство) - техническое средство (устройство) приема, передачи и обработки информации, преднамеренно устанавливаемое на объекте информатизации или в контролируемой зоне в целях перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы. Местами установки закладочных средств (устройств) на охраняемой территории могут быть любые элементы контролируемой зоны, например: ограждение, конструкции, оборудование, предметы интерьера, транспортные средства.

Закладочные устройства бывают различных видов. В них могут располагаться средства записи. Закладочные устройства могут снимать информацию и ретранслировать её на приёмник расположенный вблизи объекта информатизации. Основными закладочными устройствами следует считать средства съёма акустической информации (микрофонного типа) и видеоинформации (мини видеокамеры). Они могут записывать информацию на встроенные носители или ретранслировать её за пределы объекта.

Использование программного обеспечения технических средств объекта информатизации может быть осуществлено путём:

- «маскировки под зарегистрированного пользователя»;
- использованием дефектов программного обеспечения ОИ («люков» и др.)
- использования программных закладок;
- применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

Программная закладка- преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Вредоносная программа- программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

Компьютерный вирус - вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы.

10.2 ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ СО СТОРОНЫ СУБЪЕКТИВНЫХ ИСТОЧНИКОВ

СУБЪЕКТИВНЫЕ, ВНЕШНИЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ (классификация)

Виды субъективных, внешних угроз	Способы реализации субъективных, внешних угроз
1. Доступ к ЗИ с применением технических средств (получение ЗИ разведаками)	1.1 Разведки: *-средств радиоэлектронной разведки* *-средств оптико - электронной разведки* *-средств фотографической разведки.* *-средств визуально-оптической разведки* *-средств акустической разведки* *-средств гидроакустической разведки* *-средств компьютерной разведки* 1.2 Доступ к ЗИ с применением технических средств съёма информации
2.Несанкционированный доступ к ЗИ	2.1 Подключение к техническим средствам и системам ОИ. 2..2 Использование закладочных устройств 2..3 Использование программного обеспечения технических средств ОИ 2.4 Применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов) 2.5 Несанкционированный физический доступ 2.6 Хищение носителя с защищаемой информацией
3. Блокирование доступа к ЗИ	3.1 Путём перегрузки ИС (сервера) ложными заявками на обработку 3.2 Путём установки специального программного обеспечения (программных вирусов и т.п.)
4. Действия криминальных групп и отдельных преступных групп	**4.1 Диверсия в отношении ОИ** 4.2 Диверсия в отношении элементов ОИ.
5. Искажение, уничтожение или блокирование информации с применением технических средств путем	5.1 Преднамеренного силового электромагнитного воздействия; 5.2 Преднамеренного силового воздействия различной физической природы; 5..3 Использования программных или программно-аппаратных средств при осуществлении: 1) компьютерной атаки; 2) сетевой атаки 5.4 Воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

7

10.2 ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ СО СТОРОНЫ СУБЪЕКТИВНЫХ ИСТОЧНИКОВ

СУБЪЕКТИВНЫЕ, ВНЕШНИЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СПОСОБЫ ИХ РЕАЛИЗАЦИИ (классификация)

Доступ к информации ограниченного доступа с применением технических средств разведки.

Способы доступа зависят от применяемых средств технической разведки. Они основаны на том, что технические средства обработки информации имеют уязвимости. Такими уязвимостями являются излучения технических средств обработки и обеспечения объекта информатизации, создающие информативные физические поля:

- излучения, функционально присущие объекту информатизации;
- побочные электромагнитные излучения,
- паразитные излучения;
- наводки в цепях электропитания, заземления и т.п.

Искажение, уничтожение или блокирование информации с применением технических средств путём преднамеренного силового электромагнитного воздействия может осуществляться:

1) по сети электропитания на порты электропитания постоянного и переменного тока;
2) по проводным линиям связи на порты ввода-вывода сигналов и порты связи;
3) по металлоконструкциям на порты заземления и порты корпуса;
4) посредством электромагнитного быстроизменяющегося поля на порты корпуса, порты ввода-вывода сигналов и порты связи.

Преднамеренное силовое электромагнитное воздействие на информацию - несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем.

8

10.3 УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

КЛАССЫ УЯЗВИМОСТЕЙ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ И ИХ ХАРАКТЕРИСТИКА

Класс уязвимостей	Зависимость	Возможности по устранению
Объективные	Зависят от особенностей построения и технических характеристик оборудования ОИ	Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами защиты информации
Субъективные	Зависят от действий сотрудников	В основном устраняются организационными и программно-аппаратными методами
Случайные	Зависят от особеннос-тей окружающей защи-щаемый ОИ среды, и непредвиденных обстоятельств	Как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам

9

10.3 УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

ОБЪЕКТИВНЫЕ УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

Факторами, обуславливающими появление информативных физических полей и объективных уязвимостей являются:

- ✓ **передача сигналов по проводным линиям связи;**
- ✓ **передача сигналов по оптико-волоконным линиям связи;**
- ✓ **передача сигналов в диапазоне радиоволн и в оптическом диапазоне длин волн;**
- ✓ **излучения сигналов, функционально присущие техническим средствам (устройствам) объекта информатизации;**
- ✓ **побочные электромагнитные излучения (ПЭМИ);**
- ✓ **паразитное электромагнитное излучение;**
- ✓ **наводки;**
- ✓ **наличие акустоэлектрических преобразований в элементах технических средств объекта информатизации.**

ПЭМИ – это излучение, присущее работе технических средств и не предназначенное для их функционирования. Несут информативный сигнал.

Выделяется две подгруппы ПЭМИ:

ПЭМИ сигналов (видеоимпульсов) от информационных цепей. Например -монитор ПК;

ПЭМИ сигналов (радиоимпульсов) от всех электрических цепей технических средств ОИ.

Наводки. *Наводки:* токи и напряжения в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями. Выделяют две подгруппы наводок:

1) наводки в электрических цепях технических средств, имеющих выход за пределы ОИ (цепи электропитания, цепи заземления, линии связи)

2) наводки на технические средства, провода, кабели и иные токопроводящие коммуникации и конструкции, гальванически не связанные с техническими средствами ОИ, вызванные ПЭМИ, несущими ЗИ.

10

10.3 УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

КЛАССИФИКАЦИЯ ОБЪЕКТИВНЫХ УЯЗВИМОСТЕЙ.

Группа уязвимостей	Подгруппа	Слабость, недостаток, элемент обуславливающий уязвимость
Сопутствующие техническим средствам излучения	Электромагнитные	1) ПЭМИ технических средств, 2) ПЭМИ кабельных линий ТС 3) излучения на частотах работы генераторов, 4) излучения на частотах самовозбуждения усилителей
	Электрические	1) наводки ЭМИ на линии и проводники 2) просачивание сигналов в цепи электропитания и заземления 3) неравномерность потребления тока электропитания
	Звуковые	1) акустические, 2) виброакустические
Активизируемые	Аппаратные закладки устанавливаемые	1) в телефонные линии 2) в сети электропитания, 3) в помещениях, 4) в технических средствах
	Программные закладки	1) вредоносные программы, 2) технологические выходы из программ, 3) нелегальные копии ПО
Определяемые особенностями элементов	Элементы обладающие электроакустическими преобразованиями	1) телефонные аппараты, 2) громкоговорители и микрофоны 3) катушки индуктивности, 4) дроссели, трансформаторы и пр.
	Элементы подверженные воздействию электромагнитного поля	1) магнитные носители, 2) микросхемы, 3) нелинейные элементы подверженные ВЧ навязыванию
Определяемые особенностями защищаемого объекта	Местоположением объекта	1) отсутствие контролируемой зоны, 2) наличие прямой видимости объектов, 3) наличие удалённых и мобильных элементов объекта 4) наличие вибрирующих отражающих поверхностей
	Организацией каналов обмена информацией	1) использование радиоканалов, 2) глобальных информационных сетей, 3) арендуемых каналов

11

10.3 УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

КЛАССИФИКАЦИЯ СУБЪЕКТИВНЫХ УЯЗВИМОСТЕЙ.

Группа Уязвимостей	Подгруппа	Слабость, недостаток, элемент обуславливающий уязвимость
Ошибки	**При подготовке и использовании программного обеспечения**	1) при разработке алгоритмов и ПО 2) при инсталляции и загрузке ПО 3) при эксплуатации ПО 4) при вводе данных
	При управлении сложными системами	1) при использовании возможностей самообучения систем 2) настройке сервисов универсальных систем 3) организации управления потоками обмена информацией
	При эксплуатации ТС	1) при включении/выключении ТС 2) при использовании техн-х средств охраны 3) при использовании средств обмена информацией
Нарушения	**Режима охраны и защиты**	1) доступа на объект 2) доступа к техническим средствам (ИС)
	Режима эксплуатации ТС	1) энергообеспечения 2) жизнеобеспечения
	Режима использования информации	1) обработки и обмена информацией 2) хранения и уничтожения носителей информации 3) уничтожение производственных отходов и брака

12

10.3 УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

КЛАССИФИКАЦИЯ СЛУЧАЙНЫХ УЯЗВИМОСТЕЙ.

Группа Уязвимостей	Подгруппа	Слабость, недостаток, элемент обуславливающий уязвимость
Сбои и отказы	**Отказы и неисправности технических средств**	1) обрабатывающих информацию 2) обеспечивающих работоспособность средств обработки информации 3) обеспечивающих охрану и контроль доступа
	Старение и размагничивание носителей информации	1) дискет и съёмных носителей 2) жёстких дисков 3) элементов микросхем 4) кабелей и соединительных линий
	Сбои программного обеспечения	1) ОС и СУБД 2) прикладных программ 3) сервисных программ, 4) антивирусных программ
	Сбои электроснабжения	1) оборудования, обрабатывающего информацию 2) обеспечивающего и вспомогательного оборудования
Повреждения	**Жизнеобеспечивающих коммуникаций**	1) электро -, водо-, газо-,теплоснабжения, канализации 2) кондиционирования и вентиляции
	Ограждающих конструкций	1) внешних ограждений территорий 2) стен и перекрытий зданий 3) корпусов технологического оборудования

Тема 11
КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И МЕТОДЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

ВОПРОСЫ:

11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

11.2 МЕТОДЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ КАНАЛОВ

11.3 НЕФОРМАЛЬНАЯ МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ АС

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .- Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Источники указанные в Методических рекомендациях к курсу.

1

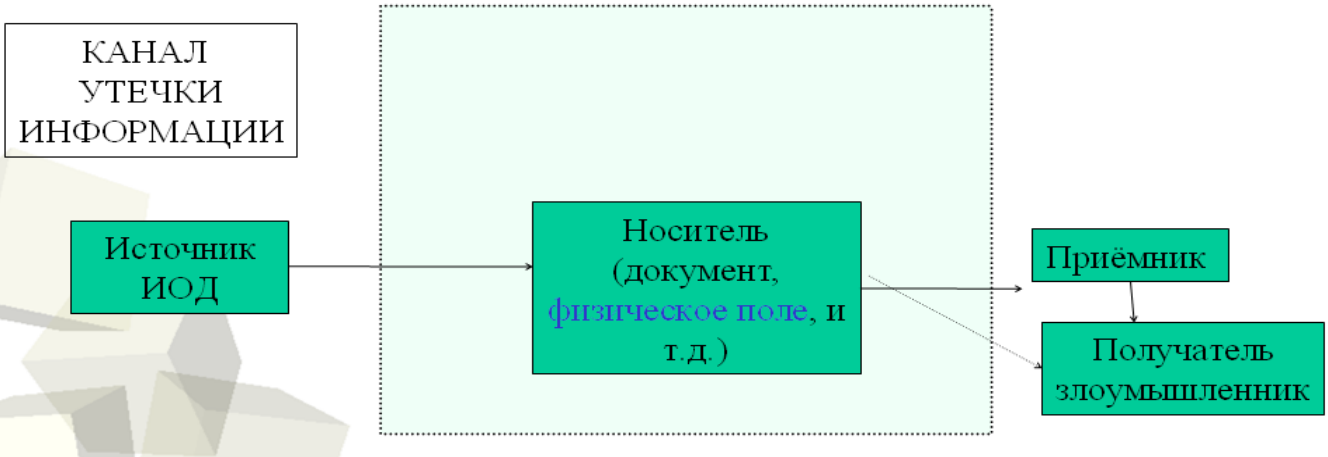
11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

ПОНЯТИЕ КАНАЛА УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Канал – это маршрут передачи информации.

Канал утечки информации - неконтролируемый физический путь от источника информации ограниченного доступа за пределы организации или круга лиц, обладающих охраняемыми сведениями, или за пределы объекта информатизации, посредством которого возможно неправомерное овладение злоумышленниками конфиденциальной (секретной) информацией.

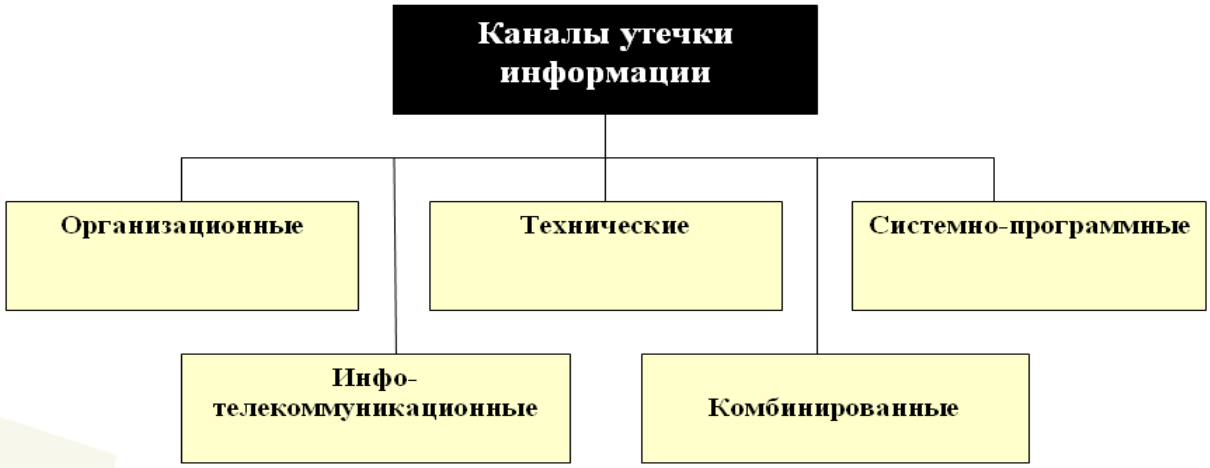
Канал утечки информации имеет смысл только для информации ограниченного доступа!



