ПРИОРИТЕТНЫЙ НАЦИОНАЛЬНЫЙ ПРОЕКТ «ОБРАЗОВАНИЕ»
РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

А.А. ВАРФОЛОМЕЕВ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Москва
2008

Инновационная образовательная программа
Российского университета дружбы народов

«Создание комплекса инновационных образовательных программ и формирование инновационной образовательной среды, позволяющих эффективно реализовывать государственные интересы РФ через систему экспорта образовательных услуг»

Экспертное заключение –

кандидат технических наук, доцент *С.В. Запечников*

Варфоломеев А.А.

Основы информационной безопасности: Учеб. пособие. – М.: РУДН, 2008. – 412 с.: ил.

Учебное пособие посвящено основополагающим вопросам теории и практики обеспечения информационной безопасности и защиты информации. Опираясь на различные международные и национальные стандарты, раскрываются все основные понятия в данной области, в систематизированном виде рассматривается нормативно-правовая база. Много внимания в пособии уделено банковской тематике для демонстрации рассматриваемых общих понятий и положений. Изучение материала учебного пособия является первым этапом для дальнейшего изучения других разделов информационной безопасности, которые выделены в связи с их важностью и излагаются в курсах «Современная прикладная криптография», «Управление информационными рисками», «Технические средства защиты информации», «Защита информации с использованием интеллектуальных карт».

Учебное пособие выполнено в рамках инновационной образовательной программы Российского университета дружбы народов, направление «Комплекс экспортоориентированных инновационных образовательных программ по приоритетным направлениям науки и технологий», и входит в состав учебно-методического комплекса, включающего описание курса, программу и электронный учебник.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Курс с названием «Основы информационной безопасности» (Information Security) входит в целый ряд государственных образовательных стандартов по различным специальностям, например: 090102 – «Компьютерная безопасность», 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем», 090106 – «Информационная безопасность телекоммуникационных систем» и других. Тематика курса разрабатывается многими авторами, ими к настоящему времени подготовлено достаточно много книг, в том числе и учебных пособий. Обилие этих книг говорит об огромной величине рассматриваемой области, ее постоянном изменении и увеличении. Актуальность тематики обеспечена высокой динамикой развития информационных технологий и большой зависимостью их от обеспечения информационной безопасности.

В качестве основы для курса были выбраны следующие книги.

Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.

Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.

Галатенко В.А. Основы информационной безопасности: Курс лекций. – М.: ИНТУИТ. РУ, 2006. – 205 с.

Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с.

Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.

Все книги написаны известными специалистами в области информационной безопасности и во многом основаны на передовом зарубежном и отечественном опыте. Однако даже за прошедшее время с момента выхода книг произошли существенные изменения в данной области, например, вышли новые стандарты и рекомендации по вопросам информационной безопасности и новым технологиям, приняты новые законы и другие акты. В связи с этим должно быть переработано и дополнено содержание всех этих книг и курса на их основе. По-видимому, в последующем также надо будет учесть и процесс гармонизации международных и отечественных стандартов, особенности новых отраслевых стандартов.

Данный курс является основой для изучения других курсов, таких как «Управление информационными рисками», «Технические средства защиты информации», «Современная прикладная криптография», «Защита информации с использованием интеллектуальных карт», в которых должны быть расширены и углублены соответствующие разделы данного курса.

В настоящее время приобрело популярность получение международных сертификатов путем сдачи соответствующих квалификационных экзаменов. Одними из наиболее признанных являются сертификаты CISA и CISSP, выдаваемые Международным Информационным Консорциумом по Сертификации Защиты Систем (Information Security Certification Consortium (ISC)2 – www.isc2.org). Содержание курса должно учитывать требования и соответствующие разделы программ этих экзаменов, чтобы в последующем позволить студентам сдать данные экзамены без больших дополнительных усилий.

Отличительной особенностью данного курса является привлечение банковской тематики для демонстрации основных понятий и положений информационной безопасности. В настоящее время в России идет процесс формирования системы требований информационной безопасности для

организаций банковской системы, созданы несколько стандартов, система сертификации, методика проверки требований. Конечно, при этом использовался зарубежный опыт, но отечественные разработчики и специалисты по информационной безопасности внесли много нового в этот процесс.

Раздел 1. ОСНОВНЫЕ ПОНЯТИЯ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Изучению основ информационной безопасности должно предшествовать изучение курса информатики, где объясняется сам термин «информации» (от латинского informatio— «научение», «сведение», «оповещение»). В целях замкнутости изложения напомним некоторые сведения, которые будут использоваться далее.

Что такое «информация»? Ответить достаточно сложно. На общелексическом, бытовом уровне понятие «информация» обычно толкуется как «сообщение, осведомляющее о положении дел, о состоянии чего-нибудь». Заметим, что и в нормативных правовых актах чаще всего данное понятие употребляется именно в этом смысле. [Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. – М., 1992. – 255 с.]

Норберт Винер (1894–1964) определял информацию как «обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления». Он же говорил, что «информация есть информация, а не материя и не энергия».

Можно встретить и более глубокий подход к информации как «опосредованный формами связи результат отражения изменяемого объекта изменяющимся с целью сохранения их системной целостности» (см., например, Википедия).

Информация первична и содержательна – это категория, поэтому в категориальный аппарат науки она вводится описанием, через близкие категории: материя, система, структура, отражение. С информацией связаны понятия – знание, данные, сигналы, сообщения, смысл, семантика. Не следует путать категорию «информация» с понятием «знание». Знание определяется через категорию информация.

В материальном мире человека информация материализуется через свой носитель и благодаря ему существует. Сущность материального мира предстает перед исследователем в единстве формы и содержания. Передается информация через носитель. Материальный носитель придает информации форму. В процессе формообразования производится смена носителя информации.

В XX в. слово «информация» стало термином во множестве научных областей, получив особые для них определения и толкования.

Чтобы зафиксировать термин для дальнейшего обращения с ним, воспользуемся Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Итак, «**информация** – сведения (сообщения, данные) независимо от формы их представления».

В общем, это согласуется с трактовкой информации в справочной философской литературе последнего времени как «одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.».

Интересно отметить, что в отмененном Законе от 1995 г. «Об информации, информатизации и защите информации» указывалось, что «информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления». Как видим, старое определение хуже, перечисление страдает существенной неполнотой.

Приведем и некоторые другие понятия, связанные с термином «информация», из нового закона.

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

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

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Доступ к информации – возможность получения информации и ее использования.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети (иногда можно встретить термин **«компьютерная информация»** – информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ [Комментарии к УК РФ. Под ред. Скуратова Ю.И. и Лебедева В.М. – М.: НОРМА, 1996. – 832 с.]).

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Особо можно выделить понятие **конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В качестве комментария можно заметить, что это только часть возможных требований или свойств, которые возможны. Например, как будет подчеркнуто далее, можно выделить «целостность информации», «доступность информации» и другое.

Продолжая перечень понятий, выделим из [ГОСТ Р 50922-96] понятие: **защищаемая информация** – «информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми **собственником информации».**

Однако теперь по закону № 149-ФЗ к собственнику информации добавился еще и обладатель информации, защищающий ее ограничением доступа, как сказано в определении**.** К тому же в законе № 149-ФЗ понятие «защищаемая информация» отсутствует, хотя в старом законе оно было и говорилось, что **«защищаемая информация** – любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу». По-видимому, решили убрать ограничение, связанное с документированностью информации.

Согласно закону № 149-ФЗ, информация в зависимости **от категории доступа** к ней подразделяется на **общедоступную информацию**, а также на информацию, доступ к которой ограничен федеральными законами (**информация ограниченного доступа**).

К **общедоступной информации** относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. «Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации».

Кроме того, по закону, информация в зависимости **от порядка предоставления или распространения** подразделяется на информацию:

1) свободно распространяемую;

2) предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) подлежащую предоставлению или распространению в соответствии с федеральными законами;

4) ограниченную или запрещенную для распространения в Российской Федерации.

Закон РФ «О средствах массовой информации», принятый в 1991 г., определяет понятие **«массовая информация»** как «предназначенные для неограниченного круга лиц печатные, аудиовизуальные и иные сообщения и материалы». Довольно специфичной информацией являются так называемые **«кредитные истории»** и **«персональные данные»**, которые рассматриваются специальными законами, о которых будет говориться далее.

Хотя в новом законе № 149-ФЗ нет определения «защищаемая информация», в нем есть определение «защиты информации». (Защиту информации иногда путают с информационной безопасностью.)

«Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

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».

Это определение, конечно, требует комментария и сравнения с другими определениями из других документов. В п. 1 есть перечисление неправомерных действий, хотя неполное, но информативное. П. 2 касается только конфиденциальности, хотя можно потребовать и целостность и

доступность и другое. П. 3 некоторым образом все же касается обеспечения доступности информации.

Забегая вперед можно сказать, что это определение в своих пунктах фактически перефразирует требования по целостности, конфиденциальности и доступности информации, о которых будет сказано далее.

Для сравнения приведем ряд других определений, собранных в словаре Парфенова В.И., который вышел в 2003 г.

Защита информации –

1) деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [ГОСТ Р 50922-96 ЗИ. Основные термины и определения];

2) все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей. Она включает криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера [Указ Президента РФ № 1268 от 26 августа 1996 г.];

3) комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации [Положение о государственном лицензировании в области защиты информации от 27 апреля 1994 г.];

4) организационные, программные и технические методы и средства, направленные на удовлетворение ограничений, установленных для типов данных или экземпляров типов данных в системе обработки данных [Толковый словарь по информатике, 1991];

Далее отдельно будет рассмотрено понятие **«количества информации»,** которое изучалось и оценивалось многими

исследователями (Шеннон, Винера, Бриллюэн и др.). Например, К.Шеннон определял количество информации в сообщении как «меру неопределенности, которую оно устраняет для получателя». Отсюда путь через неопределенность, случайные величины, энтропию.

К. Шеннон предложил единицу измерения информации – бит. Количество информации описывается формулой вида:

$H = - \Sigma_{i=1}^{n} p_i \log p_i$

где p_i – вероятность появления i-го сигнала; n – количество возможных сигналов. (В обыденном понимании – чем неожиданнее новость, тем больше ее информативность.)

Колмогоров А.Н. в работе «Три подхода к определению понятия "Количество информации"» сформулировал три способа определения количества информации: комбинаторный, вероятностный и алгоритмический. [Новое в жизни, науке, технике. Серия «Математика, кибернетика», N 1, 1991. – С. 24–29 или «Проблемы передачи информации», N 1, 1965. – С. 1–7].

Однако математическая теория информации не охватывает всего богатства содержания информации, поскольку она, прежде всего, абстрагируется от содержательной (семантической) стороны сообщения. С точки зрения этой теории, «совокупность 100 букв, выбранных случайным образом, фраза в 100 слов из газеты, пьесы Шекспира или теорема Эйнштейна имеют в точности одинаковое количество информации». Тем не менее, глубокие теоретические и практические результаты были получены, например, в области секретной связи.

Актуальными являются сегодня и понятия «**информационная инфраструктура**», «**критические сегменты информационной инфраструктуры**» и др.

Предметом защиты является не только информация. В настоящее время в связи с рассматриваемой областью говорят об **активах (ресурсах),** а информация рассматривается как их часть.

В ряде документов **активы** или **ресурсы** (assets) – это «все, что имеет ценность для организации» [См., например, ISO/IEC 13335-1:2004]. Стандарт банка России СТО БР ИББС 1.0-2006 уточняет это определение. В частности, согласно стандарту **активы организации банковской системы Российской Федерации**: «все, что имеет ценность для организации банковской системы Российской Федерации и **находится в ее распоряжении»**.

К активам организации (Банка) могут относиться:

- банковские ресурсы (финансовые, людские, вычислительные, телекоммуникационные и пр.);

- информационные активы на следующих фазах их **жизненного цикла**: генерация (создание), обработка, хранение, передача, уничтожение;

- банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы, процессы жизненного цикла автоматизированных банковских систем и др.);

- банковские продукты и услуги.

В свою очередь информационные активы делятся на следующие типы:

финансово - аналитическая информация;

служебная информация;

управляющая информация общего и специального назначения;

справочная информация;

информация операционной и телекоммуникационной среды

платежная информация.

В качестве одного из важнейших активов также рассматривается **репутация организации**. В последнее время часто оценивается и так называемый **брэнд** организации или торговой марки.

Все активы организации должны быть идентифицированы и классифицированы удобным и приемлемым для нее образом. Примеры

рекомендаций для этого даны в проекте рекомендаций Банка России **РС БР ИББС-2.3-2008**.

Среди объектов защиты особую роль играют приводимые ниже объекты, определение которым мы приводим в данном разделе.

Помимо понятия «информационная система», важны и используются понятия «автоматизированная система», «автоматизированная информационная система» и, в частности, «автоматизированная банковская система».

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [ГОСТ 34.003-90]. В зависимости от вида деятельности выделяют виды автоматизированных систем:

АСУ – автоматизированная система управления,

САПР – система автоматизации проектирования, … .

Обращает внимание то, что персонал учитывается при определении автоматизированной системы, в отличие от определения «информационной системы» и следующего определения.

Автоматизированная информационная система – комплекс программных и технических средств, предназначенных для сбора, хранения, поиска и выдачи информации по запросам [Толковый словарь по информатике. – М.: Ф. и Ст., 1991].

Автоматизированная банковская система – автоматизированная система, реализующая банковский технологический процесс или его часть.

Сразу определим, что такое «банковский технологический процесс», упомянутый в определении. **Банковский технологический процесс** – технологический процесс, содержащий операции по изменению и (или) определению состояния банковской информации, используемой при функционировании или необходимой для реализации банковских услуг. В зависимости от вида деятельности выделяют: **банковский**

информационный технологический процесс, **банковский платежный технологический процесс** и др.

Чтобы определить, что такое «информационная безопасность», рассмотрим сначала само понятие «**безопасности**». Здесь тоже имеет место различие мнений и определений.

Вл. Даль определял, что «**безопасность** – есть отсутствие опасности, сохранность, надежность». В толковом словаре русского языка Ожегова С.И. сказано, что «**безопасность** – состояние, в котором не угрожает опасность, есть защита от опасности».

Закон «О безопасности» 1992 г. гласит, что «**безопасность** – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних **угроз**». Появилось новое понятие «угрозы», близкое к понятию «опасности», упоминавшемуся у Даля и Ожегова.

Приведем некоторые определения понятия «угрозы» по времени их появления в документах.

1. **Угроза** – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства [ФЗ «О безопасности» 05.03.1992].

2. **Угроза** – потенциальный источник возникновения **ущерба** [ГОСТ Р 51898-2002 п. 3.5].

3. **Угроза** – потенциальная причина **инцидента**, который может нанести **ущерб** системе или организации [ISO/IEC 13335-1:2004].

Как видно, в определениях появляются новые понятия «инцидента» и «ущерба».

Сначала рассмотрим понятие «инцидент», но не просто, а именно «инцидент информационной безопасности».

Инцидент информационной безопасности (information security incident)[ГОСТ ИСО/МЭК 13335-1] – любое непредвиденное или

нежелательное событие, которое может нарушить деятельность или информационную безопасность.

В качестве некоторых примеров инцидентов в ГОСТе указаны:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политик или рекомендаций;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Более сложно понятие «инцидента» определено в стандарте [ISO/IEC 18044: 2004], через «событие информационной безопасности».

Инцидент – событие, являющееся следствием одного или нескольких нежелательных или неожиданных **событий (информационной безопасности)**, имеющих значительную вероятность компрометации бизнес-операции и создания угрозы [ISO/IEC 18044: 2004].

Событием (информационной безопасности) является идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение **политики информационной безопасности,** или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [ISO/IEC 18044: 2004].

В стандарте Банка России понятие «инцидента» распространено на организацию банковской системы РФ.

Инцидент информационной безопасности организации банковской системы Российской Федерации – событие, вызывающее действительное, предпринимаемое или вероятное нарушение информационной безопасности организации банковской системы Российской Федерации.

Нарушение может вызываться либо ошибкой людей, либо неправильным функционированием технических средств, либо природными факторами (например, пожар или наводнение), либо преднамеренными злоумышленными действиями, приводящими к нарушению конфиденциальности, целостности, доступности, учетности или неотказуемости.

С инцидентом связано следующее понятие.

Воздействие (impact) – результат нежелательного инцидента информационной безопасности.

Говоря об угрозах, часто используется понятие **«модели угроз»**, которая, согласно стандарту СТО БР ИББС 1.0-2006, «включает описание **источников угроз**, **уязвимостей**, используемых угрозами, **методов и объектов нападений**, пригодных для реализации угрозы, **типов возможной потери**, **масштабов потенциального ущерба**».

Разберем понятие «модели угроз» по составляющим.

Источник угроз – субъект, материальный объект или физическое явление, создающее угрозу безопасности информации.

Для источников угроз – людей – разрабатывается **модель нарушителя.** В модели нарушителя конкретизируются субъекты, их средства, знания и опыт, с помощью которых они могут реализовать угрозы и нанести ущерб объектам, а также мотивации их действий.

Частным видом нарушителя является злоумышленник. **Злоумышленник** – основной субъект угроз, источник противоборства с собственником в борьбе за активы и доходы.

Уязвимость – недостатки или слабые места активов, которые могут быть использованы угрозой [СТО БР ИББС-1.0-2006]. Наличие уязвимости без присутствия угрозы не причиняет ущерба, но все уязвимости должны контролироваться на предмет изменения ситуации. Также и угрозы, не имеющие соответствующих уязвимостей, не приводят к ущербу, но должны учитываться.

Ущерб – физическое повреждение или другой вред здоровью людей, имуществу (активам) или окружающей среде. Количественная величина ущерба не всегда поддается оценке. В этих случаях для оценки ущерба может использоваться качественное описание.

Отечественный ГОСТ Р 51898-2002 определяет, что «**безопасность** – отсутствие недопустимого **риска**». То есть определяет безопасность через другое понятие «риск», которое более емко, чем просто понятие «опасности». К тому же упоминается не просто риск, а недопустимый риск. На этом понятии остановимся подробнее. Приведем ряд определений.

Риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба [ГОСТ Р 51898-2002. Аспекты безопасности].

В этом документе [ГОСТ Р 51898-2002] также сказано, что термин «риск» обычно используют только тогда, когда существует возможность негативных последствий, а в некоторых ситуациях риск обусловлен возможностью отклонения от ожидаемого результата или события.

Риск – сочетание вероятности события и его последствий [Guide 73: 2002 Risk Management – Vocabulary – Guidelines for use in standards].

Риск – неопределенность, предполагающая возможность потерь (ущерба) [СТО БР ИББС 0.1-2006].

Следует пояснить суть употребления слова «**вероятность**» в этих определениях. Об этом подчеркивается, например, и в известном австралийском стандарте AS/NZS 4360:2004 «Risk management». Вероятность здесь не математическое понятие и число между 0 и 1, а возможность или частота события. Часто вероятность оценивается качественно, например, в терминах «низкая», «средняя», «высокая».

На практике можно встретить следующие виды рисков: стратегический риск, юридический риск, операционный риск, репутационный риск, рыночный риск, кредитный риск, инвестиционный

риск, политический риск, проектный риск, ИТ- риск, риск информационной безопасности и другие.

Не вдаваясь здесь в подробное описание всех перечисленных рисков, приведем определение некоторых из важнейших.

Информационный риск (ИТ-риск) – это опасность возникновения убытков или ущерба в результате применения информационных технологий. Иными словами, ИТ-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи (М. Мур). С информационным риском наиболее связаны операционный риск и риск информационной безопасности.

Операционный риск – риск убытков, связанных с неадекватными либо неудачными внутренними процессами, действиями персонала или систем, а также в связи с внешними событиями. Операционный риск включает в себя юридический риск, но не включает стратегический и репутационный риски.

Это определение из рекомендаций Базель-2 в переводе ЦБ РФ. В подлиннике оно такое: «**Operational risk** is defined as: .the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events».

На мой взгляд, лучше следующий перевод: «**Операционный риск** определяется как риск прямых или косвенных потерь от неадекватных или имеющих недостатки внутренних процессов, от людей и систем или от внешних событий».

Суть в том, что персонал – это только часть людей. Внешние злоумышленники сюда не входят. Это один из примеров сложности перевода англоязычных терминов.

Определение **риска информационной безопасности** будет далее.

Завершая тему «риска», необходимо дать определение из [ГОСТ Р ИСО/МЭК 17799].

Менеджмент риска (risk management) – скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание. Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска [ISO/IEC Guide 73:2002].

Или

Менеджмент риска (risk management) – полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий. Это одно из определений, взятое из [ГОСТ Р ИСО/МЭК 13335-1].

Далее вопросу менеджмента или управления информационными рисками будет уделено внимание в отдельном курсе. Там будет нужна целая терминосистема по рискам.

Остаточный риск (residual risk) – риск, остающийся после его обработки.

Анализ риска (risk analysis) – систематический процесс определения величины риска.

Оценка риска (risk assessment) – процесс, объединяющий идентификацию риска, анализ риска и оценивание риска.

(Оценка риска (risk assessment) – общий процесс анализа риска и оценка степени риска. Это определение из [ISO/IEC Guide 73:2002] используется в ГОСТ Р ИСО/МЭК 17799-2005. Там же используется следующее понятие: **Оценивание риска (risk evaluation)** – процесс сравнения оцененного риска с данными критериями риска с целью определения значимости риска [ISO/IEC Guide 73:2002]. Это еще один из примеров трудности перевода.)

Обработка риска (risk treatment) – процесс выбора и осуществления мер по модификации риска. (Аналогично как в [ISO/IEC Guide 73:2002] и [ГОСТ Р ИСО/МЭК 17799-2005].) Обработка риска

включает: предотвращение, перенос, снижение и принятие риска. После обработки рисков могут оставаться **остаточные риски**.

Другие элементы терминосистемы по рискам будут рассмотрены отдельно.

Защитная мера (или мера защиты, контрмера, мера контроля) – мера, используемая для уменьшения риска [ГОСТ Р 51898-2002, ISO/IEC Guide 51].

Или, по другому, **защитная мера (safeguard)** – сложившаяся практика, процедура или механизм обработки риска. В контексте безопасности информационно-телекоммуникационных технологий термин «защитная мера» может считаться синонимом термина «**контроль**» [ГОСТ Р ИСО/МЭК 13335-1]. (Иногда говорят о «мерах и средствах защиты». В этом случае имеют в виду организационные меры и технические средства защиты.)

Базовые защитные меры (baseline controls) – минимальный набор защитных мер, установленный для системы или организации [ГОСТ Р ИСО/МЭК 13335-1]. Они соответствуют **базовому уровню безопасности** (Baseline Security) – обязательный минимальный уровень защищенности для информационных систем. В ряде стран существуют требования к системе защитных мер, соответствующих этому уровню (CCTA Baseline security survey – Великобритания, BSI IT-Grundschutz – Германия, ISACA, …).

Контрмеры базового уровня служат для защиты от стандартного набора наиболее распространенных угроз (вирусы, сбои оборудования, не санкционируемый доступ и т.д.).

В целом средства контроля могут обеспечивать один или несколько из следующих **видов защиты**: предупреждение, сдерживание, обнаружение, снижение, восстановление, исправление, мониторинг и информированность.

Защитные меры (контроли) имеют разветвленную сложную структуру и состоят из **организационных** и **программно-технических мер (или средств)** на верхнем уровне. В свою очередь, организационные меры включают **законодательные, административные и процедурные меры** защиты.

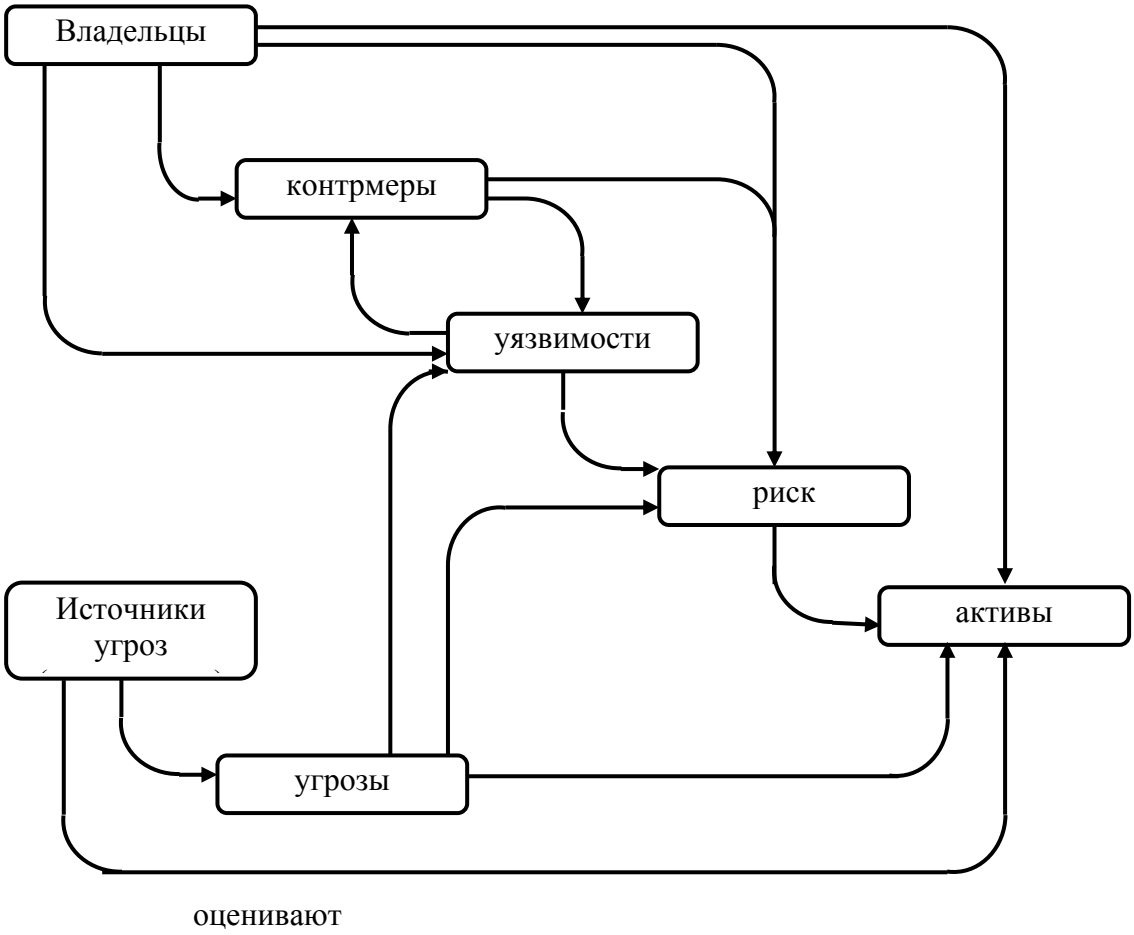


Рис. 1. Общие подходы к безопасности в соответствии с «Общими критериями»

Удобно далее говорить о **системе обеспечения безопасности**. Она включает силы и средства обеспечения безопасности, которые действуют и используются на основе разработанных заранее и закрепленных некоторым формальным образом принципов и правил (в виде нормативно-правовых актов, ведомственных инструкций, положений и т.п.).

Можно говорить, что **сущность функционирования системы безопасности** заключается в выявлении, прогнозировании, предотвращении, нейтрализации, пресечении, локализации, устранении, отражении и уничтожении угроз защищаемому объекту, а также формировании условий, благоприятствующих деятельности данного объекта, достижения им своих целей, защиты его интересов.

Система обеспечения безопасности того или иного объекта решает следующие задачи:

1. Своевременное выявление и прогнозирование внешних и внутренних угроз.
2. Осуществление комплекса оперативных и долговременных мер по предупреждению и нейтрализации внутренних и внешних угроз.
3. Создание и поддержание в готовности сил и средств для обеспечения безопасности.
4. Управление силами и средствами обеспечения безопасности в нормальных (повседневных) условиях и при возникновении чрезвычайных ситуаций.
5. Осуществление системы мер по нормальному функционированию объектов безопасности после возникновения чрезвычайных ситуаций.
6. Участие в мероприятиях по обеспечению безопасности за пределами своего объекта в соответствии с договоренностями (соглашениями) внутри корпорации или объединения фирм (предприятий).

В последнее время все чаще в обиход входит понятие «**система комплексной безопасности»** [92]. Под этим термином понимается «совокупность организационных мероприятий и действий подразделений охраны и служб безопасности организаций и автоматизированных систем по защите информации, направленных на обеспечение установленного режима, порядка и правил поведения, предотвращение, обнаружение и ликвидацию угроз жизни, среде обитания, имуществу и информации, а также поддержание работоспособности технических средств и систем на

охраняемом объекте с целью ограничения или предотвращения действий нарушителя для осуществления опасных несанкционированных операций на объекте, приводящих к частичному или полному нарушению функционирования данного объекта».

Фактически в этом определении просто расширен список угроз безопасности.

Говоря о безопасности, уместно вспомнить ФЗ «О техническом регулировании» 2002 г. В нем определена «**безопасность продукции, процессов производства, эксплуатации**, **хранения, перевозки, реализации и утилизации»** как «состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государству или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений».

Перейдем от понятия «безопасность» к понятию «информационная безопасность».

Понятие «**информационная безопасность**» было нормативно закреплено в качестве самостоятельной составляющей понятия безопасности в ФЗ «О безопасности» в 1992 г.

Далее в 1996 г. в ФЗ «Об участии в международном информационном обмене» сказано, что «**информационная безопасность** – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства». Здесь «**информационная среда** – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации».

В Доктрине информационной безопасности РФ от 2000 г. это определение приспособлено и уточнено для России. Именно под «**информационной безопасностью Российской Федерации**» понимается – состояние защищенности ее национальных интересов в

информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Вообще, обычно понятие «информационной безопасности» (ИБ) надо уточнять – информационная безопасность чего?

В словаре Парфенова В.И. [61] можно встретить определения: ИБ автоматизированных систем (АС), ИБ государства, ИБ личности, ИБ мирового сообщества, ИБ новых информационных технологий, ИБ общества, ИБ РФ. Этот список можно продолжать. Приведем здесь только одно из определений.

Информационная безопасность автоматизированных систем (АС) – область науки и техники, охватывающая совокупность программно-аппаратных, криптографических, технических и организационно-правовых методов и средств обеспечения безопасности информации в автоматизированных системах при ее обработке, хранении и передаче с использованием современных информационных технологий (Погорелов Б.А., Мацкевич И.Б. 1977).

Здесь вызывает возражение только упоминание «современных» технологий. Обращает на себя внимание другая классификация мер защиты, выделение криптографических методов и средств.

Многие вариации определений информационной безопасности были основаны на определении из британского стандарта BS 7799, вышедшего в 1995 г., где сказано, что **информационная безопасность** – защищенность ресурсов информационной системы от факторов, представляющих угрозу для конфиденциальности, целостности и доступности.

Доступность (availability) – свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта [ИСО/МЭК 7498-2]. Или проще, **доступность** – это возможность за приемлемое время получить требуемую информационную услугу.

Целостность (integrity) – свойство сохранения правильности и полноты активов [ГОСТ Р ИСО/МЭК 13335-1]. Или **целостность** – это актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность (confidentiality) – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса. [ИСО/МЭК 7498-2].

Есть и другие аспекты безопасности. К тому же приведенные аспекты конфиденциальности, целостности и доступности в разных системах имеют разный вес.

В ГОСТ Р ИСО/МЭК 13335-1:2005 это перечисление в определении больше.

Информационная безопасность (information security) – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Приведем те, которые еще не определены ранее.

Неотказуемость (non-repudiation) – способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты [ИСО/МЭК 13888-1, ИСО/МЭК 7498-2, ГОСТ Р 13335-1].

Подотчетность (учетность, отслеживаемость) (accountability) – свойство, обеспечивающее однозначное прослеживание действий любого логического объекта [ИСО/МЭК 7498-2]. Иногда переводится как **«учетность»,** например, в стандарте Банка России.

Аутентичность (authenticity) – свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Примечание. Аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

Достоверность (reliability) – свойство соответствия предусмотренному поведению и результатам.

Исторически к конфиденциальности было больше внимания. С этим понятием связано понятие **«тайна»**, которое имеет множество производных: государственная тайна, коммерческая тайна, адвокатская тайна, банковская тайна, врачебная тайна, налоговая тайна, нотариальная тайна, персональные данные, личная и семейная тайна, служебная тайна, тайна голосования, тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, тайна следствия и судопроизводства, тайна совещания судей, тайна страхования, тайна усыновления (удочерения), аудиторская тайна и др. (всего около 40). Приведем некоторые из них, которым посвящены отдельные законы Российской Федерации в силу их важности.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации [Закон РФ «О государственной тайне»].

В этом определении не уточняется, какие свойства сведений защищаются. Да и вообще, определение «тайны» через «сведения» не очень хорошо. Лучше следующее определение.

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [ФЗ РФ «О коммерческой тайне», 2004]. Далее формулировка была изменена на следующую:

Коммерческая тайна – режим конфиденциальной 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 [в редакции ФЗ от 02.02.06 № 19-ФЗ и от 24.07.07 «214-ФЗ]. Приведенные определения показывают, насколько сложен и динамичен процесс формирования основных понятий в данной области. Есть еще и определение из ст. 139 Гражданского кодекса РФ (см. далее).

Хотелось бы дать и собственное определение **информационной безопасности** как «безопасности, связанной с информацией или с информационной сферой». По аналогии с этим определением можно понять и определить, что такое: **государственная безопасность, экономическая безопасность, энергетическая безопасность, экологическая безопасность, пожарная безопасность, транспортная безопасность, банковская безопасность** и другие.

Информационная безопасность включает в себя **компьютерную безопасность** в качестве неотъемлемой составной части. Кроме того, по своему содержанию информационная безопасность включает: компьютерную безопасность; безопасность информационных систем и процессов; безопасность среды для реализации информационных процессов.

Приведем здесь определение компьютерной безопасности из словаря Парфенова В.И. [61]. **Компьютерная безопасность** – свойство компьютерной информации, ЭВМ, системы ЭВМ, сети ЭВМ, при котором с требуемой вероятностью обеспечивается защита компьютерной информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, копирования, блокирования, а также защита ЭВМ, системы ЭВМ, сети ЭВМ от неправомочного доступа, создания, использования и распространения вредоносных программ, нарушения правил эксплуатации, несанкционированной модификации программ и т.п..

Помимо **системы обеспечения (информационной) безопасности,** важна **система менеджмента информационной безопасности**.

В частности, для организаций банковской системы есть определение: **система менеджмента (управления – в некоторых документах) информационной безопасности организации банковской системы Российской Федерации; СМИБ (СУИБ) –** это часть общей системы менеджмента организации банковской системы Российской Федерации, основывающаяся на подходе бизнес-риска, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности организации банковской системы Российской Федерации [ISO/IEC IS 27001].

Система менеджмента включает структуру, политики, деятельности по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

Международный стандарт ISO/IEC IS 27001 содержит модель непрерывного циклического процесса менеджмента ИБ организации (**модель Деминга, модель Деминга-Шухарта**).

На **стадии планирования** устанавливают политики информационной безопасности, цели, задачи, процессы и процедуры, адекватные потребностям в менеджменте риска ИБ и совершенствованию СМИБ, для достижения результатов в соответствии с политиками и целями организации.

На **стадии реализации** осуществляются внедрение и поддержка политики информационной безопасности организации, средств управления (защитных мер), регламентов, процессов и процедур СМИБ организации.

На **стадии проверки** осуществляются оценка и, если необходимо, измерение эффективности процессов менеджмента ИБ организации на соответствие требованиям политики информационной безопасности, целям и установленным практикам, обеспечивается отчетность высшему руководству о результатах для проведения соответствующего анализа.

На **стадии совершенствования** осуществляются выработка и принятие корректирующих и превентивных действий, основанных на результатах анализа, для достижения непрерывного усовершенствования СМИБ организации.

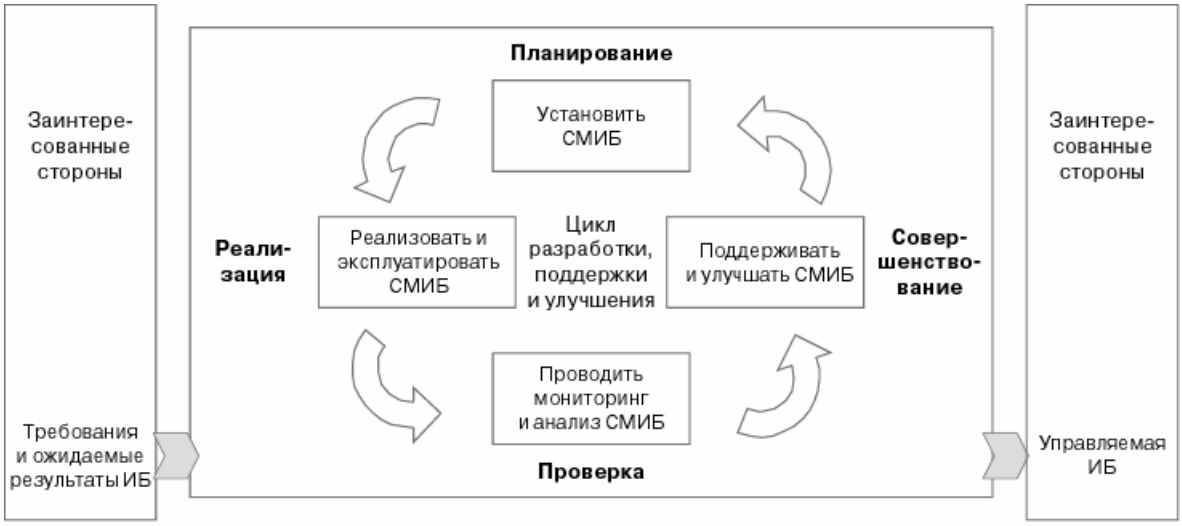


Рис. 2. Элементы процесса менеджмента ИБ

Использование для обеспечения ИБ «**процессного подхода»** на базе циклической модели Деминга, который является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ГОСТ Р ИСО 14001, позволит обеспечить поддержку и интеграцию требований к различным системам менеджмента в рамках общего корпоративного менеджмента в организациях.

Под **процессом** понимается совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующих входы в выходы (ГОСТ Р ИСО 9000-2001 «Системы менеджмента качества. Основные положения и словарь»).

Деятельность организации, направленную на цели бизнеса, можно представить в виде совокупности трех групп высокоуровневых процессов:

- основные процессы (процессы основной деятельности);

- вспомогательные процессы;

- процессы менеджмента (управления) организацией.

По определению система менеджмента ИБ (СМИБ), предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ, является частью общей системы менеджмента организации (BS 7799-2).

Построенный на основе методологии **IDEF0** рис. 3 иллюстрирует общую модель структур и связей деятельности в области ИБ и основной деятельности организации.

На модели видно, что **входными параметрами** для обеспечения ИБ организации являются:

- информация о среде организации;

- потребности организации в обеспечении ИБ (мнения менеджеров организации относительно ценности информационных активов);

- описания реализации бизнес-процессов;

- информация по контролю бизнес-процессов и технологий основной деятельности организации (как обратный цикл реализации нормативов по обеспечению ИБ организации).

Кроме того, для управления и обеспечения деятельности в этой области необходимы законы, нормативные документы, стандарты, относящиеся конкретно к этой проблеме, интеграция в общую систему менеджмента организации, а также ресурсы (финансовые, материальные, информационные), люди и оборудование.

В модели явно не представлена еще одна важнейшая деятельность – деятельность по менеджменту (управлению) организацией. Косвенно она представлена как управляющий сигнал на основную деятельность.

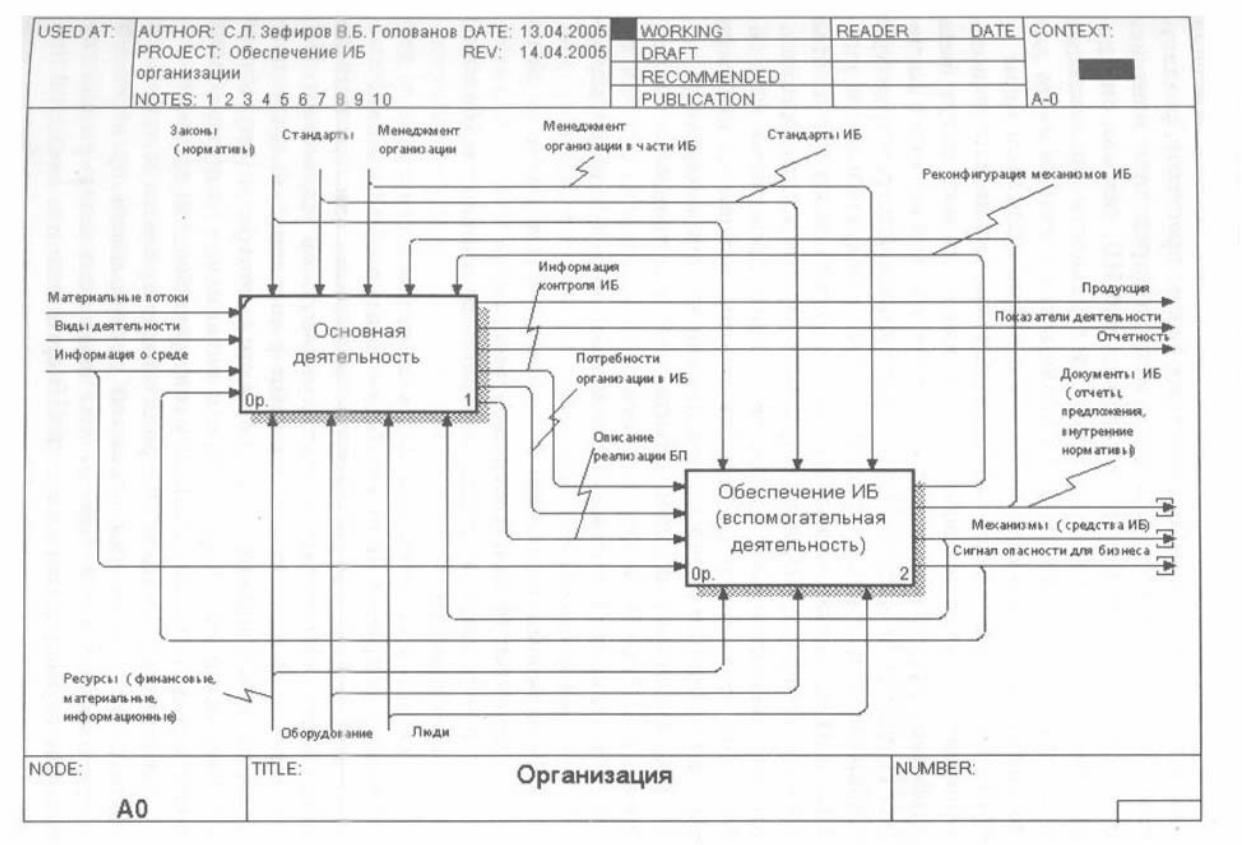


Рис. 3. Модель интеграции информационной безопасности в основную деятельность организации

Важнейшими исходными данными для эффективной деятельности служб ИБ являются информационные модели основной деятельности организации (описания бизнес-процессов, реализуемых технологий и т.п.). Данные модели определяют контекст и акценты внимания деятельности служб ИБ, так как они позволяют понять, где в структуре деятельности организации в части информатики имеются уязвимости для потенциальных злоумышленников, какие защитные меры могут потребоваться и какие из них могут быть наиболее эффективными.

Результатами (выходами) деятельности и процессов по обеспечению ИБ организации являются:

- документы (отчеты, предложения, внутренние нормативные документы);

- механизмы (средства) обеспечения ИБ и решения по их реконфигурации (совершенствованию);

- сигнал опасности для основной деятельности (бизнеса) организации.

Механизмы обеспечения ИБ, являющиеся результатом деятельности и процессов по ее обеспечению в организации, выступающие в качестве ресурсного обеспечения для основной деятельности организации, эксплуатируются службами ИБ, а в отдельных случаях и основными функциональными подразделениями организации. Информация контроля результатов применения и функционирования механизмов (защитных мер) поступает для анализа в службу информационной организации.

Остановимся подробнее на важном понятии «**политика безопасности**». Приведем несколько определений.

Политика безопасности организации – одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Далее появились разновидности этого определения. Например, такое.

Политика безопасности информационно-телекоммуникационных технологий (политика безопасности ИТТ) (ICT security policy) – правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию [ГОСТ Р 13335-1].

Нас будет в основном интересовать «политика информационной безопасности». Согласно [ГОСТ Р ИСО/МЭК 17799-2005] **политика информационной безопасности** должна быть утверждена высшим руководством, издана и доведена до сведения всех сотрудников и соответствующих внешних сторон. Документ о политике информационной безопасности должен устанавливать ответственность руководства и

излагать подход организации к управлению информационной безопасностью. Политика должна содержать следующие положения:

а) определение информационной безопасности, ее общих целей и сферы действия, а также упоминание значения безопасности как инструмента, обеспечивающего возможность совместного использования информации (см. Введение);

б) изложение намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;

в) основание для установки целей контроля и мер контроля, включая структуру оценки риска и менеджмент риска;

г) краткое изложение наиболее существенных для организации политик безопасности, принципов, стандартов и требований, включающее:

1) соответствие законодательным, регулятивным требованиям и договорным обязательствам;

2) требования в отношении обучения и осведомленности в вопросах безопасности;

3) управление непрерывностью бизнеса;

4) ответственность за нарушения политики информационной безопасности;

д) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

е) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Такая политика информационной безопасности должна быть доведена до сведения пользователей в рамках всей организации в уместной, доступной и понятной форме.

Политика информационной безопасности может быть частью документа общей политики. Если политика информационной безопасности распространяется вне организации, то нужно обратить внимание на неразглашение секретной информации. Дополнительную информацию можно найти в ISO/IEC 13335-1:2004.

Политика информационной безопасности должна пересматриваться через запланированные промежутки времени или в случае появления существенных изменений в целях обеспечения ее непрерывной стабильности, адекватности и эффективности.

Политика информационной безопасности должна иметь владельца, который утвердил административную ответственность за развитие, пересмотр и оценку политики безопасности. Пересмотр должен включать возможности оценки для улучшения политики информационной безопасности организации и подход к управлению информационной безопасностью в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.

В стандарте Банка России приводится понятие политики ИБ банковской системы, похожее на предыдущие определения. **Политика информационной безопасности организации банковской системы Российской Федерации** – одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется организация банковской системы Российской Федерации в своей деятельности.

Завершает раздел **исходная концептуальная схема (парадигма) обеспечения информационной безопасности**, которая обсуждается в книге [82] и стандарте Банка России СТО БР ИББС 0.1-2006. **Суть парадигмы ИБ –** противоборство собственника и злоумышленника за

права на информационные активы в целях последующего извлечения дохода.

На самом деле, цели злоумышленника могут быть и другие. Поэтому это понятие трактуется и конкретизируется в стандарте Банка России следующим образом.

В основе **исходной концептуальной схемы информационной безопасности организаций БС РФ** лежит противоборство собственника и злоумышленника за контроль над информационными активами. В случае если злоумышленник устанавливает контроль над информационными активами, как самой организации БС РФ, так и клиентам, которые доверили ей свои собственные активы, может быть нанесен ущерб.

Далее по разделам будут появляться характерные им термины и определения.

Раздел 2. ПОНЯТИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ, ВИДЫ БЕЗОПАСНОСТИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РФ

Материал данного раздела основан на материалах учебных пособий [86 и 92]. Фактически здесь демонстрируется применение понятия «информационной безопасности» к такому объекту, как Российская Федерация.

В Концепции национальной безопасности РФ, утвержденной Указом Президента РФ от 17.12.1997 г. № 1300 (в редакции Указа Президента РФ от 10.01.2000 г. № 24), дается следующее определение национальной безопасности.

Под **национальной безопасностью РФ** понимается безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в РФ.

Национальные интересы России – это совокупность сбалансированных интересов личности, общества и государства в различных сферах жизнедеятельности: экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других. В теории национальной безопасности используется понятие **«жизненно важные интересы».** Жизненно важные интересы – это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства [55]. Как правило, понятия «национальные интересы» и «жизненно важные интересы» являются идентичными.

Национальные интересы носят долгосрочный характер. В области внутренней и внешней политики государства этими интересами определяются: основные цели этой политики; стратегические и текущие задачи.

Национальные интересы обеспечиваются **институтами государственной власти**, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ общественными организациями.

Интересы личности состоят в реализации конституционных прав и свобод [55], в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина.

Интересы общества состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

Национальные интересы России в **информационной сфере** заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Важнейшими составляющими национальных интересов России являются защита личности, общества и государства от терроризма, в том числе международного, а также от чрезвычайных ситуаций природного и техногенного характера и их последствий, а в военное время – от опасностей, возникающих при ведении военных действий или вследствие этих действий.

Достижению национальных интересов препятствуют те или иные уязвимости и угрозы.

Уязвимостями для национальной безопасности страны, например, являются: состояние отечественной экономики, несовершенство системы организации государственной власти и гражданского общества, наличие преступности и терроризма, обострение межнациональных и осложнение международных отношений и другие.

Усиливаются угрозы национальной безопасности РФ в информационной сфере. Серьезными угрозами являются: стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции **информационных войн**; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Обеспечение национальной безопасности РФ во многом определяется состоянием информационной безопасности.

Важнейшими задачами обеспечения информационной безопасности РФ являются:

• реализация конституционных прав и свобод граждан РФ в сфере информационной деятельности;

• совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

• противодействие угрозе развязывания противоборства в информационной сфере.

Основу системы обеспечения национальной безопасности РФ составляют органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера,

направленные на обеспечение безопасности личности, общества и государства.

Полномочия органов и сил обеспечения национальной безопасности РФ, их состав, принципы и порядок действий определяются соответствующими законодательными актами РФ.

Условно можно выделить следующие **составляющие национальной безопасности**: экономическую, внутриполитическую, социальную, духовную, международную, информационную, военную, пограничную, экологическую.

Содержание каждой из перечисленных составляющих отражено в соответствующих **нормативных правовых актах**.

Информатизация является характерной чертой жизни современного общества. Новые информационные технологии активно внедряются во все сферы народного хозяйства. Компьютеры являются основой множества автоматизированных систем обработки информации (АСОИ). По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. **Информационная сфера** представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений [Доктрина ИБ РФ, 2000].

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенным образом зависит от

обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать [Доктрина ИБ РФ, 2000].

Напомним, что под **информационной безопасностью РФ** понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [Доктрина ИБ РФ, 2000].

Доктрина информационной безопасности РФ дает **две классификации национальных интересов в информационной сфере**:

• первую можно назвать классификацией по принадлежности интересов;

• вторую можно назвать классификацией по важности интересов.

В соответствии с первой классификацией национальные интересы – это совокупность интересов личности, интересов общества и интересов государства.

Интересы личности:

• Реализация конституционных прав на доступ к информации.

• Использование информации в интересах осуществления не запрещенной законом деятельности.

• Физическое, духовное и интеллектуальное развитие.

• Защита информации, обеспечивающей личную безопасность.

Интересы общества:

• Обеспечение интересов личности в информационной сфере.

• Упрочение демократии, создание правового, социального государства.

• Достижение и поддержание общественного согласия.

• Духовное обновление России.

Интересы государства:

• Гармоничное развитие российской информационной инфраструктуры.

• Реализация конституционных прав человека и гражданина в области получения информации и пользования ею.

• Незыблемость конституционного строя, суверенитета и территориальной целостности России.

• Политическая, экономическая и социальная стабильность.

• Безусловное обеспечение законности и поддержание правопорядка.

• Развитие равноправного и взаимовыгодного международного сотрудничества.

Угрозы и источники угроз в информационной сфере Российской Федерации

По своей общей направленности угрозы информационной безопасности РФ подразделяются на следующие виды [Доктрина ИБ РФ, 2000]:

• угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

• угрозы информационному обеспечению государственной политики РФ;

• угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

• угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Источники угроз информационной безопасности РФ подразделяются на внешние и внутренние.

Внешними источниками угроз, например, являются:

• иностранные политические, экономические, военные, разведывательные и информационные структуры, направленные против интересов РФ в информационной сфере;

• международные террористические организации;

• увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

• разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Внутренними источниками угроз, например, являются:

• критическое состояние отечественных отраслей промышленности;

• неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

• недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ 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;

• недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;

• недостаточная экономическая мощь государства;

• снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

• недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

• отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Хотя в Доктрине и приведены эти внутренние источники, но фактически они являются не источниками, а уязвимостями. Все зависит от понимания этих понятий.

Общая структура государственной системы обеспечения информационной безопасности Российской Федерации

На рис. 4 представлена указанная структура в виде схемы из работы [76].

Рис. 4. Структура государственной системы обеспечения информационной безопасности Российской Федерации

Рассмотрим **структуру государственной системы информационной безопасности** и основные функции ее составных частей.

Основным органом, координирующим действия государственных структур по вопросам защиты информации, является Межведомственная комиссия по защите государственной тайны, созданная Указом Президента РФ № 1108 от 8.11.1995 г. Она действует в рамках Государственной системы защиты информации от утечки по техническим каналам, положение о которой введено в действие постановлением Правительства РФ от 15.09.1993 г. № 912-51. В этом постановлении определены структура, задачи и функции, а также организация работ по защите информации применительно к сведениям, составляющим государственную тайну. Основной задачей государственной системы защиты информации является проведение единой технической политики, организация и

координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности страны.

Президент РФ, Совет Безопасности, Государственная Дума, Межведомственная комиссия по защите государственной тайны, ФСТЭК, ФСБ, СВР и др.

Общая организация и координация работ в стране по защите информации, обрабатываемой техническими средствами, осуществляется **Федеральной службой по техническому и экспортному контролю (ФСТЭК России).**

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по следующим вопросам в области обеспечения информационной безопасности:

1) обеспечение безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;

2) противодействие иностранным техническим разведкам на территории РФ;

3) обеспечение защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории РФ;

4) защита информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

Основными задачами в области обеспечения информационной безопасности для ФСТЭК России являются:

1) реализация в пределах своей компетенции государственной политики в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;

2) осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

3) 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;

4) осуществление самостоятельного нормативно-правового регулирования вопросов: обеспечения безопасности информации в ключевых системах информационной инфраструктуры; противодействия техническим разведкам; технической защиты информации; размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров РФ, иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ; координации деятельности органов государственной власти по подготовке развернутых перечней сведений, подлежащих засекречиванию, а также методического руководства этой деятельностью;

5) обеспечение в пределах своей компетенции безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

6) прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;

7) противодействие добыванию информации техническими средствами разведки, техническая защита информации;

8) осуществление координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ и организаций по государственному регулированию размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров РФ, иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ;

9) осуществление в пределах своей компетенции контроля деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

10) осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны.

ФСТЭК России в своей деятельности руководствуется Конституцией РФ, федеральными конституционными законами, федеральными законами, актами Президента РФ и Правительства РФ, международными договорами РФ, приказами и директивами Министра обороны РФ в части, касающейся ФСТЭК России, положением о ФСТЭК России, а также другими нормативными правовыми актами РФ, касающимися деятельности ФСТЭК России.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов РФ, федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, органами местного самоуправления и организациями.

ФСТЭК России осуществляет свою деятельность во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, органами местного самоуправления и организациями.

Обеспечение информационной безопасности является одним из основных направлений деятельности органов **Федеральной службы безопасности (ФСБ) России**.

Обеспечение информационной безопасности осуществляется ими в пределах своих полномочий:

• при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;

• при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в РФ и ее учреждениях, находящихся за пределами РФ.

Служба внешней разведки РФ для осуществления своей деятельности может при собственных лицензировании и сертификации приобретать, разрабатывать (за исключением криптографических средств защиты), создавать, эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации от утечки по техническим каналам.

Министерство обороны (Минобороны России) организует деятельность по обеспечению информационной безопасности, защите государственной тайны в Вооруженных силах, а также в установленном порядке в пределах своей компетенции работы по сертификации средств защиты информации.

Другие органы государственного управления (министерства, ведомства) в пределах своей компетенции:

• определяют перечень охраняемых сведений;

• обеспечивают разработку и осуществление технически и экономически обоснованных мер по защите информации на подведомственных предприятиях;

• организуют и координируют проведение НИОКР в области защиты информации в соответствии с государственными (отраслевыми) программами;

• разрабатывают отраслевые документы по защите информации;

• контролируют выполнение на предприятиях отрасли установленных норм и требований по защите информации;

• создают отраслевые центры по защите информации и контролю эффективности принимаемых мер;

• организуют подготовку и повышение квалификации специалистов по защите информации.

Для осуществления указанных функций в составе органов государственного управления функционируют научно-технические подразделения (центры) защиты информации и контроля.

На предприятиях, выполняющих оборонные и иные секретные работы, функционируют научно-технические подразделения защиты информации и контроля, координирующие деятельность в этом направлении научных и производственных структурных подразделений предприятия, участвующие в разработке и реализации мер по защите информации, осуществляющие контроль эффективности этих мер.

Кроме того, в отраслях промышленности и в регионах страны создаются и функционируют лицензионные центры, осуществляющие организацию и контроль за лицензионной деятельностью в области оказания услуг по защите информации, органы по сертификации средств вычислительной техники и средств связи, испытательные центры по сертификации конкретных видов продукции по требованиям безопасности информации, органы по аттестации объектов информатики.

Государственная система обеспечения информационной безопасности создается для решения следующих проблем, требующих законодательной поддержки:

• защита персональных данных;

• борьба с компьютерной преступностью, в первую очередь в финансовой сфере;

• защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;

• защита государственных секретов;

• создание системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;

• обеспечение безопасности АСУ потенциально опасных производств;

• страхование информации и информационных систем;

• сертификация и лицензирование в области безопасности, контроль безопасности информационных систем;

• организация взаимодействия в сфере защиты данных со странами – членами СНГ и другими государствами.

Ключевыми проблемами также являются:

1. Формирование законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, нормативного закрепления ответственности должностных лиц и граждан по соблюдению требований информационной безопасности.

2. Разработка механизмов реализации прав граждан на информацию.

3. Формирование системы информационной безопасности, обеспечивающей реализацию государственной политики в этой области.

4. Совершенствование методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

5. Разработка критериев и методов оценки эффективности систем и средств информационной безопасности.

6. Исследование форм и способов цивилизованного воздействия государства на формирование общественного сознания.

7. Комплексное исследование деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

Огромную роль в информационной сфере в России в настоящее время также играют Мининформсвязи и ФАИТ. Большую работу для обеспечения информационной безопасности кредитно-финансовой сферы РФ проводит Центральный банк.

Государственная информационная политика обеспечения информационной безопасности России

Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах [Доктрина ИБ РФ]:

• соблюдении Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ;

• открытости в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающей информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;

• правовом равенстве всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающемся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

• приоритетном развитии отечественных современных информационных и телекоммуникационных технологий, производстве технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Первоочередными **мероприятиями по реализации государственной политики обеспечения информационной безопасности РФ** являются [Доктрина]:

• разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности РФ;

• разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;

• принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов РФ, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов РФ, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;

• развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ;

• гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

Раздел 3. МЕЖДУНАРОДНАЯ, НАЦИОНАЛЬНАЯ И ВЕДОМСТВЕННАЯ НОРМАТИВНАЯ ПРАВОВАЯ БАЗА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информация в жизни современного общества играет значительную роль. Современные информационные технологии проникли практически во все сферы общественных отношений. Это привело к необходимости создания правовых норм, регулирующих область информационных отношений. Такие нормы необходимы в силу того, что информация обладает рядом специфических свойств, которые принципиально отличают ее от других объектов права. Украсть информацию можно, не проникая в помещение, в котором она хранится, к тому же, информация после похищения, как правило, остается в распоряжении владельца в неизменном виде.

Правовое обеспечение информационной безопасности заключается в исполнении существующих или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц, руководителей, пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной им информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к техническим средствам и информации. Целью законодательных мер по защите информации являются предупреждение и сдерживание потенциальных нарушителей.

Для уяснения правовой сущности различных документов, с помощью которых осуществляется регулирование отношений, связанных с обеспечением информационной безопасности, рассмотрим общеправовые понятия, прежде всего **понятие нормативности**, производными от

которого являются понятия **правовой нормы**, **нормативного правового акта**, **нормативного документа**.

Всякий акт (документ), принятый уполномоченным законом органом или лицом в пределах своей компетенции, является правовым, поскольку он регулирует соответствующие отношения. Правовые акты могут быть обязательными для неопределенного круга лиц, иметь персональный или рекомендательный характер. Акты обязательные именуются **нормативными правовыми актами**, все другие – **ненормативными правовыми актами**. Географические границы действия нормативных правовых актов определяются статусом принимающего их органа или должностного лица (федеральный, субъекта Российской Федерации, муниципальный). Нормативные правовые акты, принимаемые организациями, именуются **локальными**.

В законодательстве отсутствует определение понятия нормативного правового акта. Основные признаки нормативного правового акта даются в теории права, документах органов власти. В одном из постановлений Государственной Думы Федерального Собрания Российской Федерации за 1996 г. **нормативный правовой акт** определен как письменный официальный документ, принятый (изданный) в определенной форме правотворческим органом в пределах его компетенции и направленный на установление, изменение или отмену правовых норм. Под **правовой нормой** понимается общеобязательное правило поведения, установленное уполномоченным государственным органом и предназначенное для неоднократного применения.

Пленум Верховного Суда Российской Федерации в Постановлении от 25 мая 2000 г. № 19 разъяснил, что под **нормативным правовым актом** понимается изданный в установленном порядке акт уполномоченного на то органа государственной власти, органа местного самоуправления или должностного лица, устанавливающий правовые нормы (правила поведения), обязательные для неопределенного круга лиц,

рассчитанные на неоднократное применение, действующие независимо от того, возникли или прекратились конкретные правоотношения, предусмотренные актом. Приведенное определение повторено в Постановлении Пленума Верховного Суда Российской Федерации от 20 января 2003 г. № 2 (п. 12).

В отличие от нормативного правового акта акт, устанавливающий, изменяющий или отменяющий права и обязанности конкретных лиц, именуется **правовым актом индивидуального характера**, или **ненормативным правовым актом**. К таким актам относятся, в частности, документы, используемые в правоприменительной деятельности.

Таким образом, нормативными правовым актами являются соответствующие законы Российской Федерации и субъектов Российской Федерации, указы Президента Российской Федерации, постановления Правительства Российской Федерации, акты федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, муниципальных органов, руководящих органов организаций.

Согласно Указу Президента Российской Федерации от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» право принимать нормативные акты имеют не все федеральные органы исполнительной власти, а только федеральные министерства. Но эти министерства в соответствии с Федеральным законом «О техническом регулировании» лишены такого права в сфере технического регулирования, где могут издавать только акты рекомендательного характера. Исключение из данного правила установлено в ст. 5 данного Закона в отношении специальной продукции, работ и услуг.

С учетом сказанного информацию в правовой системе по ее роли можно разделить на правовую и не правовую, как показано на рис. 5.

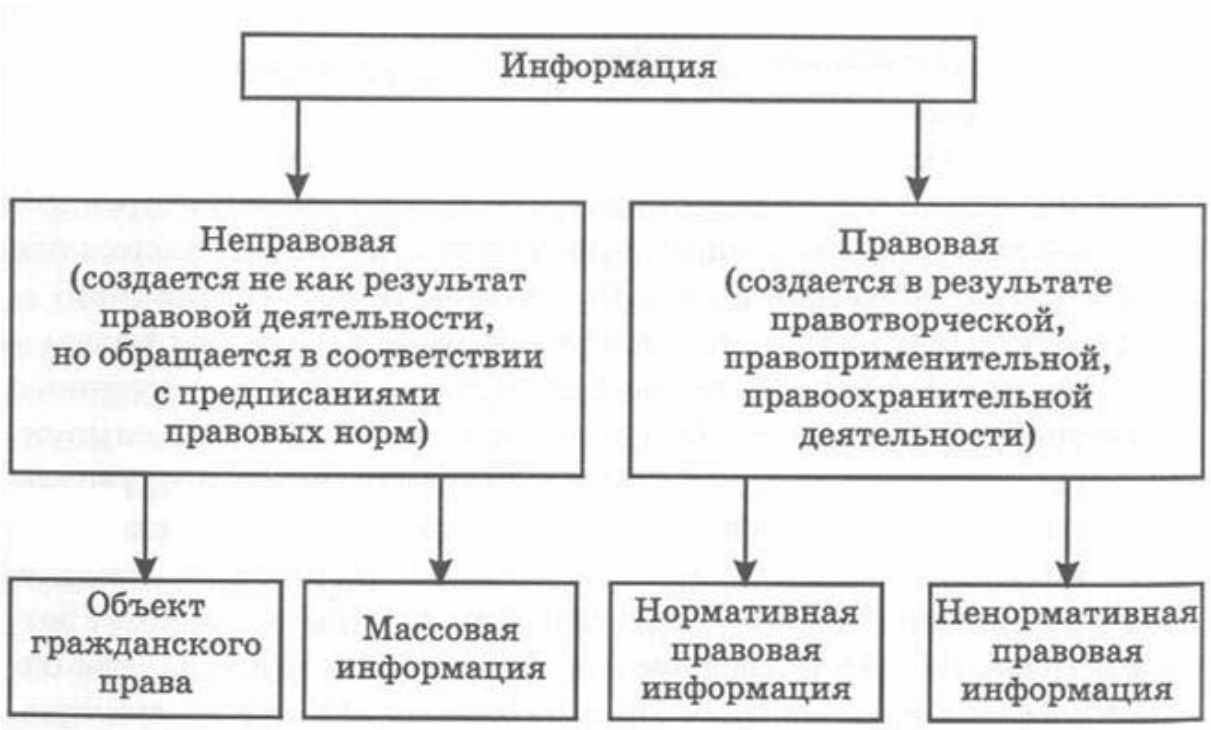


Рис. 5. Классификация информации по ее роли в правовой системе

Нормативная правовая информация создается в порядке правотворческой деятельности и содержится в нормативных правовых актах. Классификация такой информации по уровню принятия актов или по видам актов приведена на рис. 6.

Ненормативная правовая информация создается, как правило, в порядке правоприменительной и правоохранительной деятельности. С помощью такой информации реализуются предписания правовых норм. Эта информация создается в объекте управления и движется в контуре обратной связи системы правового управления.

Рис. 6. Классификация нормативной правовой информации по видам актов

На следующем рис. 7 представлена обобщенная схема нормативно-правового и справочного обеспечения информационной безопасности (ИБ) информационных технологий (ИТ).

Рис. 7. Обобщенная схема нормативно-справочного обеспечения информационной безопасности (ИБ) информационных технологий

В соответствии с Конституцией России международные документы, подписанные от имени Российской Федерации, имеют приоритет над соответствующими документами федерального уровня. Документы, не подписанные от имени России, могут использоваться, если они не противоречат законодательству страны.

Закон – это нормативно-правовой акт, принимаемый высшим представительным органом государственной власти в особом законодательном порядке, обладающий высшей юридической силой и регулирующий наиболее важные общественные отношения с точки зрения интересов и потребностей населения страны.

Подзаконные нормативно-правовые акты – это правотворческие акты компетентных органов, которые основаны на законе и не противоречат ему. По своему содержанию подзаконные акты, как правило,

являются актами различных органов исполнительной власти. По субъектам издания и кругу распространения они подразделяются на общие, местные, ведомственные и внутриорганизационные акты.

Общие подзаконные акты – это нормативно-правовые акты общей компетенции, действие которых распространяется на всех лиц в пределах территории страны. По своей юридической силе и значению – следуют за законами. Они исходят от президента страны или главы правительства.

Указы Президента – в системе подзаконных актов обладают высшей юридической силой и издаются на основе и в развитии законов.

Постановления Правительства – это подзаконные нормативные акты, принимаемые в контексте с указами президента и призванные урегулировать более мелкие вопросы государственного управления экономикой, образованием и т.д.

Местные подзаконные акты – это нормативно-правовые акты органов представительной власти на местах. Действие этих актов ограничено подвластной им территорией.

Ведомственные нормативно-правовые акты (приказы, инструкции) – это нормативно-правовые акты общего действия, однако они распространяются лишь на ограниченную область общественных отношений (таможенные, банковские, транспортные и др.

Внутриорганизационные подзаконные акты – это такие нормативно- правовые акты, которые издаются различными организациями для регламентации своих внутренних вопросов и распространяются на членов этих организаций.

К числу **международных актов** относят: декларации; конвенции; рекомендации; соглашения; стандарты. Разработкой этих документов занимаются различные структурные подразделения международных организаций, такие как:

Организация Объединенных Наций;

Совет Европы (комитет министров);

Европейский комитет по проблемам преступности;

Комитет экспертов по преступности в киберпространстве (КЭ-ПК);

Международная электротехническая комиссия (МЭК/IEC);

Международная организация по стандартизации (ИСО/ISO);

Британский институт стандартов (BSI);

Американский институт AICPA

и др.

Россия неоднократно выступала с инициативами в области международной информационной безопасности (резолюции Генеральной ассамблеи ООН A/RES/56/19 – ноябрь 2001 г., A/RES/57/53 – ноябрь 2002 г., A/RES/58/32 – декабрь 2003 г.). В соответствии с принятыми резолюциями с 2002 г. проходят Всемирные встречи на высшем уровне по вопросам информационного общества. Последняя из них состоялась 16–18 ноября 2005 г. в Тунисе.

В 2004 г. была создана специальная Группа правительственных экспертов государств – членов ООН. Эта группа должна провести всестороннее исследование проблем международной информационной безопасности, подготовить свои рекомендации для их решения.

Среди всех международных нормативных актов в области информационной безопасности в нашей стране чаще всего применяются **организационно-технические документы**, в частности **стандарты**. Большая часть из них принята в качестве национальных стандартов в сфере защиты информации.

Отечественная федеральная и ведомственная нормативная база по защите информации к настоящему времени включает более сотни нормативных документов, относящихся к вопросам информационной безопасности на государственном, региональном, местном, ведомственном уровнях. По своему назначению и содержанию их можно разделить на **три группы:**

1. Концептуальные документы, определяющие основу защиты информации в России.

2. Федеральные законы, определяющие систему защиты информации в России.

3. Вспомогательные нормативные акты в виде указов Президента РФ, постановлений Правительства РФ, межведомственных и ведомственных руководящих документов и стандартов, регулирующих процесс и механизмы исполнения положений и требований к системе обеспечения информационной безопасности государства.

Концептуальные документы

Информационное право как нормативная база информационного общества, как и само информационное общество, только формируется. Бурное наступление реалий информационного общества требует пересмотра представлений об информационной индустрии, ее роли и месте в обществе. Если рассматривать проблему формирования информационного общества в целом, то специфика современного момента выражается в том, что дальнейший прогресс информационных и телекоммуникационных технологий зависит не столько от прорывов собственно в технологиях, сколько от того, насколько быстро будут приспособлены к новым реалиям старые нормы, регулирующие традиционно разные сектора – телекоммуникации, телевидение и иные средства массовой информации.

Окинавская хартия

В июле 2000 г. в Окинаве «восьмерка» развитых стран приняла **Хартию глобального информационного общества**, в которой устанавливаются основные принципы вхождения государств и стран в это общество. «Восьмерка» провозгласила основные положения, которые страны будут применять при осуществлении политики по формированию и развитию информационного общества:

- информационно-коммуникационные технологии (ИТ) – один из наиболее важных факторов, влияющих на формирование общества XXI в.;

- суть стимулируемой ИТ экономической и социальной трансформации заключается в ее способности содействовать людям и обществу в использовании знаний и идей;

- стремясь к достижению этих целей, руководители стран «восьмерки» подтверждают свою приверженность принципу участия в этом процессе исходя из того, что все люди повсеместно без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества;

- руководители стран «восьмерки» будут осуществлять руководство в продвижении усилий правительств по укреплению соответствующей политики и нормативной базы, стимулирующих конкуренцию и новаторство, по обеспечению экономической и финансовой стабильности, содействующих сотрудничеству, по оптимизации глобальных сетей, борьбе со злоупотреблениями, которые подрывают целостность сети, по сокращению разрыва в цифровых технологиях, инвестированию в людей и обеспечению глобального доступа и участия в этом процессе;

- Хартия является, прежде всего, призывом ко всем как в государственном, так и в частном секторах ликвидировать международный разрыв в области информации и знаний.

В Хартии выделяются четыре раздела, раскрывающих основные подходы по использованию возможностей цифровых технологий, преодолению электронно-цифрового разрыва, содействию всеобщему участию, дальнейшему развитию. Отмечается, что задача создания предсказуемой, транспарентной и не дискриминационной политики и нормативной базы, необходимой для информационного общества, лежит на правительствах. Необходимо заботиться о том, чтобы правила и процедуры, имеющие отношение к ИТ, соответствовали коренным изменениям в экономических сделках с учетом принципов эффективного

партнерства между государственным и частным секторами, а также транспарентности и технологической нейтральности. Такие правила должны быть предсказуемыми и способствовать укреплению делового и потребительского доверия.

«Восьмерка» рекомендует, в частности, совместную работу представителей органов власти стран по защите интеллектуальной собственности в области информационных технологий, подтверждает обязательство правительств использовать только лицензированное программное обеспечение, продвижение рыночных стандартов, включая, например, технические стандарты функциональной совместимости, повышение доверия потребителя к электронным рынкам в соответствии с руководящими принципами ОЭСР, в том числе посредством эффективных саморегулирующих инициатив, таких, как кодексы поведения, маркировка и другие программы подтверждения надежности, и изучение вариантов устранения сложностей, которые испытывают потребители в ходе трансграничных споров, включая использование альтернативных механизмов разрешения споров, развитие эффективного и значимого механизма защиты личной жизни потребителя, а также защиты личной жизни при обработке личных данных, с обеспечением при этом свободного потока информации, дальнейшее развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций.

Отмечается также, что усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности кибер-пространства. «Восьмерка» берет на себя обязательство обеспечить осуществление эффективных мер, как это указано в Руководящих принципах по безопасности информационных систем ОЭСР, в борьбе с преступностью в

компьютерной сфере. Будет расширено сотрудничество стран «группы восьми» в рамках Лионской группы по транснациональной организованной преступности. «Восьмерка» будет и далее содействовать установлению диалога с представителями промышленности о безопасности и доверии в киберпространстве. Необходимо также найти эффективные политические решения таких актуальных проблем, как, например, попытки несанкционированного доступа и компьютерные вирусы. «Восьмерка» будет и далее привлекать представителей промышленности и других посредников для защиты важных информационных инфраструктур.

«Восьмерка» согласилась учредить Группу по возможностям информационной технологии (Группа ДОТ), чтобы объединить усилия в целях формирования широкого международного подхода. Группа будет изыскивать пути к принятию конкретных мер в приоритетных областях, в том числе по формированию политического, нормативного и сетевого обеспечения.

Таким образом, Окинавская хартия являет собой важнейший документ, призванный организовать и активизировать деятельность стран и правительств на пути активного формирования глобального информационного общества планеты Земля. Большая роль в этом сложном комплексном процессе в Хартии отводится нормативному обеспечению. «Восьмерка» говорит о необходимости создания и укрепления нормативной базы информационного общества, его дальнейшем развитии, подготовке специалистов в нормативной сфере, о продвижении международного сотрудничества в области нормативного обеспечения информационного общества.

Директивы ОЭСР

25 июля 2002 г. Совет **Организации экономического сотрудничества и развития (ОЭСР)** принял Директивы по безопасности информационных систем и сетей «**К культуре безопасности**» (далее —

Директивы). Директивы состоят из 9 принципов, составляющих структуру рассматриваемых вопросов безопасности. Принципы имеют краткие и основополагающие формулировки, благодаря которым доступны для понимания всеми участниками. Директивы уделяют внимание развивающимся рискам и все большей взаимосвязанности сетевой экономики. Эти новые обстоятельства также расширили масштаб применимости Директив. До относительно недавнего времени безопасность ИТ была специальной областью, которая редко привлекала внимание кого-либо в сфере бизнеса или правительствах, кроме профессионалов в сфере ИТ. Мировые события, связанные с вирусными атаками, способными разрушить бизнес, и вопросами, затрагивающими физическую безопасность, выдвинули информационную безопасность в ряд главнейших забот бизнеса, правительства и гражданского общества. Это меняющееся отношение к безопасности отразилось в новом подзаголовке Директив «К культуре безопасности» и в том факте, что они адресованы всем участникам в соответствии с их ролями.

Девять принципов Директив могут быть сгруппированы в три основные категории.

1. Опорные принципы: осознание; ответственность; реакция.
2. Общественные принципы: этика; демократия.
3. Принципы жизненного цикла безопасности: оценка риска; проектирование и реализация безопасности; менеджмент безопасности; ревизия.

Опорные принципы сосредоточиваются на необходимости сознавать риски, предпринимать ответственное действие, связанное с этими рисками, и координировать это действие в своевременной реакции. Общественные принципы обращаются к вопросам, связанным с поведением, честностью, открытостью, прозрачностью и ценностями. Последние четыре принципа более оперативны по своему характеру и обращаются к «жизненному циклу безопасности». Они сосредоточиваются на необходимости:

- идентифицировать и оценивать риски;

- проектировать и реализовывать системы и решения, соответствующие требуемому уменьшению рисков;

- разрабатывать политики, процессы и процедуры, необходимые для обращения с этими системами и решениями;

- пересматривать риски, системы, решения, политику, процедуры и процессы в свете новых рисков, новых технологий, инцидентов и нормального жизненного цикла систем.

В Директивах указывается на роль бизнеса в культуре безопасности. Отмечается, что все стороны играют свои роли в культуре безопасности, но бизнес, как основной новатор, разработчик, пользователь и поставщик информационных технологий и технологий связи, играет более важную роль, чем большинство других сторон. Бизнес может быть разработчиком, реализатором и пользователем технологии, практических приемов и политики безопасности, как сказано в принципе 7 Директив: «Безопасность должна быть основным элементом всех продуктов, услуг, систем и сетей, а также интегральной частью проекта и архитектуры системы. Для конечных пользователей проектирование и реализация безопасности в значительной степени состоит из выбора и компоновки продуктов и услуг для их системы».

Бизнес может помочь обеспечить планирование безопасности в продуктах, повысить осознание клиентов в отношении значимости безопасности и шагов, которые они могут предпринять для развития культуры безопасности, может способствовать развитию безопасной технологии, обеспечить информацию и содействие для безопасного конфигурирования и внедрения технологии.

Бизнес, в свою очередь, может извлечь из Директив определенную пользу. Хотя эти Директивы являются добровольными и распространяются межправительственной организацией, они были разработаны в партнерстве со всеми секторами бизнеса и общества и адресованы им. Их основной

посыл – безопасность представляет сейчас интегральную часть гражданской ответственности каждого – имеет далеко идущее значение для бизнеса, занимающего уникальное положение по отношению к обществу. Бизнес является преимущественным владельцем и оператором информационных систем и сетей, составляющих сетевую экономику. Бизнес обладает наибольшим оперативным контролем над текущей и будущей безопасностью этих систем и сетей и является основным разработчиком и инициатором решений, мер, практических приемов и политики безопасности. Международные деловые круги должны рассматривать эту ответственность как подтверждение значимости безопасности, как обязывающий и способствующий фактор для существующего и развивающегося бизнеса.

Концепция культуры безопасности заключает в себе понятие того, что уместно для роли индивидуальных участников и ситуаций. Хотя многие концепции безопасности и вопросы политики кажутся уместными только на уровне предприятия, они применяются и в домашнем офисе, и на малых и средних предприятиях. Культура безопасности должна вылиться в интуитивное поведение и реакцию. Инструментальные средства, такие как программы проверки на вирусы, могут быть полезны только в том случае, если они используются и обновляются. Пароли и другие аутентификационные процедуры будут эффективны только в том случае, если они хранятся в тайне. Эти концепции должны стать рефлекторными.

С точки зрения бизнеса, наиболее важная роль Директив заключается в том, что они дополняют и в некотором смысле делают более совершенной существующую иерархию практических приемов, процессов и политики бизнеса в сфере безопасности информационных технологий и технологий связи. Обеспечивая основополагающий набор общих принципов, Директивы включают существующую структуру бизнеса в более широкий общественный контекст. Они соединяются со все более строгими инструктивными и юридическими рамками, в которых

функционирует бизнес в глобальном масштабе. Подобные рамки, например документы **Банка международных расчетов (Базель II)** по контролю операционного риска в финансовом секторе, требуют, чтобы фирмы проводили свои операции безопасным управляемым образом.

В приведенной ниже таблице показано соответствие Базельских требований (Basel II) и Директив ОЭСР.

Таблица 1

Принципы операционного риска Базель II	**Директивы ОЭСР**
1. Директора должны определить структуру менеджмента операционного риска	Принцип 1
2. Должен существовать внутренний аудит структуры менеджмента операционного риска	Принцип 8
3. Ответственность за структуру операционного риска должна возлагаться на высшее руководство	Принцип 2 Принцип 7
4. Для всех новых систем должна осуществляться оценка операционного риска	Принцип 6
5. Должен проводиться регулярный мониторинг операционного риска и существовать механизм предоставления отчетов правлению	Принцип 9
6. Должны проводиться периодическая проверка и корректировка стратегии менеджмента операционного риска	Принцип 9
7. Должны существовать план на случай непредвиденных обстоятельств и план обеспечения непрерывности бизнеса	Принцип 3
8. Должна существовать структура для идентификации, оценки, мониторинга, контроля/уменьшения материальных операционных рисков	Принцип 8
9. Должно производиться независимое внешнее оценивание политики, процедур и практических приемов, связанных с операционным риском	Принцип 5
10. Необходимо достаточное публичное раскрытие информации, чтобы сделать возможной оценку механизмов контроля операционного риска	Принцип 4 Принцип 5

У больших и малых фирм существуют многообразные потребности безопасности, ресурсы и возможности. Нет решения, которое подошло бы всем, часто даже в пределах одного предприятия. Требования безопасности для критических приложений отличаются от требований безопасности для более рутинных приложений, однако все они связаны и должны трактоваться таким образом.

Международная торговая палата и Консультативный комитет ОЭСР по предпринимательству и промышленности от имени мирового делового сообщества надеются способствовать распространению и реализации Директив. Этот документ должен стать жизненным документом, он будет обновляться по мере необходимости, чтобы отражать меняющиеся обстоятельства и развивающиеся настоятельные требования безопасности. В 2003 г. с этой целью они выпустили **комментарии для международного бизнеса по Директивам ОЭСР 2002 г.** по безопасности сетей и информационных систем «К культуре безопасности» под названием «**Доверие информационной безопасности для руководящих работников**». В этом документе отмечается, что бизнес должен быть в состоянии использовать Директивы и данные комментарии, чтобы:

- обеспечить контекст для понимания руководящими работниками деловых результатов безопасности на предприятии и в обществе;

- обеспечить высокоуровневые ресурсы, которые он может использовать, чтобы гарантировать, что его компании продолжают отвечать ожиданиям причастной стороны, клиентов, служащих, распорядительных органов и широкой публики;

- повысить осознание, касающееся безопасности, у тех фирм, которые не имеют в штате или по договору специалистов в сфере информационных технологий и технологий связи или только недавно вступили в сферу электронной торговли;

- помочь бизнесу понять, какую роль он может играть в содействии определению и разработке культуры безопасности.

Представляет интерес обзор законодательства ряда развитых в технологическом отношении стран. Но это требует дополнительного изучения.

Конституция Российской Федерации

Конституция Российской Федерации определяет базовые принципы отношений в информационной сфере. Этого вопроса касаются, в частности, следующие статьи.

Ст. 15 (из п. 3). Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.

Ст. 23. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права осуществляется только на основании судебного решения.

Ст. 24. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Ст. 29. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Гарантируется свобода массовой информации. Цензура запрещается.

Ст. 42. Каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии и на возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением.

Ст. 44. Интеллектуальная собственность охраняется законом.

Ст. 55. В Российской Федерации не должны издаваться законы, отменяющие или умаляющие права и свободы человека и гражданина.

Права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Концепция национальной безопасности Российской Федерации

Пока в Российской Федерации не существует ни отдельного органа исполнительной власти, создающего и проводящего информационную политику, ни, тем более, единого властного органа (по примеру США или Германии), который мог бы объединить все функции, связанные с обеспечением информационной безопасности. Реализация функций в настоящее время рассредоточена между Федеральной службой безопасности (ФСБ), Федеральной службой охраны (ФСО), Федеральной службой по техническому и экспортному контролю (ФСТЭК), Министерством обороны, Министерством информационных технологий и связи.

Основы государственной политики Российской Федерации в области информатизации и обеспечения информационной безопасности сформулированы в **Концепции национальной безопасности Российской Федерации**, утвержденной Указом Президента Российской Федерации от 17 декабря 1997 г. № 1300 (в редакции Указа Президента Российской Федерации от 10 января 2000 г. № 24), и **Доктрине информационной безопасности Российской Федерации**, утвержденной Президентом Российской Федерации 9 сентября 2000 г.

Концепция национальной безопасности Российской Федерации отражает систему взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних

угроз во всех сферах жизнедеятельности. В ней сформулировано понятие национальных интересов России в информационной сфере. В Концепции отмечается усиление угроз национальной безопасности Российской Федерации в информационной сфере.

Доктрина информационной безопасности Российской Федерации

Напомним, что под информационной безопасностью РФ в Доктрине понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В Доктрине подчеркивается, что обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Утверждается, что воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

- система государственной статистики;

- кредитно-финансовая система;

- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

- системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

В качестве основных мер по обеспечению информационной безопасности Российской Федерации в сфере экономики Доктриной провозглашаются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;

- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;

- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

В работе [91] содержится конструктивная критика Концепции и Доктрины.

Концепция использования информационных технологий

Концепция использования ИТ в деятельности федеральных органов государственной власти России до 2010 г. разработана Министерством информационных технологий и связи. В результате реализации Концепции ожидается формирование эффективной системы предоставления государственных услуг на основе использования ИТ.

В Концепции поставлен ряд задач, решение которых позволит повысить эффективность использования ИТ. Среди этих задач имеются и связанные с защитой информации:

1. Обеспечение информационной безопасности деятельности федеральных органов государственной власти (ОГВ) и элементов информационно-технологической инфраструктуры.

2. Развитие единой защищенной телекоммуникационной инфраструктуры для государственных нужд, системы удостоверяющих центров в области электронной цифровой подписи (ЭЦП) и электронной среды взаимодействия, обеспечивающей эффективный межведомственный информационный обмен.

3. Разработка стандартов в сфере использования ИТ в деятельности федеральных органов государственной власти, создание государственных ИС, их интеграции и совместного использования в рамках создания общего информационного пространства федеральных органов власти.

4. Защита интеллектуальной собственности, недопущение использования в деятельности федеральных органов власти ПО, не имеющего соответствующей лицензионной поддержки.

Концепция определяет основные приоритеты в следующих областях:

- социально-экономического развития;
- государственного управления;
- обеспечения информационной открытости;
- **информационной безопасности;**

- формирования информационного пространства и защищенной информационной среды федеральных органов власти;
- разработки единых требований к основным элементам информационно-технологического обеспечения;
- создания общегосударственных информационных ресурсов;
- совершенствования нормативной правовой базы в области ИТ и др.

В сфере ***информационной безопасности*** должны быть развиты основные положения Доктрины информационной безопасности Российской Федерации. Предлагается применить единые требования защиты информации от НСД или изменений, воздействия компьютерных атак и вирусов, а также требования использования сертифицированных отечественных средств предупреждения и обнаружения компьютерных атак и защиты информации, разрабатываемых и производимых организациями, получившими в установленном порядке необходимые лицензии.

Для ИС и ресурсов, содержащих сведения, составляющие государственную тайну, считать обязательным применение криптографических средств ЗИ.

Контроль использования и защита государственных информационных ресурсов и систем от НСД должны обеспечиваться на основе создания комплексной системы мониторинга и учета операций при работе с государственными ИС и ресурсами.

В качестве основных направлений повышения уровня защищенности объектов общей информационно-технологической инфраструктуры выделяются следующие:

1. Обеспечение комплексного подхода к решению задач ИБ с учетом необходимости ее дифференцирования на разных уровнях власти.

2. Разработка модели угроз ИБ.

3. Определение технических требований и критериев определения критических объектов информационно-технологической инфраструктуры,

создание реестра критически важных объектов, разработка мер по их защите и средств надзора за соблюдением соответствующих требований.

4. Обеспечение эффективного мониторинга состояния ИБ.

5. Совершенствование нормативной правовой и методической базы в области защиты государственных ИС и ресурсов, формирование единого порядка согласования ТЗ на обеспечение ИБ.

6. Проведение уполномоченными федеральными органами власти аттестации государственных ИС и ресурсов, используемых в органах власти, и контроль их соответствия требованиям ИБ.

7. Создание физически обособленного телекоммуникационного сегмента специального назначения, обеспечивающего возможность обмена в электронном виде информацией, содержащей государственную тайну, ограниченным кругом органов власти.

8. Развитие средств ЗИ, систем обеспечения безопасности электронного документооборота, системы контроля действий госслужащих при работе с информацией, развитие и совершенствование защищенных средств обработки информации общего применения, систем удостоверяющих центров в области ЭЦП, а также систем их сертификации и аудита.