2

11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

ОБЩАЯ КЛАССИФИКАЦИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ



3

11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

ОРГАНИЗАЦИОННЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Специально создаваемые злоумышленником каналы на основе коммуникационных каналов передачи информации или ошибки персонала – обуславливают существование угроз путём реализации субъективными источниками различных методов

Источники ИОД	Организационные каналы передачи ИОД	Методы НСД
- персонал допущенный к ИОД **- носители** ИОД; **- ТСОИ** (экраны, мониторы и т.п) ИОД; **- средства коммуникации** для передачи ИОД (почта, секретная почта); **- передаваемые сообщения** содержащие ИОД (связь и т.п.)	-конфиденциальное (секретное) делопроизводство; -совместные работы с другими организациями с использованием ИОД; - совещания (конфиденциального характера) - рекламная и публикаторская деятельность; - мероприятия в области сотрудничества с иностранными предприятиями; - передача сведений в территориальные инспекторские и надзорные органы	**1. Несанкционированный физический доступ на ОИ и к ИОД:** 1.1 преодоление рубежей территориальной защиты обманным путём и доступ к незащищенным ИР; 1.2 хищение документов и носителей информации; 1.3 визуальный перехват информации, выводимой на экраны мониторов и принтеры, а также подслушивание. **2. Внедрение агентов в организацию (агентурная разведка)** **3. Вербовка персонала, путём подкупа, шантажа, угроз** (конкурентами, разведками) **4. Выпытывание, выведывание**

4

11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

ОРГАНИЗАЦИОННЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Специально создаваемые злоумышленником каналы на основе коммуникационных каналов передачи информации или ошибки персонала – обуславливают существование угроз путём реализации субъективными источниками различных методов

Методы НСД	Методы выявления
1. Несанкционированный физический доступ на ОИ и к ИОД: 1.1 преодоление рубежей территориальной защиты обманным путём и доступ к незащищенным ИР; 1.2 хищение документов и носителей информации; 1.3 визуальный перехват информации, выводимой на экраны мониторов и принтеры, а также подслушивание.	- Анализ территориального расположения зданий и помещений предприятия - Анализ наличия и качества рубежей территориальной защиты, контролируемых зон (зон безопасности), их периметра, наличия и качества средств предотвращения несанкционированного физического доступа на территорию, в контролируемые зоны, помещения (двери, окна, замки, сигнализация, видеонаблюдение, СКУД и т.п.). -Анализ наличия и качества хранилищ носителей ИОД - Анализ пропускного режима и нормативных и методических документов по обеспечению этого режима и режима доступа к ИОД и носителям ИОД
2. Внедрение агентов в организацию (агентурная разведка)	- взаимодействие и получение информации из органов правопорядка и обеспечения безопасности в РФ - анализ документов и деятельности сотрудников во взаимодействии с отделом кадров предприятия и службы безопасности - аналитическая работа с персоналом (специальное тестирование, беседы, детектор лжи и т.п.)
3. Вербовка персонала, путём подкупа, шантажа, угроз (конкурентами, разведками)	
4. Выпытывание, выведывание	

11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Технический канал утечки информации - совокупность источника информации, материального носителя или среды распространения несущего конфиденциальную информацию сигнала и средства выделения информации из сигнала или носителя.

Классификация технических каналов утечки информации	
1. Радиоэлектронный (электромагнитный) канал	носителем информации являются электрические, магнитные и электромагнитные поля в **радиодиапазоне**, за счёт излучений функционально присущих ОИ, ПЭМИ а также наводок.
2.Акустический канал	Носителем информации являются механические упругие акустические волны в инфразвуковом (менее 16Гц), звуковом (16Гц-20КГц) и ультразвуковом (свыше 20кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твёрдой среде. **виброакустический и акустоэлектрический**.
3. Оптический (визуально – оптический) канал	Носителем информации является электромагнитное поле в диапазоне 0.46-0.76мкм (видимый свет) и 0.76-13мкм (инфракрасные излучения). Позволяет осуществить доступ с использованием средств **визуально – оптической, фотографической, оптико - электронной разведки**.
4. Материально – вещественный канал.	Носителем информации являются материалы и вещества (твёрдые, жидкие, газообразные) которые в виде отходов или некачественных промежуточных продуктов бесконтрольно могут попасть за пределы контролируемой (охраняемой) зоны.

11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

МЕТОДЫ НСД С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ

ТКУИ	Методы НСД
1. Радиоэлектронный (электромагнитный) канал	Доступ с использованием средств РЭР (СНПИ) к радиоканалам организации предназначенным для передачи информации и её перехват Перехват с использованием средств РЭР (СНПИ) **ПЭМИ** и выделение из них полезного сигнала несущего ИОД без проникновения в КЗ. Подключение к техническим средствам и системам за пределами КЗ выделение сигнала из **наводок** на сети электропитания, заземления и т.п. и получение ИОД
2.Акустический канал	Перехват акустических и электроакустических сигналов с использованием специальных средств (СНПИ) без проникновения в КЗ Использование закладочных устройств в контролируемой зоне (микрофоны, диктофоны, магнитофоны, радиомикрофоны и т.п.) изготовленными специально для ведения разведки
3. Оптический (визуально – оптический) канал	Видеонаблюдение с использованием средств оптической и оптико-электронной разведки без проникновения в КЗ Использование закладочных устройств в контролируемой зоне (скрыто устанавливаемые фото и видеокамеры с выходным отверстием объектива несколько мм и др. изготовленными специально для ведения разведки и позволяющих как делать запись так и передавать по каналу видеосигнал
4. Материально – вещественный канал.	Добывание материалов и веществ, которые в виде отходов или некачественных промежуточных продуктов бесконтрольно могут попасть за пределы контролируемой (охраняемой) зоны, некачественно уничтоженных бумажных, фото и других носителей в виде черновиков и т.п.

11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

ИНФО – ТЕЛЕКОММУНИКАЦИОННЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Инфо – телекоммуникационные каналы утечки информации
Каналы носителем информации в которых являются сообщения «пакеты» передаваемые помощью специальных протоколов (Интернет - протоколы) на сетевом и транспортном уровнях (III-IV) взаимодействия открытых систем (ВОС) международного стандарта модели ISO/OSI.. (протоколы TCP/IP).

МЕТОДЫ НСД

подключение к ИТКС с использованием которой осуществляется обмен ЗИ	**перехват передаваемых по сети сообщений** («пакетов») путём подключения к ИТКС, выходящей за пределы КЗ, компьютера (ноутбука), и использование стандартного ПО для получения информации (ИОД)
	перехват передаваемых по сети сообщений («пакетов») путём подключения к к ИТКС, выходящей за пределы КЗ компьютера (ноутбука), и использование специального ПО («снифферов», криптоанализаторов для расшифровки специальных протоколов (IPsec и др.))
	доступ к компьютеру сети, выполняющему функции маршрутизации и получение ЗИ теми же методами;
	внедрение в сеть несанкционированного маршрутизатора с перенаправлением через него потока сообщений на компьютер злоумышленника и получение ЗИ.

11.1 КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

СИСТЕМНО – ПРОГРАММНЫЙ (С-П) КАНАЛ УТЕЧКИ ИНФОРИАЦИИ

Системно - программный канал
- канал, перенос информации в котором, осуществляется с использованием программ (программных кодов) средств на V – VII уровнях модели ВОС. Выделение такого канала в самостоятельный, позволяет рассматривать множество угроз с использованием программных средств **(канал общесистемного и прикладного ПО).**

МЕТОДЫ НСД С ИСПОЛЬЗОВАНИЕМ С-П КАНАЛА

«Маскировка под зарегистрированного пользователя»;	Маскировка под зарегистрированного пользователя осуществляется путем похищения паролей и других реквизитов разграничения доступа к информации, используемой в системах обработки (АС). В этом случае пользователь присваивает себе каким - либо образом полномочия другого пользователя выдавая себя за него.
Использование дефектов программного обеспечения	- наличие средств отладки и тестирования в конечных продуктах; -«чёрные ходы», « люки», скрытые возможности проникновения в компьютерную сеть;
Использование программных закладок;	Внедрение закладки в компьютерную систему может выполняться : - с помощью аппаратных средств, - через электронные документы; - с помощью обычных программ; - с помощью мобильных программ; по вирусной технологии.
Применение программных вирусов.	Вирус рассылается через сеть.

11.3 НЕФОРМАЛЬНАЯ МОДЕЛЬ НАРУШИТЕЛЯ АС

Уровень	Уровень знаний об АС	Уровень возможностей	Способ НСД (атаки)
1	Знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами	Запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации	Непосредственное обращение к объектам доступа;
2	Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;	Возможность создания и запуска собственных программ с новыми функциями по обработке информации.	Создание програм-х и техн-х средств, выполняющих обращение к объектам доступа в обход средств защиты;
3	Обладает высоким уровнем знаний в области програм-я и ВТ, проектирования и эксплуатации АС;	Возможность управления функционированием АС, т.е. воздействием на базовое ПО системы и на состав и конфигурацию ее оборудования.	Модификация средств защиты, позволяющая осуществить НСД;
4	Знает структуру, функ Ции и механизм действия средств защиты, их сильные и слабые стороны.	Весь объем возможностей лиц, осуществл-их проектирование, реализацию и ремонт техн-х средств АС, вплоть до включения в состав СВТ собственных техн-х средств с новы-ми функциями по обработке инф-ции	Внедрение в СВТ или АС прогр-ых или техн-их меха низмов, нарушающих предполагаемую структуру и функции СВТ или АС и позво ляющих осуществить НСД.

Тема 12

НАПРАВЛЕНИЯ, ВИДЫ И ОСОБЕННОСТИ ДЕЯТЕЛЬНОСТИ РАЗВЕДЫВАТЕЛЬНЫХ СЛУЖБ ПО НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ВОПРОСЫ:

12.1 ГОСУДАРСТВЕННЫЕ РАЗВЕДЫВАТЕЛЬНЫЕ СЛУЖБЫ ЗАРУБЕЖНЫХ СТРАН

12.2 СТРУКТУРА РАЗВЕДЫВАТЕЛЬНЫХ СЛУЖБ ЧАСТНЫХ ОБЪЕДИНЕНИЙ

12.3 НАПРАВЛЕНИЯ И ВИДЫ РАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

12.4 СПОСОБЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ АГЕНТУРНОЙ РАЗВЕДКИ

12.5 КОМПЬЮТЕРНАЯ РАЗВЕДКА

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .– Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Источники указанные в Методических рекомендациях к курсу.

1

12.1 ГОСУДАРСТВЕННЫЕ РАЗВЕДЫВАТЕЛЬНЫЕ СЛУЖБЫЗАРУБЕЖНЫХ СТРАН

Жизненная необходимость в информации для любой государственной или коммерческой структур вынуждает их расходовать людские, материальные и финансовые ресурсы на ее постоянное добывание. Так как любую работу эффективнее выполняют профессионалы, то эти структуры создают специализированные органы, предназначенные для добывания информации. Такими органами являются органы разведки.

США

В разведывательное сообщество США входят 16 структур

1.Центральное разведывательное управление -**ЦРУ**
(ЦРУ, подчиняется NIC -национальный совет по разведке).
2. Разведывательные организации Министерства обороны США.
3. Разведывательные организации, входящие в гражданские ведомства США.
4. Штаб разведки разведывательного сообщества или Центральная разведка.
5. Министерство внутренней безопасности (против терроризма)

ИЗРАИЛЬ

- «Моссад (служба секретной разведки)
- АМАН
.Шин Бет.

ВЕЛИКОБРИТАНИЯ

MI6 - главная разведывательная служба Великобритании
MI5 - контрразведка Соединенного Королевства

ТУРЦИЯ

Национальная разведывательная организация Турции (MIT)

КИТАЙ

Все отделения спецслужб называются **"Бюро".**
2-е бюро– зарубежные операции,
6- контрразведка, 11 –е РЭР и компьютерная безопасность.
Остальные бюро занимаются определенным регионом, специфической деятельностью или сбором информации.

ЯПОНИЯ

Службы по сбору и анализу информации о зарубежных странах имеются в Минобороны, в полиции

2

12.1 ГОСУДАРСТВЕННЫЕ РАЗВЕДЫВАТЕЛЬНЫЕ СЛУЖБЫЗАРУБЕЖНЫХ СТРАН

ЗАДАЧАМИ РАЗВЕДКИ ЯВЛЯЮТСЯ СБОР И ПОСЛЕДУЮЩАЯ ОБРАБОТКА СВЕДЕНИЙ:

1. В военной и оборонной сферах других государств (вероятных противников, конкурентов)
- о содержании стратегических и оперативных планов вооруженных сил, их боеспособности и мобилизационной готовности, о создании и использовании мобилизационных ресурсов;
- о направлениях развития вооружения и военной техники, научно-исследовательских и опытно-конструкторских работах по созданию и модернизации образцов вооружения и военной техники;
- о количестве, устройстве и технологии производства ядерного и специального оружия;
- о тактико-технических характеристиках и возможностях боевого применения вооружения и военной техники;
- о дислокации, численности и технической оснащенности войск и сил флота;
- о степени подготовки территории страны к ведению боевых действий;
- об объемах поставок и запасах стратегических видов сырья и материальных ресурсов;
- о функционировании промышленности, транспорта и связи;
- об объемах, планах государственного оборонного заказа, выпуске и поставках вооружения, военной техники и другой оборонной продукции;

2. О научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение;

3. О сельском хозяйстве, финансах, торговле;

4 О внешнеполитической и внешнеэкономической деятельности государства;

5. О системе правительственной и иных видов специальной связи, о государственных шифрах;

6. О выполнении условий международных договоров. Прежде всего, об ограничении вооружений и др.