Определены девять основополагающих принципов *государственной политики* в области использования ИТ. Среди них отметим такие, как:

- подчинение процессов использования ИТ решению задач обеспечения обороноспособности и национальной безопасности страны;
- согласованность нормативной правовой и методической базы в сфере ИТ на всех уровнях;
- унификация элементов информационно-технологической инфраструктуры, использование типовых решений при создании ИС.

В сфере формирования *общего информационного пространства* и защищенной информационной среды предполагается развитие:

- единой защищенной телекоммуникационной инфраструктуры для государственных нужд;
- системы удостоверяющих центров в области ЭЦП уполномоченных лиц государственной власти;
- электронной среды взаимодействия органов власти.

Единая защищенная телекоммуникационная инфраструктура для государственных нужд создается на основе интеграции существующих и создаваемых телекоммуникационных сетей органов власти всех уровней. Она должна обеспечивать гарантированный уровень функциональности государственных ИС, ресурсов и технологий.

Система удостоверяющих центров в области ЭЦП должна включать:
- федеральный удостоверяющий центр в области ЭЦП;
- удостоверяющие центры федеральных органов власти и их территориальных подразделений;
- уполномоченный федеральный орган исполнительной власти в области использования ЭЦП, ведущий единый государственный реестр сертификатов ключей подписей (СКП) удостоверяющих центров и реестр СКП уполномоченных лиц органов власти.

Электронная среда взаимодействия органов власти должна обеспечивать интеграцию и совместную работу государственных ИС, автоматизированный обмен данными между ними на межведомственном уровне на основе создания:
- реестра, содержащего описание государственных ИС и ресурсов, способов и интерфейсов взаимодействия с ними, а также используемых схем организации обмена данными;
- инфраструктуры и механизмов маршрутизации, трансформации и гарантированной доставки сообщений и данных между отдельными государственными ИС.

В области разработки единых требований к основным элементам информационно-технологического обеспечения предполагается

формирование общих стандартов создания, интеграции и совместного использования типовых элементов информационно-технологической инфраструктуры. Общие стандарты определяют общие требования и порядок выполнения работ по проектированию, реализации, внедрению, эксплуатации и развитию типовых элементов информационно-технологической инфраструктуры.

Стандарты утверждаются для следующих типовых элементов информационно-технологической инфрастуктуры органов власти:

- системы взаимодействия с гражданами и организациями, обеспечивающими предоставление им справочной информации, в том числе и через Интернет;
- учетные системы;
- системы межведомственного взаимодействия и обмена информацией;
- системы управления государственными ресурсами;
- офисные системы, используемые сотрудниками органов власти для подготовки документов и обмена информацией;
- информационно-аналитические системы, обеспечивающие сбор, обработку, хранение и анализ данных о состоянии закрепленных за органами власти сфер государственного регулирования и результатах выполнения ими основных задач и функций;
- системы управления электронными архивами документов;
- системы управления проектами;
- системы ИБ;
- системы управления эксплуатацией.

В целях интеграции, совместного использования с информационного взаимодействия государственных ИС на межведомственном уровне утверждаются:

- стандарты метаданных информационных объектов;
- стандарты описания государственных ИС и ресурсов;
- стандарты предоставления информационных сервисов;

- стандарты информационного электронного обмена и сетевого взаимодействия.

Для координации и согласования действий органов власти в этой сфере предлагается создать межведомственный координационный (совещательный) орган при Министерстве информационных технологий и связи.

В сфере создания *общегосударственных ресурсов* предлагается в их состав включать: регистры, кадастры, классификаторы.

Основным механизмом реализации единой согласованной государственной политики в сфере ИТ является федеральная целевая программа «**Электронная Россия (2002–2010 годы)».**

В сфере обеспечения *защиты интеллектуальной собственности* в области ИТ ответственность за соблюдение соответствующих нормативных актов возлагается на федеральные органы власти. Предлагается вести ускоренную разработку отечественных программно-технических средств, свободного распространения типовых решений, разработанных за счет федерального бюджета. Необходимо обеспечить открытость и возможность анализа кода закупаемого готового ПО зарубежного производства.

Нормативно-правовые акты Российской Федерации

Кодексы

Гражданский кодекс Российской Федерации

(Часть первая от 30 ноября 1994 г. № 51-ФЗ, Часть вторая от 26 января 1996 г.
№ 14-ФЗ, Часть третья от 26 ноября 2001 г. № 146-ФЗ, с изменениями и дополнениями, Часть четвертая от 18.12.2006 г. № 230-ФЗ).

Определяет правовое положение участников гражданского оборота, основания возникновения и порядок осуществления права собственности и других вещных прав, исключительных прав на результаты

интеллектуальной деятельности (интеллектуальной собственности), регулирует договорные и иные обязательства, а также другие имущественные и связанные с ними личные неимущественные отношения, основанные на равенстве, автономии воли и имущественной самостоятельности их участников.

Участниками регулируемых гражданским законодательством отношений являются граждане и юридические лица. В регулируемых гражданским законодательством отношениях могут участвовать также РФ, субъекты РФ и муниципальные образования.

Впервые в правовой практике России информация как один из объектов права определяется в **Гражданском кодексе Российской Федерации**.

Ст. 128 (Виды объектов гражданских прав) гласит: «К объектам гражданских прав относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права; работы и услуги; информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность)…».

Статья 138. **Интеллектуальная собственность**

В случаях и в порядке, установленных настоящим Кодексом и другими законами, признается исключительное право (интеллектуальная собственность) гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.).

Использование результатов интеллектуальной деятельности и средств индивидуализации, которые являются объектом исключительных прав, может осуществляться третьими лицами только с согласия правообладателя.

Данная статья определяет, что результаты интеллектуальной деятельности, как и приравненные к ним в правовом режиме средства индивидуализации товаров и их изготовителей, относятся к категории нематериальных объектов. Духовная природа таких объектов обусловливает основные особенности правового регулирования отношений, связанных с использованием и защитой исключительных прав. К этим отношениям неприменимы нормы о праве собственности, относящиеся к вещным правам.

Охрана интеллектуальной собственности в России гарантируется нормами статьи 44 Конституции. Здесь ГК, устанавливая общий принцип закрепления исключительных прав за гражданином или юридическим лицом на объекты интеллектуальной собственности, отсылает к специальным законам, определяющим условия возникновения, использования, защиты этих прав, а также сроки их действия. В частности, исключительные права делятся на несколько групп, для которых установлен различный правовой режим использования и защиты. Традиционно выделяются две основные группы: «промышленные права» («промышленная собственность») и «художественные права» («художественная собственность»), к которым примыкают «смежные» права исполнителей, производителей фонограмм, организаций эфирного и кабельного вещания. Технический прогресс способствует расширению сферы исключительных прав, включению в нее новых видов нематериальных объектов (топологий ИМС, программ для ЭВМ, баз данных и др.).

Исключительные права на объекты промышленной собственности удостоверяются охранными документами: патентами на изобретения и промышленные образцы, свидетельствами на полезные модели, товарные знаки, наименования мест происхождения. Патенты и свидетельства выдаются в соответствии с установленной процедурой патентным

ведомством РФ на основе акта государственной регистрации заявленных объектов.

Охрана исключительных прав на художественную собственность (произведения литературы, науки и искусства), а также объекты смежных прав и топологий ИМС не требует государственной регистрации или иного оформления. Основанием для защиты служит сам факт создания произведения в форме, доступной для восприятия другими лицами, что не препятствует их регистрации по желанию правообладателя. В частности, патентное ведомство ведет соответствующие регистрационные реестры.

Статья 139. **Служебная и коммерческая тайна**

1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.
(Интересно сравнить это определение с определением из ФЗ «О коммерческой тайне»).

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Данная статья предусматривает защиту прав обладателя сведений, для определения которых применено широкое понятие «информация», не подпадающих под охрану норм патентного, авторско-правового или иного специального законодательства. Правила статьи распространяются также на охраноспособные решения (изобретения, полезные модели и др.), не запатентованные правообладателем по каким-либо, как правило, экономическим, мотивам.

Статья не раскрывает содержание сведений, составляющих служебную или коммерческую тайну, и не приводит их перечень. Установлен только один общий признак, которым должна обладать охраняемая информация, – «коммерческая ценность», т.е. способность быть объектом рыночного оборота. Условием предоставления защиты служит принятие правообладателем всех необходимых мер для обеспечения ее конфиденциальности. При соблюдении этих требований под правила статьи подпадают, таким образом, любые знания, включая практический опыт специалистов, применяемые не только в производстве, но и в других областях хозяйственной деятельности: торговле, маркетинге, менеджменте, иных управленческих услугах.

Нормы о коммерческой тайне содержатся и в ряде других российских законов, в частности в законе «О коммерческой тайне». Права на коммерческую тайну действуют, пока соблюдаются условия их защиты. Признание тех или иных сведений конфиденциальными является прерогативой правообладателя. Исключения из этой общей нормы устанавливаются законом или иным правовым актом.

Вместе с тем, в некоторых источниках высказывается сомнение в правомерности распространения условий охраны коммерческой тайны на служебную. Это разноплановые понятия. Сохранение в тайне служебной информации, как правило, не обусловлено ее коммерческой ценностью (хотя такая информация и может содержать сведения коммерческого характера). Запрет ее разглашения основывается на законодательстве,

регламентирующем отдельные сферы деятельности (например, Законы РФ «О страховании», «О связи» и др.). Определенные категории работников такой сферы деятельности обязаны сохранять в тайне сведения, к которым они имеют доступ в связи с выполняемой работой (банковские служащие, работники связи, налоговые инспекторы, страховые агенты, врачи и др.).

Закрепление исключительных прав обладателя коммерческой тайны имеет свои особенности. Эта защита основывается на *системе конфиденциальности*, ее нарушение влечет прекращение прав. Условием же предоставления охраны изобретениям, полезным моделям, промышленным образцам, напротив, служит их *опубликование*.

Охраняемая информация может быть использована другими лицами при соблюдении двух условий: получения самой информации законным путем и получения разрешения правообладателя на такое использование («беспатентная лицензия»). Отношения между правообладателем (лицензиаром) и пользователем (лицензиатом) оформляются лицензионным договором. Элементы лицензионного договора могут включаться в другие гражданско-правовые договоры (на выполнение научно-исследовательских, опытно-конструкторских и технологических работ, подряда, о создании акционерного общества и др.).

Защита служебной и коммерческой тайны от неправомерных посягательств может осуществляться на основе норм гражданского, административного либо уголовного права. В качестве основного гражданско-правового способа защиты статья указывает возмещение причиненных правообладателю убытков. При определении их размера может быть учтен как реальный ущерб, так и упущенная выгода.

Существенным новшеством в ГК является введение *имущественной ответственности* лица перед своим *работодателем* за разглашение служебной или коммерческой тайны, что предполагает необходимость включения соответствующих условий в трудовое соглашение. Вместе с

тем, санкции за нарушение служебной тайны устанавливаются также нормами законов о соответствующих видах деятельности.

Статья 771. Конфиденциальность сведений, составляющих предмет договора

1. Если иное не предусмотрено договорами на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, стороны обязаны обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов. Объем сведений, признаваемых конфиденциальными, определяется в договоре.

2. Каждая из сторон обязуется публиковать полученные при выполнении работы сведения, признанные конфиденциальными, только с согласия другой стороны.

Данная статья определяет, что обязанности сторон по обеспечению конфиденциальности относятся в практике к одним из основных договорных обязательств. Результаты НИОКР не могут быть иначе защищены от незаконного использования третьими лицами. Кроме того, преждевременное разглашение может препятствовать патентной защите охраноспособных технических решений.

Состав и объем конфиденциальной информации определяется сторонами. В нее включаются сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них, а также любые другие сведения научного, технического, экономического, организационного характера, которые могут быть отнесены к коммерческой тайне. Эти сведения должны быть неизвестны третьим лицам, что служит предпосылкой их коммерческой ценности, и закрыты для доступа третьих лиц на законном основании.

Нарушением обязательств по обеспечению конфиденциальности признается не только разглашение и прямая передача подобных сведений одной из сторон другим заинтересованным пользователям без согласия

партнера, но и непринятие мер к их охране, исключающих свободный доступ к сведениям и возможность их утечки. Правила статьи относятся как к сведениям, которыми стороны обладают на момент заключения договора, так и к полученным в процессе выполнения работ.

Статья 857. Банковская тайна

1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом.

3. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

Данная статья определяет обязанность хранить банковскую тайну, которая распространяется на кредитные, аудиторские организации и Центральный банк Российской Федерации (ЦБ РФ). Перечень лиц, обязанных сохранять банковскую тайну, включает в себя всех служащих перечисленных организаций, независимо от их должности и от того, входит ли работа с охраняемыми сведениями в круг их непосредственных служебных обязанностей.

В **состав банковской тайны** входят сведения о счетах и вкладах, операциях по счетам и вкладам, о клиентах и корреспондентах, а также иная информация, устанавливаемая кредитной организацией, если это не противоречит федеральному закону («О банках и банковской деятельности»). Следовательно, кредитная организация не обязана хранить в тайне сведения о контрагентах своих клиентов, а также другую информацию, не имеющую непосредственного отношения к банковскому счету (кроме сведений о клиенте), если она не взяла на себя такие

обязательства. Тайна распространяется, однако, на движение вкладов (размер, время и сумма поступления или изъятия, от кого и по каким основаниям поступают суммы и пр.). Сведения, составляющие банковскую тайну, должны быть получены кредитной организацией в процессе осуществления ею банковских операций и других сделок, предусмотренных Законом о банках.

Помимо указанных сведений, ЦБ РФ не вправе разглашать данные о счетах, вкладах, конкретных сделках и операциях, полученных им из отчетов кредитных организаций или в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Аудиторские организации не вправе раскрывать третьим лицам сведения об операциях, счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

Пределы раскрытия банковской тайны определяются законодательством. Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются им самим (а также их представителям), судам и арбитражным судам (судьям), Счетной палате РФ, органам федеральной налоговой службы, таможенным органам РФ, следственным органам – в случаях, предусмотренных законодательными актами об их деятельности, а также по решению суда.

В числе органов и должностных лиц, которым должны быть предоставлены сведения, составляющие банковскую тайну, отсутствуют судебные приставы-исполнители. Они вправе получать интересующие их сведения через налоговые органы.

За разглашение банковской тайны ЦБ РФ, кредитные и аудиторские организации могут быть привлечены к ответственности в форме

возмещения убытков. Их должностные лица и иные работники несут уголовную ответственность.

Статья 946. Тайна страхования

Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными статьей 139 или статьей 150 настоящего Кодекса.

Данная статья вводит понятие **тайны страхования**. К ней относятся ставшие известными страховщику сведения, составляющие служебную и/или коммерческую тайну страхователей, выгодоприобретателей и застрахованных лиц, а также личную и/или семейную тайну этих лиц и, кроме того, сведения о здоровье и имущественном положении этих лиц.

Ответственность страховщика как юридического лица за разглашение тайны страхования носит общий характер, однако она наступает только, если использование или разглашение полученных страховщиком сведений является незаконным. Иными словами, ответственность за использование или разглашение тайны страхования не может быть возложена на страховщика, если какой-либо закон не предусматривает запрет на использование или разглашение этих сведений.

Статья играет такую же роль и при защите тайны страхования от ее несанкционированного корыстного использования и распространения работниками страховщика, поскольку ответственность работника страховщика за ее разглашение или за несанкционированное корыстное использование также наступает только, если эти действия являются незаконными.

С 1 января 2008 года вступила в силу **Часть IV Гражданского кодекса РФ**. Эта часть регулирует отношения в сфере интеллектуальной собственности.

Налоговый кодекс Российской Федерации

(Часть первая от 31 июля 1998 г. № 146-ФЗ, Часть вторая от 5 августа 2000 г. № 117-ФЗ, с изменениями и дополнениями).

Кодекс устанавливает *систему налогов и сборов*, взимаемых в федеральный бюджет, а также общие принципы налогообложения и сборов в Российской Федерации, в том числе: виды налогов и сборов, взимаемых в Российской Федерации; основания возникновения (изменения, прекращения) и порядок исполнения обязанностей по уплате налогов и сборов; принципы установления, введения в действие и прекращения действия ранее введенных налогов и сборов субъектов Российской Федерации и местных налогов и сборов; права и обязанности налогоплательщиков, налоговых органов и других участников отношений, регулируемых законодательством о налогах и сборах; формы и методы налогового контроля; ответственность за совершение налоговых правонарушений; порядок обжалования актов налоговых органов и действий (бездействия) их должностных лиц.

Статья 32 Кодекса определяет обязанность налоговых органов *бесплатно информировать* (в том числе в письменной форме) налогоплательщиков о действующих налогах и сборах, законодательстве о налогах и сборах и принятых в соответствии с ним нормативных правовых актах, порядке исчисления и уплаты налогов и сборов, правах и обязанностях налогоплательщиков, полномочиях налоговых органов и их должностных лиц, а также предоставлять формы налоговой отчетности и разъяснять порядок их заполнения.

Статья 102 Кодекса устанавливает понятие ***налоговой тайны***. Налоговую тайну составляют любые полученные налоговым органом,

органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений:

- разглашенных налогоплательщиком самостоятельно или с его согласия;
- об идентификационном номере налогоплательщика;
- о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения;
- предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация.

Трудовой кодекс Российской Федерации

(от 30 декабря 2001 г. № 197-ФЗ, с изменениями и дополнениями).

Кодекс устанавливает государственные гарантии трудовых прав и свобод граждан, благоприятных условий труда, защиты прав и интересов работников и работодателей.

Глава 14 Кодекса регулирует вопросы, связанные с защитой персональных данных работника.

Семейный кодекс Российской Федерации

(от 29 декабря 1995 г. № 223-ФЗ, с изменениями и дополнениями).

Семейное законодательство устанавливает условия и порядок вступления в брак, прекращения брака и признания его недействительным, регулирует личные неимущественные и имущественные отношения между членами семьи: супругами, родителями и детьми (усыновителями и усыновленными), а в случаях и в пределах, предусмотренных семейным законодательством, между другими родственниками и иными лицами, а также определяет формы и порядок устройства в семью детей, оставшихся без попечения родителей.

Статья 139 Кодекса определяет **тайну усыновления ребенка.**

Кодекс Российской Федерации об административных правонарушениях (от 30 декабря 2001 г. № 195-ФЗ, с изменениями и дополнениями).

Задачами законодательства об административных правонарушениях являются защита личности, охрана прав и свобод человека и гражданина, охрана здоровья граждан, санитарно-эпидемиологического благополучия населения, защита общественной нравственности, охрана окружающей среды, установленного порядка осуществления государственной власти, общественного порядка и общественной безопасности, собственности, защита законных экономических интересов физических и юридических лиц, общества и государства от административных правонарушений, а также предупреждение административных правонарушений.

В данном Кодексе вопросам информационной безопасности и интеллектуальной собственности посвящены следующие главы и статьи.

Глава 5. Административные правонарушения, посягающие на права граждан

Статья 5.39. Отказ в предоставлении гражданину информации

Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации.

Глава 8. Административные правонарушения в области охраны окружающей природной среды и природопользования

Статья 8.5. Сокрытие или искажение экологической информации

Сокрытие, умышленное искажение или несвоевременное сообщение полной и достоверной информации о состоянии окружающей природной среды и природных ресурсов, об источниках загрязнения окружающей природной среды и природных ресурсов или иного вредного воздействия на окружающую природную среду и природные ресурсы, о радиационной

обстановке, а равно искажение сведений о состоянии земель, водных объектов и других объектов окружающей природной среды лицами, обязанными сообщать такую информацию.

Глава 13. Административные правонарушения в области связи и информации

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (**персональных данных**).

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну).

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну).

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну.

Статья 13.13. Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии),

если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна).

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну без лицензии.

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Статья 13.15. Злоупотребление свободой массовой информации

Изготовление и (или) распространение теле-, видео-, кинопрограмм, документальных и художественных фильмов, а также относящихся к специальным средствам массовой информации информационных компьютерных файлов и программ обработки информационных текстов, содержащих скрытые вставки, воздействующие на подсознание людей и (или) оказывающие вредное влияние на их здоровье.

Статья 13.16. Воспрепятствование распространению продукции средства массовой информации

Воспрепятствование осуществляемому на законном основании распространению продукции средства массовой информации либо установление незаконных ограничений на розничную продажу тиража периодического печатного издания.

Статья 13.17. Нарушение правил распространения обязательных сообщений

Нарушение правил распространения обязательных сообщений.

Статья 23.45. Органы, осуществляющие контроль за обеспечением защиты государственной тайны

1. Органы, осуществляющие контроль за обеспечением защиты государственной тайны, рассматривают дела об административных правонарушениях, предусмотренных частями 3 и 4 статьи 13.12, частью 2 статьи 13.13 настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органов, указанных в части 1 настоящей статьи, вправе:

1) руководитель федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности Российской Федерации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители;

2) руководитель федерального органа исполнительной власти, уполномоченного в области обороны, его заместители;

3) руководитель федерального органа исполнительной власти, уполномоченного в области внешней разведки, его заместители;

4) руководитель федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, его заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители;

5) руководители подразделений федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности Российской Федерации, обороны Российской Федерации, внешней разведки, противодействия техническим разведкам и технической защиты информации, осуществляющих лицензирование видов деятельности, которые связаны с использованием и защитой сведений, составляющих государственную тайну.

Уголовный кодекс Российской Федерации

(от 13 июня 1996 г. № 63-ФЗ, с изменениями и дополнениями).

Устанавливает основание и принципы уголовной ответственности, определяет, какие опасные для личности, общества или государства деяния признаются преступлениями, и устанавливает виды наказаний и иные меры уголовно-правового характера за совершение преступлений.

В Уголовном кодексе Российской Федерации вопросам безопасности информации и интеллектуальной собственности посвящены следующие главы и статьи.

Глава 19. Преступления против конституционных прав и свобод человека и гражданина

Статья 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан.

2. Те же деяния, совершенные лицом с использованием своего служебного положения.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации.

3. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.

Статья 140. Отказ в предоставлении гражданину информации

Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан.

Статья 144. Воспрепятствование законной профессиональной деятельности журналистов

1. Воспрепятствование законной профессиональной деятельности журналистов путем принуждения их к распространению либо к отказу от распространения информации.

2. То же деяние, совершенное лицом с использованием своего служебного положения.

Статья 146. Нарушение авторских и смежных прав

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб (свыше 100 МРОТ) автору или иному правообладателю.

2. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере.

3. Деяния, предусмотренные частью второй настоящей статьи, если они совершены: неоднократно; группой лиц по предварительному сговору или организованной группой; в особо крупном размере (свыше 500 МРОТ); лицом с использованием своего служебного положения.

Статья 147. Нарушение изобретательских и патентных прав

1. Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя

сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой.

Глава 20. Преступления против семьи и несовершеннолетних

Статья 155. Разглашение тайны усыновления (удочерения)

Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну, либо иным лицом из корыстных или иных низменных побуждений.

Глава 22. Преступления в сфере экономической деятельности

Статья 155. Мошенничество

Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Статья 163. Вымогательство

Вымогательство, то есть требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких.

Статья 165. Причинение имущественного ущерба путем обмана или злоупотребления доверием

Причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием при отсутствии признаков хищения.

Статья 179. Принуждение к совершению сделки или к отказу от ее совершения

Принуждение к совершению сделки или к отказу от ее совершения под угрозой применения насилия, уничтожения или повреждения чужого имущества, а равно распространения сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего или его близких, при отсутствии признаков вымогательства.

Статья 180. Незаконное использование товарного знака

1. Незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров, если это деяние совершено неоднократно или причинило крупный ущерб.

2. Незаконное использование предупредительной маркировки в отношении не зарегистрированного в Российской Федерации товарного знака или наименования места происхождения товара, если это деяние совершено неоднократно или причинило крупный ущерб.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой.

Статья 182. Заведомо ложная реклама

Использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей (исполнителей, продавцов), совершенное из корыстной заинтересованности и причинившее значительный ущерб.

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия.

Статья 185. Злоупотребления при эмиссии ценных бумаг

1. Внесение в проспект эмиссии ценных бумаг заведомо недостоверной информации, утверждение содержащего заведомо недостоверную информацию проспекта эмиссии или отчета об итогах выпуска ценных бумаг, а равно размещение эмиссионных ценных бумаг, выпуск которых не прошел государственную регистрацию, если эти деяния причинили крупный (свыше 2000 МРОТ) ущерб гражданам, организациям или государству.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой.

Статья 185.1. Злостное уклонение от предоставления инвестору или контролирующему органу информации, определенной законодательством Российской Федерации о ценных бумагах

Злостное уклонение от предоставления информации, содержащей данные об эмитенте, о его финансово-хозяйственной деятельности и ценных бумагах, сделках и иных операциях с ценными бумагами, лица, обязанного обеспечить указанной информацией инвестора или контролирующий орган, либо предоставление заведомо неполной или ложной информации, если эти деяния причинили крупный ущерб гражданам, организациям или государству.

Статья 186. Изготовление или сбыт поддельных денег или ценных бумаг

1. Изготовление в целях сбыта или сбыт поддельных банковских билетов Центрального банка Российской Федерации, металлической монеты, государственных ценных бумаг или других ценных бумаг в валюте Российской Федерации либо иностранной валюты или ценных бумаг в иностранной валюте.

2. Те же деяния, совершенные в крупном размере либо лицом, ранее судимым за изготовление или сбыт поддельных денег или ценных бумаг.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой.

Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов

1. Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами.

2. Те же деяния, совершенные неоднократно или организованной группой.

Статья 189. Незаконный экспорт технологий, научно-технической информации и услуг, сырья, материалов и оборудования, которые могут использоваться при создании оружия массового поражения, вооружения и военной техники

Незаконный экспорт технологий, научно-технической информации и услуг, сырья, материалов и оборудования, которые могут быть использованы при создании оружия массового поражения, средств его доставки, вооружения и военной техники и в отношении которых установлен специальный экспортный контроль.

Глава 23. Преступления против интересов службы в коммерческих и иных организациях

Статья 201. Злоупотребление полномочиями

1. Использование лицом, выполняющим управленческие функции в коммерческой или иной организации, своих полномочий вопреки законным интересам этой организации и в целях извлечения выгод и преимуществ для себя или других лиц либо нанесения вреда другим лицам, если это деяние повлекло причинение существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

2. То же деяние, повлекшее тяжкие последствия.

Статья 202. Злоупотребление полномочиями частными нотариусами и аудиторами

1. Использование частным нотариусом или частным аудитором своих полномочий вопреки задачам своей деятельности и в целях извлечения выгод и преимуществ для себя или других лиц либо нанесения вреда другим лицам, если это деяние причинило существенный вред правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

2. То же деяние, совершенное в отношении заведомо несовершеннолетнего или недееспособного лица либо неоднократно.

Статья 203. Превышение полномочий служащими частных охранных или детективных служб

1. Превышение руководителем или служащим частной охранной или детективной службы полномочий, предоставленных им в соответствии с лицензией, вопреки задачам своей деятельности, если это деяние совершено с применением насилия или с угрозой его применения.

2. То же деяние, повлекшее тяжкие последствия.

Глава 25. Преступления против здоровья населения и общественной нравственности

Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей

1. Сокрытие или искажение информации о событиях, фактах или явлениях, создающих опасность для жизни или здоровья людей либо для окружающей среды, совершенные лицом, обязанным обеспечивать население и органы, уполномоченные на принятие мер по устранению такой опасности, указанной информацией.

2. Те же деяния, если они совершены лицом, занимающим государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, а равно главой органа местного самоуправления либо если в результате таких деяний причинен вред здоровью человека или наступили иные тяжкие последствия.

Глава 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо

копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

2. То же деяние, повлекшее по неосторожности тяжкие последствия.

Глава 29. Преступления против основ конституционного строя и безопасности государства

Статья 275. Государственная измена

Государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, совершенная гражданином Российской Федерации.

Статья 276. Шпионаж

Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Федерации, если эти деяния совершены иностранным гражданином или лицом без гражданства.

Статья 283. Разглашение государственной тайны

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или

работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены.

2. То же деяние, повлекшее по неосторожности тяжкие последствия.

Статья 284. Утрата документов, содержащих государственную тайну

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий.

Законы Российской Федерации

В настоящее время в **Государственной Думе РФ** за информационную безопасность отвечают три Комитета:

1. Комитет по информационной политике,

2. Комитет по безопасности,

3. Комитет по энергетике, транспорту и связи.

В положении о каждом из этих трех комитетов указано, что он отвечает за информационную безопасность.

Законодательные органы в рамках развития информационного законодательства на практике осуществляли конкретизацию видов и форм представления информации и информационных объектов при регулировании конкретных информационных отношений.

Комплексное исследование процессов в информационной сфере, правовых норм, регулирующих отношения, возникающие в этих процессах, действий, совершаемых с информацией, позволяет установить такие ее особенности и свойства, как:

- свойство физической неотчуждаемости информации. Оно основано на том, что знания не отчуждаемы от человека, их носителя. Исходя из этого при передаче информации от одного лица к другому и юридического

закрепления этого факта процедура отчуждения информации должна заменяться передачей прав на ее использование и передаваться вместе с этими правами;

- свойство обособляемости информации. Для включений в оборот информация всегда овеществляется в виде символов, знаков, волн, вследствие этого обособляется от ее производителя (создателя) и существует отдельно и независимо от него. Это подтверждает факт оборотоспособности информации как самостоятельного отдельного объекта правоотношений, в результате чего появляется возможность передачи информации в такой форме от одного субъекта к другому;

- свойство информационной вещи (информационного объекта). Это свойство возникает в силу того, что информация передается и распространяется только на материальном носителе или с помощью материального носителя и проявляется как «двуединство» информации (ее содержания) и носителя, на котором эта информация (содержание) закреплено. Это свойство позволяет распространить на информационную вещь (объект) совместное и взаимосвязанное действие двух институтов – института авторского права и института вещной собственности;

- свойство тиражируемости (распространяемости) информации. Информация может тиражироваться и распространяться в неограниченном количестве экземпляров без изменения ее содержания. Одна и та же информация (содержание) может принадлежать одновременно неограниченному кругу лиц (неограниченный круг лиц может знать содержание этой информации). Отсюда следует, что юридически необходимо закреплять объем прав по использованию информации (ее содержания) лицами, обладающими такой информацией (обладающими знаниями о содержании информации);

- свойство организационной формы. Информация, находящаяся в обороте, как правило, представляется в документированном виде, т.е. в форме документа. Это могут быть подлинник (оригинал) документа, его

копия, массив документов на бумажном или электронном носителе (банк данных или база данных) тоже в виде оригинала или копии, библиотека, фонд документов, архив и т.п. Такое свойство дает возможность юридически закреплять факт «принадлежности» документа конкретному лицу, например, закрепив его соответствующей подписью в традиционном или в электронном виде (с помощью электронной цифровой подписи). Это свойство позволяет также относить к информационным вещам (информационным объектам) как отдельные документы, так и сложные организационные информационные структуры;

- свойство экземплярности информации. Это свойство заключается в том, что информация распространяется, как правило, не сама по себе, а на материальном носителе, вследствие чего возможен учет экземпляров информации через учет носителей, содержащих информацию. Понятие экземплярности дает возможность учитывать документированную информацию и тем самым связывать содержательную сторону информации с ее «вещным» обрамлением, т.е. с отображением на носителе, вводить понятие учитываемой копии документа, а отсюда и механизма регистрации информации, в особенности учитывать обращение оригиналов (подлинников) документов. Экземплярность информации уже сегодня активно реализуется при обращении информации ограниченного доступа.

Указанные юридические особенности и свойства должны учитываться при правовом регулировании информационных отношений.

Рассмотрим основные законы в области информационной безопасности, останавливаясь на главных из них.

Закон Российской Федерации от 9 июля 1993 г. № 5351-1 «Об авторском праве и смежных правах» (с изменениями и дополнениями в соответствии с Федеральным законом от 20 июля 2004 г. № 72-ФЗ)

Регулирует отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права). Закон развивает основные принципы правового регулирования авторских и смежных прав. Закон отвечает международным стандартам в этой области и позволил России присоединиться к ряду международных договоров.

Статья 1 Закона устанавливает общую сферу его действия и определяет наличие двух различных категорий прав: 1) авторских прав, которые возникают в отношении произведений науки, литературы и искусства, и 2) смежных прав, объектами которых являются фонограммы, исполнения, постановки, передачи эфирного и кабельного вещания.

В статье 2 содержится указание на то, что другие акты законодательства Российской Федерации по авторскому праву и смежным правам издаются «в соответствии с настоящим Законом».

В Законе об авторском праве и смежных правах имеются несколько норм, специально посвященных охране программ для ЭВМ и баз данных. Такими специальными нормами являются нормы **статьи 25**; они содержатся также в **статьях 6 (пункт 2) и 18 (пункт 2).**

Статья 3 Закона содержит известный принцип о приоритете международных договоров над национальным законодательством.

В области авторского права Россия является участницей: Всемирной конвенции об авторском праве (в редакции 1952 года); Всемирной конвенции об авторском праве (в редакции 1971 года); Бернской конвенции об охране литературных и художественных произведений; двусторонних соглашений с рядом государств.

В области смежных прав Россия является участницей: Конвенции об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм; Конвенции, учреждающей Всемирную Организацию Интеллектуальной Собственности; Конвенции о распространении несущих программы сигналов, передаваемых через спутники; Соглашения о сотрудничестве в области охраны авторского права и смежных прав.

Статья 4 определяет основные понятия. Среди них наиболее интересными в контексте данного издания являются следующие.

Автор – физическое лицо, творческим трудом которого создано произведение.

База данных – объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

Воспроизведение произведения – изготовление одного или более экземпляров произведения или его части в любой материальной форме, в том числе в форме звуко- и видеозаписи, изготовление в трех измерениях одного или более экземпляров двухмерного произведения и в двух измерениях – одного или более экземпляров трехмерного произведения; запись произведения в память ЭВМ также является воспроизведением.

Программа для ЭВМ – объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, включая подготовительные материалы,

полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Экземпляр произведения – копия произведения, изготовленная в любой материальной форме.

Обнародование произведения – осуществленное с согласия автора действие, которое впервые делает произведение доступным для всеобщего сведения путем его опубликования, публичного показа, публичного исполнения, передачи в эфир или иным способом.

Опубликование (выпуск в свет) – выпуск в обращение экземпляров произведения, фонограммы с согласия автора произведения, производителя фонограммы в количестве, достаточном для удовлетворения разумных потребностей публики исходя из характера произведения, фонограммы.

Статья 5 Закона определяет, что произведение получает охрану, если оно отвечает хотя бы одному критерию – критерию гражданства автора или критерию места первого обнародования. При этом под гражданством автора имеется в виду то гражданство (подданство), которое автор имеет на момент создания произведения, а если произведение было обнародовано – то на момент обнародования произведения. Последующее изменение гражданства не меняет правового статуса произведения.

Статьи 6–8 Закона определяют объекты авторского права. К ним относятся *произведения науки, литературы и искусства*, являющиеся результатом *творческой деятельности*, независимо от назначения и достоинства произведения, а также от способа его выражения. При этом авторское право распространяется как на *обнародованные* произведения, так и на *необнародованные* произведения, существующие в какой-либо объективной форме: письменной, устной, звуко- или видеозаписи, изображения, объемно-пространственной или в других формах.

Конкретными объектами авторского права в том числе являются:

- литературные произведения (включая *программы для ЭВМ*);

- аудиовизуальные произведения (кино-, теле- и видеофильмы, слайдфильмы, диафильмы и другие кино- и телепроизведения);

- фотографические произведения и произведения, полученные способами, аналогичными фотографии;

- географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам;

- сборники (энциклопедии, антологии, *базы данных*) и другие составные произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Охрана программ для ЭВМ распространяется на все виды программ для ЭВМ (в том числе на операционные системы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код.

Авторское право **не распространяется** на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты (это объект патентного законодательства).

Закон различает субъективную и объективную новизну творческого результата. Субъективная новизна – это неожиданность, неизвестность полученного результата для самого создателя. Объективная новизна – это неизвестность полученного творческого результата не только для лица, получившего этот результат, но и для остальных лиц. Авторское право охраняет лишь те творческие результаты, которые обладают объективной новизной.

Кроме того, не являются объектами авторского права: официальные документы (законы, судебные решения, иные тексты законодательного, административного и судебного характера), а также их официальные переводы; государственные символы и знаки (флаги, гербы, ордена, денежные знаки и иные государственные символы и знаки); произведения

народного творчества; сообщения о событиях и фактах, имеющие информационный характер.

Статьи 9–16 Закона содержат основное положение законодательства об авторском праве: авторское право на произведение науки, литературы и искусства возникает в силу факта его создания.

Для возникновения и осуществления авторского права не требуется регистрации произведения, иного специального оформления произведения или соблюдения каких-либо формальностей.

Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из: латинской буквы «С» в окружности; имени (наименования) обладателя исключительных авторских прав; года первого опубликования произведения.

Авторское право действует в течение всей жизни автора и 70 лет после его смерти. Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно (**статья 27**).

Истечение срока действия авторского права на произведения означает их переход в общественное достояние.

Автору сборника и других составных произведений (составителю) принадлежит авторское право на осуществленный им подбор или расположение материалов, представляющих результат творческого труда (составительство). Составитель пользуется авторским правом при условии соблюдения им прав авторов каждого из произведений, включенных в составное произведение. Авторское право составителя не препятствует другим лицам осуществлять самостоятельный подбор или расположение тех же материалов для создания своих составных произведений.

Авторское право на произведение, созданное в порядке выполнения *служебных обязанностей* или служебного задания работодателя (служебное произведение), принадлежит автору служебного произведения.

Исключительные права на использование служебного произведения принадлежат лицу, с которым автор состоит в трудовых отношениях (работодателю), если в договоре между ним и автором не предусмотрено иное.

Допускается *без согласия автора* и без выплаты авторского вознаграждения воспроизведение правомерно обнародованного произведения исключительно в личных целях, за исключением случаев, предусмотренных статьей 26 настоящего Закона и применительно к программам для ЭВМ и базам данных.

Допускается *без согласия автора* и без выплаты авторского вознаграждения, но с обязательным указанием имени автора, произведение которого используется, и источника заимствования:

- цитирование в оригинале и в переводе в научных, исследовательских, полемических, критических и информационных целях из правомерно обнародованных произведений;

- использование правомерно обнародованных произведений и отрывков из них в качестве иллюстраций в изданиях, в радио- и телепередачах, звуко- и видеозаписях учебного характера;

- воспроизведение в газетах, передача в эфир или сообщение по кабелю для всеобщего сведения правомерно опубликованных в газетах или журналах статей по текущим экономическим, политическим, социальным и религиозным вопросам;

- воспроизведение в газетах, передача в эфир или сообщение по кабелю для всеобщего сведения публично произнесенных политических речей обращений, докладов и других аналогичных произведений;

- воспроизведение или сообщение для всеобщего сведения в обзорах текущих событий средствами фотографии, путем передачи в эфир или сообщения для всеобщего сведения по кабелю произведений, которые становятся увиденными или услышанными в ходе таких событий.

Статья 25 Закона определяет порядок *свободного воспроизведения* программ для ЭВМ и баз данных и *декомпилирования* программ для ЭВМ.

Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения разрешения автора или иного обладателя исключительных прав на использование произведения и без выплаты дополнительного вознаграждения:

- внести в программу для ЭВМ или базу данных изменения, осуществляемые исключительно в целях ее функционирования на технических средствах пользователя, осуществлять любые действия, связанные с функционированием программы для ЭВМ или базы данных в соответствии с ее назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также исправление явных ошибок, если иное не предусмотрено договором с автором;

- изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал программы для ЭВМ или базы данных утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром этой программы для ЭВМ или базы данных перестает быть правомерным.

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия автора или иного обладателя исключительных прав и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

- информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;

- указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;

- информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, если это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления любого другого действия, нарушающего авторское право.

Разделы III и IV Закона (статьи 35–47) посвящены смежным правам и касаются, в основном, вопросов исполнения, постановки и использования фонограмм и т.п. произведений в средствах массовой информации и выпуска соответствующей развлекательной продукции, а также коллективного управления смежными правами.

Раздел V Закона (статьи 48–50) касается охраны авторских прав. В нем, в частности, говорится: незаконное использование произведений или объектов смежных прав либо иное нарушение предусмотренных настоящим Законом авторского права или смежных прав влечет за собой гражданско-правовую, административную, уголовную ответственность в соответствии с законодательством Российской Федерации.

Техническими средствами защиты авторского права и смежных прав признаются любые технические устройства или их компоненты, контролирующие доступ к произведениям или объектам смежных прав,

предотвращающие или ограничивающие осуществление действий, которые не разрешены автором, обладателем смежных прав или иным обладателем исключительных прав, в отношении произведений или объектов смежных прав.

Контрафактными являются экземпляры произведения и фонограммы, изготовление или распространение которых влечет за собой нарушение авторских и смежных прав. Контрафактными являются также экземпляры охраняемых в Российской Федерации в соответствии с настоящим Законом произведений и фонограмм, импортируемые без согласия обладателей авторских и смежных прав в Российскую Федерацию из государства, в котором эти произведения и фонограммы никогда не охранялись или перестали охраняться.

Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями) (вместо ФЗ от 25 сентября 1998 г. № 158-ФЗ**).**

Регулирует отношения, возникающие в связи с осуществлением лицензирования отдельных видов деятельности. Распространяется на все органы государственной власти, органы местного самоуправления, юридические лица и индивидуальных предпринимателей.

Определяет порядок лицензирования и виды деятельности, на осуществление которых требуются лицензии.

В связи с тем, что лицензирование деятельности в отдельных сферах регулируется другими федеральными законами и иными нормативными правовыми актами данный Закон в статье 1 оговаривает, на какие сферы его действие не распространяется:

деятельность кредитных организаций;

деятельность, связанная с защитой государственной тайны;

деятельность в области производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции;

деятельность в области связи;

биржевая деятельность;

деятельность в области таможенного дела;

нотариальная деятельность;

страховая деятельность;

деятельность профессиональных участников рынка ценных бумаг;

осуществление внешнеэкономических операций;

осуществление международных автомобильных перевозок грузов и пассажиров;

приобретение оружия и патронов к нему;

использование результатов интеллектуальной деятельности;

использование орбитально-частотных ресурсов и радиочастот для осуществления телевизионного вещания и радиовещания (в том числе вещания дополнительной информации);

использование природных ресурсов, в том числе недр, лесного фонда, объектов растительного и животного мира;

деятельность, работы и услуги в области использования атомной энергии;

образовательная деятельность.

К *лицензируемым видам деятельности* относятся виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам, законным интересам, здоровью граждан, обороне и безопасности государства, культурному наследию народов Российской Федерации и регулирование которых не может осуществляться иными методами, кроме как лицензированием (**статья 4**).

В целях обеспечения единства экономического пространства на территории Российской Федерации Правительство Российской Федерации в соответствии с определенными Президентом Российской Федерации основными направлениями внутренней политики государства (**статья 5**):

утверждает положения о лицензировании конкретных видов деятельности; определяет федеральные органы исполнительной власти, осуществляющие лицензирование конкретных видов деятельности; устанавливает виды деятельности, лицензирование которых осуществляется органами исполнительной власти субъектов Российской Федерации.

Лицензирующие органы осуществляют следующие полномочия: предоставление лицензий; переоформление документов, подтверждающих наличие лицензий; приостановление действия лицензий; возобновление действия лицензий; аннулирование лицензий; ведение реестра лицензий; контроль за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.

Перечень федеральных органов исполнительной власти, осуществляющих лицензирование, утвержден **постановлением Правительства Российской Федерации от 11 февраля 2002 г. № 135.**

Порядок осуществления полномочий лицензирующих органов устанавливается положениями о лицензировании конкретных видов деятельности.

В целях Федерального закона применяются следующие понятия:

Лицензия – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

Лицензируемый вид деятельности – вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с Федеральным законом.

Лицензирование – мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих выдачу лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за

нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, аннулированием лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, введением регистра лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании.

Лицензиат – юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.

Лицензионные требования и условия – совокупность установленных положениями о лицензировании конкретных видов деятельности требований и условий, выполнение которых лицензиатом обязательно при осуществлении лицензируемого вида деятельности.

Лицензирующие органы – федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с Федеральным законом.

Соискатель лицензии – юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии на осуществление конкретного вида деятельности.

Реестр лицензий – совокупность данных о предоставлении лицензий, переоформлении документов, подтверждающих наличие лицензий, приостановлении и возобновлении действия лицензий и об аннулировании лицензий.

На каждый вид лицензируемой деятельности (перечень изложен в **статье 17 Закона**) предоставляется лицензия. Вид деятельности, на осуществление которого предоставлена лицензия, может выполняться

только получившим лицензию юридическим лицом или индивидуальным предпринимателем.