3

12.2 СТРУКТУРА РАЗВЕДЫВАТЕЛЬНЫХ СЛУЖБ ЧАСТНЫХ ОБЪЕДИНЕНИЙ

Разведка коммерческих структур (коммерческая разведка) добывает информацию в интересах их успешной деятельности на рынке в условиях острой конкурентной борьбы. Задачи органов коммерческой разведки, их состав и возможности зависят от назначения и капитала фирмы, но принципы добывания информации су-щественно не отличаются от государственных разведок.

Основными областями, представляющими интерес для коммерческой разведки, являются:

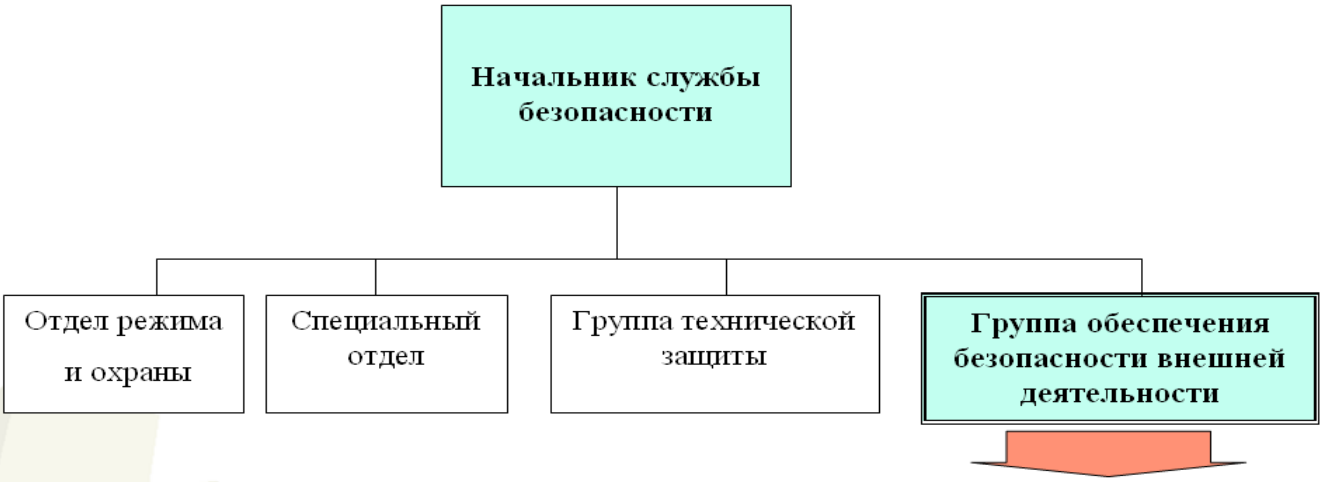
- коммерческая философия и деловая стратегия руководителей фирм-конкурентов. их личные и деловые качества;
- научно-исследовательские и конструкторские работы;
- финансовые операции фирм;
- организация производства, в том числе данные о вводе в строй новых, расширении и модернизации существующих производственных мощностей, объединение с другими фирмами;
- технологические процессы при производстве новой продукции, резуль-таты ее испытаний;
- маркетинг фирмы, в том числе режимы поставок, сведения о заказчиках и заключаемых сделках, показатели реализации продукции.

Кроме того, коммерческая разведка занимается

- изучением и выявлением организаций, потенциально являющихся союзниками или конкурентами;
- добыванием, сбором и обработкой сведений о деятельности потенциальных и реальных конкурентов:
- учетом и анализом попыток несанкционированного получения коммерческих секретов конкурентами;
- оценкой реальных отношений между сотрудничающими и конкурирующими организациями:
- анализом возможных каналов утечки конфиденциальной информации.

12.2 СТРУКТУРА РАЗВЕДЫВАТЕЛЬНЫХ СЛУЖБ ЧАСТНЫХ ОБЪЕДИНЕНИЙ

Органы коммерческой разведки входят в состав в службы безопасности организации



добыванием информации о конкуренте занимается группа обеспечения внешней деятельности организации

функции системы добывания информации могут быть реализованы одним или несколькими работникам службы безопасности малочисленной фирмы

5

12.3 НАПРАВЛЕНИЯ И ВИДЫ РАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

НАПРАВЛЕНИЯ РАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Агентурная разведка

является наиболее древним и традиционным видом разведки. Добывание информации производится путем проникновения агента - разведчика к источнику информации на расстояние доступности его органов чувств или используемых им технических средств, копирования ин-формации и передачи ее потребителю.

Техническая разведка

Применение **технической разведки** снижает риск задержания агента органами контрразведки или службы безопасности, за счет дистанционного контакта его с источником информации, а также создаёт возможность ведения разведки без нарушения государственной границы средствами космической, воздушной, компьютерной разведки иностранных государств.

Разведки иностранных государств

заинтересованы в первую очередь в получении <u>сведений, составляющих государственную тайну</u>

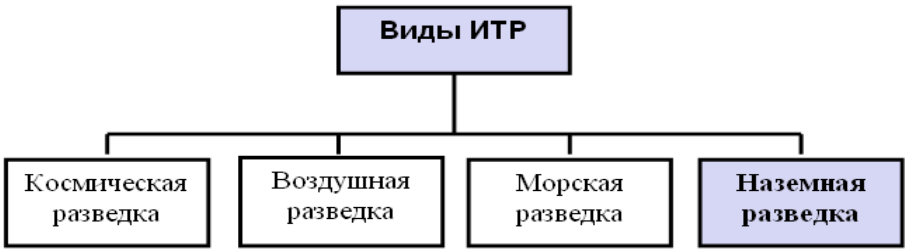
Разведки Коммерческих структур

Разведки коммерческих структур и криминальные структуры в первую очередь заинтересованы в сведениях составляющих <u>коммерческую тайну и персональные данные</u>.

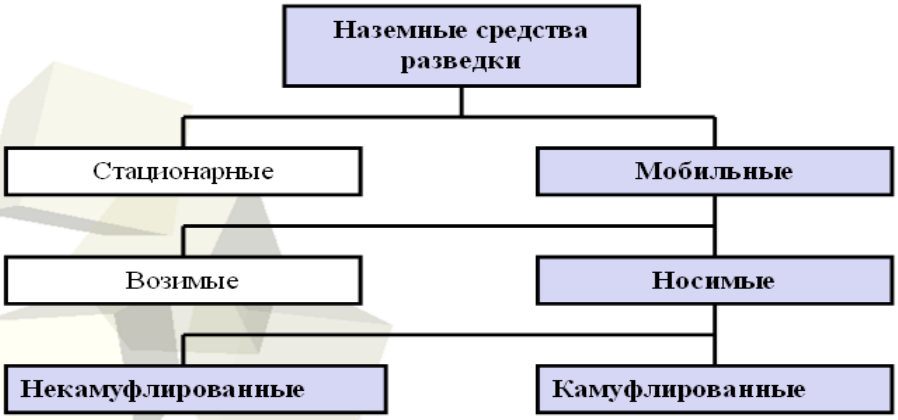
6

12.3 НАПРАВЛЕНИЯ И ВИДЫ РАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

ИНОСТРАННАЯ ТЕХНИЧЕСКАЯ РАЗВЕДКА (ИТР)



Основной целью ИТР является обеспечение высшего политического руководства своего государства своевременной информацией по разведываемой стране, по ее Вооруженным Силам (ВС), по военно-экономическому потенциалу и др. в соотв. с задачами



Криминальные структуры и разведки частных объединений (коммерческие разведки) используют такие же средства наземной разведки как ИТР, как иностранного производства, так и Российского.

7

12.4 СПОСОБЫ ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ АГЕНТУРНОЙ РАЗВЕДКИ

Способы доступа к КИ агентурной разведкой

Физическое проникновение к источнику информации

(на объект)

- скрытое проникновение;
- с применением силы;
- внедрение в штат сотрудников

Способ проникновения зависит от вида информации и способов ее использования.

Сотрудничество с сотрудником, имеющим доступ к КИ

- инициативное сотрудничество;
- подкуп (вербовка);
- сотрудничество под угрозой

предполагает привлечение людей, которые ищут контакты с разведкой зарубежного государства или конкурента, к сотрудничеству с целью добывания секретной или конфиденциальной информации по месту работы.

Выпытывание

- скрытое выпытывание;
- выпытывание под пыткой.

скрытое выпытывание может быть в устной или письменной форме при фиктивном найме сотрудника конкурирующей фирмы на более высокооплачиваемую или интересную работу, на конференциях и др. Выпытывание под пыткой характерно для криминальных элементов

8

12.5 КОМПЬЮТЕРНАЯ РАЗВЕДКА

КОМПЬЮТЕРНАЯ РАЗВЕДКА
– целенаправленная деятельность по добыванию с помощью СВТ и ПО разведывательной информации, обрабатываемой в информационно-вычислительных сетях и (или) СВТ, а так же информации об особенностях их построения и функционирования.

Цель компьютерной разведки
добывание сведений о предмете, конечных результатах, формах и способах деятельности субъектов, являющихся пользователями ИТКС и АС (ИС) и используемом аппаратном и программном обеспечении, протоколах управления и информационного взаимодействия и используемых средствах и методах защиты информации.

Компьютерная (виртуальная) разведка включает в себя три основных направления:
1. Разведку в ИТКС и АС(ИС).
2. Разведку в бумажных и электронных СМИ.
3. Разведку в непериодических изданиях, в том числе, в открытых и т.н. «серых» (т.е. не имеющих грифа секретности, но не предназначенных для массового распространения - отчетах о НИР, аналитических справках, деловой переписке, диссертациях и т.п.).

Компьютерную разведку разделяют на: **добывающую (предварительную и непосредственную) и обрабатывающую**.

9

12.5 КОМПЬЮТЕРНАЯ РАЗВЕДКА

ДОБЫВАЮЩАЯ КОМПЬЮТЕРНАЯ РАЗВЕДКА

Цели **предварительной** разведки достигаются путем добывания **открытых** и **закрытых** сведений.

Открытые :
-о характере и режиме работы АС объекта разведки;
-квалификации его персонала;
-составе и структуре самой АС,
-используемом ПО;
протоколах управления и взаимодействия;
средствах и методах защиты информации, используемых в АС.

Важнейшим достоинством перехвата открытых сведений при ведении компьютерной разведки является то, что эти сведения могут быть получены без нарушения принятых в АС правил разграничения доступа к информации.

Добывание закрытых сведений

Во внешних ИТКС
- Чтение электронной почты
- Изменение маршрутизации
- Фальсификация сервера-адресата

В АС (ИС) объекта
- Внедрение в АС объекта ПО с недекларированными возможностями
- Проникновение в АС объекта из внешних сетей через сетевые периферийные устройства
- Проникновение в АСОД объекта через несетевые периферийные устройства

К таким (закрытым) сведениям относятся:
- пароли, коды доступа,
-информация о принятых в АС ПРД,
- сетевые адреса вычислительных средств противника.

ДОБЫВАЮЩАЯ КОМПЬЮТЕРНАЯ РАЗВЕДКА

1. ДОБЫВАНИЕ ЗАКРЫТЫХ СВЕДЕНИЙ ВО ВНЕШНИХ СЕТЯХ (в общедоступных ИТКС, ИТКС международного информационного обмена (Интернет))

Можно выделить следующие способы перехвата закрытых сведений во внешних сетях:

1. Изменение маршрутизации при пересылке сообщений, что позволяет отправлять информацию через «свой» сервер, на котором производится перехват и запись данных;

2. Чтение электронной почты, которая как правило является легкой добычей и на сервере отправителя, и на сервере получателя;

3. Фальсификация сервера-адресата, что в случае успеха позволяет выманить у отправителя ту или иную закрытую информацию.

2.ПРОНИКНОВЕНИЕ ИЗ ВНЕШНИХ СЕТЕЙ

Проникновение из внешних сетей.
Можно выделить два основных пути такого проникно-вения:
1.Проникновение с использованием паролей и идентификаторов, найденных в результате предварительной разведки;
2. поиск ошибок (т.н. «люков», «черных ходов», «лазеек») в программном обеспечении, исполь-зуемом в АС;

3. КРИПТОАНАЛИЗ

С помощью средств компьютерной разведки можно не только анализировать конкретные данные, циркулирующие во всей сети, безотноси-тельно к их источнику, но и отслеживать деятельность конкретных организаций и отдельных лиц

Тема 13

ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

ВОПРОСЫ:

13.1 ПОНЯТИЕ И КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ

13.2 ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ

13.3 ПОМЕЩЕНИЯ, В КОТОРЫХ УСТАНОВЛЕНЫ СРЕДСТВА ОБРАБОТКИ И ПОМЕЩЕНИЯ ДЛЯ КОНФИДЕНЦИАЛЬНЫХ ПЕРЕГОВОРОВ КАК ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Литература

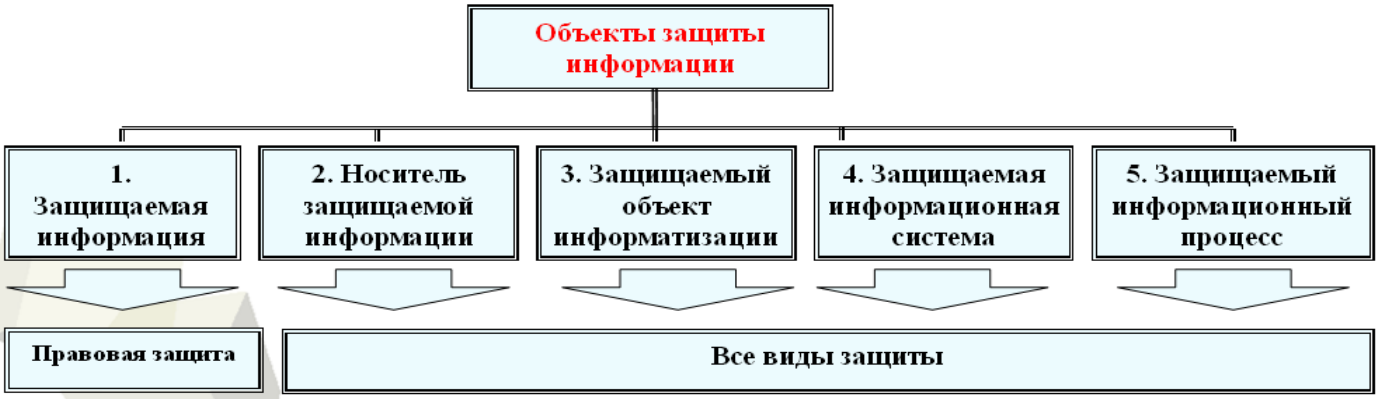
1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .- Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Источники указанные в Методических рекомендациях к курсу.

1

13.1 ПОНЯТИЕ И КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ

ОБЪЕКТ - любая часть, элемент, устройство, подсистема, функциональная единица, аппаратура или система, которые можно рассматривать в отдельности (Международный стандарт CEI IEC 50 (191). Надежность и качество услуг).

Объект защиты информации:
Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.



К объектам защиты информации (физической и организационной) могут быть отнесены:
- контролируемая зона (охраняемая территория, здание (сооружение)),
- выделенное помещение,
- информация и (или) информационные ресурсы объекта информатизации.

13.1 ПОНЯТИЕ И КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ

Защищаемый объект информатиза-ции (ЗОИ)

Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.
объект информатизации это:
совокупность: а) информационных ресурсов, б) средств и систем обработки информации, используемых в соответствии с заданной ИТ, в) средств обеспечения объекта информатизации, г) помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или **помещения и объекты, предназначенные для ведения конфиденциаль-ных переговоров**
(ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию)

Защищаемая информацион ная система (ЗИС)

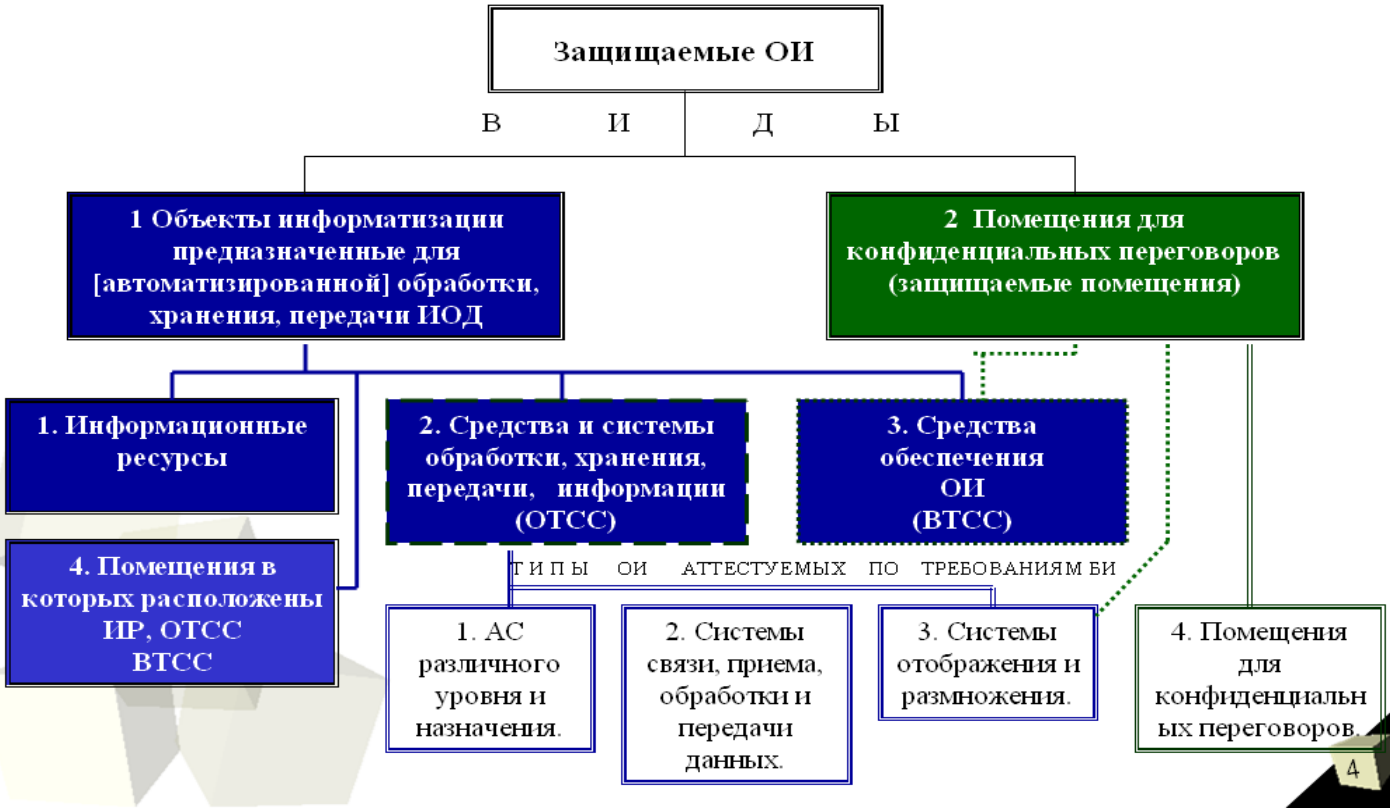
Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.
Информационная система:
Совокупность содержащейся в БД информации и обеспечивающих ее обработку ИТ и технических средств.
При аттестации по требованиям безопасности составляет основу АС

Защищаемые информацион ные процессы (ЗИП)

процессы обработки информации с использованием информационных технологий и технических средств в защищаемых ИС и на защищаемых ОИ.
Обработка информации
- совокупность операций сбора, накопления, ввода, вывода, приема, передачи, тиражирования, записи, хранения, регистрации, уничтожения, преобразования, отображения информации

13.2 ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ

КЛАССИФИКАЦИЯ ЗАЩИЩАЕМЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ



13.2 ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ

СРЕДСТВА И СИСТЕМЫ ОБРАБОТКИ, ХРАНЕНИЯ, ПЕРЕДАЧИ ИНФОРМАЦИИ (ОТСС)

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной (секретной) информации

1. АС различного уровня и назначения

(IT-система)

Создаются на базе средств вычислительной техники СВТ (ПЭВМ) и информационных технологий (ПО), которые в свою очередь являются самостоятельными объектами защиты:
- технические элементы систем обработки данных (аппаратная платформа);
- операционные системы (ОС семейства Windows , NetWare, UNIX и т.п),
- СУБД (Oracle, Microsoft SQL Server, Informix и др.);
- программное обеспечение (электронный документооборот, справочные системы, электронная бухгалтерия, а также мобильные программы (JAVA, JavaScript, VBScript) и данные (конфиденциальные и др);
Сертифицируются как защищённые СВТ по стандартам защиты для СВТ или по стандартам для безопасности информационных технологий.

2. Системы связи, приема, обработки и передачи данных.

Системы телефонии, переговорные и телевизионные устройства и другие ТС обработки речевой, графической, видео, смысловой и буквенно - цифровой информации (аттестуются по требованием безопасности информации на основе криптографических и др. сертифицированных средств защиты).

3. Системы отображения и размножения.

Системы звукозаписи, звукоусиления, звуковоспроизведения, телевизионные устройства, мультимедиа, проекционное оборудование, средства изготовления, тиражирования документов

13.2 ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ

Средства обеспечения ОИ (ВТСС)

3.1 ВТСС вспомогательные технические системы и средства

- технические средства и системы, не предназначенные для передачи, обработки и хранения ИОД, устанавливаемые совместно с ОТСС или в защищаемых (выделенных) помещениях. К ВТСС относятся:
- различного рода телефонные средства и системы;
- средства и системы передачи данных в системе радиосвязи;
- средства и системы охранной и пожарной сигнализации;
- средства и системы оповещения и сигнализации;
- контрольно-измерительная аппаратура;
- средства и системы кондиционирования;
- средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (телевизоры и радиоприемники и т.д.);
- средства электронной оргтехники;
- средства и системы электрочасофикации;
- иные технические средства и системы.

3.2 Системы электропитания и заземления

Системы электропитания;
Системы заземления

Системы отопления
Канализация
Турникеты
другие

13.3 ПОМЕЩЕНИЯ, В КОТОРЫХ УСТАНОВЛЕНЫ СРЕДСТВА ОБРАБОТКИ И ПОМЕЩЕНИЯ ДЛЯ КОНФИДЕНЦИАЛЬНЫХ ПЕРЕГОВОРОВ КАК ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Требования по защищённости помещений, как объектов защиты определены в нормативных документах Гостехкомиссии России: СТР 97 для ОИ на которых обрабатывается ГТ, СТР-К-2001 для конфиденциальной информации.

Помещения, в которых установлены средства обработки и обеспечения объекта информатизации как объекты защиты характеризуются расположением в здании (этаж) или на территории предприятия, наличием окон, дверей, прохождением систем тепло и водоснабжения, вентиляции.

На защищённость информации будет влиять, например, расположение офиса фирмы в смежном (через стену) помещении с другой фирмой, в том случае когда в одном здании сдаются в аренду помещения различным фирмам.
Материал, из которого сделаны стены, может обладать высокими акустическими свойствами.
Расположение окон. Например, окна могут выходить на улицу на противоположной стороне которой, расположено здание, из которого возможно наблюдение и съём информации с помощью бинокля с экранов мониторов.

К помещениям по всем указанным параметрам предъявляются соответствующие требования: по звукоизоляции помещений, затенению стёкол или установку жалюзи, установку металлических решёток на окна, систем контроля и управления доступа в помещения (СКУД) и другие мероприятия и средства.

7

13.3 ПОМЕЩЕНИЯ, В КОТОРЫХ УСТАНОВЛЕНЫ СРЕДСТВА ОБРАБОТКИ И ПОМЕЩЕНИЯ ДЛЯ КОНФИДЕНЦИАЛЬНЫХ ПЕРЕГОВОРОВ КАК ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

При аттестации помещений на защищённость по требованиям безопасности информации им присваивается соответствующая категория, в зависимости от степени секретности обрабатываемой и хранимой информации. Если в помещении хранится информация, составляющая государственную тайну, помещение аттестуется как режимный объект. Для помещений установлены категории: 1 категория - "ОВ"; 2 категория - "СС"; 3 категория - "С". Если на объекте не хранится секретная информация (помещение для конфиденциальных переговоров, совещаний), он аттестуется как выделенное помещение.

Контролируемая зона (КЗ) - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
Границей КЗ могут являться:
периметр охраняемой территории учреждения (предприятия);
ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

Защищаемые помещения (ЗП) – помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

8

Раздел 4
ОБЪЕКТЫ, СРЕДСТВА, МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 14

КЛАССИФИКАЦИЯ ВИДОВ, СПОСОБОВ, МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ВОПРОСЫ:

14.1 ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ И СФЕРЫ ИХ ДЕЙСТВИЯ

14.2 ОБЩИЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

14.3 ОБЩАЯ КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

14. 4 ХАРАКТЕРИСТИКА СПОСОБОВ И СРЕДСТВ ПО ВИДАМ ЗАЩИТЫ ИНФОРМАЦИИ

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .– Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Источники указанные в Методических рекомендациях к курсу.

1

14.1 ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ И СФЕРЫ ИХ ДЕЙСТВИЯ

Виды защиты	Сфера действия
Правовая защита информации	Территория государства, территория охватываемая международными соглашениями в области информационной безопасности
Организационная защита информации	Территория организации (предприятия) или объекта информатизации.
Техническая защита информации ***Инженерно-техническая*** ***Программно - аппаратная***	*Контролируемая зона, здание или помещение объекта информатизации (выделенное помещение)* *Масштаб: от одного отдельного компьютера до вычислительной сети (ЛВС)*
Криптографическая защита информации	Масштаб сети (канала) связи, ИТКС (от организации до глобальной сети)
Физическая защита информации	Контролируемая зона, здание или помещение объекта информатизации (выделенное помещение)

2

14.1 ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ И СФЕРЫ ИХ ДЕЙСТВИЯ

Правовая защита информации

это защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Организационная защита информации

это организация деятельности по защите, регламентирование доступа к защищаемым ресурсам и на объекты информатизации. Организационная защита направлена на предотвращение утечки ИОД и несанкционированного (неправомерного) доступа к ней по организационным каналам. Подразделяется на организационно – правовую, организационно-техническую, организацию физической защиты

Техническая защита информации

ИТЗИ

ПАЗИ

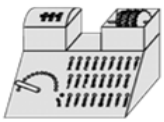
Техническая защита информации. Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. Техническую защиту разделяют на инженерно-техническую и программно-аппаратную.

Инженерно-техническая защита направлена на предотвращение утечки ИОД по ТКУ и ПДТР

Программно - аппаратная защита направлена на защиту информации в СВТ и АС функционирующих на их основе, а также в ИТКС от НСД и НСВ.