Деятельность, на осуществление которой лицензия предоставлена федеральным органом исполнительной власти или органом исполнительной власти субъекта Российской Федерации, может осуществляться на всей территории Российской Федерации.

Срок действия лицензии не может быть менее чем *пять лет*. Срок действия лицензии по его окончании может быть продлен по заявлению лицензиата. Положениями о лицензировании конкретных видов деятельности может быть предусмотрено бессрочное действие лицензии.

Статья 9 Закона определяет перечень документов, предоставляемых соискателем для получения лицензии. При этом указывается, что ряд документов, обязательных для предоставления, могут быть предусмотрены иными нормативными правовыми актами, предусмотренными положениями о лицензировании конкретных видов деятельности.

Лицензирующий орган принимает решение о предоставлении или об отказе в предоставлении лицензии в срок, не превышающий сорока пяти дней со дня поступления заявления о предоставлении лицензии со всеми необходимыми документами. Соответствующее решение оформляется приказом лицензирующего органа.

Основанием отказа в предоставлении лицензии является: наличие в документах, представленных соискателем лицензии, недостоверной или искаженной информации; несоответствие соискателя лицензии, принадлежащих ему или используемых им объектов лицензионным требованиям и условиям.

Соискатель лицензии имеет право обжаловать в порядке, установленном законодательством Российской Федерации, отказ лицензирующего органа в предоставлении лицензии или его бездействие.

Наряду с обычным порядком вводится и *упрощенный порядок лицензирования*. Он может применяться, если соискатель лицензии

заключил договор страхования гражданской ответственности либо имеет сертификат соответствия осуществляемого им лицензируемого вида деятельности международным стандартам. При применении упрощенного порядка лицензирования срок рассмотрения предоставленных документов составляет не более 15 дней.

Контроль за соблюдением лицензиатом лицензионных требований и условий, определенных положением о лицензировании конкретного вида деятельности, осуществляется лицензирующими органами в пределах их компетенции (**статья 12**).

Лицензирующие органы имеют право: проводить проверки деятельности лицензиата на предмет ее соответствия лицензионным требованиям и условиям; запрашивать у лицензиата необходимые объяснения и документы при проведении проверок; составлять на основании результатов проверок акты (протоколы) с указанием конкретных нарушений; выносить решения, обязывающие лицензиата устранить выявленные нарушения, устанавливать сроки устранения таких нарушений; выносить предупреждение лицензиату.

Лицензирующие органы вправе приостанавливать действие лицензии в случае выявления лицензирующими органами неоднократных нарушений или грубого нарушения лицензиатом лицензионных требований и условий (**статья 13**).

Лицензирующий орган обязан установить срок устранения лицензиатом нарушений, повлекших за собой приостановление действия лицензии. Указанный срок не может превышать шести месяцев. В случае, если в установленный срок лицензиат не устранил указанные нарушения, лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии.

Статья 17 Закона определяет исчерпывающий перечень лицензируемых видов деятельности (всего 103 наименования). К **защите информации** среди них относятся:

- деятельность по распространению шифровальных (криптографических) средств;

- деятельность по техническому обслуживанию шифровальных (криптографических) средств;

- предоставление услуг в области шифрования информации;

- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

- деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

- деятельность по технической защите конфиденциальной информации;

- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

- деятельность по проведению экспертизы промышленной безопасности;

- производство работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений;

- деятельность по эксплуатации электрических сетей (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- негосударственная (частная) охранная деятельность;

- негосударственная (частная) сыскная деятельность;

- публичный показ аудиовизуальных произведений, если указанная деятельность осуществляется в кинозале;

- воспроизведение (изготовление экземпляров) аудиовизуальных произведений и фонограмм на любых видах носителей;

-аудиторская деятельность.

Здесь также перечислены виды деятельности, по отношению к которым может применяться упрощенный порядок лицензирования. Кроме того, дан перечень видов деятельности, лицензирование которых прекратилось с 1 января 2006 и 2007 годов.

Введение лицензирования иных видов деятельности возможно только путем внесения дополнений в предусмотренный настоящим Федеральным законом перечень видов деятельности, на осуществление которых требуются лицензии.

В связи с рассматриваемой нами областью представляет интерес Постановление Правительства РФ от **29 декабря 2007 г. N 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»** (вместо П**остановления от 23 сентября 2002 г. N 691**).

Постановление утверждает:

Положение о лицензировании деятельности **по распространению** шифровальных (криптографических) средств;

Положение о лицензировании деятельности **по техническому обслуживанию** шифровальных (криптографических) средств;

Положение о лицензировании **предоставления услуг** в области шифрования информации;

Положение о лицензировании **разработки, производства** шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Новым является:

1. Положения не распространяются на деятельность для:

- шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну;
- шифровальных (криптографических) средств независимо от их назначения, реализующих симметричные криптографические алгоритмы и обладающих максимальной длиной криптографического ключа **менее 56 бит**, а также реализующих асимметричные криптографические алгоритмы, основанные либо на разложении на множители целых чисел, либо на вычислении дискретных логарифмов в мультипликативной группе конечного поля, либо на дискретном логарифме в группе, отличной от названной, и обладающих максимальной длиной криптографического ключа **128 бит**;
- беспроводного оборудования, осуществляющего шифрование информации только в радиоканале с максимальной дальностью беспроводного действия без усиления и ретрансляции менее 400 м в соответствии с техническими условиями производителя (за исключением оборудования, используемого на критически важных объектах);

- шифровальных (криптографических) средств, используемых для защиты технологических каналов информационно-телекоммуникационных систем и сетей, не относящихся к критически важным объектам.

2. Уменьшилось число лицензионных требований, но теперь они могут быть дополнены требованиями ФСБ, которые в настоящее время неизвестны.

3. Незначительно изменился перечень представляемых документов.

4. Лицензионный контроль за соблюдением лицензиатом лицензионных требований и условий будет осуществляться в соответствии с Федеральным законом «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)».

5. Исчезло определение деятельности по техническому обслуживанию.

6. Появился новый пункт о деятельности с нарушением и определение грубого нарушения.

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

Регулирует отношения, возникающие при разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг; разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг; оценке соответствия.

Данный закон вступил в силу с 1 июля 2003 г. При этом утратили силу ряд законов и постановлений Правительства, связанных со стандартизацией и сертификацией продукции и услуг, в частности:

Закон Российской Федерации от 10 июня 1993 г. № 5151-1 «О сертификации продукции и услуг» с последующими изменениями и дополнениями;

Закон Российской Федерации от 10 июня 1993 г. № 5154-1 «О стандартизации».

Федеральный закон «О техническом регулировании» является системообразующим для построения принципиально новой системы сертификации и стандартизации, в которой бы учитывались демократические принципы нормативного регулирования, повышался бы уровень безопасности потребителей продукции и услуг, а также учитывались реалии рыночного устройства экономических отношений.

В настоящее время этот Закон для интересующей нас области следует рассматривать вместе с **Федеральным законом от 01.05.2007 № 65-ФЗ «О внесении изменений в ФЗ «О техническом регулировании».**

Основной упор в Федеральном законе «О техническом регулировании» делается на сужение сферы обязательной стандартизации и подтверждения соответствия и расширении добровольности таких действий. При этом подразумевается, что именно рыночная конъюнктура подтолкнет производителей осуществлять данную деятельность, чтобы обеспечить конкурентоспособность производимой продукции.

В законе даны определения ряда понятий.

Аккредитация – официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия.

Знак соответствия – обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту.

Сертификация – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

Сертификат соответствия – документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров.

Стандарт – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

Стандартизация – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышения конкурентоспособности продукции, работ или услуг.

Техническое регулирование – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнение работ или оказание услуг и правовое регулирование отношений в области оценки соответствия.

Технический регламент – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством, или федеральным законом, или указом Президента, или постановлением Правительства, и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации).

В качестве основных принципов технического регулирования в Законе приняты следующие:

независимость органов по аккредитации и сертификации от изготовителей, продавцов, исполнителей и приобретателей;

единая система и правила аккредитации;

единство правил и методов исследований (испытаний) и измерений при проведении процедур обязательной оценки соответствия;

единство применения требований технических регламентов независимо от видов или особенностей сделок;

недопустимость совмещения одним органом полномочий на аккредитацию и сертификацию и др.

В Законе предписано федеральным органам исполнительной власти издавать в сфере технического регулирования акты только рекомендательного характера, за исключением случаев, связанных с оборонной продукцией и продукцией, сведения о которой составляют государственную тайну.

Основное новшество в новом Законе – **технический регламент**, который устанавливает минимально необходимые требования, обеспечивающие безопасность в различных сферах, а также электромагнитную совместимость в части обеспечения безопасности работы приборов и оборудования, а также единство измерений.

В качестве основы технического регламента могут использоваться международные и/или национальные стандарты.

Технический регламент принимается федеральным законом или постановлением Правительства РФ и вступает в силу не ранее чем через 6 месяцев со дня его официального опубликования.

В России действуют общие и специальные технические регламенты. В качестве разработчика технического регламента может выступить любое лицо. Проект технического регламента должен быть опубликован в печатном издании или в информационной системе общего пользования.

Федеральным органом исполнительной власти в области технического регулирования определено ***Федеральное агентство по техническому регулированию и метрологии***, входящее в Министерство промышленности и энергетики. Публичное обсуждение проекта технического регламента должно быть не менее 2-х месяцев. Подробно описан механизм прохождения закона о техническом регламенте в Госдуме и перечень необходимых документов. В исключительных случаях Президент России вправе издать технический регламент без его публичного обсуждения. До вступления в силу Федерального закона о техническом регламенте Правительство России вправе издать постановление о соответствующем регламенте.

Большое внимание в Законе уделено вопросам стандартизации. Определены цели и принципы стандартизации. Одним из принципов является **добровольное применение стандартов.**

К документам в области стандартизации, используемым на территории Российской Федерации, относятся: национальные стандарты; правила стандартизации, нормы и рекомендации в области стандартизации; общероссийские классификаторы технико-экономической и социальной информации; стандарты организаций.

Стандарты организаций, в том числе коммерческих, общественных, научных и саморегулируемых организаций, объединений юридических лиц могут разрабатываться в целях, не противоречащих настоящему закону. Проект стандарта может представляться в технический комитет по стандартизации, который проводит его экспертизу.

Четвертая глава закона посвящена подтверждению соответствия, означающему, что представляемая продукция, процессы и др. соответствуют техническим регламентам, стандартам, условиям договоров. Подтверждение соответствия на территории РФ может носить добровольный или обязательный характер.

В **пятой главе** закона рассмотрены вопросы, связанные с аккредитацией органов по сертификации и испытательных лабораторий (центров).

Шестая глава посвящена государственному контролю (надзору) за соблюдением технических регламентов.

Седьмая глава посвящена ответственности за несоответствие продукции и др. требованиям технических регламентов и порядка отзыва продукции из обращения.

Восьмая глава «Информация о технических регламентах и документах по стандартизации» определяет порядок публикации информации о технических регламентах. Здесь также описано назначение Федерального информационного фонда технических регламентов и стандартов.

В заключительных положениях записано, что технические регламенты должны быть приняты в течение 7 лет со дня вступления в силу этого закона. Здесь также описан порядок работы до вступления в силу технических регламентов.

Реализация положений этого закона и контроль их исполнения возложены на *Федеральное агентство по техническому регулированию и метрологии*. Положение о нем утверждено **постановлением Правительства от 17 июня 2004 г. № 294.**

Применительно к потребностям сферы защиты информации, законодательство о техническом регулировании необходимо было совершенствовать. Эта работа завершилась принятием **Федерального закона от 01.05.2007 № 65-ФЗ «О внесении изменений в ФЗ «О техническом регулировании».**

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (в ред. Федеральных законов от 02.02.2006 № 19-ФЗ, от 18.12.2006 № 231-ФЗ, от 24.07.2007 № 214-ФЗ)

Регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау) (…с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну – старая редакция ФЗ «98-ФЗ от 29.07.2004).

Данный Закон вводит в правовое поле все принятые ранее документы федерального и регионального уровней, касающиеся коммерческой тайны, и конкретизирует положения статьи 139 Гражданского кодекса Российской Федерации «Служебная и коммерческая тайна».

Положения Закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

В Законе используются следующие основные понятия:

Коммерческая тайна – 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 (секрет производства), – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о

результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны (п. 2 в ред. Федерального закона от 18.12.2006 N 231-ФЗ).

Режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности (утратило силу с 01.01.2008 –ФЗ № 231-ФЗ)

Обладатель информации, составляющей коммерческую тайну, – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайне.

Доступ к информации, составляющей коммерческую тайну, – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача информации, составляющей коммерческую тайну, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Контрагент – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Предоставление информации, составляющей коммерческую тайну, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, или иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

В Законе однозначно определен перечень сведений, которые не могут составлять коммерческую тайну:

1. Содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры.

2. Содержащиеся в документах, дающих право на осуществление предпринимательской деятельности.

3. О составе имущества государственного или муниципального унитарного предприятия и об использовании ими средств соответствующих бюджетов.

4. О загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом.

5. О численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест.

6. О задолженности работодателей по выплате заработной платы и по иным социальным выплатам.

7. О нарушении законодательства и фактах привлечения к ответственности за совершение этих нарушений.

8. Об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности.

9. О размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации.

10. О перечне лиц, имеющих право действовать без доверенности от имени юридического лица.

11. Обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами (п. 4 ст.8 ФЗ № 149-ФЗ, ст. 7 ФЗ № 5485-1, ст. 26 ФЗ «О банках …).

Закон однозначно определяет круг лиц и организаций, кому необходимо предоставлять информацию, составляющую коммерческую тайну.

Такую информацию по мотивированному требованию необходимо предоставлять органу государственной власти, иного государственного органа, органа местного самоуправления. Информация предоставляется безвозмездно. Само мотивированное требование должно быть подписано уполномоченным лицом и содержать указание цели и правового основания затребования информации, срок предоставления информации. Если обладатель информации, составляющей коммерческую тайну,

отказывается ее предоставлять, то соответствующие органы вправе потребовать ее предоставление по суду.

На всех документах, предоставляемых по требованию соответствующих органов, должен быть нанесен **гриф «коммерческая тайна»** с указанием ее обладателя (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество и место жительства).

Обладатель информации, имеющей гриф «коммерческая тайна», должен принимать меры по ее охране. Эти меры должны включать:

- перечень информации, составляющей коммерческую тайну;

- установление порядка доступа и порядка обращения с такой информацией, а также способы контроля за установленным порядком;

- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «коммерческая тайна» с указанием обладателя этой информации.

Кроме этих мер обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие, не противоречащие законодательству меры.

Для осуществления принимаемых мер работодатель обязан:

- ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения своих обязанностей, с перечнем такой информации;

- ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушения;

- создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

Работник обязан выполнять установленный работодателем режим коммерческой тайны и не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;

Трудовым договором с руководителем организации должны предусматриваться его обязательства по обеспечению охраны конфиденциальности информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны ее конфиденциальности.

При увольнении работник обязан передать работодателю все имеющиеся в его распоряжении материальные носители с информацией, содержащей коммерческую тайну.

Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет

дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности.

Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями и дополнениями).

Определяет основные понятия, полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты. Дает перечень сведений, которые могут быть отнесены к государственной тайне. Указывает принципы засекречивания сведений, перечисляет сведения, не подлежащие засекречиванию, устанавливает степени секретности сведений и грифы секретности носителей этих сведений. Описывает порядок отнесения сведений к государственной тайне, порядок рассекречивания сведений.

Правовой институт государственной тайны самый разработанный из числа правовых систем ограничения в доступе к информации. Однако развитие компьютерных систем создало для традиционной системы обеспечения режима секретности, в основном ориентированной на оборот документированной информации на бумажных носителях, много проблем.

Положения Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной властей, местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя

обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне (**статья 1**).

В Законе используются следующие основные понятия:

государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

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;

допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений;

доступ к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они

реализованы, а также средства контроля эффективности защиты информации.

перечень сведений, составляющих государственную тайну, – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации «О безопасности» и включает настоящий Закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны (**статья 3**).

В Законе определяются и законодательно закрепляются полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты (статья 4), а также задается в общем виде перечень сведений, которые могут быть отнесены к государственной тайне (**статья 5**).

Засекречивание сведений и их носителей – введение в предусмотренном Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям. Засекречивание сведений осуществляется в соответствии с принципами законности, обоснованности и своевременности.

Законность засекречивания сведений заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 Закона и законодательству Российской Федерации о государственной тайне.

Обоснованность засекречивания сведений 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 засекречивания сведений заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым **распоряжением Президента России от 17 января 2000 г. № 6-рп.** Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Закон определяет сведения, не подлежащие засекречиванию (**статья 7**):

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах Российской Федерации;

о состоянии здоровья высших должностных лиц Российской Федерации;

о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

Должностные лица, наделенные полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан, если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению. При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну в соответствии с действующим законодательством.

Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника информации, его права. Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации.

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих работ. При этом до передачи сведений, составляющих государственную тайну, заказчик обязан убедиться в наличии у предприятия, учреждения или организации лицензии на проведение работ с использованием сведений соответствующей степени секретности, а у граждан – соответствующего допуска.

Предприятия, учреждения или организации, в том числе и негосударственных форм собственности, при проведении совместных и других работ (получении государственных заказов) и возникновении в связи с этим необходимости в использовании сведений, составляющих государственную тайну, могут заключать с государственными предприятиями, учреждениями или организациями договоры об использовании услуг их структурных подразделений по защите государственной тайны, о чем делается соответствующая отметка в лицензиях на проведение работ с использованием сведений, составляющих государственную тайну, обеих договаривающихся сторон.

В Законе устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «*особой важности», «совершенно секретно» и «секретно»*. Использование

перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Статья 12 Закона определяет реквизиты носителей сведений, составляющих государственную тайну. На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

о регистрационном номере;

о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, они указываются в сопроводительной документации на этот носитель.

Статья 20 раздела VI Закона относит к органам, осуществляющим защиту государственной тайны на территории Российской Федерации, следующие органы:

- межведомственную комиссию по защите государственной тайны;

- федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы;

- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством Российской Федерации.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

- принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

- согласие на частичные, временные ограничения их прав в соответствии со статьей 24 настоящего Закона (право выезда за рубеж, право неприкосновенности частной жизни, право на распространение сведений об открытиях и изобретениях);

- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

- определение видов, размеров и порядка предоставления льгот, предусмотренных настоящим Законом;

- ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо.

Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий.

Закон (**статья 27**) определяет порядок допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, и порядок сертификации средств защиты информации (**статья 28**).

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

- выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

- наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

- наличие у них сертифицированных средств защиты информации.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации.

Координация работ по организации сертификации средств защиты информации возлагается на Межведомственную комиссию по защите государственной тайны. Положение об этой комиссии и ее состав утверждены Указом Президента Российской Федерации от 6.10.2004 г. № 1286.

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях осуществляют федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности (Федеральная служба безопасности Российской Федерации), федеральный орган исполнительной власти, уполномоченный в области обороны (Министерство обороны Российской Федерации), федеральный орган исполнительной власти, уполномоченный в области внешней разведки (Служба внешней разведки Российской Федерации), федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), и их территориальные органы, на которые эта функция возложена законодательством Российской Федерации.

Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с изменениями и дополнениями).

Устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Статья 63 Закона устанавливает понятие **тайны связи.**

На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по

сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

Операторы связи обязаны обеспечить соблюдение тайны связи.

Федеральный закон от 31 мая 2002 г. N 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (с изменениями и дополнениями).

Адвокатской деятельностью является квалифицированная юридическая помощь, оказываемая на профессиональной основе лицами, получившими статус адвоката в порядке, установленном настоящим Федеральным законом, физическим и юридическим лицам в целях защиты их прав, свобод и интересов, а также обеспечения доступа к правосудию.

Статья 8 Закона определяет понятие **адвокатской тайны**.

Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

Закон Российской Федерации от 27 ноября 1992 г. № 4015-1 «Об организации страхового дела в Российской Федерации» (с изменениями и дополнениями).

Регулирует отношения между лицами, осуществляющими виды деятельности в сфере страхового дела, или с их участием, отношения по осуществлению государственного надзора за деятельностью субъектов страхового дела, а также иные отношения, связанные с организацией страхового дела.

Статья 33 Закона предписывает соблюдение коммерческой и иной охраняемой законом тайны субъекта страхового дела должностными лицами органа страхового надзора, за исключением случаев, предусмотренных законодательством Российской Федерации.

Федеральный закон от 3 февраля 1996 г. № 17-ФЗ «О внесении изменений и дополнений в Закон РСФСР от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности в РСФСР» (с изменениями и дополнениями).

Регулирует деятельность банковской системы Российской Федерации, которая включает в себя Банк России, кредитные организации, а также филиалы и представительства иностранных банков.

Статья 26 Закона определяет понятие **банковской тайны**:

Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, налоговым органам, таможенным органам Российской Федерации в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора – органам предварительного следствия по делам, находящимся в их производстве.

Федеральный закон от 7 августа 2001 г. № 119-ФЗ «Об аудиторской деятельности» (с изменениями и дополнениями).

Определяет правовые основы регулирования аудиторской деятельности в Российской Федерации.

Статья 8 Закона определяет понятие **аудиторской тайны.**

Аудиторские организации и индивидуальные аудиторы обязаны хранить тайну об операциях аудируемых лиц и лиц, которым оказывались сопутствующие аудиту услуги.

Аудиторские организации и индивидуальные аудиторы обязаны обеспечивать сохранность сведений и документов, получаемых и (или) составляемых ими при осуществлении аудиторской деятельности, и не вправе передавать указанные сведения и документы или их копии третьим лицам либо разглашать их без письменного согласия организаций и (или) индивидуальных предпринимателей, в отношении которых осуществлялся аудит и оказывались сопутствующие аудиту услуги, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами.

Федеральный орган исполнительной власти, осуществляющий государственное регулирование аудиторской деятельности, и иные лица, получившие доступ к сведениям, составляющим аудиторскую тайну в соответствии с настоящим Федеральным законом и другими федеральными законами, обязаны сохранять конфиденциальность в отношении таких сведений.

Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (с изменениями и дополнениями).

Устанавливает правовую основу деятельности в области массовой информации, включая термины и определения, принципы, организационные основы и ограничения в распространении информации.

Федеральный закон от 18 июля 1995 г. № 108-ФЗ «О рекламе» (с изменениями и дополнениями).

Регулирует отношения, возникающие в процессе производства, размещения и распространения рекламы на рынках товаров, работ, услуг Российской Федерации, включая рынки банковских, страховых и иных услуг, связанных с пользованием денежными средствами граждан (физических лиц) и юридических лиц, а также рынки ценных бумаг.

Статья 27 Закона определяет право доступа к любой информации сотрудников антимонопольных органов и обязует их хранить коммерческую тайну, а также иметь при необходимости допуск к государственной тайне.

Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности» (с изменениями и дополнениями).

Закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «Об органах федеральной службы безопасности в Российской Федерации» (с изменениями и дополнениями).

Определяет назначение, правовые основы, принципы, направления деятельности, полномочия, силы и средства органов федеральной службы безопасности, а также порядок контроля и надзора за их деятельностью.

Статья 7 Закона определяет защиту сведений о федеральной службе безопасности:

1. Граждане Российской Федерации, принимаемые на военную службу (работу) в органы федеральной службы безопасности, а также

допускаемые к сведениям об органах федеральной службы безопасности, проходят процедуру оформления допуска к сведениям, составляющим государственную тайну, если иной порядок не предусмотрен законодательством Российской Федерации. Такая процедура включает в себя принятие обязательства о неразглашении указанных сведений.

2. В случаях, предусмотренных федеральными законами и иными нормативными правовыми актами Российской Федерации, указанный порядок распространяется на граждан Российской Федерации, принимаемых на военную службу (работу) в пограничные войска, а также допускаемых к сведениям о пограничных войсках.

Кроме того, **статьи 17 и 19** Закона определяют:

1. Сведения о сотрудниках органов федеральной службы безопасности, выполнявших (выполняющих) специальные задания в специальных службах и организациях иностранных государств, в преступных группах, составляют государственную тайну и могут быть преданы гласности только с письменного согласия указанных сотрудников и в случаях, предусмотренных федеральными законами.

2. Сведения о лицах, оказывающих или оказывавших органам федеральной службы безопасности содействие на конфиденциальной основе, составляют государственную тайну и могут быть преданы гласности только с письменного согласия этих лиц и в случаях, предусмотренных федеральными законами.

Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с изменениями и дополнениями).

Определяет содержание оперативно-розыскной деятельности, осуществляемой на территории Российской Федерации, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий.

Статья 12 Закона определяет защиту сведений об органах, осуществляющих оперативно-розыскную деятельность.

Сведения об используемых или использованных при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и о тактике проведения оперативно-розыскных мероприятий составляют *государственную тайну* и подлежат рассекречиванию только на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность.

Федеральный закон от 25 июля 1998 г. № 130-ФЗ «О борьбе с терроризмом» (с изменениями и дополнениями).

Определяет правовые и организационные основы борьбы с терроризмом в Российской Федерации, порядок координации деятельности осуществляющих борьбу с терроризмом федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, общественных объединений и организаций независимо от форм собственности, должностных лиц и отдельных граждан, а также права, обязанности и гарантии граждан в связи с осуществлением борьбы с терроризмом.

Статья 15 Закона определяет порядок информирования общественности о ходе контртеррористической операции.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (вместо ФЗ от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите

информации») (с изменениями и дополнениями в соответствии с ФЗ от 10 января 2003 г. № 15-ФЗ).

Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации.

Определяет условия для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защиту интересов России, ее субъектов и муниципальных объединений, а также физических и юридических лиц при международном информационном обмене.

Рассмотрим основные положения этого закона.

О части основных понятий, используемых в ФЗ, уже говорилось. Это следующие понятия: информация, информационные технологии, информационная система, информационно-телекоммуникационная сеть, обладатель информации, доступ к информации, конфиденциальность информации, электронное сообщение, документированная информация.

Они фактически являются основными понятиями всего курса. Приведем те, которые еще не рассматривались:

- *предоставление информации* – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

- *распространение информации* – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

- *оператор информационной системы* – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Статья 5, п. 2, отмечает, что информация в зависимости от категории доступа к ней подразделяется на **общедоступную информацию**, а также на информацию, доступ к которой ограничен федеральными законами (**информация ограниченного доступа**).

Далее понятие общедоступной информации раскрывается в **статье 7:**

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Важно, что согласно **п. 4 статьи 8** не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

В **статье 9** излагаются ограничения доступа к информации.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим **коммерческую тайну** (№ 98-ФЗ от 29 июля 2004 г. «О коммерческой тайне»), **служебную тайну** и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (**профессиональная тайна**), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей **личную или семейную тайну**, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами. Порядок доступа к **персональным данным** граждан (физических лиц) устанавливается федеральным законом «О персональных данных» (№ 152-ФЗ от 27 июля 2006 г.).

Статья 6 посвящена обладателю информации. Им может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование. Обладатель информации вправе:

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.

Далее в **статье 13, п. 3,** о информационных системах говорится, что «права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных».

Важны и обязанности обладателя информации:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 11 касается документированной информации.

Здесь важно отметить, что электронное сообщение, подписанное **электронной цифровой подписью** или **иным аналогом собственноручной подписи**, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

Статья 12 о государственном регулировании в сфере применения ИТ гласит в частности, что оно предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации);

2) **развитие информационных систем** 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 Российской Федерации информационно-телекоммуникационных сетей, в том числе сети **Интернет** и иных подобных информационно-телекоммуникационных сетей.

Статья 13 об информационных системах (ИС) отмечает, что **оператором информационной системы** является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с **техническими регламентами**, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем. Порядок создания и эксплуатации информационных систем, **не являющихся государственными ИС или муниципальными ИС**, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

Непосредственно государственных ИС касается **статья 14**. Здесь важно отметить, что **технические средства**, предназначенные для обработки информации, содержащейся в государственных ИС, в том числе программно-технические средства и **средства защиты информации**, должны соответствовать требованиям законодательства Российской Федерации **о техническом регулировании**.

Наконец, **статья 16** дает определение и посвящена защите информации.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

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.

Важно, что обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

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

2) своевременное обнаружение фактов несанкционированного доступа 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.

Обращает на себя внимание **п. 6 статьи 16,** согласно которому федеральными законами могут быть установлены **ограничения использования определенных средств защиты** информации и

осуществления отдельных видов деятельности в области защиты информации.

В **статье 17** устанавливается ответственность (дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с законодательством Российской Федерации) за правонарушения ИТ и защиты информации. Именно: лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

Но при этом требование о возмещении убытков **не может быть удовлетворено** в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

В случае если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации **не несет** лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».

Обеспечивает правовые условия использования электронной цифровой подписи (ЭЦП) в электронных документах. Приведены основные понятия, используемые в электронных документах, и условия использования ЭЦП.

Закон Российской Федерации от 23 сентября 1992 г. № 3526-1 «О правовой охране топологий интегральных микросхем» (с изменениями и дополнениями).

Регулирует отношения, связанные с созданием, правовой охраной и использованием топологий.

Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

Регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Важно, что он **не распространяется** на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда РФ и других архивных документов в соответствии с законодательством об архивном деле в РФ;

3) обработке подлежащих включению в **единый государственный реестр индивидуальных предпринимателей** сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством РФ в связи с деятельностью физического лица в качестве индивидуального предпринимателя;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

В Законе используются следующие основные понятия:

1) **персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Здесь обращает на себя внимание в приводимом списке «другая информация». Интересно сравнить это определение с определением из ФЗ от 19.12.2005 № 160 «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», где «персональные данные» означают любую информацию об определенном или поддающемся определению физическом лице (субъект данных);

2) **оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

3) **обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

4) **распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом (это несколько отличается от понятий «предоставления информации» и «распространения информации» из Закона № 149-ФЗ от 27.07.2006, которые отличаются в основном кругом лиц, определенным или неопределенным);

5) **использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

6) **блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

7) **уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

8) **обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

9) **информационная система персональных данных** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

10) **конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

11) **трансграничная передача персональных данных** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

12) **общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

К закону было подготовлено **Постановление Правительства РФ от 17 ноября 2007 г. N 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»**. ФСБ и ФСТЭК России подготовили и другие документы.

Положение устанавливает **требования к обеспечению безопасности** персональных данных при их обработке в информационных системах (ИС)

персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее – информационные системы).

Под **техническими средствами**, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью **системы защиты персональных данных**, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Методы и способы защиты информации в информационных системах устанавливаются **Федеральной службой по техническому и экспортному контролю (ФСТЭК)** и **Федеральной службой безопасности (ФСБ)** Российской Федерации в пределах их полномочий (подготовлены в марте 2008 г.).

Безопасность персональных данных при их обработке в ИС обеспечивает **оператор** или **уполномоченное лицо**, которому на основании договора оператор поручает обработку персональных данных. Эти лица при обработке персональных данных в ИС должны обеспечить:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

Важные разделы касаются разработчиков средств защиты информации, на которых возлагается реализация требований по обеспечению безопасности.

В отношении разработанных **шифровальных (криптографических) средств защиты** информации проводятся тематические исследования и контрольные тематические исследования. При этом под **тематическими исследованиями** понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами

информационных систем, а под **контрольными тематическими исследованиями** – периодически проводимые тематические исследования.

Результаты оценки соответствия и (или) результаты тематических исследований средств защиты информации оцениваются в ходе экспертизы, осуществляемой ФСТЭК и ФСБ Российской Федерации в пределах их полномочий.

Далее вопросы обеспечения безопасности персональных данных были уточнены в Приказе ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», а также 4-х документах ФСТЭК России ограниченного распространения:

1.«Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).

2. «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).

3. «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» (утверждены 15 февраля 2008 г. заместителем директора ФСТЭК России).

4. «Рекомендации по обеспечению безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждены 15 февраля 2008 г. заместителем директора ФСТЭК России).

Эти документы должны быть опубликованы, иначе по ст. 15 Конституции РФ их выполнение необязательно.

В соответствии с **Приказом № 55/86/20** информационные системы (ИС) персональных данных подразделяются на типовые и специальные.

Типовые ИС – «информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных». **Специальные ИС** – «информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий)». В скобках указано общепринятое требование о целостности информации, но ничего не сказано, например, о доступности ее.

Особо подчеркнуто, что к специальным ИС должны быть отнесены те:

- в которых обрабатываются ПД, касающиеся состояния здоровья субъектов персональных данных;
- в которых предусмотрено принятие на основании исключительно автоматизированной обработки ПД решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Таблица 2

Классификация типовой информационной системы

X_пд \ X_нпд	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

Класс типовой ИС (К1, …, К4) определяется в соответствии с таблицей, в зависимости от двух параметров X_пд (категория ПД) и X_нпд (объем обрабатываемых ПД).

Типовой ИС присваивается один из следующих классов:

класс 1 (К1) – ИС, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

класс 2 (К2) – ИС, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

класс 3 (К3) – ИС, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

класс 4 (К4) – ИС, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Значения для Х_пд следующие:

категория 1 – ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 – ПД, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 – ПД, позволяющие идентифицировать субъекта персональных данных;

категория 4 – обезличенные и (или) общедоступные персональные данные.

Второй параметр Х_нпд принимает следующие 3 значения:

1 – в ИС одновременно обрабатываются ПД более чем 100 000 субъектов или ПД субъектов в пределах субъекта РФ или РФ в целом;

2 – в ИС одновременно обрабатываются ПД от 1000 до 100 000 субъектов или ПД субъектов, работающих в отрасли экономики РФ, в

органе государственной власти, проживающих в пределах муниципального образования;

3 – в ИС одновременно обрабатываются ПД менее чем 1000 субъектов или ПД субъектов персональных данных в пределах конкретной организации.

Процедура классификации типовых ИС прописана в Приказе достаточно подробно, но вероятно большинство ИС относятся к специальным ИС. А для таких ИС класс определяется по результатам анализа исходных данных на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781.

В общем случае при классификации ИС, помимо приведенных двух параметров Х_пд и Х_нпд, учитываются следующие данные:

- характеристики безопасности (конфиденциальность, целостность, доступность, …);
- структура ИС (автономные АРМ, локальные ИС, распределенные ИС);
- наличие подключений к Интернет и сетям общего пользования;
- режим обработки персональных данных (однопользовательские и многопользовательские);
- режим разграничения прав доступа (ИС с разграничением прав доступа и без);
- местонахождение технических средств (все в пределах РФ, частично или целиком за пределами РФ).

Классификация специальных ИС прописана в 4 приведенных выше документах ФСТЭК, которые необходимо каждой заинтересованной организации или оператору ПД получить индивидуально во ФСТЭК.

Необходимо также рассмотреть следующие акты:

№ 153-ФЗ «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О ратификации Конвенции Совета Европы о предупреждении терроризма» и ФЗ «О противодействии терроризму».

№ 218-ФЗ от 30.12.2004 «О кредитных историях».

№ 35-ФЗ от 6.03.2006 «О противодействии терроризму».

№ 16-ФЗ от 09.02.2007 «О транспортной безопасности».

Основные подзаконные акты в области защиты информации

Количество подзаконных актов федерального уровня и уровня субъектов федерации, изданных во исполнение рассмотренных выше законов, выпущено более сотни. Кроме того, в них постоянно вносятся изменения и уточнения. Ниже представлено краткое содержание только основных из таких подзаконных актов, определяющих либо основы деятельности в различных сферах, связанных с защитой информации, либо наиболее часто требующихся на практике. Все такие акты разделены на три категории: указы Президента Российской Федерации, Постановления Правительства Российской Федерации и ведомственные документы. Более подробно о них можно посмотреть в учебнике [Тихонов-Райх].

Отметим, что в связи с проведением административной реформы в Российской Федерации названия соответствующих органов исполнительной власти, упоминающихся в рассматриваемых документах, изменены на новые или на названия преемников ликвидированных ведомств (например, ФАПСИ – ликвидировано 11.03.2003 г.), за исключением Гостехкомиссии (ныне Федеральной службы по техническому и экспортному контролю, ФСТЭК).

Указы Президента Российской Федерации

1. Указ Президента Российской Федерации от 31 декабря 1993 г. № 2334 **«О дополнительных гарантиях прав граждан на информацию»** (с изменениями от 17 января 1997 г., 1 сентября 2000 г.).

Указ определяет, что деятельность государственных органов, организаций и предприятий, общественных объединений, должностных лиц должна осуществляться на следующих принципах информационной открытости:

- доступность для граждан информации, представляющей общественный интерес или затрагивающей личные интересы граждан;

- систематическое информирование граждан о предполагаемых или принятых решениях;

- осуществление гражданами контроля за деятельностью государственных органов, организаций и предприятий, общественных объединений, должностных лиц и принимаемыми ими решениями, связанными с соблюдением, охраной и защитой прав и законных интересов граждан;

- создание условий для обеспечения граждан Российской Федерации зарубежными информационными продуктами и оказание им информационных услуг, имеющих зарубежное происхождение.

Устанавливается, что в информационных программах государственных телерадиовещательных компаний до сведения граждан в обязательном порядке должны доводиться основные положения правовых актов и решений государственных органов по основными вопросам внутренней и внешней политики *в день их выпуска*. Государственные телерадиовещательные компании должны создать циклы передач (программы), разъясняющие деятельность федеральных органов законодательной, исполнительной и судебной власти, существо принимаемых решений с привлечением к работе над этими программами

ведущих специалистов, экспертов, разработчиков соответствующих документов.

2. Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «**О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»** (с изменениями от 25 июля 2000 г.).

Указ определяет порядок использования шифровальных средств.

Запрещается использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата ФСБ России, а также размещение государственных заказов на предприятиях, в организациях, использующих указанные технические и шифровальные средства, не имеющие соответствующего сертификата.

Центральному банку России указывается принять необходимые меры в отношении коммерческих банков РФ, уклоняющихся от обязательного использования имеющих сертификат ФСБ России защищенных технических средств хранения, обработки и передачи информации при их информационном взаимодействии с подразделениями Центрального банка России.

В интересах информационной безопасности РФ и усиления борьбы с организованной преступностью запрещается деятельность юридических и физических лиц, связанная с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением

услуг в области шифрования информации, без лицензий, выданных ФСБ России.

Федеральной таможенной службе Российской Федерации указывается принять меры к недопущению ввоза на территорию Российской Федерации шифровальных средств иностранного производства без соответствующей лицензии Министерства торговли и экономического развития, выданной по согласованию с ФСБ России.

3. Указ Президента Российской Федерации от 9 января 1996 г. № 21 «**О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации»** (с изменениями от 30 декабря 2000 г.).

В соответствии с Федеральным законом «Об оперативно-розыскной деятельности» Указ возлагает на ФСБ России следующие обязанности:

- лицензирование деятельности не уполномоченных на осуществление оперативно-розыскной деятельности физических и юридических лиц, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввозом в Российскую Федерацию и вывозом за ее пределы специальных технических средств, предназначенных для негласного получения информации, а также сертификацию, регистрацию и учет таких специальных технических средств;

- выявление и пресечение случаев проведения оперативно-розыскных мероприятий и использования специальных и иных технических средств, разработанных, приспособленных, запрограммированных для негласного получения информации, неуполномоченными лицами;

- координация деятельности федеральных органов исполнительной власти, осуществляемой в соответствии с Федеральным законом «Об оперативно-розыскной деятельности», в области разработки, производства, закупки, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности.

Положение о лицензировании деятельности, связанной со специальными техническими средствами, предназначенными для негласного получения информации, утверждено Постановлением Правительства Российской Федерации от 15 июля 2002 г. № 526.

Положение о ввозе в Российскую Федерацию и вывозе из Российской Федерации указанных технических средств утверждено Постановлением Правительства Российской Федерации от 10 марта 2000 г. № 214.

Перечень видов специальных технических средств, предназначенных для негласного получения информации, утвержден Постановлением Правительства Российской Федерации от 1 июля 1996 г. № 770.

4. Указ Президента Российской Федерации от 15 февраля 2006 г. № 116 «**О мерах по противодействию терроризму**».

В соответствии с данным Указом образован Национальный антитеррористический Комитет. Председатель Комитета – директор ФСБ России. Созданы антитеррористические комиссии в субъектах РФ. Увеличена численность Центрального аппарата ФСБ на 300 человек.

5. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «**О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-**

телекоммуникационных сетей международного информационного обмена».

Постановления Правительства Российской Федерации

1. Постановление Правительства РФ от 15 апреля 1995 г. № 333 «**О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»** (с изменениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г., 3 октября 2002 г.)

Данным Постановлением утверждено Положение о лицензировании деятельности, связанной с работой со сведениями, составляющими государственную тайну. В нем, в частности, сказано, что органами, уполномоченными на ведение лицензионной деятельности, являются:

- по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, – Федеральная служба безопасности Российской Федерации и ее территориальные органы (на территории Российской Федерации), Служба внешней разведки Российской Федерации (за рубежом);

- на право проведения работ, связанных с созданием средств защиты информации, – Государственная техническая комиссия при Президенте Российской Федерации (здесь и далее следует подразумевать новое название данной организации – ФСТЭК России), Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба безопасности Российской Федерации (в пределах их компетенции);

- на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – Федеральная служба безопасности Российской Федерации и ее территориальные органы,

Государственная техническая комиссия при Президенте Российской Федерации, Служба внешней разведки Российской Федерации (в пределах их компетенции).

Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, и при выполнении следующих условий:

- соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

- наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны;

- наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее трех и более пяти лет.

Государственными органами, ответственными за организацию и проведение специальных экспертиз предприятий, являются Федеральная служба безопасности Российской Федерации, Государственная техническая комиссия при Президенте Российской Федерации, Служба внешней разведки Российской Федерации, другие министерства и ведомства Российской Федерации, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий.

2. Постановление Правительства РФ от 26 июня 1995 г. № 608 «**О сертификации средств защиты информации»** (с изменениями от 23.04.1996 г., 29.03.1999 г.).

Данным Постановлением утверждено Положение о сертификации средств защиты информации, которое устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

Система сертификации средств защиты информации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам.

Системы сертификации создаются Государственной технической комиссией при Президенте Российской Федерации, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, Службой внешней разведки Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации.

Сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных

документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции. Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны. В каждой системе сертификации разрабатываются и согласовываются с Межведомственной комиссией положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

Основными схемами проведения сертификации средств защиты информации являются:

- для единичных образцов средств защиты информации – проведение испытаний этих образцов на соответствие требованиям по защите информации;

- для серийного производства средств защиты информации – проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований. Кроме того, допускается предварительная проверка производства по специально разработанной программе.

Срок действия сертификата не может превышать пяти лет.

3. Постановление Правительства РФ от 10 марта 2000 г. № 214 «**Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию»** (с изменениями от 19 октября 2000 г.).

Контроль за ввозом в Российскую Федерацию и вывозом из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, не уполномоченными на осуществление оперативно-розыскной деятельности юридическими лицами обеспечивает Федеральная служба безопасности Российской Федерации и Федеральная таможенная служба Российской Федерации.

Лицензирование деятельности по ввозу указанных средств осуществляет Министерство экономического развития и торговли Российской Федерации на основании решений Центра Федеральной службы безопасности Российской Федерации по лицензированию, сертификации и защите государственной тайны.

4. Постановление Правительства РФ от 11 февраля 2002 г. № 135 «**О лицензировании отдельных видов деятельности»**.

Устанавливает перечень федеральных органов исполнительной власти, осуществляющих лицензирование в определенных областях, а также виды деятельности, лицензируемые органами исполнительной власти субъектов Российской Федерации.

Защиты информации в данном Постановлении касается лицензирование следующих видов деятельности.

МВД России: негосударственная (частная) охранная деятельность, негосударственная (частная) сыскная деятельность;

МЧС России: производство работ по монтажу, ремонту и обслуживанию средств обеспечения пожарной безопасности зданий и сооружений;

ФСБ России:

- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными

предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- деятельность по распространению шифровальных (криптографических) средств;

деятельность по техническому обслуживанию шифровальных (криптографических) средств;

- предоставление услуг в области шифрования информации;

- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

- деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

ФСТЭК России:

- деятельность по технической защите конфиденциальной информации;

-деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

5. Постановление Правительства РФ от 30 апреля 2002 г. № 290 «**О лицензировании деятельности по технической защите конфиденциальной информации**».

Положение определяет порядок лицензирования деятельности юридических и физических лиц по технической защите конфиденциальной информации.

Под *технической защитой конфиденциальной информации* понимается комплекс мероприятий и (или) услуг по защите ее от НСД, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней.

Право выдачи лицензий имеет ФСТЭК России.

Лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

а) осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности «компьютерная безопасность», «комплексное обеспечение информационной безопасности автоматизированных систем» или «информационная безопасность телекоммуникационных систем», либо специалистами, прошедшими переподготовку по вопросам защиты информации;

б) соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами Российской Федерации и нормативно-методическими документами по технической защите информации;

в) использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;

г) использование третьими лицами программ для электронно-вычислительных машин или баз данных на основании договора с их правообладателем.

Положение также определяет перечень необходимых документов для получения лицензии и порядок ее выдачи. Срок действия лицензии установлен в 5 лет, потом она должна переоформляться. Один раз в год производится проверка выполнения лицензионных требований.

6. Постановление Правительства РФ от 27 мая 2002 г. № 348 «**Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»**.

Это Положение определяет порядок лицензирования деятельности юридических и физических лиц по разработке и (или) производству средств защиты конфиденциальной информации.

Лицензирование осуществляет ФСТЭК России, а в части разработки средств защиты для объектов Администрации Президента РФ, Совбеза РФ, Федерального Собрания РФ, Правительства РФ, Конституционного, Верховного и Высшего Арбитражного судов – ФСБ России.

Разрабатываемые устройства должны удовлетворять требованиям госстандартов РФ, соответствующей документации и иных нормативных актов, а также по уровню подготовки специалистов и выдерживать соответствие помещений и оборудования требованиям по защите информации. Для деятельности, лицензируемой ФСБ России в данной сфере, набор лицензионных требований значительно шире.

Перечень необходимых документов для получения лицензии, порядок ее выдачи, срок действия лицензии и контроль ее выполнения установлены Положением практически аналогично Постановлению № 290, рассмотренному выше.

7. Постановление Правительства РФ от 23 сентября 2002 г. № 691 «**Об утверждении положений о лицензировании отдельных видов**

деятельности, связанных с шифровальными (криптографическими) средствами».

Данным документом утверждаются 4 положения, касающиеся лицензирования отдельных видов деятельности в области криптографических средств:

1. Положение о лицензировании деятельности *по распространению* шифровальных (криптографических) средств.

2. Положение о лицензировании деятельности *по техническому обслуживанию* шифровальных (криптографических) средств.

3. Положение о лицензировании *предоставления услуг* в области шифрования информации.

4. Положение о лицензировании *разработки, производства* шифровальных (криптографических) средств защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

В перечисленных положениях дан перечень средств шифрования, имитозащиты, электронной цифровой подписи, кодирования, изготовления ключей и ключевых документов. При этом указано, что *не требуется* лицензирование для криптографических средств, осуществляющих преобразование информации с длиной ключа до 40 бит при использовании симметричного алгоритма и 128 бит – при использовании асимметричного алгоритма.

В качестве лицензирующего органа выступает ФСБ России. Здесь также определены лицензионные требования, а также перечень необходимых документов, представляемых в лицензионный орган, и порядок рассмотрения и выдачи лицензии.

8. Постановление Правительства РФ от 30 мая 2003 г. № 313 «**Об уполномоченном федеральном органе исполнительной власти в области использования электронной цифровой подписи»**.

В соответствии с Федеральным законом «Об электронной цифровой подписи» функции уполномоченного федерального органа исполнительной власти в области использования электронной цифровой подписи возлагаются на Министерство информационных технологий и связи Российской Федерации. При этом его деятельность в области использования ЭЦП в органах государственной власти России должна согласовываться с ФСБ России.

Ведомственная нормативная база

Нормативные документы и инструктивные материалы МВД РФ:

Приказ МВД РФ от 22 августа 1992 г. № 292 «Об организации исполнения органами внутренних дел Закона Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации» (с изменениями от 14 ноября 1994 г.).

Приказ МВД РФ от 31 декабря 1999 г. № 1105 «О мерах по усилению контроля органами внутренних дел за частной детективной и охранной деятельностью».

РД-78.143-92 «Системы и комплексы охранной сигнализации, элементы технической укрепленности объектов. Нормы проектирования».

РД-78.147-93 «Единые требования по технической укрепленности и оборудованию сигнализации охраняемых объектов».

Нормативные документы и инструктивные материалы ФСБ РФ:

1. Приказ ФСБ РФ от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

2. Приказ ФСБ РФ от 9 февраля 2005 г. № 66. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005).

Данное положение распространяется на СКЗИ, предназначенные для защиты информации с ограниченным доступом, но не содержащей сведения, составляющие государственную тайну.

3. Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Нормативные документы и инструктивные материалы ФСТЭК (Гостехкомиссии) России:

1. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации». Руководящий документ Гостехкомиссии России.

2. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Руководящий документ Гостехкомиссии России.

3. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Руководящий документ Гостехкомиссии России.

4. «Защита информации. Специальные защитные знаки. Классификация и общие требования». Руководящий документ Гостехкомиссии России.

5. «Защита от несанкционированного доступа к информации. Термины и определения». Руководящий документ Гостехкомиссии России.

6. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Руководящий документ Гостехкомиссии России.

7. «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий». Часть 1. Часть 2. Часть 3. Руководящий документ Гостехкомиссии России.

8. «Инструкция о порядке проведения специальных экспертиз предприятий, учреждений и организаций на право осуществления мероприятий и (или) оказания услуг в области противодействия иностранной технической разведке». Утверждена Председателем Гостехкомиссии 17 октября 1995 г.

9. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России.

10. Решение Гостехкомиссии от 3 октября 1995 г. № 42 «О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте».

11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Председателем Гостехкомиссии России 25 ноября 1994 г.

12. Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям

безопасности информации. Утверждено Председателем Гостехкомиссии России 25 ноября 1994 г.

13. Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3.

14. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3.

15. Типовое положение об испытательной лаборатории. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3.

16. «Перечень средств защиты информации, подлежащих сертификации в системе сертификации Гостехкомиссии России» (N РОСС RU.0001.01БИ00).

17. «Положение о государственном лицензировании деятельности в области защиты информации». Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27.04.1994 г. № 10.

18. «Положение о сертификации средств защиты информации по требованиям безопасности информации». Введено в действие Приказом Председателя Гостехкомиссии России от 27.10.1995 г. № 199.

19. «Положение по аттестации объектов информатизации по требованиям безопасности информации». Утверждено Председателем Гостехкомиссии при Президенте Российской Федерации 25 ноября 1994 г.

20. «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР-97)» от 23 мая 1997 г. № 55.

21. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности

от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России.

22. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России.

23. «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации». Руководящий документ Гостехкомиссии России.

24. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»,

25. «Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам». Руководящий документ Гостехкомиссии России.

26. «Положение о государственном лицензировании деятельности в области защиты информации». Утверждено решением Гостехкомиссии при Президенте Российской Федерации и ФАПСИ при Президенте Российской Федерации от 24 апреля 1994 г. № 10 (в редакции решения от 24 июня 1997 г. № 60).

Раздел 4. УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

История классификации угроз информационной безопасности

Материал раздела подготовлен на основе целого ряда источников [45, 2, 60, …]

На протяжении всего периода регулярного использования вычислительной техники для решения практических задач предпринимались попытки классифицировать источники угроз безопасности информации и сами угрозы с целью дальнейшей стандартизации средств и методов, применяемых для защиты информации.

В достаточно известной монографии Л. Дж. Хоффмана «Современные методы защиты информации» [2] были выделены 5 групп различных угроз: хищение носителей, запоминание или копирование информации, несанкционированное подключение к аппаратуре, несанкционированный доступ к ресурсам ЭВМ, перехват побочных излучений и наводок.

В книге [3] предпринята попытка классификации угроз по источнику возможной опасности: человек, аппаратура, и программа**.**

К группе угроз, в реализации которых основную роль играет человек, отнесены: хищение носителей, чтение информации с экрана, чтение информации с распечаток.

К группе, где основным средством выступает **аппаратура**: подключение к устройствам, перехват излучений.

К группе, где основное средство – **программа**: несанкционированный программный доступ, программное дешифрование зашифрованных данных, программное копирование информации с носителей.

Аналогичный подход предлагается и группой авторов учебных пособий по защите информации от несанкционированного доступа [13, 14]. Ими выделено три класса угроз:

- природные (стихийные бедствия, магнитные бури, радиоактивное излучение и наводки),

- технические (отключение или колебания напряжения сети электропитания, отказы и сбои аппаратно-программных средств, электромагнитные излучения и наводки, утечки через каналы связи),

- созданные людьми, причем в последнем случае различают непреднамеренные и преднамеренные действия различных категорий лиц.

В **руководящем документе Гостехкомиссии России** [РД. Концепция защиты средств вычислительной техники в АС от НСД к информации, 1992] введено понятие **модели нарушителя** в автоматизированной системе обработки данных. В качестве такового рассматривается субъект, имеющий доступ к работе со штатными средствами АС. При этом в зависимости от возможностей, предоставляемых нарушителям штатными средствами, угрозы делятся на четыре уровня:

самый низкий – возможности запуска задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции обработки информации;

промежуточный 1 – дополнительно к предыдущему имеются возможности создания и запуска собственных программ с новыми функциями обработки информации;

промежуточный 2 – дополнительно к предыдущему предполагается наличие возможностей управления функционированием АС, т.е. воздействия на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования;

самый высокий – определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав системы собственных технических средств с новыми функциями обработки информации (в этом случае предполагается, что нарушитель является специалистом высшей

квалификации, знает все об АС, в том числе и об используемых средствах защиты информации).

Согласно [СТР-К] различают 4 уровня возможностей **внутреннего нарушителя**, которые увеличиваются от уровня к уровню.

первый уровень – возможность запуска программ из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации (пользователь АРМ, пользователь сети);

второй уровень – возможность создания и запуска собственных программ с новыми функциями по обработке информации (прикладной программист, разработчик программного обеспечения);

третий уровень – возможность получения управления функционированием системы, а также воздействия на базовое программное обеспечение, состав и конфигурацию оборудования (системный программист, администратор сервера (ЛВС), администратор информационной системы (базы данных), разработчик);

четвертый уровень – определяется возможностью проектирования, установки и ремонта средств электронно-вычислительной техники, вплоть до включения в их состав собственных технических и программных средств с новыми функциями по обработке информации (администратор информационной системы, администратор сервера (ЛВС), администратор безопасности информации, разработчик системы, разработчик средств защиты информации, обслуживающий АС персонал).

Еще один вид источников угроз безопасности информации, связанный с ее хищением, достаточно подробно классифицирован в монографии [10]. Автор выделяет четыре способа хищения информации: по каналам побочных электромагнитных излучений; посредством негласного копирования, причем выделено две разновидности копирования: «ручное» вывод информации на печать или на экран оператором) и «вирусное» (вывод информации с помощью встроенной

в ЭВМ радиозакладки); хищение носителей информации; хищение персональной ЭВМ.

В монографии В.А.Герасименко [11] предпринята попытка системной классификации угроз информации исходя из целей ее защиты.

Достаточно подробный анализ угроз несанкционированного получения информации проведен также в учебном пособии В.Ю. Гайковича и Д.В. Ершова [Основы безопасности информационных технологий. – МИФИ, 1995].

Ретроспективный анализ указанных и других известных подходов к решению этой задачи ясно свидетельствует о многообразии имеющихся здесь точек зрения. Мы видим, что можно проводить классификацию:

- **по отношению источника угрозы** к АС (внешние и внутренние угрозы);

- **по виду источника угрозы** (**физические** – отражают физические действия на систему; **логические** – средства, при помощи которых человек получает доступ к логической информации системы; **коммуникационные** – относятся к процессам передачи данных по линиям связи; **человеческие** – являются наиболее трудно контролируемыми и непосредственно связанными с физическими и логическими угрозами);

- **по степени злого умысла** (случайные и преднамеренные) и т.д.;

- **по способам их воздействия.**

Преднамеренные угрозы, в свою очередь, могут быть подразделены на **активные** (несанкционированная модификация данных или программ) и **пассивные** (несанкционированное копирование данных или программ).

Такая классификация (поддерживается подавляющим большинством специалистов) предусматривает подразделение угроз на **информационные, программно-математические, физические и организационные.**

Информационные угрозы реализуются в виде:

- нарушения адресности и своевременности информационного обмена;

- противозаконного сбора и использования информации;

- осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

- хищения информационных ресурсов из банков и баз данных;

- нарушения технологии обработки информации.

Программно-математические угрозы реализуются в виде:

- внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;

- разработки и распространения программ, нарушающих нормальное функционирование информационных систем или их систем защиты информации.

Физические угрозы реализуются в виде:

- уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;

- уничтожения, повреждения, разрушения или хищения машинных и других носителей информации;

- хищения программных или аппаратных ключей и средств криптографической защиты информации;

- перехвата информации в технических каналах связи и телекоммуникационных системах;

- внедрения электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения;

- перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;

- воздействия на парольно-ключевые системы защиты средств обработки и передачи информации.

Организационные угрозы реализуются в виде:

- невыполнения требований законодательства в информационной сфере;
- противоправной закупки несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации и связи.

Учитывая важность вопроса классификации угроз безопасности информации и существование в этой области большого числа различных подходов, необходимо провести системный анализ данной проблемы.

Системная классификаций и общий анализ угроз безопасности информации

Из предыдущего изложения следует, что к настоящему времени известно большое количество разноплановых угроз безопасности информации различного происхождения. Мы видели, что различными авторами предлагается целый ряд подходов к их классификации. При этом в качестве критериев деления множества угроз на классы используются виды порождаемых опасностей, степень злого умысла, источники проявления угроз и т.д. Все многообразие предлагаемых классификаций с помощью подходов, предложенных В.А.Герасименко [11], на основе методов системного анализа может быть сведено к некоторой системной классификации, приведенной в таблице 3.

Дадим краткий комментарий к использованным в таблице 3 параметрам классификации, их значениям и содержанию.

1. Виды угроз. Данный параметр является основополагающим, определяющим целевую направленность защиты информации.

2. Происхождение угроз. В таблице выделено два значения данного параметра: случайное и преднамеренное.

Таблица 3

Системная классификация угроз безопасности информации

Параметры классификации	Значения параметров	Содержание значения параметра (примеры)
1 . Виды угроз. Целевая направленность	1.1. Физическая целостность	Уничтожение (искажение)
	1.2. Логическая структура	Искажение структуры
	1.3. Содержание	Несанкционированная модификация
	1.4. Конфиденциальность	Несанкционированное получение
	1.5. Право собственности	Присвоение чужого права
2.Природа происхождения	2.1.Случайная	Отказы, сбои, ошибки, стихийные бедствия, побочные влияния
	2.2.Преднамеренная	Злоумышленные действия людей
3.Предпосылки появления	3.1.Объективные	Количественная недостаточность элементов системы, качественная недостаточность элементов системы
	3.2. Субъективные	Развед. органы иностранных государств, промышленный шпионаж, уголовные элементы, недобросовестные сотрудники, хакеры, фишеры, спамеры, операторы зомби-сетей, создатели шпионского/злонамеренного ПО, террористы

Окончание табл. 3

Параметры классификации	Значения параметров	Содержание значения параметра (примеры)
4. Источники угроз	4. 1. Люди	Посторонние лица, пользователи, персонал
	4.2. Технические устройства	Техн. устройства регистрации, передачи, хранения, переработки, выдачи
	4.3. Модели, алгоритмы, программы	Общего назначения, прикладные, вспомогательные
	4.4. Технологические схемы обработки	Ручные, интерактивные, внутримашинные, сетевые
	4.5. Внешняя среда	Состояние атмосферы, побочные шумы, побочные сигналы

Под случайным понимается такое происхождение угроз, которое обуславливается спонтанными и независящими от воли людей обстоятельствами, возникающими в АС в процессе ее функционирования. Наиболее известными событиями данного плана являются отказы, сбои, ошибки, стихийные бедствия и побочные влияния. Сущность перечисленных событий (кроме стихийных бедствий, сущность которых ясна) определяется следующим образом:

отказ – нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций;

сбой – временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;

ошибка – неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

побочное влияние – негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

Преднамеренное происхождение угрозы обуславливается злоумышленными действиями людей.

3. Предпосылки появления угроз. В таблице приведены две возможные разновидности предпосылок: **объективные** (количественная или качественная недостаточность элементов системы) и **субъективные** (деятельность разведорганов иностранных государств, промышленный шпионаж, деятельность уголовных элементов, действия недобросовестных сотрудников системы).

Перечисленные разновидности предпосылок интерпретируются следующим образом:

количественная недостаточность – физическая нехватка одного или нескольких элементов системы, вызывающая нарушения технологического процесса обработки данных и/или перегрузку имеющихся элементов;

качественная недостаточность – несовершенство конструкции (организации) элементов системы, в силу чего могут появляться возможности случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

деятельность разведорганов иностранных государств – специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами. К основным видам разведки относятся **агентурная** (несанкционированная деятельность профессиональных разведчиков, завербованных агентов и так называемых «доброжелателей», «инициативников») и **техническая**, включающая **радиоразведку** (перехват

радиоэлектронными средствами информации, циркулирующей в телекоммуникационных каналах), **радиотехническую разведку** (регистрацию спецсредствами электромагнитных излучений технических систем) и **космическую разведку** (использование космических кораблей и искусственных спутников Земли для наблюдения за территорией, ее фотографирования, регистрации радиосигналов и получения полезной информации любыми другими доступными способами);

промышленный шпионаж – негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной ее утечки или хищения, с целью создания для себя благоприятных условий и получения максимальных выгод (недобросовестная конкуренция);

злоумышленные действия уголовных элементов – хищение информации или компьютерных программ в целях наживы;

действия недобросовестных сотрудников – хищение (копирование) или уничтожение информационных массивов и/или программ по эгоистическим или корыстным мотивам, а также в результате несоблюдения установленного порядка работы с информацией.

4. Источники угроз. Под источником угроз понимается непосредственный ее генератор или носитель. Таким источником могут быть люди, технические средства, модели (алгоритмы), программы, внешняя среда.

Модели угроз и нарушителей ИБ для организации БС РФ рассматриваются в стандарте СТО БР ИББС 0.1-2006 (Раздел 7). В стандарте выделено следующее.

Модели угроз и нарушителей должны быть основным инструментом менеджмента организации при развертывании, поддержании и совершенствовании системы обеспечения ИБ организации.

Деятельность организации БС РФ поддерживается входящей в ее состав **информационной инфраструктурой,** которая обеспечивает

реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- банковских технологических процессов и приложений;
- бизнес-процессов организации.

На каждом из уровней угрозы и их источники (в т.ч. злоумышленники), методы и средства защиты и подходы к оценке эффективности являются различными.

Главной целью злоумышленника является получение контроля над активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов, например, путем раскрытия конфиденциальной банковской аналитической информации, более эффективно для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через нижние уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективное по соотношению «затраты/получаемый результат».

Организация должна определить конкретные **объекты защиты** на каждом из уровней информационной инфраструктуры.

Наиболее актуальные **источники угроз** на физическом, сетевом уровнях и уровне сетевых приложений:

- внешние источники угроз: лица, распространяющие вирусы и другие вредоносные программы, хакеры, фрикеры; и иные лица, осуществляющие несанкционированный доступ (НСД);
- внутренние источники угроз, реализующие угрозы в рамках своих полномочий и за их пределами (персонал, имеющий права доступа к

аппаратному оборудованию, в том числе сетевому, администраторы сетевых приложений и т.п.);

- комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно.

Наиболее актуальные **источники угроз** на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

- внутренние, реализующие угрозы в рамках своих полномочий и за их пределами (администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.);
- комбинированные источники угроз: внешние и внутренние, действующие в сговоре.

Наиболее актуальные **источники угроз** на уровне бизнес-процессов:

- внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами (авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.);
- комбинированные источники угроз: внешние (например, конкуренты) и внутренние, действующие в сговоре.

Также необходимо учитывать угрозы, связанные с природными и техногенными катастрофами и террористической деятельностью.

Источники угроз для реализации угрозы используют **уязвимости объектов и системы защиты.**

Хорошей практикой является разработка моделей угроз и нарушителей ИБ для данной организации.

Модель угроз ИБ включает описание источников угрозы, уязвимостей, используемых угрозами, методов и объектов нападений, пригодных для реализации угрозы, типов возможной потери (например, конфиденциальности, целостности, доступности активов), масштабов потенциального ущерба.

Для источников угроз – людей – может быть разработана **модель нарушителя ИБ**, включающая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, и возможной мотивации их действий.

Степень детализации параметров моделей угроз и нарушителей ИБ может быть различна и определяется реальными потребностями для каждой организации в отдельности.

При анализе угроз ИБ необходимо исходить из того, что эти угрозы непосредственно влияют на операционные риски деятельности организации. Операционные риски сказываются на бизнес-процессах организации.

Операционные риски порождаются следующими эксплуатационными факторами: технические неполадки, ошибочные (случайные) и/или преднамеренные злоумышленные действия персонала организации, ее клиентов при их непосредственном доступе к АБС организаций и другими факторами.

Наиболее эффективным способом **минимизации рисков** нарушения ИБ для собственника является разработка совокупности мероприятий, методов и средств, создаваемых и поддерживаемых для обеспечения требуемого уровня безопасности информационных активов в соответствии с политикой ИБ организации БС РФ, разрабатываемой в том числе и на основе моделей угроз и нарушителей ИБ.

Угрозы АБС из Методики оценки соответствия ИБ организации стандарту СТО БР ИББС 1.0-2006.

Приведем конкретные формулировки частных показателей из указанной методики, используемой при аудите информационной безопасности.

М2.3 Применяются (применялись) ли на стадии разработки АБС разработчиками меры для защиты от угроз ИБ:

- принятия неверных проектных решений;
- внесения дефектов на уровне архитектурных решений;
- внесения недокументированных возможностей в АБС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к АБС;
- угрозы разработки некачественной документации;
- сборки АБС разработчиком/производителем с нарушением требований;
- неверного конфигурирования АБС;
- приемки АБС, не отвечающей требованиям заказчика;
- внесения недокументированных возможностей в АБС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ?

М2.6 Обеспечивают ли на стадии эксплуатации применяемые меры и средства обеспечения ИБ защиту от угроз:
- несанкционированного раскрытия,
- модификации или уничтожения информации,
- недоставки или ошибочной доставки информации,
- отказа в обслуживании или ухудшения обслуживания,
- отказа от авторства сообщений?

М2.8 Применяются ли на стадии сопровождения меры
для защиты от угрозы внесения изменений в АБС, приводящих к нарушению функциональности АБС либо к появлению недокументированных возможностей,
а также для защиты от угрозы невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и состояния АБС?

М2.9 Применяются ли на стадии снятия с эксплуатации меры для защиты от угроз ненадежного удаления информации, несанкционированное использование которой может нанести ущерб бизнес–деятельности организации, и информации, используемой

средствами обеспечения ИБ, из постоянной памяти АБС или с внешних носителей?

Как видно, какие-то угрозы для АБС перечислены для каждой стадии жизненного цикла. То, что это не полный список угроз, следует из приводимых далее мер и средств защиты (защитных мер, контролей).

Каналы несанкционированного получения информации (КНПИ)

КНПИ – это физический канал от источника защищаемой информации к злоумышленнику, по которому возможна утечка охраняемых сведений [40].

Классифицируем все возможные каналы несанкционированного получения информации (КНПИ) по двум критериям: необходимости доступа (физического или логического) к элементам АС для реализации того или иного КНПИ и зависимости появления КНПИ от состояния АС.

По первому критерию КНПИ могут быть разделены на **не требующие доступа**, т.е. позволяющие получать необходимую информацию дистанционно (например, путем визуального наблюдения через окна помещений АС), и **требующие доступа** в помещения АС.

В свою очередь, КНПИ, воспользоваться которыми можно только получив доступ в помещения АС, делятся на **не оставляющие следы** в АС (например, визуальный просмотр изображений на экранах мониторов или документов на бумажных носителях) и на КНПИ, использование которых **оставляет те или иные следы** (например, хищение документов или машинных носителей информации).

По второму критерию КНПИ делятся на **постоянно существующие** независимо от состояния АС (например, похищать носители информации можно независимо от того, в рабочем состоянии находятся средства АС или нет) и **существующие только в рабочем состоянии** АС (например, побочные электромагнитные излучения и наводки).

КНПИ 1-го класса – каналы, проявляющиеся безотносительно к обработке информации и без доступа злоумышленника к элементам системы. Сюда может быть отнесено **подслушивание разговоров**, а также **провоцирование на разговоры** лиц, имеющих отношение к АС, и **использование злоумышленником визуальных**, **оптических и акустических средств.** Данный канал может проявиться и путем хищения носителей информации в момент их нахождения за пределами помещения, где расположена АС.

КНПИ 2-го класса – каналы, проявляющиеся в процессе обработки информации без доступа злоумышленника к элементам АС. Сюда могут быть отнесены **электромагнитные излучения** различных устройств ЭВМ, аппаратуры и линий связи, **паразитные наводки** в цепях питания, телефонных сетях, системах теплоснабжения, вентиляции и канализации, шинах заземления, **подключение к информационно-вычислительной сети** генераторов помех и регистрирующей аппаратуры. К этому же классу может быть отнесен **осмотр отходов производства,** попадающих за пределы контролируемой зоны.

КНПИ 3-го класса – каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АС, но без изменения последних. К ним относятся **всевозможные виды копирования** носителей информации и документов, а также **хищение производственных отходов.**

КНПИ 4-го класса – каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АС, но без изменения последних. Сюда может быть отнесено **запоминание и копирование** информации в процессе обработки, **использование программных ловушек**, недостатков языков программирования и операционных систем, а также **поражение программного обеспечения** вредоносными закладками, **маскировка** под зарегистрированного пользователя.

КНПИ 5-го класса – каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АС и с изменением последних. Среди этих каналов: **подмена и хищение носителей** информации и аппаратуры, **включение в программы блоков** типа «троянский конь», «компьютерный червь» и т.п., чтение остаточной информации, содержащейся в памяти, после выполнения санкционированных запросов.

КНПИ 6-го класса – каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АС и с изменением последних. Сюда может быть отнесено незаконное **подключение к аппаратуре и линиям связи**, а также **снятие информации на шинах питания** различных элементов АС.

Угрозы в методе CRAMM

Раскроем часто встречаемую в литературе абривиатуру CRAMM. CRAMM – CCTA Risk Analysis & Managment Method (в свою очередь CCTA – Central Computer & Telecommunications Agency), UK). То есть это метод анализа и управления рисками Центрального компьютерного и телекоммуникационного агентства Великобритании.

В переводе Симонова С. в работе [Анализ рисков, управление рисками http://www.jetinfo.ru/1999/1/1/article1.1.1999.html] представлены следующие классы угроз (в скобках указаны примеры из классов):

1. Форс-мажорные угрозы (пожар; затопление; природные катаклизмы; нехватка персонала).

2. Организационные недостатки.

3. Человеческие ошибки (ошибки при маршрутизации; ошибки пользователей).

4. Технические неполадки (неисправность: сервера, сетевого сервера, запоминающих устройств, печатающих устройств, сетевых распределяющих

компонент, сетевых шлюзов, средств сетевого управления или управляющих серверов, сетевых интерфейсов, сетевых сервисов, электропитания, кондиционеров; сбои: системного и сетевого ПО, прикладного ПО).

5. Преднамеренные действия (использование чужого идентификатора: сотрудниками организации, поставщиком услуг, посторонними; несанкционированный доступ к приложению; внедрение вредоносного программного обеспечения; несанкционированное использование системных ресурсов; использование телекоммуникаций для несанкционированного доступа: сотрудниками организации, поставщиком услуг, посторонними; кражи: со стороны сотрудников, со стороны посторонних; преднамеренные несанкционированные действия: сотрудников, посторонних; терроризм.

Тема угроз информационной безопасности в документам ФСТЭК России

При составлении перечней угроз информационной безопасности, как правило, используют какой-либо **принцип классификации** этих угроз. В связи с этим явно или неявно используется та или иная модель угроз, представляющая собой их определенное формальное описание. Можно указать следующие элементы моделей, отражающие существенные особенности угроз**:**

- источник (или агент) угрозы;
- метод реализации угрозы;
- используемая уязвимость информационно-технологической среды (системы) (ИТС);
- информационные активы, подверженные угрозе;
- вид воздействия на ИТС;
- нарушаемое свойство безопасности ИТС.

Для практического применения удобно использовать классификацию угроз по различным признакам. В основу классификации обычно кладется

какой-либо из вышеприведенных элементов. Так, список разделов упомянутого выше перечня угроз из германского стандарта отражает классификацию угроз по их источникам.

Угрозы информационной безопасности, наряду с политикой безопасности организации, представляют собой важный аспект среды безопасности, учитываемый при формировании целей и требований информационной безопасности и выборе мер безопасности. Поскольку обеспечение информационной безопасности организации есть средство поддержки ее основной деятельности, предлагается формулировать цели информационной безопасности в терминах обеспечения надлежащего протекания производственных и управленческих процессов в условиях осуществления определенных угроз.

Для иллюстрации значения вышеприведенных элементов модели угроз рассмотрим примеры содержания некоторых из них.

Нарушаемое свойство безопасности. Реализация той или иной угрозы информационной безопасности организации может иметь последствием:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение (частичное или полное) работоспособности ИТС (нарушение доступности).

Используемая уязвимость системы. Реализация угроз, ведущих к нарушению прав доступа и/или конфиденциальности информации, может происходить:

- с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.);
- с использованием скрытых каналов передачи информации.

Характер воздействия на ИТС. По этому критерию различают активное и пассивное воздействие. Активное воздействие всегда связано с

выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к определенным наборам данных, программам, вскрытие пароля и т.д. Активное воздействие ведет к изменению состояния системы и может осуществляться либо с использованием доступа (например, к наборам данных), либо как с использованием доступа, так и с использованием скрытых каналов.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализе. Примером пассивного воздействия может служить прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации в ИТС, так как при нем никаких действий с объектами и субъектами не производится. Пассивное воздействие не ведет к изменению состояния системы.

Способ воздействия на объект атаки (при активном воздействии). Непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой.

Воздействие на систему разрешений (в том числе захват привилегий).

Опосредованное воздействие (через других пользователей), например, «маскарад».

Актив информационной инфраструктуры, подверженный угрозе (объект атаки).

Одной из самых главных составляющих нарушения функционирования информационно-телекоммуникационной системы (ИТС) является объект атаки, то есть компонент ИТС, который подвергается воздействию со стороны злоумышленника. Определение

объекта атаки позволяет принять меры по ликвидации последствий нарушения, восстановлению этого компонента, установке контроля по предупреждению повторных нарушений и т.д. Воздействию могут подвергаться ИТС в целом или объекты ИТС – данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных, процессы.

Причина появления используемой ошибки защиты. Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты. Такая ошибка может быть обусловлена одной из следующих причин.

1. Неадекватность политики безопасности реальной ИТС.

2. Ошибки административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной ИТС.

3. Ошибки в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программы или комплекса программ и благодаря которым их можно использовать совсем не так, как описано в документации.

4. Ошибки реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапе реализации или отладки и которые также могут служить источником недокументированных свойств.

Способ воздействия на ИТС: в интерактивном режиме или в пакетном режиме.

Используемые средства атаки. Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы.

Состояние объекта атаки. Объект атаки может находиться в одном из трех состояний: хранения информации; передачи информации; обработки информации.

Рассмотренные варианты классификации угроз безопасности приведены на рис. 8.

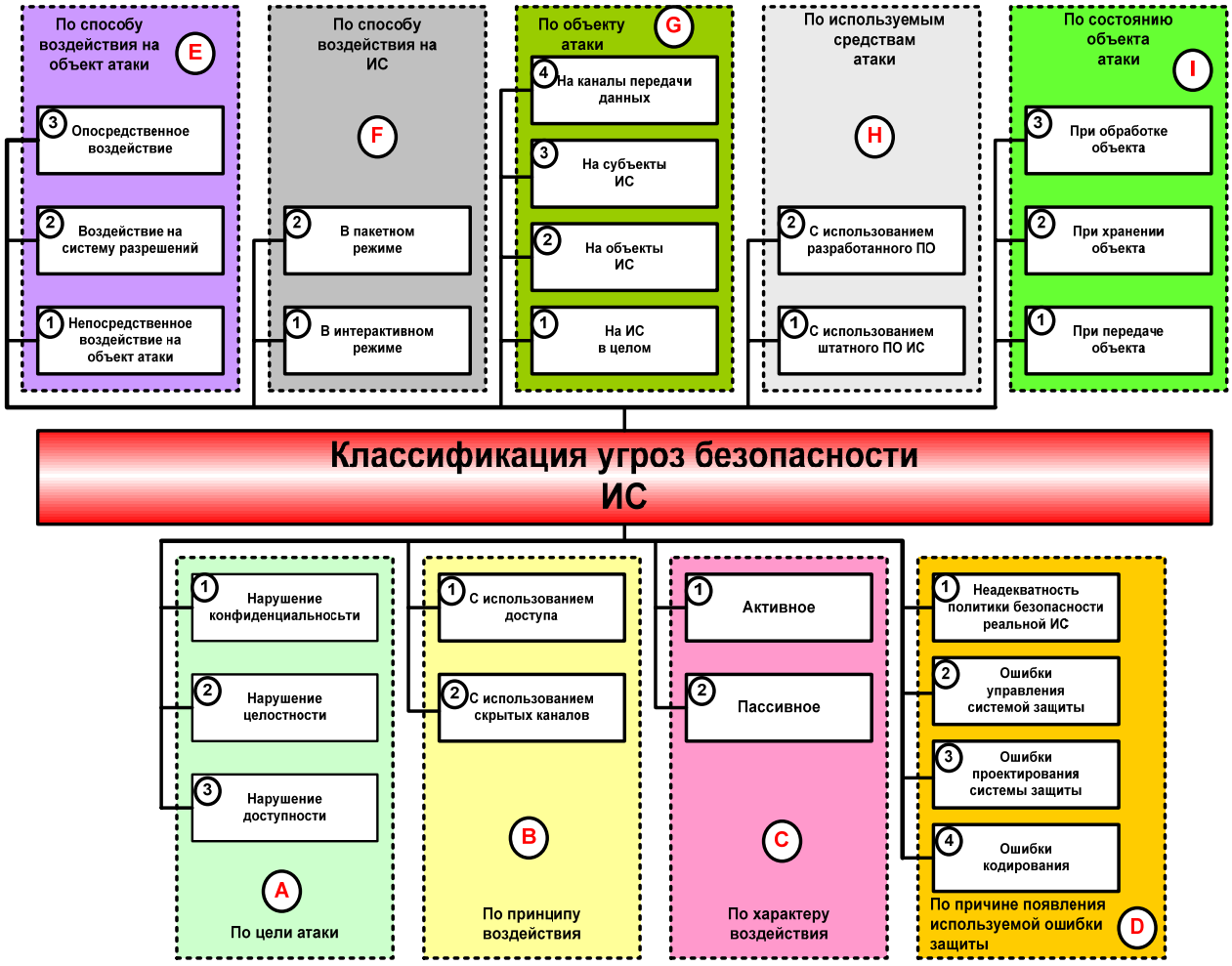


Рис. 8. Варианты классификации угроз безопасности

Подобная классификация показывает сложность полного перечисления возможных угроз и способов их реализации. Поэтому в конкретной организации необходимо, опираясь на описание ее производственных и управленческих процессов, на классификацию и перечни угроз, выделить множество угроз, критичных для данной организации, для последующего выбора контрмер.

Таблица 4

Перечень угроз для объектов критических сегментов информационной инфраструктуры

Угроза (Threat)	Описание
Операторы зомби-сетей (Bot-network operators)	Операторы зомби-сетей – это хакеры, однако вместо того, чтобы проникать в систему для захвата привилегий, они захватывают сложные системы с тем, чтобы координировать атаки и распространять фишинговые схемы, спам и злонамеренное ПО. Сервисы захваченных сетей иногда делаются доступными для подпольных рынков (например, оплата DOS-атаки, серверов для распространения спама или фишинговых атак, и т.д.).
Криминальные группы	Криминальные группы стремятся атаковать системы из-за денежной корысти. Характерно, что организованные криминальные группы используют спам, фишинг и шпионское/злонамеренное ПО для совершения кражи идентификационной информации и он-лайнового обмана. Международные корпоративные шпионы и организованные криминальные организации также нацелены и умеют вести промышленный шпионаж и огромные денежные кражи, нанимая хакеров или развивая хакерский талант.
Иностранные разведывательные органы	Иностранные разведывательные службы используют киберметоды в своих действиях по сбору информации. К тому же несколько стран агрессивно работают над развитием доктрины, программ и возможностей информационной войны. Такие возможности позволяют отдельному человеку иметь значительное и серьезное влияние через разрушение запасов, коммуникаций и экономических инфраструктур, которые обеспечивают военную мощь – влияния, которые могут воздействовать на повседневную жизнь граждан всей страны.

Продолжение табл. 4

Угроза (Threat)	Описание
Хакеры (Hackers)	Хакеры проникают в сети из-за желания решить эту сложную задачу или желания похвастаться привилегиями в хакерском сообществе. Хотя удаленное вскрытие требует значительного умения и компьютерных знаний, хакеры могут сейчас скачать из Интернета скрипты и протоколы для атаки и запустить их против сайтов-жертв. Таким образом, хотя средства атак стали более изощренными, они стали проще в использовании. Большинство хакеров, по мнению Центрального разведывательного агентства, не имеют соответствующего опыта для угрозы сложным целям, таким как критические сети США. Тем не менее, мировая популяция хакеров представляет относительно высокую угрозу для локального или широкого разрушения, вызывающего серьезные потери.
Инсайдеры (Insiders)	Сотрудник организации является одним из основных источников компьютерных преступлений. Инсайдерам нет нужды заниматься компьютерными вторжениями, так как их знание атакуемой системы часто позволяет иметь неограниченный доступ для нанесения ущерба или похищения данных системы. Инсайдерская угроза включает также сторонних производителей и служащих, которые случайно вносят злонамеренное ПО в систему.
Фишеры (Phishers)	Отдельные люди или малые группы людей, осуществляющие фишинговые схемы в попытках украсть идентификационную информацию или информацию для денежной выгоды. Фишеры могут также использовать спам и шпионское или злонамеренное ПО для достижения своих целей.

Окончание табл. 4

Угроза (Threat)	Описание
Спамеры (Spammers)	Отдельные люди или организации, которые распространяют не запрошенные электронные сообщения со скрытой или неверной информацией с целью продажи продуктов, выполнения фишинговых схем, распространения шпионского или злонамеренного ПО или атаки организаций (например, DOS-атаки)
Создатели шпионского/злонамеренного ПО (Spyware/malware)	Отдельные люди или организации со злонамеренным желанием выполнить атаки против пользователей с помощью производства и распространения шпионского и злонамеренного. Несколько разрушительных компьютерных вирусов и червей нанесли существенный ущерб файлам и жестким дискам. Это the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, и Blaster.
Террористы	Террористы стремятся разрушить, вывести из строя или использовать в своих интересах критические инфраструктуры с тем, чтобы угрожать национальной безопасности, вызывать массовые жертвы, ослаблять экономику, и наносить ущерб морали и доверию. Террористы могут использовать схемы фишинга или шпионского/злонамеренного ПО с тем, чтобы создавать денежные запасы или собирать чувствительную информацию.

В работе [GAO 2005, Critical Infrastructure Protection, US] содержится одна из последних классификаций основных угроз для объектов критических сегментов информационной инфраструктуры (ИИ). В таблице приводятся описания угроз из указанного документа. Фактически они представляют собой обобщенную классификацию угроз по источнику (агенту) угрозы.

Там же приведены типы кибератак с их описанием. К ним относятся: отказ в обслуживании (Denial of service), распределенный отказ в обслуживании (Distributed denial of service), средства эксплуатации уязвимости (Exploit tools), логические бомбы, фишинг (Phishing), снифферы (Sniffer), троянские кони, вирусы, сканирование дозвоном (War dialing), поиск на местности доступной беспроводной сети (War driving), компьютерные черви. Здесь единого принципа классификации не усматривается; наряду с результатом воздействия на систему (например, отказ в обслуживании) приведены методы реализации атак (логические бомбы, вирусы).

Таблица 5

Типы кибератак

Типы атак	Описание
Отказ в обслуживании, DOS-атака (Denial of Service)	Метод атаки с единого источника, которая приводит к тому, что система отказывает в доступе законным пользователям из-за переполнения атакуемого компьютера от сообщений и блокирования законного трафика. Это может препятствоватьсистеме обмениваться данными с другими системами или использовать Интернет.
Распределенный отказ в обслуживании, DDOS-атака (Distributed Denial of Service)	Разновидность атаки отказа в обслуживании, которая использует координированное воздействие от распределенной системы компьютеров, а не от одного компьютера. Атака часто использует компьютерных червей для распределения заданий на много компьютеров, которые могут затем атаковать цель.
Средства эксплуатации уязвимости (Exploit tools)	Открыто доступные и искусные средства, с помощью которых злоумышленники с разным уровнем подготовки могут определить уязвимости и проникнуть в атакуемые системы.
Логические бомбы	Форма саботажа, при которой программист вставляет подпрограмму, вызывающую выполнение программой деструктивных действий, когда появляется некоторое инициирующее событие, например такое, как увольнение этого программиста.

Продолжение табл. 5

Типы атак	Описание
Фишинг (Phishing)	Создание и использование электронной почты и веб-сайтов – выглядящими как у законных компаний, финансовых институтов и правительственных организаций – с тем чтобы обманом побудить пользователей Интернета к раскрытию их персональных данных, таких как информация о банковском и финансовом счете и парольные слова. Фишеры затем используют эту информацию в криминальных целях, таких как кража и обман.
Сниффер (Sniffer)	Синоним с пакетным сниффером. Это программа, которая перехватывает передаваемые данные и проверяет каждый пакет в поисках специальной информации, такой как парольные слова, посланные в открытом тексте.
Троянский конь	Компьютерная программа, которая скрывает в себе вредоносную программу. Троянский конь обычно маскируется как полезная программа, которую пользователь хотел бы использовать.
Вирус	Программа, которая заражает компьютерные файлы, обычно выполнимые программы, с помощью внесения своей копии в файл. Эти копии обычно выполняются, когда инфицированный файл загружается в память, позволяя вирусу заражать другие файлы. В отличие от компьютерного червя, вирус требует человеческого участия (обычно непреднамеренного) для распространения.
Сканирование дозвоном (War dialing)	Простые программы, которые используются для дозвона по последовательным телефонным номерам для определения модемов.
Поиск на местности доступной беспроводной сети (War driving)	Метод проникновения в беспроводные компьютерные сети, используя переносной компьютер, антенны и беспроводной сетевой адаптер, с помощью проверки на местности для получения неавторизованного доступа.

Окончание табл. 5

Типы атак	Описание
Червь	Независимая компьютерная программа, которая репродуцирует себя копированием из одной системы в другую через сеть. В отличие от компьютерных вирусов, черви не требуют привлечения человека для размножения.

Следует отметить включение в список источников угроз инсайдеров (внутренних злоумышленников). В последнее время в отечественной и зарубежной прессе им уделяется, наряду с кибертеррористами, повышенное внимание.

Можно сравнить приведенные угрозы с угрозами из более раннего документа американского института стандартов 2002 г.[Stoneburner G., Goguen A., Feringa A. The Risk Management Guide for IT Systems, NIST, sp800-30, 2002], где приводятся угрозы системам ИТ, связанные с действиями людей, мотивация этих людей и описание действия угроз. Оба списка включают угрозу терроризма, но, естественно, более поздний список более полон.

Список угроз из работы [GAO05, Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities] сильно коррелирует со списком угроз из [GAO_2005, Cybersecurity Threats to Federal Information]. Этими угрозами являются: террористы, криминальные группы, разведывательные службы иностранных государств, создатели шпионского или злонамеренного ПО, хакеры, инсайдеры, операторы зомби-сетей, фишеры и спамеры.

Как видно из представленного выше материала, множество угроз, которые надо рассматривать при анализе критически важных информационных инфраструктур, динамически меняется. Эти изменения определяются многими причинами, среди которых основную роль играет появление новых технологий и повышение зависимости от них.

В настоящее время предложен ряд перечней угроз. В качестве примера можно привести перечень угроз, содержащийся в германском стандарте по информационной безопасности **«Руководство по базовой защите информационных технологий» (BSI IT baseline protection manual).** Этот перечень, возможно, является наиболее полным из существующих. Все угрозы в каталоге угроз [Catalogues of Threats 2004] разбиты на 5 следующих групп.

Т 1. Угрозы в связи с форс-мажорными обстоятельствами. (Т1.1 – Т1.15).

Т 2. Угрозы на организационном уровне. (Т2.1 – Т1.101).

Т 3. Угрозы, связанные с ошибками людей. (Т3.1 – Т3.76).

Т 4. Угрозы, связанные с неисправностями техники. (Т4.1 – Т4.52).

Т 5. Угрозы, вызванные злонамеренными действиями. (Т5.1 – Т3.126).