3

14.1 ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ И СФЕРЫ ИХ ДЕЙСТВИЯ



Крипто-графическая защита информации

– это защита информации с помощью ее криптографического преобразования. Она предназначена для обеспечения передачи конфиденциальной информации в зашифрованном виде по каналам связи, ИТКС, подтверждения подлинности электронных документов и обеспечения их целостности, придания электронным документам юридической силы, защиты парольных систем.

Физическая защита информации

- это защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

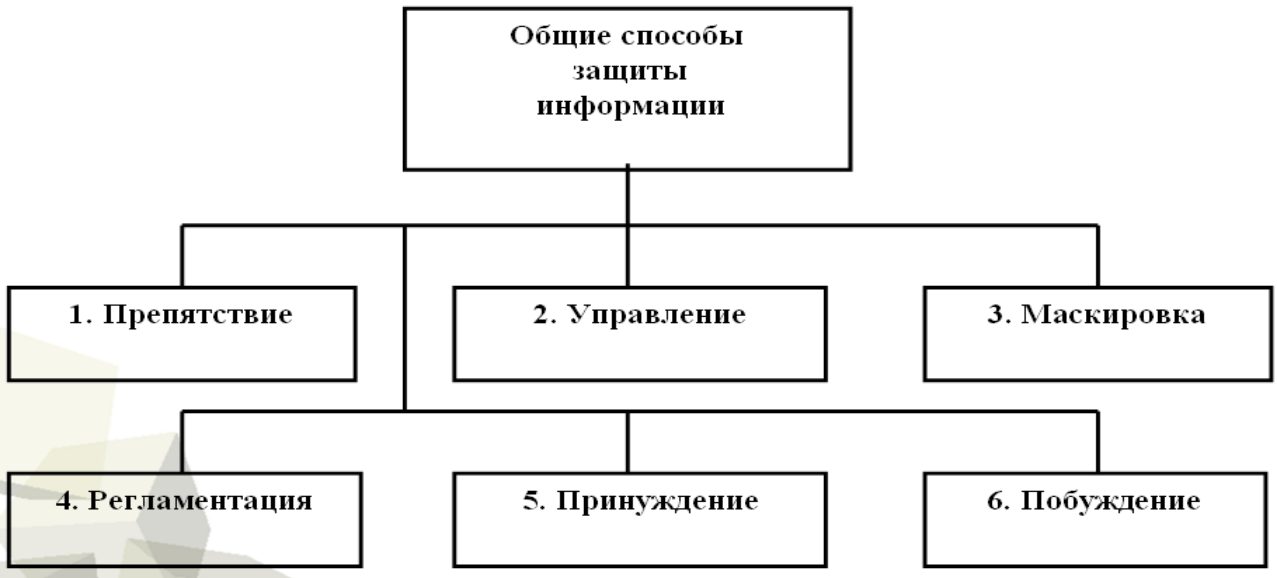
Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

4

14.2 ОБЩИЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

Способ защиты информации - это порядок и правила применения определенных принципов и средств защиты информации.



5

14.2 ОБЩИЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Препятствие → **заключается в создании на пути угрозы некоторого барьера, не позволяющего ей принять опасные размеры. Типичными примерами препятствий является создание физических препятствий на пути злоумышленников (турникеты и т.п.). , логические препятствия, представляющие собой системы идентификации и аутентификации (парольные системы) при доступе к АС.**

2. Управление → **есть определение на каждом шаге функционирования объекта таких управляющих воздействий на элементы системы, следствием которых будет решение (или способствование решению) одной или нескольких задач защиты информации.** Например, управление доступом в АС включает следующие функции защиты, осуществляемые системой управления доступом:
- идентификацию лиц, претендующих на доступ, персонала и ресурсов системы
- опознавание (аутентификацию) субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия запрашиваемых ресурсов назначенным полномочиям субъекта доступа);
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
реагирование (сигнализация, отключение, отказ в запросе) при попытке несанкционированных действий.

3. Маскировка → **скрытие защищаемой информации) предполагает такие ее преобразования, вследствие которых она становится недоступной для злоумышленников или доступ к ней существенно затрудняется. К маскировке относятся криптографические методы преобразования информации, скрытие объекта, а также меры по созданию шумовых полей, маскирующих информационные сигналы, экранирование излучающих технических средств обработки информации и т.п.**

6

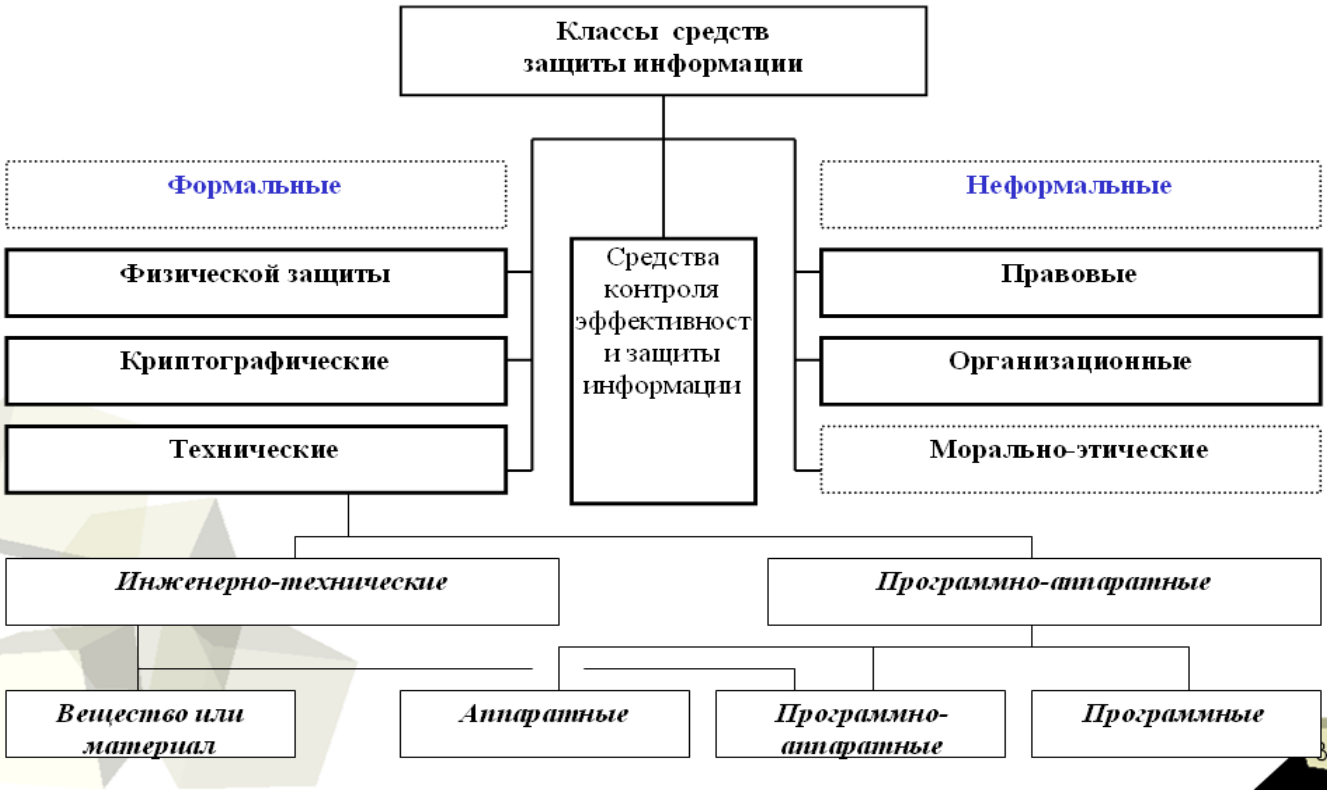
13.2 ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ

4. Регламентация	**заключается в разработке и реализации в процессе функционирования объекта комплекса мероприятий, создающих такие условия обработки информации, при которых существенно затрудняется проявление и воздействие угроз. К регламентации относится разработка таких правил обращения с конфиденциальной информацией и средствами её обработки, которые позволили бы максимально затруднить получение этой информации злоумышленником.**
5. Принуждение	**есть такой способ защиты, при котором пользователи и персонал системы вынуждены соблюдать правила и условия обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.**
6. Побуждение	**есть способ защиты информации, при котором пользователи и персонал АС внутренне (т. е. материальными, моральными, этическими, психологическими и другими мотивами) побуждаются к соблюдению всех правил обработки информации.**

7

14.3 ОБЩАЯ КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Средство защиты информации – это техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.



14.3 ОБЩАЯ КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Средство физической защиты информации

- это средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации. Средства физической защиты - механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства (замки) и си-стемы, которые функционируют автономно, создавая различного рода препятствия на пути нарушителей (злоумышленников). К ним относятся также системы контроля и управления доступом (СКУД) в охраняемые зоны, помещения, средства охранной и охранно-пожарной сигнализации, системы видеонаблюдения (в совокупности со службами охраны), специальные укреплённые двери, турникеты и т.п.

Криптографическое средство защиты информации

- это средство защиты информации, реализующее алгоритмы криптографического преобразования информации. Реализация может осуществляться с использованием аппаратуры (аппаратные), программ (программные) или с использованием того и другого (программно-аппаратные). Криптографические средства предназначены для шифрования информации с целью сохранения её конфиденциальности при передаче по сетям связи, информационно-телекоммуникационным сетям, обеспечения целостности, обеспечения подлинности и юридической значимости электронных документов (электронная цифровая подпись), защиты парольных систем в АС.

9

14.3 ОБЩАЯ КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Технические средства защиты информации

ТСЗИ= Средства ИТЗИ+ Средства ПАЗИ

(По ГОСТ Р 50922) – это технические, программно-технические, программные.

В науке и нормативных документах ТСЗИ разделяют на инженерно-технические и программно-аппаратные.

Инженерно-технические включают: аппаратные, программно-аппаратные средства, материалы и вещества, предназначенные для защиты информации. **Назначение этих средств - защита информации от утечки по техническим каналам и от технических средств разведки.**

Программно-аппаратные средства защиты информации разделяются на: аппаратные, программные, программно-аппаратные –**основное назначение защита от НСД и НСВ.**

Аппаратные средства - различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру АС или сопрягаемые с ней специально для решения задач защиты информации от НСД (в рамках ПАЗИ), а также устройства, устанавливаемые на объектах информатизации с целью защиты от утечки по техническим каналам и ПДТР (ИТЗИ).
Программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения АС с целью решения задач защиты информации, в первую очередь защиты от НСД и НСВ.
Программно – аппаратные – аппаратные средства, работающие под управлением или с использованием программ.

10

14.3 ОБЩАЯ КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Правовые (законодательные средства) – нормативные правовые акты, с по-мощью которых регламентируются права и обязанности, а также устана-вливается ответственность всех лиц и подразделений, имеющих отноше-ние к функционированию системы, за нарушение правил обработки ин-формации, следствием чего может быть нарушение ее защищенности.

Организационные средства - организационно-технические или организационно – правовые мероприятия, специально предусматриваемые в технологии функционирования объекта информатизации (АС), с целью решения задач защиты информации, а также организация физической защиты предприятия.

Морально-этические средства - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение кото-рых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

Морально-этические средства **Средство контроля эффективности защиты информации** – это средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации. Основу рассматриваемых средств составляют средства предназначенные для контроля эффективности защиты информации от утечки по техническим каналам (сканирующие приёмники, устройства для поиска закладочных устройств, сканеры безопасности сети и т.п.).

11

14.4 ХАРАКТЕРИСТИКА СПОСОБОВ И СРЕДСТВ ПО ВИДАМ ЗАЩИТЫ ИНФОРМАЦИИ

ДОСТОИНСТВА И НЕДОСТАТКИ СПОСОБОВ И СРЕДСТВ

Вид защиты	Достоинства	Недостатки
Правовые способы и средства	- универсальны в том смысле, что принципиально применимы для всех способов НСД и НСВ на ЗИ	- на реализацию требуется достаточно много времени и сил, поскольку в основном они реализуются через суд
Организа-ционные способы и средства	-широкий круг решаемых задач; -простота реализации; -гибкость реагирования на НСД; -практически неограниченные возможности изменения и развития	-необходимость использования людей; -повышенная зависимость от субъективных факторов; -высокая зависимость от общей организации работ в организации; -низкая надежность без соответствующей поддержки средствами ФЗИ, ТЗИ, СКЗИ.
ТЗИ Средства ИТЗИ Средства ПАЗИ	- -универсальность; -гибкость; -надежность функционирования; -простота реализации; -широкие возможности модификации и развития	-Не могут защитить от персонала -снижение функциональных возможностей АС; -необходимость использования ЗУ (памяти) АС; -подверженность модификациям (случайным или закономерным) -ориентация на вполне определённые типы ЭВМ и ПО (ОС, СУБД)
Крипто графические средства	- гибкость, т.е. возможность быстрого изменения алгоритма шифрования	- подверженность криптоанализу -требует защиты ключей используемых для шифрования

12

Тема 15

НАЗНАЧЕНИЕ И СТРУКТУРА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

ВОПРОСЫ:

15.1 ПОНЯТИЕ И ОБЩАЯ СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

15.2 ОБЩЕМЕТОДОЛОГИЧЕСКИЕ ТРЕБОВАНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

15.3 ТИПИЗАЦИЯ, СТАНДАРТИЗАЦИЯ, КЛАССИФИКАЦИЯ СИСТЕМ ЗАЩИТЫ

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .- Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Источники указанные в Методических рекомендациях к курсу.

1

15.1 ПОНЯТИЕ И ОБЩАЯ СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

ПОНЯТИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Теория систем

«Система – это комплекс взаимодействующих компонентов» (Л. Берталанфи);

«Система представляет собой определённое множество взаимосвязанных элементов, образующих устойчивое единство и целостность, обладающее интегральными свойствами и закономерностями» (В. П. Кузьмин);

«Система – это не просто совокупность единиц… а совокупность отношений между этими единицами» (А. Рапорт).

Среди множества определений можно выделить главную суть системы, которая заключается не только в том, что система включает некоторое множество компонентов, но и в том, что взаимодействие этих компонентов приводит к получению некоторого полезного (интегрированного) результата, который невозможно получить, используя каждый компонент в отдельности.

ГОСТ Р 50922

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ –
совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

2

15.1 ПОНЯТИЕ И ОБЩАЯ СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

ОБЩАЯ СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

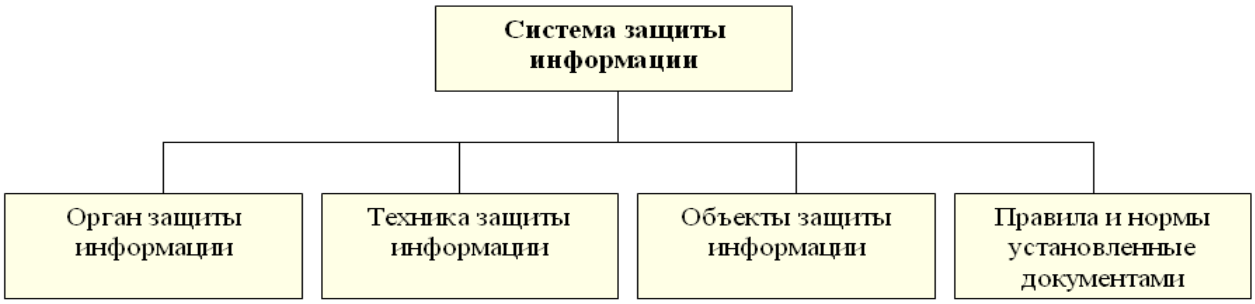


Рис.15.1 Компоненты системы защиты информации

Орган защиты информации - административный орган (отдел, служба), осуществляющий организацию защиты информации (или отдельные исполнители)

Техника защиты информации - средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации

Объект защиты информации (Т.13):

Правила и нормы, установленные соответствующими документами в области защиты информации, включают правила и нормы, установленные правовыми, организационно – распорядительными, нормативно-методическими документами, разработанными и введёнными в действие, как органами государственной власти, так и руководством организации в которых создаётся и используется система защиты информации

3

15.2 ОБЩЕМЕТОДОЛОГИЧЕСКИЕ ТРЕБОВАНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

ОБЩЕМЕТОДОЛОГИЧЕСКИЕ ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ

Целевые требования	Решаемые задачи	Результат
ФУНКЦИОНАЛЬНЫЕ	Обеспечение решения требуемой совокупности задач защиты	Удовлетворение всем требованиям защиты
ЭРГОНОМИЧЕСКИЕ	Минимизация помех пользователям	Удобство для персонала системы защиты и пользователей АС
ЭКОНОМИЧЕСКИЕ	Минимизация затрат на систему	Максимальное использование серийных средств
ТЕХНИЧЕСКИЕ	Комплексное использование средств	Оптимизация архитектуры
ОРГАНИЗАЦИОННЫЕ	Структурированность всех компонентов	Простота эксплуатации

4

15.2 ОБЩЕМЕТОДОЛОГИЧЕСКИЕ ТРЕБОВАНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

1. Концептуальное единство (Комплексность)	**означает**, что архитектура, технология, организация и обеспечение функционирования как СЗИ в целом, так и составных ее компонентов должны рассматриваться и реализовываться в строгом соответствии с основными положениями единой концепции отражающей цели и задачи защиты информации
2. Адекватность требованиям	**означает**, что СЗИ должна строиться в строгом соответствии с требованиями к защите, которые в свою очередь определяются категорией хранимой и обрабатываемой информации (вид тайны, степени секретности) и соответствующего объекта, а также факторами, влияющими на защиту информации (уязвимости, угрозы, условия обработки и др.)
3. Гибкость (адаптируемость)	**означает** такое построение и такую организацию ее функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры АС, технологических схем или условий функционирования каких-либо ее компонентов.
4. Функциональная самостоятельность	предполагает, что СЗИ должна быть самостоятельной обеспечивающей подсистемой объекта информатизации и при осуществлении функций защиты не зависеть от других подсистем.
5. Удобство использования	означает, что СЗИ не должна создавать дополнительных неудобств для пользователей и персонала АС.

5

15.2 ОБЩЕМЕТОДОЛОГИЧЕСКИЕ ТРЕБОВАНИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

6. Минимизация предоставляемых прав	***означает***, что каждому пользователю и каждому лицу из состава персонала ОИ должны предоставляться лишь те полномочия на доступ к ресурсам ОИ и ИТ, которые ему действительно необходимы для выполнения своих функций в процессе автоматизированной обработки информации. При этом предоставляемые права должны быть определены установленным порядком и утверждены заблаговременно
7. Полнота контроля	(аудит безопасности) **предполагает**, что все процедуры автоматизированной и неавтоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах.
8. Активность реагирования	означает, что СЗИ должна реагировать на любые попытки несанкционированных действий. Характер реагирования может быть различным и включать: - просьбу повторить действие; - задержку в выполнении запросов; - отключение структурного элемента, с которого осуществлено несанкционированное действие; - исключение нарушителя из числа зарегистрированных пользователей; - подача специального сигнала и др.
9.Экономичность	означает, что при условии соблюдения основных требований всех предыдущих принципов расходы на СЗИ должны быть минимальными.

6

15.3 ТИПИЗАЦИЯ, СТАНДАРТИЗАЦИЯ, КЛАССИФИКАЦИЯ СИСТЕМ ЗАЩИТЫ

Типизация

разработка типовых конструкций или технологических процессов на основе общих для ряда изделий (процессов) технических характеристик. Типизация рассматривается как один из методов стандартизации.

Стандарти-зация

это процесс установления и применения стандартов, которые в свою очередь определяются как образцы, эталоны, модели, принимаемые за исходные, для сопоставления с ними других подобных объектов

В настоящее время в России и в зарубежных странах в соответствии с законодательством «О техническом регулировании» роль стандартов выполняют:

ЗАКОН « О техническом регулировании» 2002г:

- ТЕХНИЧЕСКИЕ РЕГЛАМЕНТЫ
(имеют статус закона), - обязательны для выполнения (обязательная сертификация)

- НОРМАТИВНЫЕ ДОКУМЕНТЫ ФЕДЕРАЛЬНЫХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ
(ФСБ, ФСТЭК) –
обязательны для выполнения (обязательная сертификация),

СТАНДАРТЫ
–для добровольного исполнения (добровольная сертификация)

7

15.3 ТИПИЗАЦИЯ, СТАНДАРТИЗАЦИЯ, КЛАССИФИКАЦИЯ СИСТЕМ ЗАЩИТЫ

Уровень типизации, стандартизации	Характеристика уровня	Примеры
Высший	**Уровень СЗИ в целом (СЗИ объекта информатизации)** ***Стандартизация практически невозможна*** ***Возможна типизация***	4 типа объектов информатизации. На этом уровне становится возможна лишь стандартизация типовых факторов воздействующих на ОИ. Примером этому служит стандарт ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию.
Средний	**Уровень составных компонентов СЗИ ЗОИ** (СЗИ АС от НСД, ИТ-системы) ***Роль стандартов выполняют Руководящие документы (в перспективе технические регламенты)***	Предполагает разработку **типовых проектов** структурно или функционально ориентированных компонентов СЗИ, которые учитывают условия обработки (СЗИ от НСД в АС) **9 типовых решений – 9 классов АС, в зависимости от условий обработки и уровня конфиденциальности (секретности) информации,** **4 класса защищаемых помещений (по уровню конфиденциальности (секретности) оглашаемой ИОД)**
Низший	**Уровень проектных решений по средствам и механизмам защиты** Возможность разработки и сертификации типовых средств на основе которых можно просто собирать необходимую СЗИ ГОСТЫ и Руководящие документы	Типизация и стандартизация на низшем уровне предполагает разработку и стандартизацию типовых проектных решений по практической реализации средств защиты информации или спецификаций: - программно-аппаратных; -криптографических; -физической защиты, технической защиты. **Стандарты и руководящие документы по средствам защиты (для ОС, СУБД-ПАЗИ, для ТКУИ- ИТЗИ). Стандарты ГОСТ Р ИСО МЭК -15408 для ИТ**

8

КЛАССИФИКАЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ (ПРИМЕР)

По уровню обеспечиваемой защиты все СЗИ целесообразно разделить, например, на следующие пять категории (уровень определяется в лингвистических переменных):

1) системы слабой (тривиальной) защиты - рассчитанные на такие АС, в которых обрабатывается информация, имеющая самый низший уровень конфиденциальности и *ущерб от получения её третьими лицами не несёт значительного материального ущерба способного повлиять на деятельность организации и её бизнес процессы;*

2) системы «нормальной» (базовой) защиты - рассчитанные на такие АС, в кото-рых обрабатывается информация ограниченного доступа и (или) другая ценная информация и ущерб от получения её третьими лицами или её утрата может привести к *материальному (финансовому) или моральному ущербу способному повлиять на деятельность организации и её бизнес процессы.*

3) системы сильной защиты - рассчитанные на АС, в которых обрабатывается информация, подлежащая защите от несанкционирован-ного ее получения, *и имеющая высокую (государственную) важность (ценность) – ущерб государственной организации;*

4) системы очень сильной защиты - рассчитанные на АС, в кото-рых регулярно обрабатываются информация, имеющая очень высокую *(государственную) важность (ценность)- ущерб министерству (ведомству);*

5) системы особой защиты - рассчитанные на АС, в которых ре-гулярно обрабатывается информация *особой (государственной) важности (ценности) – ущерб государству (РФ).*

Этот подход использован в Руководящих документах Гостехкомиссии России (ФСТЭК)

- для АС: РД ГТК РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - М., 1992.

- Для межсетевых экранов (При межсетевом взаимодействии АС):

9

15.3 ТИПИЗАЦИЯ, СТАНДАРТИЗАЦИЯ, КЛАССИФИКАЦИЯ СИСТЕМ ЗАЩИТЫ

КЛАССИФИКАЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ (ПРИМЕР)

Руководящий документ АС РД ГТК РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - М., 1992.

Вид тайны	Уровень Конфиденциальности (грифы)	Уровень системы защиты АС
Персональные данные Служебная тайна Коммерческая тайна	Коммерческая тайна 2-й категории важности	Системы слабой (тривиальной) защиты
	Коммерческая тайна 1-й категории важности ДСП	Системы базовой (нормальной) защиты
Государственная тайна	Секретно	Системы сильной защиты
	Сов. секретно	Системы очень сильной защиты
	Особой важности	Системы особой защиты

10

КЛАССИФИКАЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

По активности реагирования СЗИ на не-санкционированные действия, все системы защиты можно разделить на следующие три типа:

1) **пассивные СЗИ**, в которых не предусматривается ни сигнализа-ция о несанкционированных действиях, ни воздействие системы защиты на нарушителя (например системы аудита);

2) **полуактивные СЗИ,** в которых предусматривается сигнализация о несанкционированных действиях, но не предусмотрено воздействие системы на нарушителя;

3) **активные СЗИ,** в которых предусматривается как сигнализация о несанкционированных действиях, так и воздействие системы на наруши-теля, его действия или используемые средства.

В этом случае, в качестве примера можно привести СЗИ от НСД в АС в которых функционально может быть предусмотрено блокирование доступа к защищаемым ресурсам в случае трёх попыток ввода неправильного пароля, или отключение компьютера вообще.

В общем случае можно предположить, что СЗИ каждой категории по уровню защиты могут относиться к разным типам активности реаги-рования. Однако вряд ли целесообразно строить активные СЗИ слабой защиты (хотя в некоторых случаях такие системы и могут быть допусти-мы). С другой стороны, системы особой защиты непременно должны быть активными.

Тема 16

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Кафедра ВСиИБ

ВОПРОСЫ:

16.1 ПОНЯТИЕ И ОБЩАЯ СТРУКТУРА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

16.2 КОМПОНЕНТЫ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ ИХ НАЗНАЧЕНИЕ И СТАНДАРТИЗАЦИЯ

16.3 ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Литература

1.Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие. .– Барнаул: АлтГТУ, 2010 –[элетр. с диск.]
2. Источники указанные в Методических рекомендациях к курсу.

1

16.1 ПОНЯТИЕ И ОБЩАЯ СТРУКТУРА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

КОМПЛЕКСНОСТЬ – БАЗОВЫЙ ПРИНЦИП ПОСТРОЕНИЯ КСЗИП

Основная идея этого принципа заключается в том, что:

во-первых должны быть защищены все объекты предприятия (объекты информатизации) на которых ведётся обработка информации,

во-вторых должен использоваться арсенал методов и средств всех видов защиты: правовой, организационной, технической, криптографической, физической в их оптимальном сочетании обеспечивающем соотношение цена системы защиты/эффективность системы защиты.

Основными показатели, определяющие состав и структуру КСЗИП:

- количество (объёмы) и ценность используемой и обрабатываемой на предприятии информации и информационных ресурсов;
- состав, объекты и степень конфиденциальности защищаемой информации;
- количество и технологические особенности технических средств обработки, хранения, передачи информации (средств автоматизации, связи и т.п):
- количество и уровень подготовки персонала связанного с использованием, обработкой, хранением, передачей информации вообще и ценной (конфиденциальной) в частности;
- структура и территориальное расположение предприятия;
- режим функционирования предприятия;
- конструктивные особенности (компактные, территориально-распределённые, размещённые совместно с другими предприятиями);
- количественные и качественные показатели ресурсообеспечения (возможности по выделению средств на СЗИ).
- угрозы безопасности всем видам защищаемой информации и объектам информатизации.