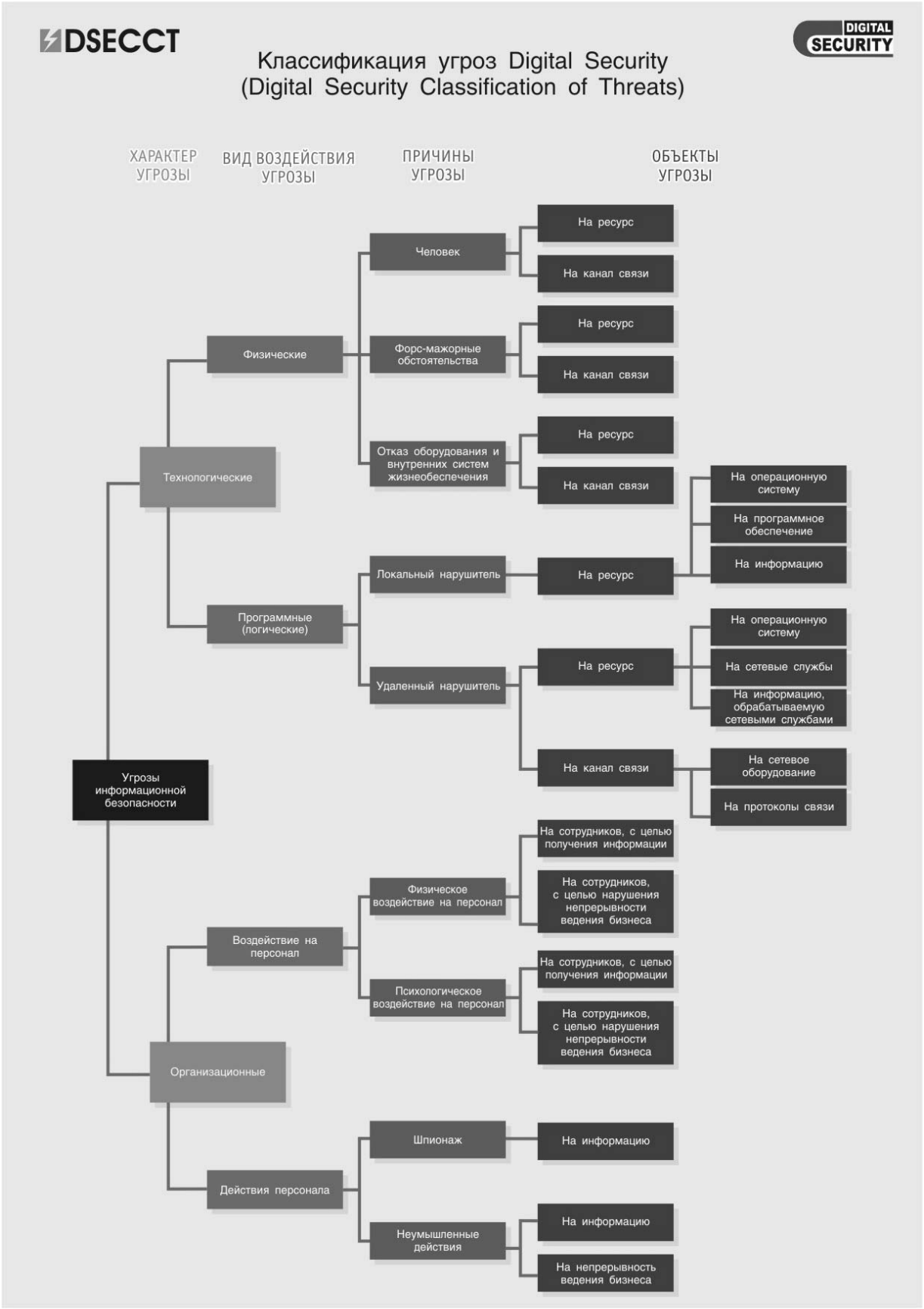
Всего 370 угроз. При ближайшем рассмотрении многие из приведенных в каталоге угроз можно отнести скорее к уязвимостям.

Немецкий стандарт «**Руководство по обеспечению безопасности ИТ**» (IT Baseline Protection Manual) разрабатывается в BSI (Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency), www.bsi.bund.de). Он имеется в свободном доступе в сети Интернет по следующему адресу: http://www.bsi.bund.de/gshb/english/menue.htm (http://www.bsi.bund.de/english/gshb/index.htm).

Данный стандарт постоянно совершенствуется с целью обеспечения его соответствия текущему состоянию дел в области ИТ и ИБ. К настоящему времени накоплена уникальная база знаний, содержащая информацию по угрозам и контрмерам в хорошо структурированном виде. http://www.bsi.bund.de/english/gshb/index.htm

Приведем классификаторы угроз некоторых фирм.

1. Схема классификации угроз Digital Security (рис. 9).



2. ЭЛВИС-ПЛЮС

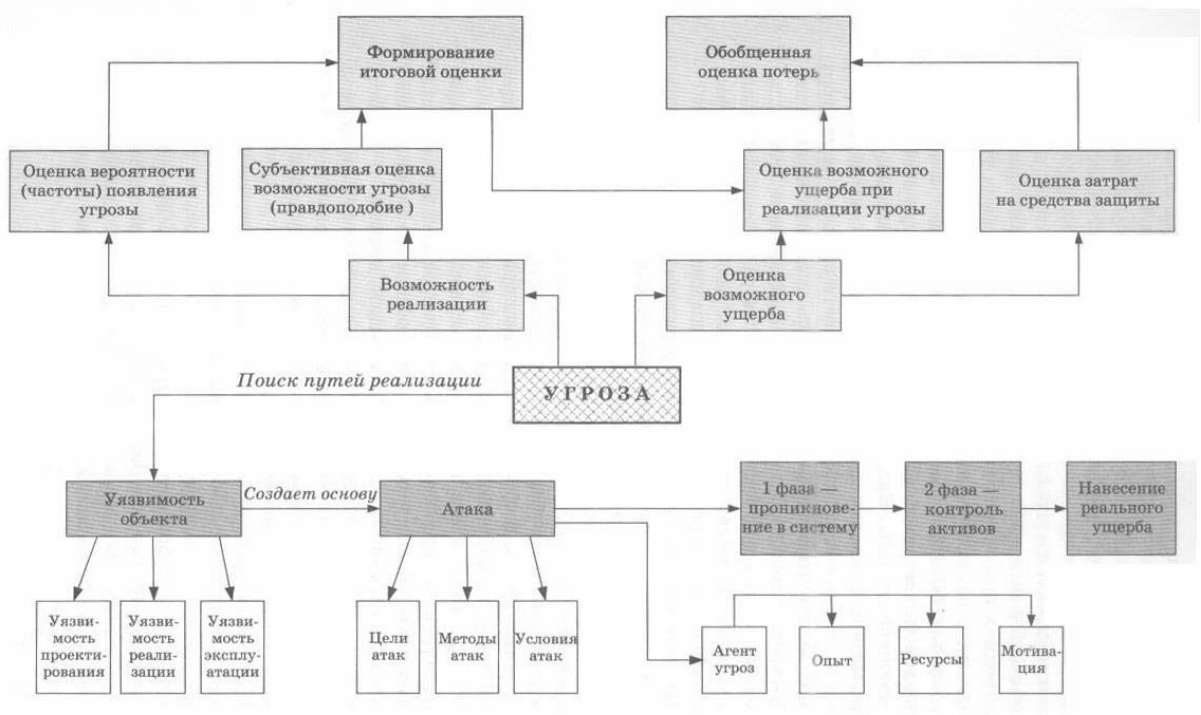


Рис. 10. Взаимосвязь факторов категории угроз

Далее приведем примеры уязвимостей и методы их оценки из Приложения В к проекту стандарта ISO 27005.

Обычные уязвимости

В приведенных ниже списках даны примеры уязвимостей в различных сферах безопасности, включая примеры угроз, которые могут использовать эти уязвимости. Эти списки могут быть полезными во время оценки уязвимостей. Следует подчеркнуть, что в некоторых случаях эти уязвимости могут использоваться и другими угрозами.

1. Внешняя среда и инфраструктура

Отсутствие физической защиты здания, дверей и окон (может быть использовано, например, угрозой хищения).

Неадекватное или небрежное использование физического управления доступом к зданиям и помещениям (может быть использовано, например, угрозой намеренного повреждения).

Нестабильная электрическая сеть (может быть использована, например, угрозой колебаний напряжения).

Размещение в местности, предрасположенной к наводнениям (может быть использовано, например, угрозой затопления).

2. Аппаратные средства

Отсутствие программ периодической замены (может быть использовано, например, угрозой ухудшения состояния носителей данных).

Чувствительность к колебаниям напряжения (может быть использована, например, угрозой колебаний напряжения).

Чувствительность к колебаниям температуры (может быть использована, например, угрозой экстремальных показателей температуры).

Чувствительность к влажности, пыли, загрязнению (может быть использована, например, угрозой пылеобразования).

Чувствительность к электромагнитному излучению (может быть использована, например, угрозой электромагнитного излучения).

Недостаточное техническое обслуживание/неправильная установка носителей данных (может быть использовано, например, угрозой ошибки технического обслуживания).

Отсутствие эффективного контроля изменений конфигурации (может быть использовано, например, угрозой ошибок операционного персонала).

3. Программные средства

Нечеткие или неполные спецификации для разработчиков (могут быть использованы, например, угрозой сбоя программы).

Отсутствующее или недостаточное тестирование программных средств (может быть использовано, например, угрозой использования программных средств неуполномоченными пользователями).

Сложный пользовательский интерфейс (может быть использован, например, угрозой ошибок операционного персонала).

Отсутствие механизмов идентификации и аутентификации, таких как аутентификация пользователей (может быть использовано, например, угрозой имитации личности пользователя).

Отсутствие контрольного журнала (может быть использовано, например, угрозой использования программных средств несанкционированным образом).

Широко известные дефекты программных средств (могут быть использованы, например, угрозой использования программных средств неуполномоченными пользователями).

Незащищенные таблицы паролей (могут быть использованы, например, угрозой имитации личности пользователя).

Плохой менеджмент паролей (легко отгадываемые пароли, хранение паролей в незашифрованном виде, недостаточная частота смены паролей) (может быть использован, например, угрозой имитации личности пользователя).

Неверное распределение прав доступа (может быть использовано, например, угрозой использования программных средств несанкционированным образом).

Неконтролируемая загрузка и использование программных средств (может быть использована, например, угрозой вредоносного программного обеспечения).

Отсутствие «конца сеанса», покидая рабочую станцию (может быть использовано, например, угрозой использования программных средств неуполномоченными пользователями).

Отсутствие эффективного контроля изменений (может быть использовано, например, угрозой сбоя программы).

Отсутствие документации (может быть использовано, например, угрозой ошибок операционного персонала).

Отсутствие резервных копий (может быть использовано, например, угрозой вредоносного программного обеспечения или угрозой пожара).

Списание или повторное использование носителей данных без надлежащего стирания (может быть использовано, например, угрозой использования программных средств неуполномоченными пользователями).

Активированные ненужные службы (могут быть использованы, например, угрозой использования несанкционированного программного обеспечения).

Недоработанное или новое программное обеспечение (может быть использовано, например, угрозой некомпетентного или неадекватного тестирования).

Широко распределенное программное обеспечение (может быть использовано, например, угрозой потери целостности в процессе распределения).

4. Система связи

Незащищенные линии связи (могут быть использованы, например, угрозой подслушивания).

Плохая разводка кабелей (может быть использована, например, угрозой проникновения в систему связи).

Отсутствие идентификации и аутентификации отправителя и получателя (может быть использовано, например, угрозой имитации личности пользователя).

Передача паролей в незашифрованном виде (может быть использована, например, угрозой получения сетевого доступа неуполномоченными пользователями).

Отсутствие подтверждения отправления или получения сообщения (может быть использовано, например, угрозой отрицания).

Коммутируемые линии (могут быть использованы, например, угрозой получения сетевого доступа неуполномоченными пользователями).

Незащищенный значимый трафик (может быть использован, например, угрозой подслушивания).

Неадекватный сетевой менеджмент (устойчивость маршрутизации) (может быть использован, например, угрозой перегрузки трафика).

Незащищенные соединения сети общего пользования (могут быть использованы, например, угрозой использования программных средств неуполномоченными пользователями)

Ненадежная сетевая архитектура (может быть использована, например, угрозой вторжения).

5. Документы

Незащищенное хранение (может быть использовано, например, угрозой хищения). Беззаботность при устранении (может быть использована, например, угрозой хищения). Неконтролируемое копирование (может быть использовано, например, угрозой хищения).

6. Персонал

Отсутствие персонала (может быть использовано, например, угрозой нехватки персонала).

Безнадзорная работа внешнего персонала или персонала, занимающегося уборкой (может быть использована, например, угрозой хищения).

Недостаточное обучение по безопасности (может быть использовано, например, угрозой ошибок операционного персонала).

Отсутствие осознания безопасности (может быть использовано, например, угрозой ошибок пользователей).

Ненадлежащее использование программных и аппаратных средств (может быть использовано, например, угрозой ошибок операционного персонала).

Отсутствие механизмов мониторинга (может быть использовано, например, угрозой использования программных средств несанкционированным образом).

Отсутствие политик по правильному использованию телекоммуникационной среды и обмена сообщениями (может быть использовано, например, угрозой использования сетевых средств несанкционированным образом).

Неадекватные процедуры набора персонала (могут быть использованы, например, угрозой намеренного повреждения).

7. Процедурные

Отсутствие санкционирования средств обработки информации (может быть использовано, например, угрозой намеренного повреждения).

Отсутствие формального процесса санкционирования общедоступной информации (может быть использовано, например, угрозой ввода искаженных данных).

Отсутствие формального процесса проверки прав доступа (надзора) (может быть использовано, например, угрозой несанкционированного доступа).

Отсутствие формальной политики по использованию портативных компьютеров (может быть использовано, например, угрозой хищения).

Отсутствие формальной процедуры контроля документации системы менеджмента информационной безопасности (может быть использовано, например, угрозой ввода искаженных данных).

Отсутствие формальной процедуры надзора за записями системы менеджмента информационной безопасности (может быть использовано, например, угрозой ввода искаженных данных).

Отсутствие формальной процедуры регистрации и отмены регистрации пользователей (может быть использовано, например, угрозой несанкционированного доступа).

Отсутствие контроля за резервными активами (может быть использовано, например, угрозой хищения).

Отсутствующее или неудовлетворительное соглашение об уровне сервиса (может быть использовано, например, угрозой ошибок технического обслуживания).

Отсутствующая или недостаточная политика «чистого стола и пустого экрана» (может быть использована, например, угрозой хищения информации).

Отсутствующие или недостаточные положения (касающиеся безопасности) в договорах с клиентами и/или третьими сторонами (могут быть использованы, например, угрозой несанкционированного доступа).

Отсутствующие или недостаточные положения (касающиеся безопасности) в договорах со служащими (могут быть использованы, например, угрозой мошенничества и хищения).

Отсутствие планов обеспечения деловой непрерывности (может быть использовано, например, угрозой технической неисправности).

Отсутствие надлежащего распределения обязанностей по обеспечению информационной безопасности (может быть использовано, например, угрозой отрицания).

Отсутствие политики по использованию электронной почты (может быть использовано, например, угрозой неправильной маршрутизации сообщений).

Отсутствие процедур идентификации и оценки риска (может быть использовано, например, угрозой несанкционированного доступа к системе).

Отсутствие процедур обращения с секретной информацией (может быть использовано, например, угрозой ошибок пользователей).

Отсутствие процедур обеспечения соблюдения прав на интеллектуальную собственность (может быть использовано, например, угрозой хищения информации).

Отсутствие процедур сообщения о слабых местах безопасности (может быть использовано, например, угрозой использования сетевых средств несанкционированным образом).

Отсутствие процедур введения программного обеспечения в действующие системы (может быть использовано, например, угрозой ошибок операционного персонала).

Отсутствие процедуры контроля изменений (может быть использовано, например, угрозой ошибки технического обслуживания).

Отсутствие процедуры мониторинга средств обработки информации (может быть использовано, например, угрозой несанкционированного доступа).

Отсутствие регулярных аудитов (надзора) (может быть использовано, например, угрозой несанкционированного доступа).

Отсутствие регулярных проверок, проводимых руководством (может быть использовано, например, угрозой злоупотребления ресурсами).

Отсутствие установленных механизмов мониторинга нарушений безопасности (может быть использовано, например, угрозой умышленного повреждения).

Отсутствие обязанностей по обеспечению информационной безопасности в перечнях служебных обязанностей (может быть использовано, например, угрозой ошибок пользователей).

Отсутствие зафиксированных в журнале регистрации администратора и оператора сообщений об ошибках (может быть использовано, например, угрозой использования программных средств несанкционированным образом).

Отсутствие записей в журнале регистрации администратора и оператора (может быть использовано, например, угрозой ошибок операционного персонала).

Отсутствие оговоренного дисциплинарного процесса в случае инцидента безопасности (может быть использовано, например, угрозой хищения информации).

8. Обычные уязвимости обработки бизнес-приложений

Неверная установка параметров (может быть использована, например, угрозой ошибок пользователей).

Применение прикладных программ к неверным данным с точки зрения времени (может быть использовано, например, угрозой недоступности данных).

Неспособность создания административных отчетов (может быть использована, например, угрозой несанкционированного доступа).

Неверные даты (могут быть использованы, например, угрозой ошибок пользователей).

9. Общеприменимые уязвимости

Единичная точка сбоя (может быть использована, например, угрозой сбоя услуг связи).

Неадекватное реагирование технического обслуживания (может быть использовано, например, угрозой сбоев аппаратных средств).

Неправильно разработанные, несоответствующим образом выбранные или плохо управляемые защитные меры (могут быть использованы, например, угрозой проникновения в систему связи).

Методы оценки уязвимостей. Тестирование информационной системы

Профилактические методы, такие как тестирование информационной системы, могут быть использованы для эффективной идентификации уязвимостей в зависимости от критичности системы ИКТ и доступных ресурсов (например, выделенных фондов, доступной технологии, лиц, обладающих компетентностью для проведения тестирования). Методы тестирования включают:

- автоматические инструментальные средства поиска уязвимостей;
- тестирование и оценивание безопасности (STE);
- тестирование на проникновение.

Автоматические инструментальные средства поиска уязвимостей используются для просмотра группы хостов или сети на предмет известных уязвимых сервисов (например, система разрешает анонимный протокол передачи файлов [FTP], ретрансляцию отправленной почты). Следует, однако, отметить, что некоторые из потенциальных уязвимостей, идентифицированных автоматическими инструментальными средствами поиска уязвимостей, могут не представлять реальных уязвимостей в контексте среды системы. Например, некоторые из этих средств поиска определяют потенциальные уязвимости, не учитывая среду и требования сайта. Некоторые из уязвимостей, отмеченных автоматическими инструментальными средствами поиска уязвимостей, могут в действительности не быть уязвимостями для конкретного сайта, а быть сконфигурированными таким образом, потому что этого требует среда. Таким образом, этот метод может давать ошибочные результаты исследования.

Другой метод, который может использоваться для определения уязвимостей системы ИКТ во время процесса оценки риска, – тестирование и оценивание безопасности. Он включает разработку и выполнение плана тестирования (например, сценарий тестирования, процедуры тестирования и ожидаемые результаты тестирования). Цель тестирования безопасности системы состоит в тестировании эффективности средств контроля безопасности системы ИКТ, которые были применены в операционной среде. Задача заключается в том, чтобы удостовериться, что применяющиеся средства контроля соответствуют утвержденной спецификации безопасности для программных и аппаратных средств, обеспечивают выполнение политики безопасности организации или соответствуют отраслевым стандартам.

Тестирование на проникновение может использоваться как дополнение к проверке средств контроля безопасности и гарантирование того, что защита различных аспектов системы ИКТ обеспечена. Когда тестирование на проникновение используется в процессе оценки риска, оно может применяться для оценки способности системы ИКТ противостоять умышленным попыткам обойти средства контроля безопасности системы. Его задача состоит в тестировании системы ИКТ, с точки зрения источника угрозы, и в идентификации потенциальных сбоев в структурах защиты системы ИКТ.

Результаты этих видов тестирования безопасности помогут идентифицировать уязвимости системы.

Важно отметить, что методы и средства тестирования на проникновение могут давать ложные результаты, если уязвимость не была успешно использована. Чтобы использовать конкретную уязвимость, нужно знать точные систему/приложение/патчи, установленные на тестируемой системе. Если во время тестирования эти данные неизвестны, может быть невозможно успешно использовать

конкретную уязвимость (например, достичь удаленного обратного соединения). Однако все же возможно взломать или перезапустить тестируемый процесс или систему. В таком случае тестируемый объект тоже должен считаться уязвимым.

Раздел 5. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время все вопросы, связанные со стандартизацией в Российской Федерации, регулируются Федеральным законом «**О техническом регулировании»**.

Статья 11 Закона определяет цели стандартизации: повышение уровня безопасности жизни или здоровья граждан, имущества, экологической безопасности, безопасности жизни или здоровья животных и растений; повышение уровня безопасности объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера; обеспечение научно-технического прогресса; повышение конкурентоспособности продукции, работ, услуг; рациональное использование ресурсов; техническая и информационная совместимость; сопоставимость результатов исследований (испытаний) и измерений, технических и экономико-статистических данных; взаимозаменяемость продукции.

Статья 13 Закона определяет виды документов в области стандартизации, к ним отнесены: национальные стандарты; правила стандартизации, нормы и рекомендации в области стандартизации; применяемые в установленном порядке классификации, общероссийские классификаторы технико-экономической и социальной информации; стандарты организаций.

Статья 14 Закона определяет статус национального органа Российской Федерации по стандартизации и технических комитетов по стандартизации. В соответствии с данной статьей на указанный орган возложено выполнение следующих задач:

- утверждение национальных стандартов;
- принятие программы разработки национальных стандартов;
- организация экспертизы проектов национальных стандартов;

- обеспечение соответствия национальной системы стандартизации интересам национальной экономики, состоянию материально-технической базы и научно-техническому прогрессу;

- осуществление учета национальных стандартов, правил стандартизации, норм и рекомендаций в этой области и обеспечение их доступности заинтересованным лицам;

- создание технических комитетов по стандартизации и координация их деятельности;

- организация опубликования национальных стандартов и их распространения;

- участие в соответствии с уставами международных организаций в разработке международных стандартов и обеспечение учета интересов Российской Федерации при их принятии;

- утверждение изображения знака соответствия национальным стандартам;

- представительство Российской Федерации в международных организациях, осуществляющих деятельность в области стандартизации.

Орган, уполномоченный на исполнение функций национального органа по стандартизации, определяет Правительство Российской Федерации.

В соответствии с постановлениями Правительства РФ от 16 июня 2004 г. № 284 и от 17 июня 2004 г. № 294 функции федерального органа по техническому регулированию и национального органа по стандартизации осуществляет **Федеральное агентство по техническому регулированию и метрологии**. (Ростехрегулирование, ФАТР и М).

Официальным изданием является «Вестник технического регулирования», зарегистрированный под номером ПИ № 77-16464 от 22 сентября 2003 г.

Так, постановлением Госстандарта РФ от 30 января 2004 г. № 4 определено, что национальными стандартами Российской Федерации

признаются государственные и межгосударственные стандарты, принятые Госстандартом России до 1 июля 2003 г.

Однако до вступления в силу соответствующих технических регламентов требования к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, установленные указанными национальными стандартами, подлежат обязательному исполнению только в части, соответствующей целям:

защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;

охраны окружающей среды, жизни или здоровья животных и растений;

предупреждения действий, вводящих в заблуждение приобретателей.

Основополагающим государственным стандартом Российской Федерации в области защиты информации является ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения» (принят постановлением Госстандарта РФ от 5 июня 2003 г. № 181-ст). Он устанавливает цель и задачи системы стандартов по защите информации, объекты стандартизации, структуру, состав и классификацию входящих в нее стандартов и правила их обозначения. Положения данного стандарта являются рекомендуемыми при разработке нормативных документов по стандартизации в области защиты информации, независимо от организационно-правовой формы и формы собственности предприятия, учреждения, организации – разработчика стандарта, а также при организации работ по стандартизации в области защиты информации органами управления Российской Федерации.

В соответствии с данным стандартом система стандартов по защите информации (ССЗИ) может включать в себя следующие нормативные документы: регламенты; стандарты; правила, нормы и рекомендации по стандартизации; общероссийские классификаторы технико-экономической

информации; нормативно-технические документы (НТД) системы общих технических требований к вооружению и военной технике (ОТТ).

В зависимости от объекта стандартизации в области ЗИ и требований, предъявляемых к нему, устанавливают стандарты следующих видов: основополагающие; на продукцию; на процессы; на технологию, включая в том числе информационные технологии; на услуги; на методы контроля; на документацию; на термины и определения.

Стандарты по ЗИ подразделяют на следующие категории:

международные (ГОСТ ИСО);

межгосударственные (ГОСТ);

государственные стандарты Российской Федерации, оформленные на основе аутентичного текста международного стандарта (ГОСТ Р ИСО/МЭК);

государственные стандарты Российской Федерации (ГОСТ Р);

государственные военные стандарты Российской Федерации (ГОСТ РВ);

стандарты отраслей, в том числе и на оборонную продукцию (ОСТ);

стандарты предприятий.

Зарубежные стандарты в области информационной безопасности

Стандарты и спецификации можно условно разделить на два вида:

- оценочные стандарты, направленные на классификацию информационных систем и средств защиты по требованиям безопасности;

- технические спецификации, регламентирующие различные аспекты реализации средств защиты.

Важно отметить, что между этими видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Технические спецификации имеют ряд положительных и отрицательных аспектов. Главные достоинства этих стандартов состоят в следующем:

Стандарт гарантирует большой сектор рынка для определенного типа оборудования или программного обеспечения. Это поощряет массовое производство и в некоторых случаях использование методов интеграции высокого и сверхвысокого уровня, что приводит к снижению цен.

Стандарт обеспечивает взаимодействие устройств, разработанных различными производителями, что обеспечивает большую гибкость при выборе и использовании оборудования.

Ниже перечислены основные недостатки технических стандартов:

Стандартизация ведет к замораживанию технологии. За то время пока стандарт разрабатывается, проходит проверку, согласуется, пересматривается и, наконец, публикуется, могут появиться новые, более эффективные технологии.

Существует множество стандартов, относящихся к одной и той же области деятельности. Это не является недостатком самих стандартов, а отражает сегодняшнюю технологию стандартизации. К счастью, в последние годы многие организации, занимающиеся разработкой стандартов, начали тесно сотрудничать. Тем не менее, существуют сферы, в которых стандарты иногда конфликтуют друг с другом.

Стандарты и регулирование

Следует различать следующие три понятия: добровольные стандарты; регулирующие стандарты; регулятивное использование добровольных стандартов.

Добровольные стандарты разрабатываются организациями, производящими стандарты. Они являются добровольными в том смысле,

что их существование не делает обязательным их применение. То есть, производители добровольно создают продукт, соответствующий стандарту, если они видят в этом выгоду для самих себя. Никаких юридических обязательств в этом нет. Эти стандарты также являются добровольными в том смысле, что они были разработаны добровольцами, предпринимаемые усилия которых не оплачивались организацией, производящей стандарты и управляющей этим процессом. Эти добровольцы являются служащими заинтересованных организаций, например производителей и государственных организаций. Работоспособность добровольных стандартов объясняется тем, что, как правило, эти стандарты разрабатывались на основе широкого консенсуса и что потребительский спрос на стандартизированные продукты поощрял применение этих стандартов производителями.

Регулирующие стандарты, напротив, разрабатываются государственными регулятивными управлениями для достижения определенной общественной цели, например, в области безопасности. Эти стандарты обладают регулятивной силой и должны выполняться производителями в контексте применения данных предписаний. Но предписания могут применяться к широкому спектру продуктов, включая компьютеры и средства связи.

Регулятивное использование добровольных стандартов – относительно новое или, по меньшей мере, недавно ставшее превалирующим явление. Типичный пример этого – предписание, требующее от государственных организаций, чтобы они приобретали только продукт, соответствующий некоторому набору добровольных стандартов. У такого подхода есть ряд достоинств:

Он уменьшает бремя производства стандартов, лежащее на государственных организациях.

Он поощряет сотрудничество между государством и организациями по стандартизации в области производства стандартов широкого применения.

Он уменьшает число стандартов, которые должны выполнять производители.

Исторически первым широко распространившимся документом, получившем статус стандарта, были **Критерии безопасности компьютерных систем** Министерства обороны США.

Впоследствии они были приняты другими ведомствами этой страны и даже другими государствами либо в исходном виде, либо после переработки с учетом развития информационных технологий. Так появились Европейские, Федеральные, Канадские критерии безопасности компьютерных систем. В настоящее время в большинстве стран, в том числе и в России, силу стандарта приобрели так называемые Общие критерии.

Интересно посмотреть на краткое содержание предыдущих разработок, чтобы показать эволюцию научно-технической мысли в сфере стандартизации вопросов обеспечения информационной безопасности в ее узком, компьютерном понимании.

Критерии безопасности компьютерных систем Министерства обороны США – «Оранжевая книга»

Критерии безопасности компьютерных систем (TCSEC – Trusted Computer System Evaluation Criteria), получившие неформальное, но прочно закрепившееся название «**Оранжевая книга»** (по цвету изданной брошюры), были разработаны Министерством обороны США в 1983 г. с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем и выработки соответствующей методологии и технологии анализа

степени поддержки политики безопасности в компьютерных системах военного назначения.

В 1985 г. «Оранжевая книга» была принята в качестве стандарта Министерства обороны США (DoD TCSEC). В 1987 и 1991 гг. стандарт был дополнен требованиями для гарантированной поддержки политики безопасности в распределенных вычислительных сетях и базах данных.

В данном документе впервые нормативно определены такие понятия, как «**политика безопасности»**, вычислительная база защиты или **ядро защиты** (TCB, Trusted Computing Base) и т.д.

Согласно «Оранжевой книге» **безопасная компьютерная система** – это система, поддерживающая управление доступом к обрабатываемой в ней информации таким образом, что только соответствующим образом авторизованные пользователи или процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию. Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

В «Оранжевой книге» предложены три категории требований безопасности – политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних – на качество самих средств защиты.

Требование 1. Политика безопасности. Система должна поддерживать точно определенную политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основании их идентификации и набора правил управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации.

Требование 2. Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности объекта и/или режимы доступа к этому объекту.

Требование 3. Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификация) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения. Они должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

Требование 4. Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность. Это необходимо для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

Требование 5. Контроль корректности функционирования средств защиты. Средства защиты должны содержать независимые аппаратные функции защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности,

идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Требование 6. Непрерывность защиты. Все средства защиты (в т.ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

Приведенные выше базовые требования к безопасности служат основой для критериев, образующих единую шкалу оценки безопасности компьютерных систем, определяющую **семь классов** безопасности.

Все системы в соответствии с «Оранжевой книгой» распределяются по следующим **классам защищенности** (в порядке возрастания защищенности, более защищенный класс включает в себя все требования предыдущих классов):

Класс D – минимальная защита. Зарезервирован для отнесения систем, не удовлетворяющих ни одному из других классов защиты.

Класс C1 – защита, основанная на разграничении доступа (DAC). Обеспечивается разграничение пользователей и данных.

Класс C2 – защита, основанная на управляемом контроле доступом. Наличие усовершенствованных средств управления доступом и распространения прав, аудит событий, имеющих отношение к безопасности системы и разделению ресурсов. Общие ресурсы должны очищаться перед повторным использование другими процессами.

Класс B1 – мандатная защита, основанная на присваивании меток объектам и субъектам, находящимся под контролем ТСВ. Необходима реализация механизма присваивания меток экспортируемым данным.

Класс B2 – структурированная защита. Управление доступом распространяется на все субъекты и объекты системы. Анализ побочных каналов утечки информации. Специальные процедуры изменения конфигурации. Возможность тестирования и полного анализа ТСВ. Разбиение ее структуры на критические с точки зрения защиты и некритические элементы.

Класс B3 – домены безопасности. Реализация концепции монитора обращений, который гарантированно защищен от несанкционированного доступа, порчи и подделки, обрабатывает все обращения, прост для анализа и тестирования (предоставляется полная система тестов, полнота которой доказана).

Класс A1 – верифицированный проект. Проект ТСВ должен быть представлен в виде формализованной и верифицированной математическими методами спецификации.

Выбор класса защиты системы рекомендуется осуществлять на основе ее **режима функционирования**. Определяется пять таких режимов:

1. Режим, в котором система постоянно обрабатывает ценную информацию одного класса в окружении, которое обеспечивает безопасность для работы с этим классом.

2. Режим особой секретности самой системы. Все пользователи и элементы системы имеют один класс и могут получить доступ к любой информации.

3. Многоуровневый режим. Обработка информации разных классов, не все пользователи имеют доступ ко всем классам информации.

4. Контролирующий режим. Многоуровневый режим, в котором защищенность ТСВ полностью не гарантируется.

5. Режим изолированной безопасности. Изолированная обработка информации различных классов. Например, защищаться может лишь один класс информации, а остальные нет.

Основой для выбора класса является **индекс риска**: разность между максимальным классом (грифом) информации и минимальным классом пользователей. Чем выше разность, тем больший класс защиты требуется.

Следует отметить, что «Критерии безопасности компьютерных систем» Министерства обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на разработчиков, потребителей и специалистов по сертификации компьютерных систем.

Основной отличительной чертой этого документа является его ориентация на системы военного применения, причем в основном на **операционные системы**. Это предопределило доминирование требований, направленных на обеспечение конфиденциальности обрабатываемой информации и исключение возможностей ее разглашения.

Критерии адекватности реализации средств защиты и политики безопасности отражены слабо, соответствующий раздел по существу ограничивается требованиями контроля целостности средств защиты и поддержания их работоспособности, что явно недостаточно.

Европейские критерии безопасности информационных технологий

Проблемы стандартизации в сфере информационной безопасности оказались актуальны не только для Соединенных Штатов. Вслед за выходом «Оранжевой книги» страны Европы разработали согласованные «**Критерии безопасности информационных технологий»** (Information Technology Security Evaluation Criteria, далее – Европейские критерии). Европейские критерии рассматривают следующие задачи средств информационной безопасности:

- защита информации от несанкционированного доступа с целью обеспечения ее **конфиденциальности;**

- обеспечение **целостности** информации посредством защиты от ее несанкционированной модификации или уничтожения;

- обеспечение **доступности** компьютерных систем с помощью противодействия угрозам отказа в обслуживании.

Для того чтобы удовлетворить требованиям конфиденциальности, целостности и доступности, необходимо реализовать соответствующий набор функций безопасности, таких как идентификация и аутентификация, управление доступом, восстановление после сбоев и т.д. Чтобы средства защиты можно было признать эффективными, требуется определенная степень уверенности в правильности их выбора и надежности функционирования. Для решения этой проблемы в Европейских критериях впервые вводится понятие **адекватности (assurance) средств защиты**.

Адекватность включает в себя два аспекта: **эффективность**, отражающую соответствие средств безопасности решаемым задачам, и **корректность**, характеризующую процесс их разработки и функционирования.

Эффективность определяется соответствием между задачами, поставленными перед средствами безопасности, и реализованным набором функций защиты – их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты. Под корректностью понимается правильность и надежность реализации функций безопасности.

Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

Главное достижение этого документа – введение понятия адекватности средств защиты и определение отдельной шкалы для критериев адекватности.

Необходимо отметить, что Европейские критерии тесно связаны с «Оранжевой книгой», что делает их не вполне самостоятельным документом.

Американские Федеральные критерии безопасности информационных технологий

Федеральные критерии безопасности информационных технологий (Federal Criteria for Information Technology Security) разрабатывались как одна из составляющих Американского федерального стандарта по обработке информации (Federal Information Processing Standart), призванного заменить «Оранжевую книгу». Разрботчиками стандарта выступили Национальный институт стандартов и технологий США (National Institute of Standarts and Technology – NIST) и Агенство национальной безопасности США (National Security Agency).

Создание Федеральных критериев безопасности информационных технологий преследовало следующие цели:

1. Определение универсального и открытого для дальнейшего развития **базового набора требований безопасности,** предъявляемых к современным информационным технологиям. Требования к безопасности и критерии оценки уровня защищенности должны соответствовать современному уровню развития информационных технологий и учитывать его прогресс в будущем. Стандарт в этой связи предлагает обоснованный и структурированный подход к разработке требований к продуктам информационных технологий с учетом областей их применения.

2. Совершенствование существующих требований и критериев безопасности. В связи с развитием информационных технологий назрела необходимость пересмотра фундаментальных принципов безопасности с

учетом появления новых областей их применения как в государственном, так и в частном секторе.

3. Приведение в соответствие принятых в разных странах требований и критериев безопасности информационных технологий.

4. Нормативное закрепление основополагающих принципов информационной безопасности. Стандарт является обобщением основных принципов обеспечения безопасности информационных технологий, разработанных в 80-е годы, и обеспечивает преемственность по отношению к ним с целью сохранения достижений в области защиты информации.

Федеральные критерии безопасности информационных технологий (далее – Федеральные критерии) охватывают практически полный спектр проблем, связанных с защитой и обеспечением безопасности, т.к. включают все аспекты обеспечения конфиденциальности, целостности и доступности.

Основными объектами применения требований безопасности Федеральных критериев являются ***продукты информационных технологий*** (Information Technology Products) и ***системы обработки информации*** (Information Technology Systems).

Под **продуктом информационных технологий (далее – ИТ-продукт)** понимается совокупность аппаратных и/или программных средств, которая представляет собой поставляемое конечному потребителю готовое к использованию средство обработки информации. Как правило, ИТ-продукт эксплуатируется не автономно, а интегрируется в систему обработки информации, представляющую собой совокупность ИТ-продуктов, объединенных в функционально полный комплекс, предназначенный для решения прикладных задач. В ряде случаев система обработки информации может состоять только из одного ИТ-продукта, обеспечивающего решение всех стоящих перед системой задач и удовлетворяющего требованиям безопасности.

С точки зрения безопасности принципиальное различие между ИТ-продуктом и системой обработки информации (СОИ) определяется **средой их эксплуатации**. Продукт информационных технологий обычно разрабатывается в расчете на то, что он будет использован во многих системах обработки информации, и, следовательно, разработчик должен ориентироваться только на самые общие предположения о среде эксплуатации своего продукта, включающие условия применения и общие угрозы. Напротив, система обработки информации разрабатывается для решения прикладных задач в расчете на требования конечных потребителей, что позволяет в полной мере учитывать специфику воздействий со стороны конкретной среды эксплуатации.

Федеральные критерии содержат положения, относящиеся только к отдельным продуктам информационных технологий. Вопросы построения систем обработки информации из набора ИТ-продуктов не являются предметом рассмотрения этого документа.

Положения Федеральных критериев касаются только собственных средств обеспечения безопасности ИТ-продуктов, т.е. механизмов защиты, встроенных непосредственно в эти продукты в виде соответствующих программных, аппаратных или специальных средств. Для повышения их эффективности могут дополнительно применяться внешние системы защиты и средства обеспечения безопасности, к которым относятся как технические средства, так и организационные меры, правовые и юридические нормы. В конечном счете, безопасность ИТ-продукта определяется совокупностью собственных средств обеспечения безопасности и внешних средств, являющихся частью среды эксплуатации.

Ключевым понятием концепции информационной безопасности Федеральных критериев является понятие «профиля защиты» (Protection Profile). **Профиль защиты** – это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, технологии разработки и квалификационному

анализу. Как правило, один профиль защиты описывает несколько близких по структуре и назначению ИТ-продуктов. Основное внимание в профиле защиты уделяется требованиям к составу средств защиты и качеству их реализации, а также их адекватности предполагаемым угрозам безопасности.

Федеральные критерии представляют процесс разработки систем обработки информации, начинающийся с формулирования требований потребителями и заканчивающийся введением в эксплуатацию, в виде следующих основных этапов:

1. Разработка и анализ профиля защиты. Требования, изложенные в профиле защиты, определяют функциональные возможности ИТ-продуктов по обеспечению безопасности и условия эксплуатации, при соблюдении которых гарантируется соответствие предъявляемым требованиям. Кроме требований безопасности, профиль защиты содержит требования по соблюдению технологической дисциплины в процессе разработки, тестирования и квалификационного анализа ИТ-продукта. Профиль защиты анализируется на полноту, непротиворечивость и техническую корректность.

2. Разработка и квалификационный анализ ИТ-продуктов. Разработанные ИТ-продукты подвергаются независимому анализу, целью которого является определение степени соответствия характеристик продукта сформулированным в профиле защиты требованиям и спецификациям.

3. Компоновка и сертификация системы обработки информации в целом. Успешно прошедшие квалификацию уровня безопасности ИТ-продукты интегрируются в систему обработки информации. Полученная в результате система должна удовлетворять заявленным в профиле защиты требованиям при соблюдении указанных в нем условий эксплуатации.

Федеральные критерии регламентируют только первый этап схемы – разработку и анализ профиля защиты. Процесс создания ИТ-продуктов и компоновка систем обработки информации остаются вне рамок этого стандарта.

Общие критерии безопасности информационных технологий

Общие критерии безопасности информационных технологий (Common Criteria for Information Technology Security Evaluation, далее – Общие критерии) являются результатом совместных усилий авторов Европейских критериев безопасности информационных технологий, американских Федеральных критериев безопасности информационных технологий и Канадских критериев безопасности компьютерных систем, направленных на объединение основных положений этих документов и создание единого международного стандарта безопасности информационных технологий.

Версия 2.1 данного стандарта утверждена Международной организацией по стандартизации (ISO) в 1999 г. в качестве международного стандарта информационной безопасности **ISO/IEC 15408**.

Первая версия Общих критериев была опубликована 31 января 1996 г. Разработчиками документа выступили Национальный институт стандартов и технологий и Агентство национальной безопасности США, а также соответствующие организации Великобритании, Канады, Финляндии и Нидерландов. Вторая версия вышла в мае 1998 г., причем она отличается от первоначальной довольно существенными исправлениями и дополнениями.

Общие критерии сохраняют совместимость с существующими стандартами и развивают их путем введения новых концепций, соответствующих современному уровню развития информационных технологий, интеграции национальных информационных систем в единое мировое информационное пространство. Общие критерии оперируют уже

знакомым понятием ИТ-продукт и используют концепцию профиля защиты.

Общие критерии разрабатывались в расчете на то, чтобы удовлетворить запросы трех групп специалистов, в равной степени являющихся пользователями таких документов: производителей и потребителей продуктов информационных технологий, а также экспертов по оценке уровня их безопасности.

Производители должны использовать Общие критерии при проектировании и разработке ИТ-продуктов, а также в подготовке их к квалификационному анализу и сертификации. Этот документ дает возможность производителям на основании анализа запросов потребителя определить набор требований, которым должен удовлетворять разрабатываемый ими продукт. Кроме того, производители могут использовать Общие критерии для определения границ своей ответственности, а также условий, которые необходимо выполнить для успешного прохождения квалификационного анализа и сертификации ими продукта.

Потребители используют предлагаемую Общими критериями технологию для обоснования своих претензий на то, что поставляемый им ИТ-продукт успешно противостоит угрозам безопасности, на основании того, что он удовлетворяет выдвинутым функциональным требованиям и их реализация осуществлена с достаточным уровнем адекватности.

Эксперты по сертификации используют этот документ в качестве критериев определения соответствия средств защиты ИТ-продукта требованиям, предъявляемым к нему потребителями, и угрозам, действующим в среде его эксплуатации. Общие критерии описывают только общую схему проведения квалификационного анализа и сертификации, но не регламентируют процедуру их осуществления. Вопросам методологии квалификационного анализа и сертификации

посвящен отдельный раздел – Общая методология оценки безопасности информационных технологий.

Таким образом, Общие критерии обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

Общие критерии рассматривают информационную безопасность, во-первых, как совокупность конфиденциальности и целостности обрабатываемой ИТ-продуктом информации, а также доступности ресурсов ВС и, во-вторых, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации. Поэтому в концепцию Общих критериев входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.

Общие критерии регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов, используя схему, заимствованную из Федеральных критериев. Они предлагают достаточно сложную и бюрократичную концепцию процесса разработки и квалификационного анализа, требующую от потребителей и производителей большой работы по составлению и оформлению весьма объемных и подробных отчетных документов.

Разработчики Общих критериев также продолжили подход Федеральных критериев, направленный на отказ от единой шкалы безопасности, и усилили гибкость предложенных в них решений путем введения частично упорядоченных шкал, благодаря чему потребители и

производители получили дополнительные возможности по выбору требований и их адаптации к своим прикладным задачам.

Особое внимание стандарт уделяет адекватности реализации функциональных требований, которая обеспечивается как независимым тестированием и анализом ИТ-продукта, так и применением соответствующих технологий на всех этапах его проектирования и разработки.