2

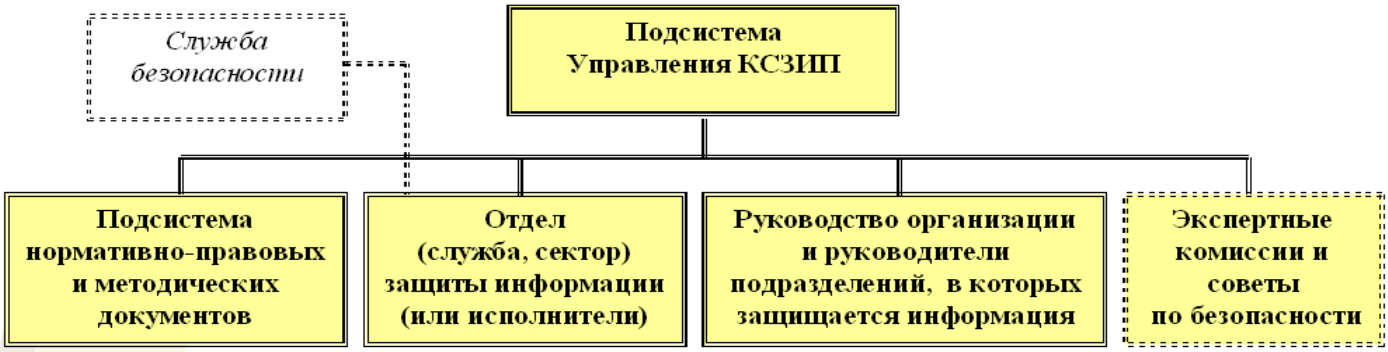
16.1 ПОНЯТИЕ И ОБЩАЯ СТРУКТУРА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ (КСЗИП)
– СЗИ реализующая правовой, организационный, технический, физический, криптографический (при необходимости) виды защиты информации и адекватная, по своему компонентному составу и функциям, угрозам безопасности информации и объектам информатизации предприятия.

16.2 ПОДСИСТЕМА УПРАВЛЕНИЯ КСЗИП

Подсистема управления КСЗИП

Подсистема управления КСЗИП
- предназначена для управления процессами защиты информации на основе законодательства и регламентации правил и порядка доступа к защищаемой информации и контроля всех процессов со стороны руководства организации и службы защиты информации.



При защите государственной тайны регламентация защиты и все элементы приведенные на рисунке создаются и функционируют в строгом соответствии с законодательством о «Гостайне» и требованиями нормативных документов разработанными органами защиты гостайны.

При защите конфиденциальной информации регламентация защиты и все элементы приведенные на рисунке создаются и функционируют в пределах норм и правил установленных для защиты КИ нормативными документами и стандартами. Для управления КСЗИ в организации может быть создана и внедрена система управления, основанная на стандартах в области управления ИБ и менеджмента качества: серии 1. ГОСТ Р ИСО/МЭК -17799, и 2. ГОСТ Р ИСО/МЭК -27001

Нормативно-правовые и методические документы.

Первая группа (нормативно –правовая база)

1) Федеральные законы РФ (включая технические регламенты), нормативные правовые акты и методические документы Президента РФ, Правительства РФ, органов исполнительной власти, стандарты по вопросам обеспечения информационной безопасности и защиты информации. Их перечень и обязательность наличия на предприятии устанавливается органами исполнительной власти уполномоченными в области безопасности, технической защиты информации и противодействия техническим разведкам;

Вторая группа (Локальные нормативно-правовые и методические документы).

Перечень этой группы определяется исходя из требований документов первой группы и условий деятельности предприятия. К ним, в частности относятся: перечни сведений конфиденциального характера (подлежащих засекречиванию), политика (концепция) информационной безопасности предприятия, положения об отделе (службе) защиты информации и др., инструкции специалистам по защите информации, персоналу, руководства;

Третья группа

Лицензии на виды деятельности, включая деятельность по защите информации, лицензии на объекты интеллектуальной собственности, аттестаты соответствия по требованиям безопасности на объекты информатизации, сертификаты на технические и криптографические средства защиты информации, средства физической защиты.

16.2 ПОДСИСТЕМА УПРАВЛЕНИЯ КСЗИП

Отдел (служба, сектор) защиты информации (или исполнители ответственные за защиту информации).

Как элемент подсистемы управления КСЗИП отделы (службы, сектор) защиты информации создаются на основе требований законодательства (законодательство о государственной тайне) или исходя из потребностей предприятия. Во втором случае правовой основой создания и функционирования такого подразделения могут служить нормы Закона РФ 1992 г. N 2487-I "О частной детективной и охранной деятельности в Российской Федерации"(ст.14), а также нормы Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 17 ноября 2007 г. N 781) – при защите только персональных данных (ст.13). Отделы могут входить в службы безопасности предприятия.

Руководство организации и руководители подразделений, в которых защищается информация

Функции руководства предприятия по защите информации зависят от ряда факторов, основными из которых являются [1]:

- виды информации ограниченного доступа используемые на предприятии (государственная, служебная, коммерческая, персональные данные и т.п.);
- форма собственности и организационно-правовая форма предприятия;
- подчинённость (подведомственность)предприятия (для предприятий государственной формы собственности);
- сфера деятельности.

Обязанности и права руководителей предприятия по вопросам защиты информации должны быть отражены в должностных инструкциях.

16.2 ПОДСИСТЕМА УПРАВЛЕНИЯ КСЗИП

Экспертные комиссии и советы по безопасности в области защиты информации

являются коллегиальными органами призванными решать те вопросы информационной безопасности и защиты информации, которые не могут быть решены узкими специалистами и отдельно руководителем организации и его заместителями.

К таким комиссиям относятся:

-**постоянно действующие технические комиссии (ПДТК)** предприятий по защите государственной тайны (создаваемые в соответствии с Положением, утверждённым совместным приказом Гостехкомиссии России и ФСБ России в 2001г.);

-**экспертные комиссии** по экспертизе материалов для открытого опубликования материалов и публичного представления, присвоения грифа конфиденциальности для отдельных видов документов (кандидатские и докторские диссертации и т.п.)

-**внутренние проверочные комиссии**, назначаемые руководителем для проверки носителей информации ограниченного доступа и проведения внутреннего аудита информационной безопасности;

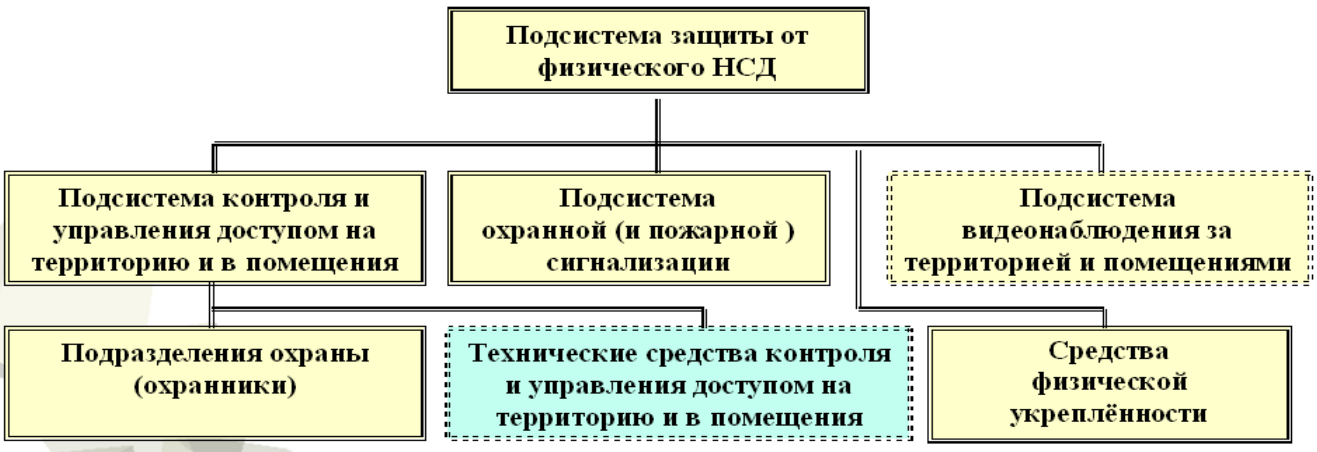
-**комиссии по экспортному контролю** при осуществлении международных связей (создаются в соответствии с требованиями зак-ва об экспортном контроле)

-**советы по безопасности** (выполняют роль консультативных органов), которые вырабатывают рекомендации руководству по вопросам защиты информации, требующим комплексного (многостороннего) подхода.

16.3 ПОДСИСТЕМА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА

Подсистема защиты от несанкционированного физического доступа

- предназначена для контроля пребывания на территории и объектах информатизации персонала организации и предотвращения неконтролируемого пребывания посторонних лиц, а также для сигнализации и извещения о случаях несанкционированного проникновения на территорию и охраняемые объекты информатизации. Она является одновременно подсистемой системы безопасности организации.



Каждая из перечисленных подсистем включает соответствующие технические средства, создаётся и внедряется в организации в рамках требований стандартов, для каждой указанной подсистемы.

Регламентируется законодательством: «О ведомственной охране», «О вневедомственной охране», «О частной детективной и охранной деятельности».

16.3 ПОДСИСТЕМА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА

Требования к СКУД

Технические требования к средствам (системам) контроля и управления доступом определены в ГОСТ Р 51241 —98 «Средства и системы контроля и управле-ния доступом. Классификация. Общие технические требования и методы испытаний»

Требования к системам охранной и пожарной сигнализации :

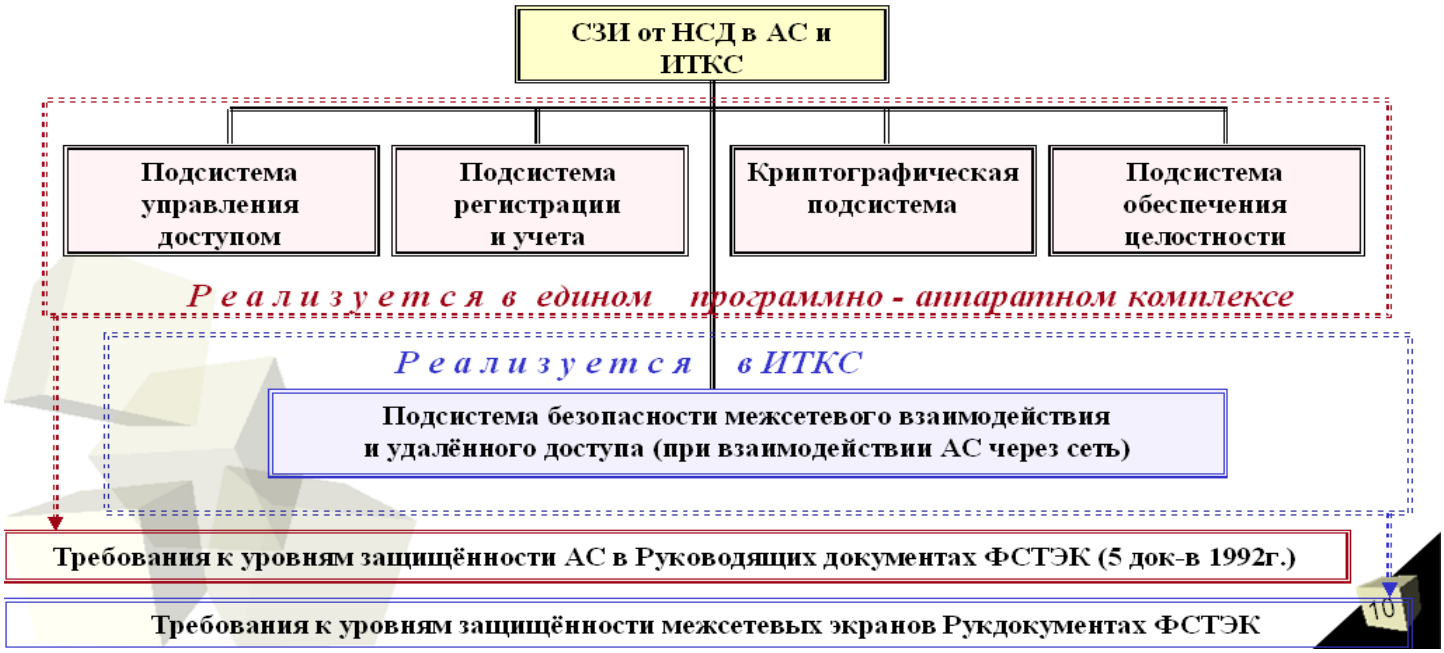
РД 78.147 — 93 /МВД России «Единые требования по укреп-лению и оборудованию сигнализации охраняемых объектов»;
РД 78.143 — 92 /МВД России «Системы и комплексы охранной сигнализации. Нормы проектирования»;
РД 78.145 — 93 /МВД России «Системы и комплексы охран-ной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ»;
Стандарт Европейского комитета по стандартизации в облас-ти электроники CENELEC 1996 г. EN 50133-1 «Устройства охранной сигнализации. Контрольно-пропускные устройства. Часть 1: требования к системе».

Требования к СТУ

ГОСТ Р 51242 — 98 «Конструкции защитные механические и электромеханические для дверных и оконных проемов. Технические требования и методы испытаний на устойчивость к разруша-ющим воздействиям»;
ГОСТ Р 51136 —98 «Стекла защитные многослойные. Общие технические условия»;
РД 78.148 —94/МВД России «Защитное остекление. Класси-фикация. Методы испытаний. Применение»;
ГОСТ Р 51072 — 97 «Двери защитные. Общие технические тре-бования и методы испытаний на устойчивость к взлому и пулестойкость»;
ГОСТ 26892 — 86 «Двери деревянные. Метод испытания на сопротивление ударной нагрузке, действующей в направлении открывания двери»;

16.4 ПОДСИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД В АС И ИТКС

Подсистема защиты информации от НСД в АС и ИТКС является самостоятельной системой и предназначена для защиты конфиденциальной (секретной) информации от несанкционированного доступа в автоматизированных системах и ИТКС организации, а также для обеспечения целостности информации и доступности для уполномоченных пользователей (предотвращения НСВ и НСД с использованием С-П и ИТ КУИ).



16.4 ПОДСИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД В АС И ИТКС

Требования к системам защиты АС и ИТКС:

ГОСТ Р 51583-2007. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования.

ГОСТ Р 51624-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

ГОСТ Р ИСО/МЭК 15408-2008 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Основными руководящими документами, содержащими требования к АС и являются :

РД ГТК РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - М., 1992.

РД ГТК РФ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992.

РД ГТК. РФ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. - М., 1997.

При организации защиты коммерческой тайны в АС и ТКС могут использоваться как указанные выше стандарты и руководящие документы, так и международные стандарты, принятые в России в 2007 году в качестве национальных:

ГОСТ Р ИСО/МЭК 13335 -2006 Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 4 Выбор защитных мер. Часть 5 Руководство по менеджменту безопасности сети. Реализуется СЗИ от НСД методами и средствами программно-аппаратной, программной, аппаратной защиты.

16.5 ПОДСИСТЕМА ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ (ПОДСИСТЕМА АНТИВИРУСНОЙ ЗАЩИТЫ).

Подсистема защиты от вредоносных программ (подсистема антивирусной защиты) - предназначена для защиты АС функционирующих на основе персональных компьютеров и вычислительных сетей от НСВ с применением компьютерных вирусов и других видов вредоносных программ.

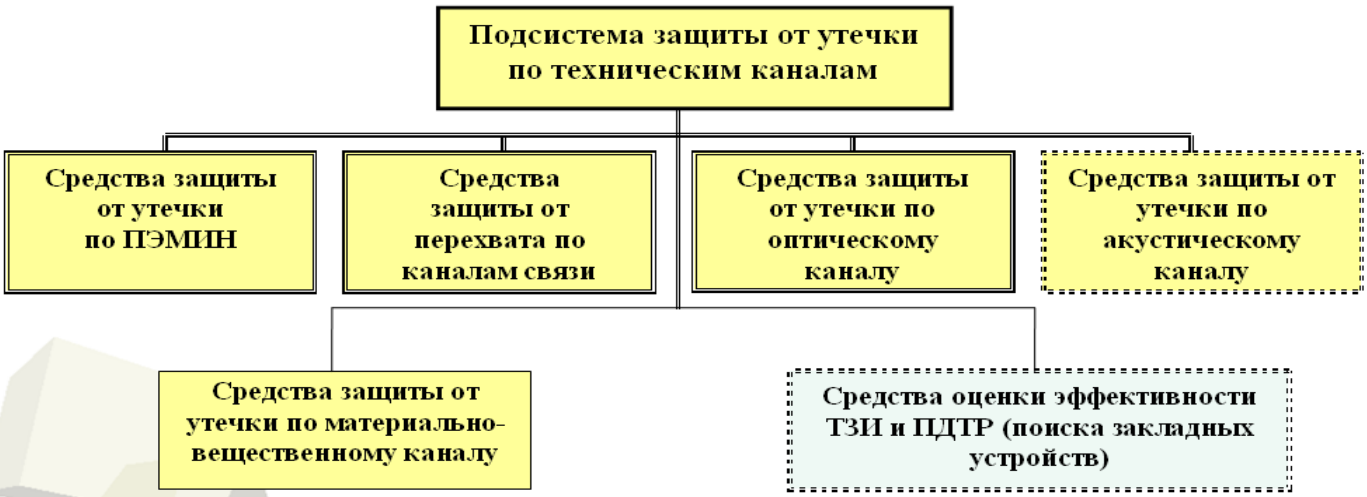
Подсистема защиты от вредоносных программ создаётся и внедряется в соответствии с требованиями нормативных документов:

1. ГОСТ Р 51188-98. Защита информации. Испытания программных средств. На наличие компьютерных вирусов. Типовое руководство.
2. РД ГТК. РФ. Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов. Показатели защищенности от вирусов. - М. 1997.

12

16.6 ПОДСИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Подсистема защиты информации от утечки по техническим каналам
- предназначена для предотвращения утечки конфиденциальной (секретной) информации по техническим каналам и незаконного получения её третьими лицами (разведками).



Основными документами, содержащими требования к указанным подсистемам являются:
Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР-97). Гостехкомиссия России. – М.: 1997.
Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Гостехкомиссия России.,-М.:2001.

13

16.6 ПОДСИСТЕМА ПРОТИВОДЕЙСТВИЯ ТЕХНИЧЕСКИМ РАЗВЕДКАМ

Подсистема противодействия техническим разведкам (ПДТР).
Подсистема ПДТР – предназначена для скрытия объектов защиты, его отдельных характеристик, свойств, навязывания разведкам ложного представления о состоянии, возможностях или предназначении защищаемого объекта.

Скрытие осуществляется путём проведения технических и организационных мероприятий.
Требования по ПДИТР определяются нормативными и методическими документами федерального органа исполнительной власти уполномоченного в области технической защиты информации и противодействия техническим разведкам.
Одним из важных требований является требование разработки и введение в действие на предприятии
Руководства по технической защите информации и противодействию техническим разведкам. Защита информации от утечки по техническим каналам в этом случае является составляющей единой подсистемы ТЗИ и ПДТР

14

16.7 ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НСД

1. Требования к АС как объектам информатизации

Определены в:

1. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
2.ГОСТ Р 51583-2006. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования.(ДСП).
3. ГОСТ Р 51624-2006. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.(ДСП)
4. Нормативные, руководящие, нормативно-методические документы ФСТЭК по ТЗИ и ПДТР. (СТР-97, СТР-К-2001, и т.п. – ограниченного доступа),

2. Требования к СЗИ АС от НСД

Определены в:

1. РД ГТК РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - М., 1992.
2. РД ГТК РФ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. М., 1992.
3. РД ГТК. РФ. Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации. - М., 1997.
4. 1997.РД ГТК РФ. Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. – М., 1999.
5. РД ГТК. РФ. Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов. Показатели защищенности от вирусов. - М.

15

16.3 ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НСД

1.ТРЕБОВАНИЯ К АС КАК ОБЪЕКТАМ ИНФОРМАТИЗАЦИИ (ГОСТЫ)

Автоматизированная система в защищенном исполнении (АСЗИ) - автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

ФУНКЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ АСЗИ (КАК ОИ) ГОСТ Р 51624-2000
.предупреждение о появлении угроз безопасности информации,
.обнаружение, нейтрализация и локализация воздействия угроз безопасности информации
.управление доступом к защищаемой информации
.регистрация событий и попыток несанкционированного доступа к защищаемой информации и несанкционированнного воздействия на нее,
.восстановление системы защиты информации и защищаемой информации после воздействия угроз,
.обеспечение контроля функционирования средств и системы защиты информации и немедленное реагирование на их выход из строя.

ОБЩИЕ ТРЕБОВАНИЯ К (АСЗИ) включают ГРУППЫ ТРЕБОВАНИЙ (ГОСТ Р 51624-20000
- функциональные требования,
- требования к эффективности,
- технические требования,
- экономические требования,
- требования к документации.

16

16.3 ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НСД

2.ТРЕБОВАНИЯ К СЗИ АС ОТ НСД

Система защиты информации автоматизированной системы - совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

Все АС по условиям обработки разделяются на три группы, в группе на классы, требования сформулированы для каждого класса в РД ГТК РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - М., 1992.

Классификация АС

Г Р У П П Ы

ПЕРВАЯ
Многопользовательские АС, с информацией разного уровня конфиденциальности. Пользователи имеют разные права доступа к информации.

КЛАССЫ

1 А | 1 Б | 1 В | 1 Г | 1 Д

Гостайна | Конф.инф

ВТОРАЯ
Многопользовательские АС, с информацией разного уровня конфиденциальности. Пользователи имеют одинаковые права доступа к информации.

КЛАССЫ

2 А | 2 Б

Гостайна | Конф.инф

ТРЕТЬЯ
Однопользовательская АС, с информацией одного уровня конфиденциальности.

КЛАССЫ

3 А | 3 Б

Гостайна | Конф.инф

17

16.3 ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ НСД

Разделение классов АС на группы для определения требований по защите информации

№ группы	Определяющие признаки АС для группирования классов			Классы для КИ	Классы Для ГТ
	Режим обработки данных в АС	Уровень полномочий субъектов доступа	Уровни конфиденциальности информации		
Третья группа	Индивидуальный (один пользователь)	Ко всей информации	Один уровень	3Б	3А
Вторая группа	Коллективный	Одинаковые права доступа ко всей информации	Различные уровни	2Б	2А
Первая группа	Коллективный	Различные права доступа	Различные уровни	1Д 1Г	1В 1Б 1А

18

Минимально необходимые классы защищенности АСЗИ для работы с информацией ограниченного доступа

Гриф конфиденциальности или вид ИОД	Классы АСЗИ АС АВС			Класс СВТ	Класс МЭ	Уровень контроля ПО	АВС
	1 группа	2 группа	3 группа				
«КТ» 1 категор. ПДн	1Д	2Б	3Б	6	5	- (4)	А5,В5
«КТ» 2 категор. ДСП ПДн	1Г	2Б	3Б	5	4	4	А5,В5
Секретно	1В	2А	3А	4	3	3	>А4, В4
Совершенно секретно	1Б	2А	3А	3	2	2	>А4, В4
Особой важности	1А	2А	3А	2	1	1	>А4, В4

СПИСОК ЛИТЕРАТУРЫ

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пособие для вузов.-М:Горячая линия-Телеком, 2004.-280с.
2. Расторгуев С.П. Основы информационной безопасности. .- М.: Издательский центр «Академия», 2008.- 192с.
3. Мельников В. П. Информационная безопасность и защита информации: учебное пособие для студ. высш. учеб. заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под. ред. С. А. Клейменова. — 3-е изд., стер. - М.: Издательский центр «Академия», 2008. — 336 с.
4. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие. - Барнаул: АлтГТУ, 2010 – 240с.
5. 6.Организационно – правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / М.: Издательский центр «Академия», 2008.-256с.
6. Загинайлов Ю.Н. Информационная безопасность в терминах и определениях стандартов защиты информации. Уч.-справ.пособие. Барнаул: Изд-во АлтГТУ, 2002.-112с. (40экз. библ.).
7. Грибунин В.Г. Комплексная система защиты информации на предприятии: учебник для студ. высш. учеб. заведений./ В.Г.Грибунин, В.В. Чудовский.- М.: Издательский центр «Академия», 2008.-320с. (25 экз. Гриф УМО)
8. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность сетевых технологий. -СПб.: БХВ - Санкт-Петербург, 2000.-320с.
9. Торокин А.А. Инженерно-техническая защита информации. М.:Гелиос АРВ, 2005
10. Бачилло И.Л.,Лопатин В.Н., Федотов М.А. Информационное право: Учебник/ Под ред.акад.РАН Б.Н. Топорнина.-СПб.:Издательство «Юридический центр Пресс»,2001.-789с. (10 экз.ч.з, + Эл. ресурс. –http://www.edu.lib.ru, гриф МО РФ)).
11. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/
12. Закон Российской Федерации "О безопасности" от 05.03.92 [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/
13. Закон РФ № 54-1 от 21.07.1993 г. «О государственной тайне». [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/
14. Федеральный Закон РФ от 29.07.2004г. №98-ФЗ «О коммерческой тайне». [электронный ресурс]: -режим доступа: http://www.garant.ru/
15. Федеральный закон РФ № 152 –ФЗ 2006г. «О персональных данных». [электронный ресурс]: -режим доступа: http://www.garant.ru/
16. Постановление Правительства Российской Федерации от 04.09.95 № 870 "Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности" [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ Ауд.94 ПК.(Платформа F1 Гарант;
17. Указ Президента Российской федерации от 06.03.97 № 188 "Об утверждении перечня сведений конфиденциального характера" [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ.(Платформа F1 Гарант);
18. Указ Президента Российской федерации от 24.01.98 № 61 "Об утверждении перечня сведений, отнесенных к государственной тайне" [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/
19. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895). [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/
20. Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. N Пр-212). [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/
21. Стратегия национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента РФ от 12 мая 2009 г. N 537). [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ; 2. http://www.garant.ru/

22. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008 -10с. [электронный ресурс]:- режим доступа: http:// www.fstec.ru
23. ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Стандартинформ, 2007 -7с. [электронный ресурс]:- режим доступа: http:// www.fstec.ru
24. ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2008-48с.
25. ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М.: Стандартинформ, 2007 -19с.
26. ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий. М.: Стандартинформ, 2007-46с.
27. ГОСТ Р ИСО/МЭК ТО 13335-4-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер. М.: Стандартинформ, 2007 -63с.
28. Руководящий документ.Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [электронный ресурс]: -режим доступа: http://www.fstec.ru/_razd/_isp0o.htm- Загл. с экрана.
29. Руководящий документ. Средства вычислительной техники Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [электронный ресурс] : -режим доступа: http://www.fstec.ru/_razd/_isp0o.htm- Загл. с экрана.
30. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [электронный ресурс] : -режим доступа: http://www.fstec.ru/_razd/_isp0o.htm- Загл. с экрана.
31. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [электронный ресурс] : -режим доступа http://www.fstec.ru/_razd/_isp0o.htm- Загл. с экрана.
32. Руководящий документ. Антивирусные средства. Показатели защищенности и требования по защите от вирусов. РД ГТК. РФ. Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов. Показатели защищенности от вирусов. - М. 1997.
33. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: http:// www.fstec.ru.
34. Правовая справочная система «Гарант» [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ.(Платформа F1 Гарант); 2. http://www.garant.ru/
35. Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: http://protect.gost.ru//