В целом требования Общих критериев охватывают практически все аспекты безопасности ИТ-продуктов и технологии их создания, а также содержат все исходные материалы, необходимые потребителям и разработчикам для формирования соответствующих документов. Как следствие, требования Общих критериев являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности информационных технологий.

Данный стандарт ознаменовал собой новый уровень стандартизации информационных технологий, подняв его на межгосударственный уровень. За этим проглядывается реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что даст возможности для интеграции национальных информационных систем, а это в свою очередь откроет совершенно новые сферы применения информационных технологий.

ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки

безопасности информационных технологий» относится к разновидности стандартов, оформленных на основе аутентичного текста. Основой для него стал описанный выше международный стандарт ISO/IEC 15408-99 «Общие критерии безопасности информационных технологий» (далее – Общие критерии или ОК).

Общие критерии состоят из 3-х частей:

1. Введение и общая модель.
2. Функциональные требования безопасности.
3. Требования доверия к безопасности.

Область использования ОК включает как процесс разработки ИТ-продуктов или АС, так и приобретение коммерческих продуктов и систем. При проведении оценки такой продукт или систему информационных технологий называют **объектом оценки** (ОО), к числу которых ОК относят: ВС, ОС, распределенные системы, вычислительные сети и приложения.

К числу основных пользователей ОК относит следующих физических и юридических лиц:

1. Сотрудников служб безопасности (СБ), ответственных за определение и выполнение политики и требований безопасности организации в области ИТ.

2. Сотрудников, ответственных за техническое состояние оборудования.

3. Аудиторов (внешних и внутренних).

4. Проектировщиков систем безопасности, ответственных за спецификацию систем безопасности и продуктов ИТ.

5. Аттестующих, ответственных за приемку системы ИТ в эксплуатацию в конкретной среде.

6. Заявителей, заказывающих оценку и обеспечивающих ее проведение.

7. Органы оценки, ответственных за руководство и надзор за программами проведения оценок безопасности ИТ.

Часть 1 стандарта включает методологию оценки безопасности ИТ, определяет виды требований безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах трех категорий пользователей: потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности ОО по методологии Общих критериев определяются исходя из целей безопасности, которые, в свою очередь, основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

В первой части определено, от чего надо защищать информацию:

от несанкционированного раскрытия (конфиденциальность);

от модификации (целостность);

от потери возможности ее использования (доступность).

Часть 2 стандарта включает универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Часть 3 стандарта включает систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. В этой же части содержится описание **оценочных уровней доверия**, определяющих шкалу требований, которые позволяют с возрастающей степенью полноты и строгости провести оценку проектной, тестовой и эксплуатационной документации, правильности функционирования комплекса средств безопасности, оценку уязвимостей продукта или системы ИТ, стойкости механизмов защиты и сделать заключение об уровне безопасности объекта оценки.

Некоторые вопросы рассматриваются как лежащие вне области действия ОК, поскольку они требуют привлечения специальных методов или являются смежными по отношению к безопасности ИТ. Часть из них перечислена ниже.

Стандарт не содержит критериев оценки безопасности, касающихся **административных мер безопасности** (организационные меры, управление персоналом, физическая защита и процедурный контроль), непосредственно не относящихся к мерам безопасности ИТ.

Оценка специальных физических аспектов безопасности ИТ, таких как контроль электромагнитного излучения, прямо не затрагивается, хотя многие концепции ОК применимы и в этой области. В частности, рассмотрены некоторые аспекты физической защиты ОО.

В ОК не рассматривается ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки и сертификации. Тем не менее, ожидается, что ОК будут использоваться для целей оценки в контексте такой структуры и такой методологии.

Процедуры использования результатов оценки при аттестации продуктов и систем ИТ находятся вне области действия ОК. Аттестация продукта или системы ИТ является административным процессом, посредством которого предоставляются полномочия на их использование в конкретной среде эксплуатации.

Критерии для оценки специфических качеств криптографических алгоритмов также не входят в ОК. Если требуется независимая оценка математических свойств криптосистем, встроенной в ОО, то в системе оценки, в рамках которой применяются ОК, необходимо предусмотреть проведение таких оценок.

ОК определяют следующий перечень сокращений, являющихся обязательными для всех частей стандарта.

ЗБ (ST) – задание по безопасности;

ИТ (IT) – информационная технология;

ИФБО (TSFI) – интерфейс ФБО;

ОДФ (TSC) – область действия ФБО;

ОК (CC) – общие критерии;

ОО (TOE) – объект оценки;

ОУД (EAL) – оценочный уровень доверия;

ПБО (TSP) – политика безопасности ОО;

ПЗ (PP) – профиль защиты;

ПФБ (SFP) – политика функции безопасности;

СФБ (SOF) – стойкость функции безопасности;

ФБ (SF) – функция безопасности;

ФБО (TSF) – функция безопасности ОО.

Часть 1. Введение и общая модель

Первая часть стандарта включает описание рассмотренной выше структуры стандарта в целом, области его применения, список основных сокращений. Далее описывается используемый глоссарий, он представлен в таблице.

Таблица 6

Глоссарий Общих критериев

№	Термин	Смысловое содержание	Английский эквивалент
1.	**Активы**	Информация или ресурсы, подлежащие защите контрмерами ОО	**Assets**
2.	**Атрибут безопасности**	Информация, связанная с субъектами, пользователями и/или объектами, которая используется для осуществления ПБО	**Security attribute**
3.	**Аутентификационные данные**	Информация, используемая для верификации предъявленного идентификатора пользователя	**Authentication data**

Продолжение табл. 6

№	Термин	Смысловое содержание	Английский эквивалент
4.	**Базовая СФБ**	Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения	**SOF-basic**
5.	**Внешний объект ИТ**	Любые продукт или система ИТ, доверенные или нет, находящиеся вне ОО и взаимодействующие с ним	**External IT entity**
6.	**Выбор**	Выделение одного или нескольких элементов из перечня в компоненте	**Selection**
7.	**Внутренний канал связи**	Канал связи между разделенными частями ОО	**Internal communication channel**
8.	**Высокая СФБ**	Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от тщательно спланированного и организованногонарушения безопасности ОО нарушителями с высоким потенциалом нападения	**SOF-high**
9.	**Данные ФБО**	Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО	**TSF data**
10.	**Данные пользователя**	Данные, созданные пользователем и для пользователя, которые не влияют на выполнение ФБО	**User data**
11.	**Доверенный канал**	Средство взаимодействия между ФБО и удалённым доверенным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании ПБО	**Trusted channel**
12.	**Доверенный маршрут**	Средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую степень уверенности в поддержании ПБО	**Trusted path**

Продолжение табл. 6

№	Термин	Смысловое содержание	Английский эквивалент
13.	**Доверие**	Основание для уверенности в том, что сущность отвечает своим целям безопасности	**Assurance**
14.	**Зависимость**	Соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть, как правило, удовлетворено, чтобы и другие требования могли бы отвечать своим целям	**Dependency**
15.	**Задание по безопасности**	Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО	**Security target**
16.	**Идентификатор**	Представление уполномоченного пользователя (например, строка символов), однозначно его идентифицирующее. Таким представлением может быть либо полное или сокращенное имя этого пользователя, либо его псевдоним	**Identity**
17.	**Интерфейс функций безопасности ОО**	Совокупность интерфейсов, как интерактивных (человеко-машинные интерфейсы), так и программных (интерфейсы прикладных программ), с использованием которых осуществляется доступ к ресурсам ОО при посредничестве ФБО или получение от ФБО какой-либо информации	**TOE security functions interface**
18.	**Итерация**	Более чем однократное использование компонента при различном выполнении операций	**Iteration**
19.	**Класс**	Группа семейств, объединенных общим назначением	**Class**
20.	**Компонент**	Наименьшая выбираемая совокупность элементов, которая может быть включена в ПЗ, ЗБ или пакет	**Component**

Продолжение табл. 6

№	Термин	Смысловое содержание	Английский эквивалент
21.	**Механизм проверки правомочности обращений**	Реализация концепции монитора обращений, обладающая следующими свойствами: защищенностью от проникновения; постоянной готовностью; простотой, достаточной для проведения исчерпывающего анализа и тестирования	**Reference validation mechanism**
22.	**Модель политики безопасности ОО**	Структурированное представление политики безопасности, которая должна быть осуществлена ОО	**TOE security policy model**
23.	**Монитор обращений**	Концепция абстрактной машины, осуществляющей политику управления доступом ОО	**Reference monitor**
24.	**Назначение**	Спецификация определенного параметра в компоненте	**Assignment**
25.	**Неформальный**	Выраженный на естественном языке	**Informal**
26.	**Область действия ФБО**	Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО	**TSF scope of control**
27.	**Объект**	Сущность в пределах ОДФ, которая содержит или получает информацию и над которой субъекты выполняют операции	**Object**
28.	**Объект оценки**	Подлежащие оценке продукт ИТ или система с руководствами администратора и пользователя	**Target of evaluation**
29.	**Орган оценки**	Организация, которая посредством системы оценки обеспечивает реализацию ОК для определенного сообщества и в связи с этим устанавливает стандарты и контролирует качество оценок, проводимых организациями в пределах данного сообщества	**Evaluation authority**
30.	**Оценка**	Оценка ПЗ, ЗБ или ОО по определенным критериям	**Evaluation**

Продолжение табл. 6

№	Термин	Смысловое содержание	Английский эквивалент
31.	**Оценочный уровень доверия**	Пакет компонентов доверия из части 3 настоящего стандарта, представляющий некоторое положение на предопределенной в стандарте шкале доверия	**Evaluation assurance level**
32.	**Пакет**	Предназначенная для многократного использования совокупность функциональных компонентов или компонентов доверия (например, ОУД), объединенных для удовлетворения совокупности определенных целей безопасности	**Package**
33.	**Передача в пределах ОО**	Передача данных между разделенными частями ОО	**Internal TOE transfer**
34.	**Передача за пределы области действия ФБО**	Передача данных сущностям, не контролируемым ФБО	**Transfer outside TSF control**
35.	**Передача между ФБО**	Передача данных между ФБО и функциями безопасности других доверенных продуктов ИТ	**Inter-TSF transfers**
36.	**Политика безопасности организации**	Одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности	**Organizational security policies**
37.	**Политика безопасности ОО**	Совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОО	**TOE security policy**
38.	**Политика функции безопасности**	Политика безопасности, осуществляемая ФБ	**Security function policy**
39.	**Полуформальный**	Выраженный на языке с ограниченным синтаксисом и определенной семантикой	**Semiformal**
40.	**Пользователь**	Любая сущность (человек-пользователь или внешний объект ИТ) вне ОО, которая взаимодействует с ОО	**User**

Продолжение табл. 6

№	Термин	Смысловое содержание	Английский эквивалент
41.	**Потенциал нападения**	Прогнозируемый потенциал для успешного (в случае реализации) нападения, выраженный в показателях компетентности, ресурсов и мотивации нарушителя	**Attack potential**
42.	**Продукт**	Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы	**Product**
43.	**Профиль защиты**	Независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя	**Protection profile**
44.	**Расширение**	Добавление в ЗБ или ПЗ функциональных требований, не содержащихся в части 2 настоящего стандарта, и/или требований доверия, не содержащихся в части 3 настоящего стандарта	**Extension**
45.	**Ресурс ОО**	Все, что может использоваться или потребляться в ОО	**TOE resource**
46.	**Роль**	Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и ОО	**Role**
47.	**Связность**	Свойство ОО, позволяющее ему взаимодействовать с объектами ИТ, внешними по отношению к ОО. Это взаимодействие включает обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации	**Connectivity**

Продолжение табл. 6

№	Термин	Смысловое содержание	Английский эквивалент
48.	**Секрет**	Информация, которая должна быть известна только уполномоченным пользователям и/или ФБО для осуществления определенной ПФБ	**Secret**
49.	**Семейство**	Группа компонентов, которые объединены одинаковыми целями безопасности, но могут отличаться акцентами или строгостью	**Family**
50.	**Система**	Специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации	**System**
51.	**Система оценки**	Административно-правовая структура, в рамках которой в определенном обществе органы оценки применяют ОК	**Evaluation scheme**
52.	**Средняя СФБ**	Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения	**SOF-medium**
53.	**Стойкость функции безопасности**	Характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности	**Strength of function**
54.	**Субъект**	Сущность в пределах ОДФ, которая инициирует выполнение операций	**Subject**
55.	**Уполномоченный пользователь**	Пользователь, которому в соответствии с ПБО разрешено выполнять какую-либо операцию	**Authorized user**
56.	**Усиление**	Добавление одного или нескольких компонентов доверия из части 3 настоящего стандарта в ОУД или пакет требований доверия	**Augmentation**

Окончание табл. 6

№	Термин	Смысловое содержание	Английский эквивалент
57.	**Уточнение**	Добавление деталей в компонент	**Refinement**
58.	**Функции безопасности ОО**	Совокупность всех функций безопасности ОО, направленных на осуществление ПБО	**TOE security functions**
59.	**Функция безопасности**	Функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО	**Security function**
60.	**Формальный**	Выраженный на языке с ограниченным синтаксисом и определенной семантикой, основанной на установившихся математических понятиях	**Formal**
61.	**Человек-пользователь**	Любое лицо, взаимодействующее с ОО	**Human user**
62.	**Цель безопасности**	Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям	**Security objective**
63.	**Элемент**	Неделимое требование безопасности	**Element**

Хотя ОК не предписывают конкретную методологию разработки или модель жизненного цикла, они, тем не менее представляют некоторые основополагающие предположения о соотношениях между требованиями безопасности и собственно разрабатываемым ОО. В основе данной методологии лежит уточнение требований безопасности, сведенных в краткую спецификацию в составе задания по безопасности, являющегося по сути исходным документом для разработки и последующей оценки (фактически некий аналог ТЗ). Каждый последующий уровень уточнения представляет декомпозицию проекта с его дополнительной детализацией. Наиболее подробным (и наименее абстрактным) представлением в итоге является непосредственно реализация ОО.

Количество уровней детализации при этом зависит от уровня доверия, который требуется обеспечить. В ОК предусмотрены следующие промежуточные этапы детализации, формируемые на основе задания по безопасности: функциональная спецификация, проект верхнего уровня, проект нижнего уровня и реализация.

С методологией создания ОО тесно связан процесс его оценки, который может проводиться как параллельно с разработкой, так и после ее окончания. Основными исходными материалами для оценки ОО являются:

- совокупность материалов, характеризующих ОО, включая прошедшее оценку ЗБ в качестве основы;

- сам ОО, безопасность которого требуется оценить;

- критерии, методология и система оценки.

Кроме того, в качестве исходных материалов для оценки возможно также использование вспомогательных материалов и специальных знаний в области безопасности ИТ, которыми располагает оценщик и сообщество участников оценок.

Ожидаемым результатом оценки является подтверждение удовлетворения объектом оценки требований безопасности, изложенных в его ЗБ, а также один или несколько отчетов, документирующих выводы оценщика относительно ОО, сделанные в соответствии с критериями оценки. Такие отчеты, помимо разработчика, очевидно, будут полезны также реальным и потенциальным потребителям продукта или системы.

Таким образом, основой разработки и эксплуатации любого ОО в Общих критериях провозглашается совокупность требований безопасности.

В ОК определены 3 группы конструкций для описания требований безопасности: пакет, профиль защиты (ПЗ) и задание по безопасности (ЗБ).

Пакет представляет собой некую промежуточную комбинацию компонентов безопасности. Он предназначен для многократного использования и определяет требования, которые известны как полезные и

эффективные для достижения некоторых установленных целей. Допускается применение пакета при создании более крупных пакетов, профилей защиты и заданий по безопасности.

Профиль защиты содержит совокупность требований безопасности, взятых из ОК или сформулированных в явном виде. ПЗ позволяет выразить независимые от конкретной реализации требования безопасности для *некоторой совокупности ОО*, которые полностью согласуются с набором целей безопасности. ПЗ также предназначен для многократного использования и определения как функциональных требований, так и требований доверия к ОО, которые полезны и эффективны для достижения установленных целей. ПЗ также содержит логическое обоснование требований и целей безопасности.

Задание по безопасности содержит совокупность требований безопасности, которые могут быть определены ссылками на ПЗ, непосредственно на функциональные компоненты или компоненты доверия или же сформулированы в явном виде. ЗБ позволяет выразить требования безопасности для *конкретного ОО*, которые по результатам оценки ЗБ признаны полезными и эффективными для достижения установленных целей безопасности. ЗБ является основой для соглашения между всеми сторонами относительно того, какую безопасность предлагает ОО.

В первой части ОК подробно описан и процесс формирования требований безопасности, поскольку данные требования, выраженные в итоге в ЗБ, должны быть обоснованы и непротиворечивы, достаточны, после чего только на их основе производится оценка ОО.

В соответствии с ОК на основании исследования политик безопасности, угроз и рисков должны быть сформированы следующие материалы, относящиеся к безопасности:

- изложение предположений, которым удовлетворяла бы среда разрабатываемой ИТ для того, чтобы она считалась безопасной;

- изложение угроз безопасности активов, в котором были бы идентифицированы все угрозы, при этом угрозы раскрываются через понятия агента угрозы (нарушителя), предполагаемого метода нападения, любых уязвимостей, которые являются предпосылкой для нападения, и идентификации активов, которые являются целью нападения;

- изложение политики безопасности, применяемой в организации; для системы ИТ такая политика может быть описана достаточно точно, тогда как для продуктов ИТ общего предназначения или класса продуктов о политике безопасности организации могут быть сделаны, при необходимости, только рабочие предположения.

Результаты анализа среды безопасности затем должны использоваться для установления **целей безопасности**, которые направлены на противостояние установленным угрозам, а также проистекают из установленной политики безопасности организации и сделанных предположений. Необходимо, чтобы цели безопасности были согласованы с определенными ранее целями применения или предназначением продукта, а также со сведениями о физической среде.

Требования безопасности являются результатом преобразования целей безопасности в совокупность требований безопасности для объекта оценки и требований безопасности для среды, которые, в случае их удовлетворения, обеспечат для него способность достижения его целей безопасности.

Имеются две различные категории требований безопасности – функциональные требования и требования доверия.

Функциональные требования налагаются на те функции, которые предназначены для поддержания безопасности ОО и определяют желательный безопасный режим функционирования. Примерами функциональных требований являются требования к идентификации, аутентификации, аудиту безопасности и т.д.

Требования доверия налагаются на действия разработчика, представленные свидетельства и действия оценщика. Примерами

требований доверия являются требования к строгости процесса разработки, по поиску потенциальных уязвимостей и анализу их влияния на безопасность.

Требования безопасности обычно включают как требования наличия желательных режимов функционирования, так и требования отсутствия нежелательных режимов. Наличие желательного режима обычно можно продемонстрировать путем непосредственного применения или испытаний (тестирования). Не всегда удается убедительно продемонстрировать отсутствие нежелательного режима. Уменьшению риска наличия нежелательного режима в значительной мере способствуют испытания (тестирование), экспертиза проекта и окончательной реализации.

Часть 2. Функциональные требования безопасности

Вторая часть стандарта определяет функциональные требования безопасности ИТ объекта оценки, которые предназначены для достижения целей безопасности, установленных в ПБ и ЗБ. В этой части перечисляются функциональные требования безопасности, которые могут быть предъявлены к объекту оценки. Оценка ОО касается, прежде всего, подтверждения того, что в отношении ресурсов ОО осуществляется определенная политика безопасности. Стандарт подчеркивает, что политика безопасности ОО (ПБО) состоит из различных политик функций безопасности (ПФБ).

В соответствии с ОК организация требований безопасности осуществляется в виде иерархии: **класс – семейство – компонент – элемент**.

Термин **класс** применяется для общего группирования требований безопасности. Составляющие класса называются **семействами**, под которыми понимается группа наборов требований безопасности, имеющих общие цели безопасности, но различающихся акцентами или строгостью. Составляющие семейства называются **компонентами**, которые представляют специфический набор требований безопасности, который

является наименьшим выбираемым набором требований безопасности для включения в структуры, определяемые ОК. Компоненты составлены из отдельных **элементов**. Каждый элемент определяет требования безопасности на самом нижнем уровне. Он является тем неделимым требованием безопасности, которое может быть верифицировано при оценке.

Для идентификации функционального элемента вводится краткая уникальная запись. Например, запись имени функционального элемента FDP_IFF.4.2 читается следующим образом:

F – функциональное требование;

DP – класс «Защита данных пользователя»;

IFF – семейство «Функции управления информационными потоками»;

4 – 4-ый компонент «Частичное устранение неразрешенных информационных потоков»;

2 – 2-ой элемент компонента.

ОК предусматривают 11 классов функциональных требований:

FAU – аудит безопасности;

FCO – связь;

FCS – криптографическая поддержка;

FDP – защита данных пользователя;

FIA – идентификация и аутентификация;

FMT – управление безопасностью;

FPR – приватность;

FPT – защита ФБО;

FRU – использование ресурсов;

FTA – доступ к ОО;

FTP – доверенный маршрут/канал.

Класс **FAU** (аудит безопасности) включает распознавание, запись, хранение и анализ информации, связанной с действиями, например, с действиями, контролируемыми в соответствии с политикой безопасности

объекта оценки. Этот класс включает 6 семейств: автоматическая реакция аудита безопасности (FAU_ARP); генерация данных аудита безопасности (FAU_GEN); анализ аудита безопасности (FAU_SAA); просмотр аудита безопасности (FAU_SAR); выбор событий аудита безопасности (FAU_SEL); хранение данных аудита безопасности (FAU_STG).

Класс **FCO** (связь) содержит два семейства, связанные с обеспечением идентификаторов сторон, участвующих в обмене данными: идентификатор отправителя переданной информации (FCO_NRO – доказательство отправления); идентификатор получателя переданной информации (FCO_NRR – доказательство получения).

Класс **FCS** (криптографическая поддержка) используется, когда объект оценки имеет криптографические функции, реализованные аппаратными, программно-аппаратными и/или программными средствами. Реализация целей этого класса должна обеспечивать: идентификацию, аутентификацию, неотказуемость сообщения, доверенный маршрут, доверенный канал, разделение данных.

Класс состоит из двух семейств: управление криптографическими ключами (FCS_CKM); криптографические операции (FCS_COP).

Класс **FDP** (защита данных пользователя) определяет требования к функциям безопасности объекта, связанным с защитой данных пользователя. Класс имеет 13 семейств, разбитых на 4 группы.

1. Политика функций безопасности ОО для защиты данных пользователя, включает 2 семейства: политика управления доступом (FDP_ACC); политика управления информационными потоками (FDP_IFC).

2. Виды защиты данных пользователя, включает 6 семейств: функции управления доступом (FDP_ACF); функции управления информационными потоками (FDP_IFF); передача в пределах ОО (FDP_ITT); защита остаточной информации (FDP_RIP); откат (FDP_ROL); целостность хранимых данных (FDP_SDI).

3. Автономное хранение, импорт и экспорт данных, включает 3 семейства: аутентификация данных (FDP_DAU); экспорт данных за пределы действий ФБО (FDP_ETC); импорт данных из-за пределов действия ФБО (FDP_ITC).

4. Связь между ФБО имеет 2 семейства: защита конфиденциальности данных пользователя при передаче между ФБО (FDP_UCT); защита целостности данных пользователя при передаче между ФБО (FDP_UIT).

Класс **FIA** (идентификация и аутентификация) обеспечивает связь пользователей с соответствующими атрибутами безопасности (идентификатор группы, уровень безопасности или целостности). Класс включает 6 семейств: отказы аутентификации (FIA_AFL); определение атрибутов пользователя (FIA_ATD); спецификация секретов (FIA_SOS); аутентификация пользователя (FIA_UAU); идентификация пользователя (FIA_UID); связывание пользователь-субъект (FIA_USB).

Класс **FMT** (управление безопасностью) предназначен для спецификации управления некоторыми аспектами ФБО: атрибутами безопасности, данными и отдельными функциями. Класс включает 6 семейств: управление отдельными функциями ФБО (FMT_MOF); управление атрибутами безопасности (FMT_MSA); управление данными ФБО (FMT_MTD); отмена (FMT_REY); срок действия атрибута безопасности (FMT_SAE); роли управления безопасностью (FMT_SMR).

Класс **FPR** (приватность) предоставляет пользователю защиту от раскрытия его идентификатора и злоупотребления этим другими пользователями. Класс содержит 4 семейства: анонимность (FPR_ANO); псевдонимность (FPR_PSE); невозможность ассоциации (FPR_UNL);скрытность (FPR_UNO).

Класс **FPT** (защита ФБО) содержит функциональные требования, которые связаны с целостностью и управлением механизмами, реализованными в ФБО. По сути, требования этого класса дублируют требования из класса FDP (защита данных пользователя), однако они

специализированы на защиту данных пользователя, а класс FPT нацелен на защиту данных функций безопасности объекта. Класс FPT содержит 16 семейств: тестирование базовой абстрактной машины (FPT_AMT); безопасность при сбое (FPT_FLS); доступность экспортируемых данных ФБО (FPT_ITA); конфиденциальность экспортируемых данных ФБО (FPT_ITO); целостность экспортируемых данных ФБО (FPT_ITI); передача данных ФБО в пределах ОО (FPT_ITT); физическая защита ФБО (FPT_PHP); надежное восстановление (FPT_RCV); обнаружение повторного использования (FPT_RPL); посредничество при обращениях (FPT_RVM); разделение домена (FPT_SEP); протокол синхронизации состояний (FPT_SSP); метки времени (FPT_STM);согласованность данных ФБО между ФБО (FPT_TDC); согласованность данных ФБО при дублировании в пределах ОО (FPT_TDC); самотестирование (FPT_TST).

Класс **FRU** (использование ресурсов) поддерживает доступность требуемых ресурсов (вычислительные возможности, память) и состоит из 3 семейств: отказоустойчивость (FRU_FLT); приоритет обслуживания (FRU_PRS); распределение ресурсов (FRU_RSA).

Класс **FTA** (доступ к ОО) определяет требования к управлению открытием сеанса пользователя и состоит из 6 семейств: ограничение области выбираемых атрибутов (FTA_LSA); ограничение на параллельные сеансы (FTA_MCS); блокирование сеанса (FTA_SSL); предупреждения перед предоставлением доступа к ОО (FTA_TAB); история доступа к ОО (FTA_TAB); открытие сеанса с ОО (FTA_TSE).

Класс **FTP** (доверенный маршрут/канал) определяет требования как к доверенному маршруту связи между пользователями и ФБО, так и к доверенному каналу связи ФБО и другими доверенными продуктами ИТ.

Под доверенным каналом понимается канал связи, который может быть инициирован любой из связывающихся сторон и обеспечивает неотказываемые характеристики, связанные с идентификаторами сторон

канала. Класс содержит два семейства: доверенный канал передачи между ФБО (FTP_ITC); доверенный маршрут (FTP_TRP).

Часть 3. Требования доверия к безопасности

Третья часть стандарта содержит систематизированный каталог функциональных требований доверия, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Стандарт определяет, что *способом достижения доверия является оценка*.

В качестве основных методов для проведения оценки используют: анализ и проверку процессов и процедур; проверку, что процессы и процедуры действительно применяются; анализ соответствия между представлениями проекта ОО; анализ соответствия каждого представления проекта ОО требованиям; верификацию доказательств; анализ руководств; анализ разработанных функциональных тестов и полученных результатов; независимое функциональное тестирование; анализ уязвимостей, включающий предположения о недостатках; тестирование проникновения.

Требования доверия строятся аналогично функциональным требованиям в виде иерархии: класс – семейство – компонент – элемент. Каждому классу присваивается уникальное имя, которое указывает на тематические разделы, на которые распространяется данный класс доверия. Имя начинается с буквы «А», за которой следуют еще две буквы латинского алфавита, относящиеся к имени класса.

Помимо классов, определяющих требования доверия, ОК также описывают три класса требований по поддержке доверия, оценке профиля защиты и задания по безопасности.

Класс **AMA** (поддержка доверия) содержит 4 семейства: план поддержки доверия (AMA_AMP); отчет о категорировании компонентов

ОО (AMA_CAT); свидетельство о поддержке доверия (AMA_EVD);анализ влияния на безопасность (AMA_SIA).

Класс **APE** (оценка профиля защиты) включает 6 семейств: профиль защиты, введение ПЗ (APE_INT); профиль защиты, описание ОО (APE_DES); профиль защиты, среда безопасности (APE_ENV); профиль защиты, цели безопасности (APE_OBJ); профиль защиты, требования безопасности ИТ (APE_REQ); профиль защиты, требования безопасности ИТ, сформулированные в явном виде (APE_SRE).

Класс **ASE** (оценка задания по безопасности) включает 8 семейств: задание по безопасности, введение ЗБ (ASE_INT);задание по безопасности, описание ОО (ASE_DES); задание по безопасности, среда безопасности (ASE_ENV); задание по безопасности, цели безопасности (ASE_OBJ); задание по безопасности, требования безопасности ИТ (ASE_REQ); задание по безопасности, утверждение о соответствии ПЗ (ASE_PPC); задание по безопасности, краткая спецификация ОО (ASE_TSS); задание по безопасности, требования безопасности ИТ, сформулированные в явном виде (ASE_SRE).

Требования для оценки профиля защиты и задания по безопасности также трактуются как классы доверия, структура которых подобна структуре других классов доверия. Отличие заключается лишь в отсутствии подраздела ранжирования компонентов в описаниях семейств. Причина в том, что каждое семейство имеет только один компонент и, следовательно, ранжирование отсутствует.

Особое внимание в 3-й части ОК уделено используемым **оценочным уровням доверия** (ОУД). ОУД образуют возрастающую шкалу, которая позволяет соотнести получаемый уровень доверия со стоимостью и возможностью достижения этой степени доверия.

В стандарте определены *семь* упорядоченных оценочных уровней доверия для ранжирования доверия к ОО. Они иерархически упорядочены, поскольку каждый ОУД представляет более высокое доверие, чем любой

из предыдущих ОУД. Увеличение доверия от ОУД1 к ОУД7 достигается заменой какого-либо компонента доверия иерархически более высоким компонентом из того же семейства доверия (т.е. увеличением строгости, области и/или глубины оценки) и добавлением компонентов доверия из других семейств доверия (т.е. добавлением новых требований).

ОУД состоят из определенной комбинации компонентов доверия. Точнее, каждый ОУД включает не больше чем один компонент каждого семейства доверия, а все зависимости каждого компонента доверия учтены.

Важно обратить внимание, что не все семейства и компоненты доверия и поддержки доверия включены в оценочные уровни доверия. Это не означает, что они не обеспечивают значимое и полезное доверие. Напротив, ожидается, что эти семейства и их компоненты будут рассматриваться для усиления ОУД в тех ПЗ и ЗБ, для которых они полезны.

Хотя в стандарте определены именно ОУД, можно представлять другие комбинации компонентов доверия. Для этого специально введено понятие «усиление» (augmentation), которое предполагает добавление компонентов доверия из семейств доверия, до этого не включенных в некоторый ОУД, или замену компонентов доверия в некотором ОУД другими, иерархически более высокими компонентами доверия из этого же самого семейства доверия. Вводящий усиление обязан строго обосновать полезность и дополнительную ценность добавленного к ОУД компонента доверия. ОУД может быть также расширен требованиями доверия, сформулированными в явном виде.

Таким образом, ОУД могут быть усилены и не могут быть ослаблены. Например, понятие «ОУД за исключением какого-либо составляющего его компонента доверия» не признается в стандарте как допустимое утверждение.

Методология и требования ОК не охватывают вопросы организации процессов оценки (сертификации и/или аттестации). Это является предметом ведения государственных органов. В нашей стране в сфере защиты информации деятельность такой системы регулируется ФСТЭК на основе выпускаемых ею руководящих документов.

Руководящие документы Гостехкомиссии (ФСТЭК) России

Гостехкомиссия России вела весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на «Общие критерии».

Рассмотрим два важных Руководящих документа – Классификацию **автоматизированных систем (АС)** по уровню **защищенности от несанкционированного доступа (НСД)** и аналогичную Классификацию **межсетевых экранов (МЭ)**.

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС,

обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса – 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Таблица 7

Требования ко всем девяти классам защищенности АС

Подсистемы и требования	**Классы**								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации.	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+

Продолжение табл. 7

1	2	3	4	5	6	7	8	9	10
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+

Окончание табл. 7

1	2	3	4	5	6	7	8	9	10
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

«–» нет требований к данному классу; «+» есть требования к данному классу; «СЗИ НСД» система защиты информации от несанкционированного доступа

По существу перед нами – минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность информации. Целостность представлена отдельной подсистемой (номер 4), но непосредственно к интересующему нас предмету имеет отношение только пункт 4.1. Доступность (точнее, восстановление) предусмотрено только для самих средств защиты.

Классификации межсетевых экранов – представляется принципиально важным, поскольку в нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Данный РД важен не столько содержанием, сколько самим фактом своего существования. РД получил высокую оценку не только в России, но и в мире.

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется **фильтрация информации**. Чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

Рекомендации X.800

Технические спецификации X.800 появились немногим позднее «Оранжевой книги», но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации X.800 – документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней

(обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем **конфиденциальность трафика** (это защита информации, которую можно получить, анализируя сетевые потоки данных).

Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является **аутентификация источника данных**.

В следующей таблице указаны уровни **эталонной семиуровневой модели** OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

Таблица 8

Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функции безопасности	**Уровень**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

«+» данный уровень может предоставить функцию безопасности; «–» данный уровень не подходит для предоставления функции безопасности.

Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

- шифрование;
- электронная цифровая подпись;
- механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
- механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
- механизмы аутентификации. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
- механизмы **дополнения трафика**;
- механизмы **управления маршрутизацией**. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
- механизмы **нотаризации**. Служат для заверения таких коммуникационных характеристик, как целостность, время,

личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

Таблица 9

Взаимосвязь функций и механизмов безопасности

Функции	**Механизмы**							
	Шифрование	**Электронная подпись**	**Управление доступом**	**Целостность**	**Аутентификация**	**Дополнение трафика**	**Управление маршрутизацией**	**Нотаризация**
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	+	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

«+» механизм пригоден для реализации данной функцию безопасности; «–» механизм не предназначен для реализации данной функции безопасности.

В таблице сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение **криптографических ключей**, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для реализации избранной политики безопасности.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям: администрирование информационной системы в целом; администрирование сервисов безопасности; администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, **реагирование** на происходящие события, **аудит** и **безопасное восстановление**.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование

механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

- управление ключами (генерация и распределение**)**;
- управление шифрованием (установка и синхронизация криптографических параметров). К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению;
- администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т.п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т.п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т.п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

Стандарты ISO/IEC 17799:2002 (BS 7799:2000) – ГОСТ Р ИСО/МЭК 17799

Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «**Управление информационной безопасностью – Информационные технологии**» (Information technology – Information security management») является одним из наиболее известных стандартов в области защиты информации. Данный стандарт был разработан на основе первой части Британского стандарта BS 7799-1:1995 «Практические рекомендации по управлению информационной безопасностью» (Information security management – Part 1: Code of practice for information security management») и относится к новому поколению стандартов информационной безопасности компьютерных ИС.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация и управление корпоративными информационными ресурсами;
- кадровый менеджмент и информационная безопасность;
- физическая безопасность;
- администрирование безопасности КИС;
- управление доступом;
- требования по безопасности к КИС в ходе их разработки, эксплуатации и сопровождения;

- управление бизнес-процессами компании с точки зрения информационной безопасности;
- внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799-2:2000 «Спецификации систем управления информационной безопасностью» («Information security management – Part 2: Specification for information security management systems») определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита ИС.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов – British Standards Institution (BSI), изданные в 1995–2003 гг. в виде следующей серии:

- «Введение в проблему управления информационной безопасностью» (Information security managment: an introduction»);
- «Возможности сертификации на требования стандарта BS 7799» («Preparing for BS 7799 sertification»);
- «Руководство BS 7799 по оценке и управлению рисками» («Guide to BS 7799 risk assessment and risk management);
- «Руководство для проведения аудита на требования стандарта» («BS 7799 Guide to BS 7799 auditing»);
- «Практические рекомендации по управлению безопасностью информационных технологий» («Code of practice for IT management).

В 2002 г. международный стандарт ISO 17799 (BS 7799) был пересмотрен и существенно дополнен. В новом варианте этого стандарта

большое внимание уделено вопросам повышения культуры защиты информации в различных международных компаниях.

Международный стандарт ISO 27001 – ГОСТ Р ИСО/МЭК 27001 «Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (этот стандарт принят 31 декабря 2006 г.).

Начиная с осени 2005 г. в России все большую известность при построении корпоративных систем менеджмента информационной безопасности (СМИБ) завоевывает международный стандарт ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Принят в России в 2006 г. как ГОСТ Р ИСО/МЭК 27001.

Истоки ISO/IEC 27001:2005 находятся в британском государственном стандарте BS 7799, который был разработан в 1995 г. Британским институтом стандартов и ведущими организациями и компаниями Великобритании. В 1999 г. первая часть BS 7799 была передана в Международную организацию по стандартизации (ISO – The International Organization for Standardization) и в 2000 г. утверждена в качестве международного стандарта как ISO/IEC 17799:2000 (BS 7799-1:2000). Следующей его версией стал стандарт ISO/IEC 17799:2005. В 1999 г. вышла в свет вторая часть британского стандарта: BS 7799-2:1999 Information Security management – Specification for ISMS (ISMS – Information Security Management System). В 2002 г. появилась новая, усовершенствованная редакция стандарта – BS 7799-2:2002. На ее основе 14 октября 2005 г. был принят стандарт ISO/IEC 27001:2005. Ожидается развитие серии стандартов 27000 и выпуск ISO/IEC 27002, который сменит ISO/IEC 17799:2005.

Выполнение требований ISO/IEC 27001:2005 позволяет организациям формализовать и структурировать процессы управления ИБ по следующим направлениям:

- разработка политики ИБ;

- организация ИБ;

- организация управления внутренними активами и ресурсами компании, составляющими основу ее ключевых бизнес-процессов;

- защита персонала и снижение внутренних угроз компании;

- физическая безопасность в компании и безопасность окружающей среды;

- управление средствами связи и эксплуатацией оборудования;

- разработка и обслуживание аппаратно-программных систем;

- управление непрерывностью бизнес-процессов в компании;

- соблюдение правовых норм по безопасности.

Цели и комплексы мероприятий ISO/IEC 27001:2005 по каждому направлению работ были заимствованы из стандарта ISO/IEC 17799:2005 (разделы 5–15) и перечислены в его приложении A (Annex A. Control objectives and controls).

Семейство Международных Стандартов на Системы Управления Информационной Безопасностью 27000 разрабатывается ISO/IEC JTC 1/SC 27. Это семейство включает в себя Международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

Для этого семейства стандартов используется последовательная схема нумерации, начиная с 27000 и далее.

ISO27000	Определения и основные принципы. Планируется унификация со стандартами COBIT и ITIL. Проект стандарта находится в разработке.
ISO27001	ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). Выпущен в июле 2005 г.
ISO27002	ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью (ранее ISO/IEC 17799:2005).
ISO27003	Руководство по внедрению системы управления информационной безопасностью. Выпуск запланирован на 2007 г.
ISO27004	Измерение эффективности системы управления информационной безопасностью. Выпуск запланирован на 2007 г.
ISO27005	Управление рисками информационной безопасности (на основе BS 7799-3:2006). Выпуск запланирован на 2007 г.
ISO27006	ISO/IEC 27006:2007 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью
ISO27007	Руководство для аудитора СУИБ (в разработке).
ISO27011	Руководство по управлению информационной безопасностью для телекоммуникаций (в разработке).

ISO (Международная Организация по Стандартизации) и **IEC** (Международная Электротехническая Комиссия) формируют специализированную систему всемирной стандартизации. Государственные органы, являющиеся членами ISO или IEC, участвуют в разработке Международных Стандартов через технические комитеты, созданные соответствующей организацией для стандартизации отдельных областей технической деятельности. Другие международные организации, правительственные и не правительственные, совместно с ISO и IEC также принимают участие в этой работе. В области информационных технологий ISO и IEC организован совместный технический комитет – ISO/IEC JTC 1. Основной задачей совместного технического комитета является подготовка Международных Стандартов. Проекты Международных Стандартов, принятые совместным техническим комитетом, передаются в государственные органы для голосования. Публикация в качестве Международного Стандарта требует одобрения не менее 75 процентов проголосовавших государственных органов. Международные Стандарты проектируются в соответствии с правилами, установленными Директивами ISO/IEC.

Германский стандарт BSI

В отличие от ISO 17799 германское «Руководство по защите информационных технологий для базового уровня защищенности» посвящено детальному рассмотрению частных вопросов управления информационной безопасностью компании.

В германском стандарте BSI представлены:

- общая методика управления информационной безопасностью (организация менеджмента в области информационной безопасности, методология использования руководства);
- описания компонентов современных ИТ;

- описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса);
- характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны);
- характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение);
- характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell NetWare, сети UNIX и Windows).
- характеристика активного и пассивного телекоммуникационного оборудования ведущих поставщиков, например Cisco Systems;
- подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).

Вопросы защиты приведенных информационных активов компании рассматриваются по определенному сценарию: общее описание информационного актива компании – возможные угрозы и уязвимости безопасности – возможные меры и средства контроля и защиты.

Стандарты и рекомендации Банка России в области информационной безопасности

Центральный банк РФ проводит большую работу по созданию системы стандартов и рекомендаций, а также методики проверки организаций банковской системы на соответствие их требованиям.

Комплекс стандартов Банка России СТО БР ИББС «**Обеспечение информационной безопасности организаций банковской системы Российской Федерации**» состоит из базового стандарта СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской

системы Российской федерации. **Общие положения**» (далее – Стандарт) и развивающей и обеспечивающей его группы стандартов и рекомендаций в области стандартизации.

Стандарт основывается на риск-ориентированном подходе, суть которого заключается в том, что деятельность организации БС РФ подвержена рискам, так как на бизнес-процессы организации БС РФ и вовлеченные в них активы могут воздействовать различного рода угрозы. В случае наличия уязвимостей в системе контрмер бизнеса (в это понятие входят, в том числе, и меры обеспечения ИБ организации), а также при наличии определенных условий (факторов риска), реализация угрозы приводит к возникновению инцидента, ведущего к возникновению ущерба для организации БС РФ. Понятие «риск» выступает в этом случае как индикатор угрозы для организации БС РФ и как мера, учитывающая вероятность реализации угрозы (возникновения инцидента) и величину ущерба, являющегося следствием реализации угрозы (возникновения инцидента).

В соответствии с риск-ориентированным подходом в организации БС РФ необходимо реализовать процессы руководства и управления в отношении риска (управление риском), направленные на минимизацию риска или снижение риска до допустимого уровня. Управление риском включает в себя определение допустимого (приемлемого) уровня риска, оценку риска (включая сравнение полученного риска с допустимым) и обработку риска (процесс выбора и осуществления защитных мер, снижающих риски ИБ до приемлемого уровня, или мер по переносу, принятию или уклонению от риска). С целью снижения рисков организация предпринимает комплекс контрмер различного характера (организационных, технических и др.). Необходимо учитывать тот факт, что понизить риски можно лишь до определенного остаточного уровня. Оставшаяся (остаточная) часть риска, определяемая факторами среды деятельности организации БС РФ, на которые организация не в силах

влиять, должна быть признана приемлемой и принята либо отклонена. В этом случае от риска следует либо уклониться (например, изменить среду деятельности), либо перенести на кого-нибудь (например, застраховать).

Риски нарушения ИБ выражаются в возможности потери состояния защищенности интересов (целей) организации БС РФ в информационной сфере и возникновения ущерба бизнесу организации БС РФ или убытков. Потеря состояния защищенности интересов (целей) организации БС РФ в информационной сфере заключается в утрате свойств конфиденциальности, целостности или доступности информационных активов, утрате параметров или доступности сервисов инфраструктуры организации БС РФ.

Для снижения рисков нарушения ИБ и управления ими (то есть для реализации и поддержания требуемого уровня ИБ) необходимо разработать, реализовать, поддерживать (изучать и анализировать с целью выявления уязвимостей) и совершенствовать (устранять уязвимости и повышать эффективность) систему обеспечения ИБ организации БС РФ.

Система обеспечения ИБ организации БС РФ **(СОИБ)** представляет собой совокупность системы ИБ и системы менеджмента ИБ организации БС РФ.

Система ИБ организации БС РФ (СИБ) представляет собой совокупность защитных мер, реализующих обеспечение ИБ организации БС РФ, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система менеджмента ИБ (СМИБ) организации БС РФ представляет собой совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов.

Для реализации и поддержания ИБ в организации БС РФ необходима реализация четырех групп процессов:

– планирование СОИБ организации БС РФ (планирование);

– реализация СОИБ организации БС РФ (реализация);

– мониторинг и анализ СОИБ организации БС РФ (проверка);

– поддержка и улучшение СОИБ организации БС РФ (совершенствование).

Указанные группы процессов составляют СМИБ организации БС РФ.

Организация и выполнение процессов СМИБ необходимы, в том числе, для обеспечения уверенности в том, что хороший практический опыт организации БС РФ документируется, становится обязательным к применению, а СОИБ совершенствуется. При этом необходимо обеспечить реализацию всех групп процессов СМИБ. Рис. 11 иллюстрирует взаимосвязь СИБ, СМИБ и СОИБ организации БС РФ.

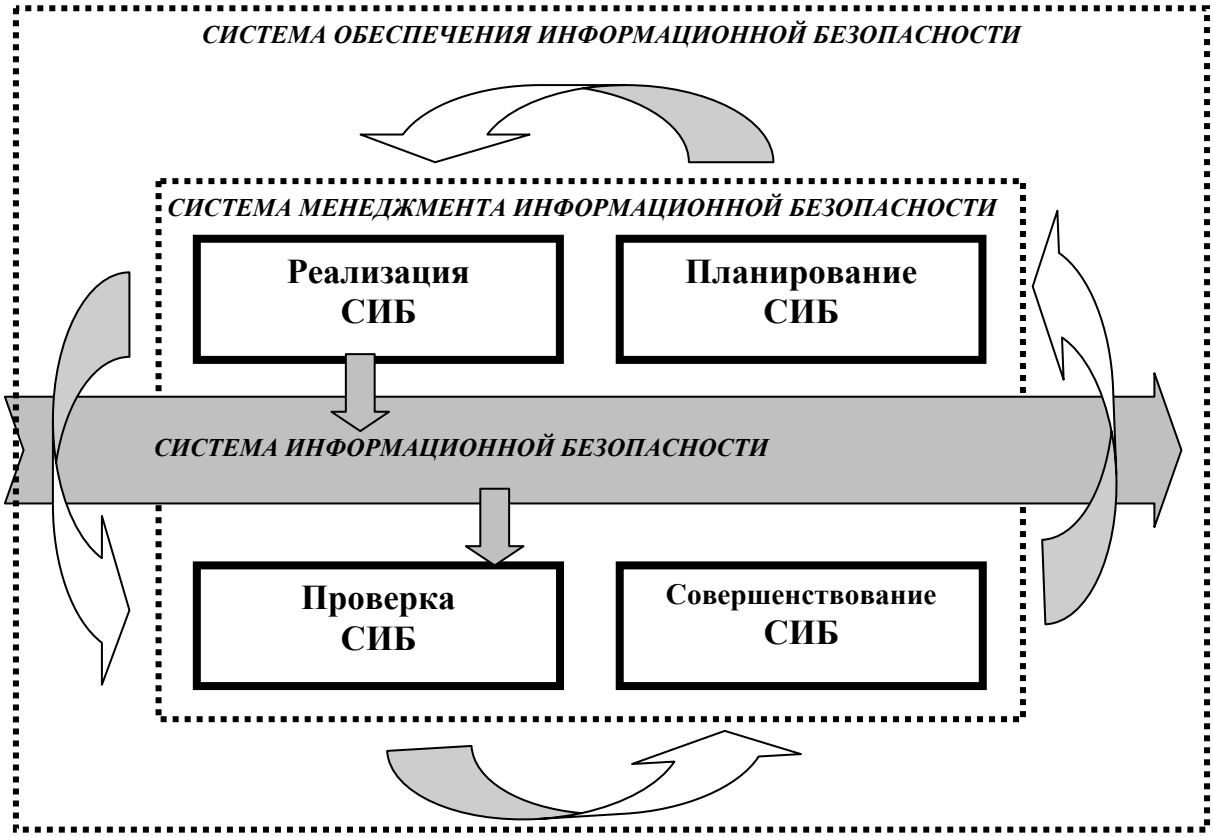


Рис. 11. Система обеспечения информационной безопасности организации БС РФ

СОИБ должна быть определена, спланирована и регламентирована в организации БС РФ. Основой для этого являются требования законодательства Российской Федерации, нормативные правовые акты Банка России, контрактные требования организации БС РФ, а также условия ведения бизнеса, выраженные на основе идентификации активов организации БС РФ и построения модели нарушителей и угроз.

Основные принципы, подходы и требования к построению модели угроз и нарушителей содержатся в седьмом разделе Стандарта.

Требования к СИБ и СМИБ организации БС РФ содержатся, соответственно, в восьмом и девятом разделах Стандарта. Однако, учитывая риск-ориентированный подход, используемый в Стандарте, выбор конкретных методов, мер и средств обеспечения ИБ остается за организацией БС РФ и ее руководством.

Даже правильно выстроенные процессы и используемые защитные меры в силу объективных причин со временем имеют тенденцию к ослаблению своей эффективности. Это неминуемо ведет к деградации СОИБ и возрастанию рисков нарушения ИБ.

Для того чтобы избежать деградации СОИБ и обеспечить требуемый уровень ИБ организации БС РФ, Стандартом определены требования проверки и оценки СОИБ, которые проводятся путем выполнения следующих процессов: мониторинга и контроля защитных мер, самооценки ИБ, внешнего аудита ИБ, анализа функционирования СОИБ (в том числе со стороны руководства). Указанные процессы являются частью группы процессов «проверка» СМИБ и описаны в десятом разделе Стандарта.

Для поддержания СОИБ на должном уровне в качестве оперативной меры Стандартом определено требование проведения мониторинга СОИБ и контроля защитных мер. В результате выполнения этих процессов может быть выработан сигнал опасности для деятельности организации БС РФ, если произошел инцидент ИБ или выявлены новые угрозы ИБ, уязвимости

СОИБ, факторы рисков, требующие введения превентивных мер. В случае возникновения инцидента ИБ должен быть использован дополнительный (специально разработанный) план действий, позволяющий свести к минимуму возможные потери и восстановить СОИБ. Кроме того, результаты выполнения процессов мониторинга и контроля защитных мер используются для анализа СОИБ, в том числе со стороны руководства.

Для оценки информационной безопасности и выявления признаков деградации СОИБ Стандартом определено требование проведения **самооценки ИБ**, а также **регулярного внешнего аудита ИБ**. При проведении аудита и самооценки ИБ необходимо руководствоваться едиными правилами и подходами и использовать стандартные процедуры. Это позволяет обеспечить точность, повторяемость и сопоставимость результатов, а следовательно, обеспечить доверие к результатам оценки. Для формирования системы оценки требованиям стандарта СТО БР ИББС-1.0 разработаны стандарты СТО БР ИББС-1.1, СТО БР ИББС-1.2 и рекомендации в области стандартизации РС БР ИББС-2.1.

Стандарт **СТО БР ИББС-1.1** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Аудит информационной безопасности**» устанавливает основные принципы проведения аудита ИБ и требования к процедуре аудита ИБ.

Рекомендации в области стандартизации РС БР ИББС-2.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0**» устанавливает порядок проведения самооценки ИБ организаций БС РФ.

Стандарт **СТО БР ИББС-1.2** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям**

СТО БР ИББС-1.0» устанавливает способы определения степени выполнения требований СТО БР ИББС-1.0, а также итогового уровня соответствия ИБ требованиям СТО БР ИББС-1.0 при проведении аудита (оценки соответствия) ИБ и самооценки ИБ.

Для этого Стандарт рекомендует использовать групповые (М1 – М32) и частные показатели (M_i,j). (Показатель ИБ – мера или характеристика для оценки ИБ.) Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки

- текущего уровня ИБ (М1-М8),
- менеджмента (М9-М27) и
- осознания ИБ(М28-М32).

Оценки групповых показателей (EV Mi) используются для получения оценки по направлениям (EV1, EV2 и EV3).

Частные показатели ИБ входят в состав каждого группового показателя и представлены в виде вопросов, ответы на которые дают возможность определить оценки (EV Mi.j), которые затем формируют оценки EV Mi (i=1,…,32).

(ЧП – оценка степени выполнения какого-либо частного требования ИБ, умноженная на значимость требования (коэффициенты значимости a_i,j).

Не все требования или частные показатели учитываются. Неактуальным требование ИБ (частный показатель) признается, только если организация не занимается деятельностью, к которой данное требование ИБ имеет отношение. Существует процедура перенормировки коэффициентов значимости.

Рекомендуемые критерии выставления оценок частных показателей ИБ следующие.

Оценка ЧП ИБ = 0: требования не установлены во внутренних нормативных документах (ВНД) и не выполняются; требования частично установлены во ВНД, но не выполняются.

Оценка ЧП ИБ = 0,25: требования полностью установлены во ВНД, но не выполняются; требования не установлены во ВНД и выполняются в неполном объеме; требования частично установлены во ВНД и выполняются в неполном объеме.

Оценка ЧП ИБ = 0,5: требования полностью установлены во ВНД и выполняются в неполном объеме; требования не установлены во ВНД, но выполняются в полном объеме.

Оценка ЧП ИБ = 0,75: требования частично установлены во ВНД, но выполняются в полном объеме.

Оценка ЧП ИБ = 1: требования полностью установлены во ВНД и выполняются в полном объеме.

Основными источниками для получения оценок являются (по степени достоверности – от наибольшей к наименьшей): свидетельства, полученные от третьей стороны в письменном виде; свидетельства, полученные от проверяемой организации и подтвержденные третьей стороной в письменном виде; свидетельства, полученные в ходе проведения аудиторских процедур (наблюдения за деятельностью, анализа данных системы мониторинга ИБ и т.д.); свидетельства, полученные в форме документов; свидетельства, полученные в устной форме.

Приведем для примера групповые показатели для оценки текущего уровня ИБ (в скобках указаны соответствующие пункты стандарта СТО БР ИББС-1.0).

М1. Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу (п. 8.2.2).

М2. Обеспечение ИБ автоматизированных банковских систем на стадиях жизненного цикла (п. 8.2.3).

М3. Обеспечение ИБ при управлении доступом и регистрации (п. 8.2.4).

М4. Обеспечение ИБ средствами антивирусной защиты (п. 8.2.5).

М5. Обеспечение ИБ при использовании ресурсов сети Интернет (п. 8.2.6).

М6. Обеспечение ИБ при использовании средств криптографической защиты информации (п. 8.2.7).

М7. Выполнение правил обеспечения ИБ банковских платежных технологических процессов (п. 8.2.8).

М8. Выполнение правил обеспечения ИБ банковских информационных технологических процессов (п. 8.2.9).

Как видно из этого перечня, не все направления обеспечения ИБ рассматриваются Стандартом и Методикой, но наиболее важные.

Результаты мониторинга, анализа защитных мер, оценки ИБ (самооценки и аудита ИБ) используются при проведении анализа СОИБ (в том числе со стороны руководства).

Анализ СОИБ позволяет выявлять новые угрозы ИБ и факторы рисков ИБ, уязвимости СОИБ. Результаты анализа СОИБ используются для управления рисками ИБ, для принятия решений по тактическим и стратегическим улучшениям СОИБ, по повышению эффективности СОИБ (совершенствование СОИБ организации БС РФ).

Согласно Стандарту, для обеспечения согласованности, целенаправленности, планомерности деятельности по обеспечению ИБ эта деятельность должна быть документирована. Разработку и коррекцию внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в организации БС РФ рекомендуется проводить с учетом рекомендаций по стандартизации Банка России **РС БР ИББС– 2.0** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0**», которые определяют состав и структуру документов, а также процессы менеджмента документов по обеспечению ИБ организации БС РФ.

Комплекс стандартов Банка России является концептуальной и методологической основой для обеспечения и поддержания уровня ИБ, необходимого для достижения целей деятельности организации БС РФ и адекватного потребностям и условиям ведения бизнеса организации БС РФ. В настоящее время комплекс стандартов Банка России активно развивается. Готовятся к выходу третья редакция стандарта СТО БР ИББС-1.0 и вторая редакция СТО БР ИББС-1.2, стандарт по терминологии и другие. (www.techcom3623.ru)

Стандарты информационной безопасности в Интернете

В Интернете уже давно существует ряд комитетов, в основном из организаций-добровольцев, которые осторожно проводят предлагаемые технологии через процесс стандартизации. Эти комитеты, составляющие основную часть рабочей группы инженеров Интернета IETF (Internet Engineering Task Force), провели стандартизацию нескольких важных протоколов, ускоряя их внедрение в Интернете. Непосредственными результатами усилий IETF являются такие протоколы, как семейство TCP/IP для передачи данных, SMTP (Simple Mail Transport Protocol) и POP (Post Office Protocol) для электронной почты, а также SNMP (Simple Network Management Protocol) для управления сетью.

Фактическая разработка новых стандартов и протоколов для Интернета выполняется рабочими группами, создаваемыми по разрешению группы IETF. Членство в рабочей группе является добровольным; участвовать может любая заинтересованная организация. При разработке спецификации рабочая группа создает документ под названием «Проект стандарта для Интернета» (Internet draft) и размещает его в Интернете для всеобщего доступа. Этот документ может оставаться проектом до шести месяцев, и заинтересованные стороны могут рецензировать и комментировать его. В течение этого времени группа IESG может одобрить публикацию проекта в виде документа RFC (Request

for Comment — запрос комментариев). Если проект не приобретает статуса документа RFC в течение шестимесячного периода, он теряет также статус проекта стандарта для Интернета. Однако впоследствии рабочая группа может опубликовать переработанную версию проекта.

Группа IETF публикует документы RFC с одобрения группы IEsG. Документы RFC представляют собой рабочие записи сообщества исследователей и разработчиков Интернета. Документ этой серии может быть чем угодно – от доклада о собрании до спецификации стандарта.

В Интернете популярны протоколы безопасной передачи данных, а именно **SSL, SET, IPSec.** Перечисленные протоколы появились в Интернете сравнительно недавно как необходимость защиты ценной информации и сразу стали стандартами де-факто.

Протокол SSL (Secure Socket Layer) – популярный сетевой протокол с шифрованием данных для безопасной передачи по сети. Он позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи. Протокол SSL обеспечивает защиту данных между сервисными протоколами (такими как HTTP, FTP и др.) и транспортными протоколами (TCP/IP) с помощью современной криптографии.

Протокол SET (Security Electronics Transaction) – перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через сеть Интернет. Протокол SET основан на использовании цифровых сертификатов по **стандарту X.509**.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и Visa при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя защищенный механизм выполнения платежей.

SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карточек в Интернете. SET обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения, шифрование ценных и уязвимых данных. Поэтому SET более правильно можно назвать стандартной технологией или системой протоколов выполнения безопасных платежей с использованием пластиковых карт через Интернет. SET позволяет потребителям и продавцам подтверждать подлинность всех участников сделки, происходящей в Интернете, с помощью криптографии, в том числе применяя цифровые сертификаты.

SET обеспечивает следующие специальные требования защиты операций электронной коммерции:

- секретность данных оплаты и конфиденциальность информации заказа, переданной наряду с данными об оплате;
- сохранение целостности данных платежей. Целостность информации платежей обеспечивается с помощью цифровой подписи;
- специальную криптографию с открытым ключом для проведения аутентификации;
- аутентификацию держателя по кредитной карточке. Она обеспечивается применением цифровой подписи и сертификатов держателя карт;
- аутентификацию продавца и его возможности принимать платежи по пластиковым карточкам с применением цифровой подписи и сертификатов продавца;
- аутентификацию того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым карточкам через связь с процессинговой карточной

системой. Аутентификация банка продавца обеспечивается использованием цифровой подписи и сертификатов банка продавца;

- готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
- безопасность передачи данных посредством преимущественного использования криптографии.

Основное преимущество SET по сравнению с другими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарта X.509), которые ассоциируют держателя карты, продавца и банк продавца с банковскими учреждениями платежных систем Visa и Mastercard. Кроме того, SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами и интегрируется с существующими системами.

Протокол IPSec. Спецификация IPSec входит в стандарт IP v.6 и является дополнительной по отношению к текущей версии протоколов TCP/IP. Она разработана Рабочей группой IP Security IETF. В настоящее время IPSec включает 3 алгоритмо-независимых базовых спецификации, представляющих соответствующие RFC-стандарты. Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и защищает информацию на основе сквозного шифрования: независимо от работающего приложения при этом шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете **виртуальные частные сети (VPN).**

Инфраструктура управления открытыми ключами PKI (Public Key Infrastructure) предназначена для защищенного управления криптографическими ключами электронного документооборота, основанного на применении криптографии с открытыми ключами. Эта инфраструктура подразумевает использование **цифровых сертификатов,**

удовлетворяющих рекомендациям международного стандарта X.509 и развернутой сети **центров сертификации** и **центров регистрации**, обеспечивающих выдачу и сопровождение цифровых сертификатов для всех участников электронного обмена документами.

Конечно, в этом разделе представлено только несколько самых известных стандартов. Общее число их огромно. Даже для банковской сферы их очень много. В стандарте ISO TR 17944-2002 была сделана попытка их разбить на некоторые классы и перечислить. Изучить их все – сложнейшая задача.

Раздел 6. МЕРЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ (МЕРЫ КОНТРОЛЯ)

Защитные меры (см., например, ГОСТ ИСО/МЭК 13335) – 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.

Эффективная безопасность обычно требует комбинации различных защитных мер для обеспечения заданных уровней безопасности при защите активов. Например, механизмы контроля доступа, применяемые к вычислительным средствам, должны подкрепляться аудитом, определенным порядком действий персонала, его обучением, а также физической защитой. Часть защитных мер может быть обеспечена внешними условиями, свойствами актива или может уже существовать в системе или организации.

Порядок выбора защитных мер очень важен для правильного планирования и реализации программы информационной безопасности. Защитная мера может выполнять много функций безопасности, и, наоборот, одна функция безопасности может потребовать нескольких защитных мер. Защитные меры могут выполнять одну или несколько из следующих функций: предотвращение; сдерживание; обнаружение; ограничение; исправление; восстановление; мониторинг; осведомление.

Некоторые защитные меры могут характеризовать позицию организации в области информационной безопасности. В связи с этим важно выбирать специфические защитные меры, не причиняющие ущерба культурной и социальной среде, в которой функционирует организация.

Примеры таких специфических защитных мер: политики и процедуры; механизмы контроля доступа; антивирусное программное

обеспечение; шифрование; цифровая подпись; инструменты мониторинга и анализа; резервный источник питания; резервные копии информации.

Меры обеспечения ИБ (или **меры контроля** в понятиях ГОСТ Р ИСО/МЭК 27001, или **защитные меры** в терминах ISO 13335-1) имеют разветвленную сложную структуру и состоят из **организационных** и **программно-технических мер** на верхнем уровне.

В свою очередь, организационные меры включают **законодательные, административные и процедурные меры** обеспечения ИБ.

Законодательные меры включают в себя законы, стандарты, регламенты и другие нормативные документы.

Основой **административных мер**, осуществляемых руководством организации, является политика безопасности.

Процедурные, то есть реализуемые людьми, **меры** безопасности включают меры по: управлению персоналом; физической защите; поддержке работоспособности; реагированию на нарушения режима безопасности; планированию восстановительных работ.

Идентификация мер защиты важна и на этапе оценки рисков. В процессе идентификации мер защиты должна быть проведена проверка, что эти средства работают корректно.

Описание мер по обеспечению ИБ, приведенное ниже, выполнено в нотациях стандарта ГОСТ Р ИСО/МЭК 27001 и ISO/IEC 17799:2005 с указанием цели и описанием требований. Стандарты ГОСТ Р ИСО/МЭК 27001 и ISO/IEC 17799:2005 выделяют следующие области контроля:

- политика безопасности;
- управление активами (ресурсами);
- безопасность кадровых ресурсов (персонала);
- физическая безопасность и безопасность от воздействия окружающей среды;
- управление средствами связи и функционированием;

- контроль доступа;

- приобретение, разработка и обслуживание информационных систем;

- управление инцидентами с информационной безопасностью;

- управление непрерывностью бизнес-процессов;

- соответствие различным требованиям.

Ориентировочно весь объем мероприятий (в денежном исчислении) по охране и защите информации (см.[92]) можно разделить в следующем соотношении:

1. Правовые меры (законы, ведомственные акты, инструкции) – 5%.

2. Физические меры (ограда по периметру, служба охраны, разграничение полномочий и др.) – 15%.

3. Технические меры (различные технические и программные средства защиты) – 25–30%.

4. Административные меры (разработка политики в области безопасности, процедур ее внедрения, кадровая политика, обучение персонала, контроль и др.) – 50%.

Выбор средств контроля (мер защиты) в соответствии с проектом стандарта ИСО/МЭК 27005

Средства контроля выбираются в соответствии с вопросами безопасности, идентифицированными в результате оценки риска (стандарт ISO/IES 27005 посвящен именно управлению рисками), принимая в расчет угрозы и, наконец, вид рассматриваемого информационного процесса или системы.

Выбор средств контроля всегда включает баланс **операционных (нетехнических) и технических средств контроля**.

Операционные средства контроля включают те, которые обеспечивают **физическую, кадровую и административную безопасность**.

Физические средства контроля безопасности включают прочность внутренних стен строения, дверные замки с кодовым набором, противопожарные системы и охрану.

Кадровая безопасность охватывает проверки, связанные с набором персонала (особенно лиц, занимающих ответственные посты), мониторинг персонала и программы повышения осознания безопасности.

Административная (Процедурная) безопасность включает надежное документирование операционных процедур, процедуры разработки и одобрения приложений, а также процедуры менеджмента инцидентов информационной безопасности. В связи с этой категорией очень важно, чтобы для каждой системы разрабатывались соответствующие **планы и стратегия** обеспечения непрерывности бизнеса, включая планирование действий в чрезвычайных ситуациях/восстановление после сбоев.

План должен включать подробности об основных функциях и приоритетах для восстановления, потребности обработки и организационные процедуры, которым нужно следовать в том случае, если происходит бедствие или прерывание обслуживания. Такие планы должны включать шаги, необходимые для контроля значимой информации, которая обрабатывается или хранится, позволяя все же при этом организации вести дела.

Техническая безопасность охватывает **аппаратную и программную защиту**, а также **средства контроля системы связи**. Эти средства контроля выбираются в соответствии с рисками для обеспечения функциональных возможностей безопасности и доверия.

Функциональные возможности будут, например, охватывать идентификацию и аутентификацию, требования логического контроля доступа, потребности контрольного журнала/журнала безопасности, обеспечение безопасности с помощью обратного звонка,

аутентификацию сообщений, шифрование и т.д. Требования доверия документируют необходимый уровень доверия к функциям безопасности и, следовательно, объем и вид проверок, тестирования безопасности и т.д., необходимых для подтверждения этого уровня. При вынесении решения о дополняющем сочетании операционных и технических средств контроля будут существовать различные варианты выполнения технических требований безопасности. Для каждого варианта должна быть определена техническая архитектура безопасности, чтобы способствовать установлению того, что безопасность может быть обеспечена, как необходимо, и что это осуществимо с доступной технологией.

Организация может решить использовать оцененные (сертифицированные) продукты и системы как часть окончательного системного решения. Оцененными продуктами являются те, которые были изучены третьей стороной. Третья сторона может быть другой частью той же организации или независимой организацией, специализирующейся на оценивании продуктов и систем. Оценивание может проводиться по совокупности заранее установленных критериев, специально разработанных для создаваемой системы, или может использоваться обобщенная совокупность критериев, которая может применяться в разнообразных ситуациях. Критерии оценивания могут определять функциональные требования и/или требования доверия. Существует целый ряд систем оценивания, многие из которых финансируются правительством или международными организациями, занимающимися стандартизацией. Организация может решить использовать оцененные продукты и системы, когда ей необходима уверенность в том, что совокупность реализованных функциональных возможностей является такой, как требуется, и когда ей необходимо доверие к правильности и завершенности реализации этих функциональных возможностей. Альтернативным образом,

сконцентрированное практическое тестирование безопасности может предоставить гарантию уверенности в обеспечиваемой безопасности.

При выборе средств контроля для реализации следует рассматривать ряд факторов, включая:

- виды выполняемых функций — предотвращение, сдерживание, обнаружение, восстановление, исправление, мониторинг, информированность;
- относительную стойкость средств контроля;
- капитальные, операционные и эксплуатационные расходы на средства контроля;
- помощь, предоставляемую пользователям для выполнения их функций;
- простоту использования средства контроля для пользователя.

Обычно средство контроля будет выполнять более чем одну из этих функций. При изучении общей безопасности или совокупности средств контроля, которые должны использоваться, следует поддерживать баланс видов функций, если вообще это возможно. Это способствует тому, чтобы общая безопасность была более эффективной и продуктивной. Может требоваться анализ затрат и выгод, как и анализ компромиссных решений (метод сравнения соперничающих альтернатив, используя совокупность критериев, которые взвешиваются на предмет относительной значимости в отношении к конкретной ситуации).

Существуют две различные совокупности средств контроля, механизмов и/или процедур, которые могут использоваться для защиты информационных систем. С одной стороны, есть довольно много **организационных категорий средств контроля**, которые обычно применимы к каждой информационной системе или системе информационно-коммуникационных технологий, если конкретные обстоятельства вызывают в них необходимость, независимо от

индивидуальных компонентов. С другой стороны, существуют **средства контроля, характерные для систем ИКТ**; выбор этих средств контроля зависит от вида и характеристик рассматриваемой системы ИКТ. Конечно, всегда возможно, что одна или более из этих категорий или специфических средств контроля не нужны в данной системе ИКТ. Например, в шифровании может не быть необходимости, если для посылаемой или получаемой информации нет потребности в конфиденциальности.

Перед реализацией выбранных средств контроля их следует тщательно проверить на соответствие уже существующим и/или планируемым средствам контроля. Следует обдумать использование более детального анализа для выбора дополнительных средств контроля. Если средства контроля выбираются в соответствии с разными критериями (например, **базовые средства контроля** и **дополнительные средства контроля**), окончательная совокупность требующих реализации средств контроля должна объединяться с осторожностью.

После проверки нескольких систем ИКТ должно быть рассмотрено, может ли быть установлена базовая линия в масштабах организации. Другой возможностью выбора средств контроля без детального рассмотрения является применение характерных для приложений базовых линий. Например, руководства по базовым линиям доступны для телекоммуникаций, здравоохранения, банковского дела и много другого. При использовании этих руководств, например, есть возможность проверки существующих или планируемых средств контроля на соответствие рекомендованным.

Процесс выбора средств контроля всегда требует некоторых знаний о виде и характеристиках рассматриваемой информационной системы (например, автономная рабочая станция или рабочая станция, подсоединенная к сети), поскольку это оказывает существенное влияние на средства контроля, выбранные для защиты системы. Также полезно иметь представление об инфраструктуре, с точки зрения строений,

помещений и т.д. Еще одним важным фактором, вовлеченным в выбор средств контроля, является оценка существующих и/или планируемых средств контроля. Это помогает избежать ненужной работы, излишней траты времени, усилий и денежных средств.

Идентификация вида системы информационно-коммуникационных технологий

Для оценки существующей или планируемой системы ИКТ рассматриваемая система ИКТ должна быть сравнена со следующими компонентами и должны быть идентифицированы компоненты, представляющие систему. В последующих пунктах предлагаются средства контроля для каждого из перечисленных ниже компонентов. Компоненты для выбора включают:

- автономную рабочую станцию;
- рабочую станцию (клиент без коллективно используемых ресурсов), подсоединенную к сети;
- сервер или рабочую станцию с коллективно используемыми ресурсами, подсоединенную к сети.

Идентификация физических условий/условий внешней среды

Оценка внешней среды включает идентификацию физической инфраструктуры, поддерживающей существующую и планируемую систему ИКТ, а также соответствующих существующих и/или планируемых средств контроля. Поскольку все средства контроля должны быть совместимы с физической средой, эта оценка очень важна для успешного выбора.

При рассмотрении инфраструктуры могут быть полезны следующие вопросы.

Периметр и здание:

- Где расположено здание – на собственной площадке с забором по периметру или на улице с интенсивным движением и т.д.?
- У здания один или несколько арендаторов?
- Если арендаторов несколько, то кто остальные арендаторы?
- Где расположены значимые/критичные сферы?

Управление доступом:

- Кто имеет доступ к зданию?
- Существует ли система физического контроля доступа?
- Насколько прочна конструкция здания?
- Насколько прочны двери, окна и т.д., и какая защита им обеспечивается?
- Охраняется ли здание, и, если это так, происходит ли это в течение всех суток или только в рабочее время?
- Оснащено ли здание и/или помещения, в которых расположено критичное оборудование ИКТ, охранной сигнализацией?

Защита на местах:

- Как защищается помещение (помещения), содержащее систему ИКТ?
- Какие системы обнаружения возгорания, пожарной сигнализации и ликвидации пожара установлены и где?
- Какие системы обнаружения утечки воды/жидкости, сигнализации и ликвидации установлены и где?
- Существуют ли поддерживающие коммунальные услуги типа водопроводно-канализационной сети, системы бесперебойного питания, кондиционирования воздуха (для контроля температуры и влажности)?

Отвечая на эти вопросы, можно легко идентифицировать существующие физические средства контроля.

Подробную информацию о выборе средств контроля в определенных охраняемых сферах можно найти также в **ИСО/МЭК 17799:2005**.

Выбор средств контроля в соответствии с проблемами и угрозами безопасности

Первый шаг заключается в идентификации и оценке проблем безопасности. Должны учитываться требования конфиденциальности, целостности, доступности, учетности, подлинности и надежности. Мощность и количество выбранных средств контроля должны соответствовать оцененным проблемам безопасности. Во-вторых, для каждой проблемы безопасности составляется список типичных угроз и для каждой угрозы предлагаются средства контроля в соответствии с рассматриваемой системой ИКТ. Таким образом, можно удовлетворить конкретные потребности безопасности и направить защиту туда, где она действительно нужна.

Оценка проблем безопасности

Для эффективного осуществления выбора соответствующих средств контроля необходимо понимание проблем безопасности деловых операций, поддерживаемых рассматриваемой системой ИКТ. Если оценка подтверждает очень серьезные проблемы безопасности, рекомендуется более детальный подход, чтобы достичь соответствующей защиты.

Проблемы безопасности могут включать: потерю конфиденциальности; потерю целостности; потерю доступности; потерю учетности; потерю подлинности; потерю надежности.

Оценка должна включать саму систему ИКТ, хранящуюся или обрабатываемую в ней информацию и бизнес-операции, которые она выполняет. Это идентифицирует цели выбираемых средств контроля. Различные части системы ИКТ или хранящейся и обрабатываемой информации могут иметь разные проблемы безопасности. Поэтому важно связывать проблемы безопасности непосредственно с активами, поскольку

это влияет на угрозы, которые могут быть применимыми, и, следовательно, на выбор средств контроля.

Проблемы безопасности могут оцениваться путем рассмотрения того, причинят ли последствия сбоя или нарушения безопасности серьезный ущерб, незначительный ущерб или нулевой ущерб бизнес-операциям. Рассмотрение возможных угроз может помочь прояснить проблемы безопасности. Оценка должна проводиться отдельно для каждого актива, так как проблемы безопасности для различных активов могут быть разными. Однако при наличии достаточных знаний о проблемах безопасности активы с одинаковыми или сходными деловыми требованиями и проблемами безопасности могут быть объединены в группы.

Если более чем один вид информации обрабатывается системой ИКТ, то может потребоваться отдельное рассмотрение различных видов. Защита, предоставляемая системе ИКТ, должна быть достаточной для всех видов обрабатываемой информации.

В случае если все возможные потери конфиденциальности, целостности, доступности, учетности, подлинности и надежности идентифицированы как, вероятно, причиняющие лишь незначительный ущерб, то достаточную безопасность рассматриваемой системы ИКТ должен обеспечить **высокоуровневый** или **базовый подход**. В случае если любая из этих потерь идентифицирована как, вероятно, причиняющая серьезный ущерб, то нужно оценить, следует ли выбирать средства контроля дополнительно к тем, которые предлагаются ниже.

Потеря конфиденциальности

Рассмотреть последствия потери конфиденциальности (намеренной или ненамеренной) проверяемого актива (активов). Например, потеря конфиденциальности может приводить:

- к утрате общественного доверия или ухудшению общественного имиджа;
- правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных;
- неблагоприятному влиянию на политику организации;
- созданию угрозы личной безопасности;
- финансовым потерям.

В соответствии с ответами на приведенные выше вопросы должно быть принято решение, будут ли последствия, которые могут вытекать из потери конфиденциальности, серьезными, незначительными или нулевыми. Это решение должно быть задокументировано.

Потеря целостности

Рассмотреть последствия потери целостности (намеренной или ненамеренной) проверяемого актива (активов). Например, потеря целостности может приводить к:

- неверным принимаемым решениям;
- мошенничеству;
- нарушению деловых функций;
- утрате общественного доверия или ухудшению общественного имиджа;
- финансовым потерям;
- правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных.

В соответствии с ответами на приведенные выше вопросы должно быть принято решение, будут ли неблагоприятные последствия, которые могут вытекать из потери целостности, серьезными, незначительными или нулевыми. Это решение должно быть задокументировано.

Потеря доступности

Рассмотреть последствия кратковременной потери доступности приложений или информации, т.е. какие деловые функции в случае их прерывания приведут к невыполнению времени реагирования или времени выполнения. Должна быть также рассмотрена крайняя форма потери доступности, необратимая потеря данных и/или физическое разрушение аппаратных или программных средств. Например, потеря доступности критических приложений или информации может приводить к:

- неверным принимаемым решениям;
- неспособности выполнения критических задач;
- утрате общественного доверия или ухудшению общественного имиджа;
- финансовым потерям;
- правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных и из невыполнения договорных предельных сроков;
- значительным расходам на восстановление.

Следует отметить, что неблагоприятные последствия, вытекающие из потери доступности, могут значительно различаться для разных временных периодов такой потери. Если это так, то целесообразно рассмотреть последствия, которые могут проистекать в различные временные периоды, и оценить последствия для каждого временного периода как серьезные, незначительные или нулевые (эта информация должна использоваться при выборе средств контроля).

В соответствии с ответами на приведенные выше вопросы должно быть принято решение, будут ли неблагоприятные последствия, которые могут вытекать из потери доступности, серьезными, незначительными или нулевыми. Это решение должно быть задокументировано.

Потеря учетности

Рассмотреть последствия потери учетности пользователей системы или объектов (например, программных средств), действующих от имени пользователя. Кроме того, это рассмотрение должно включать автоматически генерируемые сообщения, которые могут приводить к действию. Например, потеря учетности может приводить к:

- манипулированию системой пользователями;
- мошенничеству;
- промышленному шпионажу;
- неотслеживаемым действиям;
- ложным обвинениям;
- правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных.

В соответствии с ответами на приведенные выше вопросы должно быть принято решение, будут ли неблагоприятные последствия, которые могут вытекать из потери учетности, серьезными, незначительными или нулевыми. Это решение должно быть задокументировано.

Потеря подлинности

Рассмотреть последствия потери подлинности данных и сообщений, независимо от того, используются ли они людьми или системами. Это особенно важно в распределенных системах, где принятые решения распространяются среди большого сообщества или где используется справочная информация. Например, потеря подлинности может приводить:

- к мошенничеству;
- использованию правомерного процесса с недействительными данными, приводящими к вводящему в заблуждение результату;
- манипулированию организацией посторонними лицами;

- промышленному шпионажу;
- ложным обвинениям;
- правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных.

В соответствии с ответами на приведенные выше вопросы должно быть принято решение, будут ли неблагоприятные последствия, которые могут вытекать из потери подлинности, серьезными, незначительными или нулевыми. Это решение должно быть задокументировано.

Потеря надежности

Рассмотреть последствия потери надежности систем. Кроме того, важно рассмотреть функциональные возможности, являющиеся подхарактеристикой надежности (смотри ИСО 9126:дата). Например, потеря надежности может приводить:

- к мошенничеству;
- потерянной доле на рынке;
- отсутствию мотивации у персонала;
- ненадежным поставщикам;
- потери доверия клиентов;
- правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных.

В соответствии с ответами на приведенные выше вопросы должно быть принято решение, будут ли неблагоприятные последствия, которые могут вытекать из потери надежности, серьезными, незначительными или нулевыми. Это решение должно быть задокументировано.

Средства контроля конфиденциальности

Ниже перечислены виды угроз, которые могут ставить в опасность конфиденциальность, вместе с предлагаемыми средствами контроля для защиты от этих угроз. Если это уместно для выбора средств контроля, то должны приниматься в расчет вид и характеристики системы ИКТ.

Угрозы приводятся в алфавитном порядке.

Подслушивание

Одним из способов получения доступа к значимой информации является подслушивание, например, путем подключения к линии или прослушивания телефонных разговоров. Средства контроля против этой угрозы перечисляются ниже.

- Физические средства контроля. Это могут быть помещения, стены, строения и т.д., делающие подслушивание невозможным или трудновыполнимым. Еще одним способом достижения этого является добавление помех. В случае телефонов соответствующая прокладка кабеля может обеспечить определенную защиту от подслушивания.

- Политика информационной безопасности. Другой способ избежать прослушивания заключается в наличии строгих правил, касающихся того, когда, где и каким способом должен происходить обмен значимой информацией.

- Защита конфиденциальности данных. Еще одним способом защиты от подслушивания является шифрование сообщения перед обменом сообщениями.

Электромагнитное излучение

Электромагнитное излучение может использоваться нарушителем для приобретения знаний об информации, обрабатываемой системой ИКТ. Средства контроля против электромагнитного излучения перечисляются ниже.

- Физические средства контроля. Это может быть облицовка комнат, стен и т.д.; эти средства контроля не позволяют электромагнитному излучению проходить через облицовку.

- Защита конфиденциальности данных. Следует отметить, что эта защита применима, только пока информация зашифрована, а не для

обрабатываемой, выводимой на экран или распечатываемой информации.

- Использование оборудования информационно-коммуникационных технологий с низким излучением. Может быть применено оборудование со встроенной защитой.

Вредоносное программное обеспечение

Вредоносное программное обеспечение может приводить к потере конфиденциальности, например, посредством перехвата и раскрытия паролей. Средства контроля против этого перечисляются ниже.

- Защита от вредоносного программного обеспечения.

- Менеджмент инцидентов информационной безопасности. Своевременное сообщение о необычном инциденте может ограничивать ущерб в случае атак со стороны вредоносного программного обеспечения. Обнаружение вторжения может использоваться для обнаружения попыток проникновения в систему или сеть.

Имитация личности пользователя

Имитация личности пользователя может быть использована, чтобы обойти аутентификацию и все сервисы и функции безопасности, связанные с этим. В итоге это может приводить к проблемам конфиденциальности, когда такая имитация дает возможность доступа к значимой информации. Средства контроля в этой сфере перечисляются ниже.

- Идентификация и аутентификация. Имитация значительно затрудняется, если используются средства контроля идентификации и аутентификации, основанные на комбинации чего-то известного пользователю, чего-то имеющегося у пользователя, а также неотъемлемых характеристик пользователя.

- Логический контроль доступа и аудит. Средства логического контроля доступа не могут отличить уполномоченного пользователя от

лица, выдающего себя за уполномоченного пользователя, но использование механизмов контроля доступа может уменьшить сферу влияния. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность.

- Защита от вредоносного программного обеспечения. Поскольку одним из способов получения паролей является введение вредоносного программного обеспечения для перехвата паролей, должна присутствовать защита против такого программного обеспечения.

- Сетевой менеджмент. Еще один способ захвата значимого материала состоит в том, чтобы выдать себя за пользователя в трафике, например в электронной почте. ИСО/МЭК работают сейчас над несколькими документами, содержащими дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности.

- Защита конфиденциальности данных. Если по некоторым причинам приведенный выше вид защиты невозможен или недостаточен, может быть обеспечена дополнительная защита, использующая шифрование хранимых значимых данных.

Неправильная маршрутизация/изменение маршрутизации сообщений

Неправильная маршрутизация – это умышленное или случайное неверное направление сообщений, тогда как изменение маршрутизации может происходить как с хорошими, так и с плохими целями. Изменение маршрутизации может, например, осуществляться для поддержки сохранности доступности. Неправильная маршрутизация и изменение маршрутизации сообщений могут приводить к потере конфиденциальности, если они делают возможным несанкционированный доступ к этим сообщениям. Средства контроля против этого перечисляются ниже.

- Сетевой менеджмент. Средства контроля для защиты от неправильной маршрутизации или изменения маршрутизации можно

найти в других документах, над которыми сейчас работают ИСО/МЭК и которые содержат дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности.

- Защита конфиденциальности данных. Чтобы избежать несанкционированного доступа в случае неправильной маршрутизации или измерения маршрутизации, сообщения могут шифроваться.

Сбой программы

Сбой программы может подвергать опасности конфиденциальность, если это программное средство обеспечивает защиту конфиденциальности, например, программные средства управления доступом или шифрования, или если сбой программы создает дыру, например, в операционной системе. Средства контроля для защиты конфиденциальности в этом случае перечисляются ниже.

- Менеджмент инцидентов. Каждый, кто замечает неправильное срабатывание программы, должен сообщить об этом ответственному лицу, чтобы как можно скорее могли быть приняты меры.

- Операционные вопросы. Некоторые сбои программ можно избежать путем тщательного тестирования программного средства перед его использованием и посредством контроля изменений программных средств.

Хищение

Хищение может подвергать опасности конфиденциальность, если похищенный компонент информационно-коммуникационных технологий содержит значимую информацию, к которой может получить доступ похититель. Средства контроля против хищения перечисляются ниже.

- Физические средства контроля. Это может быть физическая защита, затрудняющая доступ к строению, сфере или помещению, содержащим оборудование ИКТ, или специальные средства контроля против хищения.

- Кадровые. Должны существовать средства контроля для персонала (контроль внешнего персонала, соглашения об обеспечении конфиденциальности и т.д.), затрудняющие хищение.

- Защита конфиденциальности данных. Это средство контроля должно быть реализовано, если кажется вероятным хищение оборудования информационно-коммуникационных технологий, содержащего значимую информацию, например, лэптопов.

- Средства контроля носителей данных. Любой носитель данных, содержащий значимую информацию, должен быть защищен от хищения.

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям может быть угрозой, если возможен доступ к любому значимому материалу. Средства контроля для защиты от несанкционированного доступа включают соответствующую идентификацию и аутентификацию, логический контроль доступа, аудит на уровне системы ИКТ и сетевое разделение на сетевом уровне.

- Идентификация и аутентификация. Соответствующие средства контроля идентификации и аутентификации должны применяться в сочетании с логическим контролем доступа для предотвращения несанкционированного доступа.

- Логический контроль доступа и аудит. Должны использоваться механизмы управления доступом для обеспечения логического контроля доступа. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность лиц, имеющих права доступа к системе.

- Сетевое разделение. Чтобы затруднить несанкционированный доступ, должно существовать сетевое разделение.

- Физический контроль доступа. Помимо логического контроля доступа, защита может обеспечиваться физическим контролем доступа.

- Средства контроля носителей данных. Если значимые данные хранятся на другом носителе (например, дискете), должны присутствовать средства контроля носителей данных для защиты носителей от несанкционированного доступа.

- Защита конфиденциальности данных. Если по некоторым причинам приведенный выше вид защиты невозможен или недостаточен, может быть обеспечена дополнительная защита, использующая шифрование хранимых значимых данных.

Несанкционированный доступ к носителям данных

Несанкционированный доступ к носителям данных и их использование могут подвергать опасности конфиденциальность, если на этих носителях хранится любой конфиденциальный материал. Средства контроля для защиты конфиденциальности перечисляются ниже.

- Операционные вопросы. Могут быть применены средства контроля носителей данных для обеспечения, например, физической защиты и учетности носителей данных, а гарантированное удаление хранимой информации обеспечивает, чтобы никто не мог получить конфиденциальный материал с ранее стертого носителя данных. Особую заботу следует проявлять для обеспечения защиты сменных носителей, таких как дискеты, резервные магнитные ленты и бумажные носители.

- Физическая безопасность. Соответствующая защита комнат (прочные стены и окна, а также физический контроль доступа) и принадлежности защиты могут обеспечить защиту от несанкционированного доступа.

- Защита конфиденциальности данных. Дополнительная защита хранящегося значимого материала может быть достигнута путем

шифрования материала. Необходима хорошая система менеджмента ключей, позволяющая надежное применение шифрования.

Средства контроля целостности

Ниже перечислены виды угроз, которые могут подвергать опасности целостность, вместе с предлагаемыми средствами контроля для защиты от этих угроз. Если это уместно для выбора средств контроля, то должны приниматься в расчет вид и характеристики системы ИКТ.

Ухудшение состояния носителей данных

Ухудшение состояния носителей данных угрожает целостности всего, что хранится на этих носителях. Если целостность важна, должны применяться следующие средства контроля.

- Средства контроля носителей данных. Достаточные средства контроля носителей данных включают верификацию целостности, которая обнаруживает искажение хранящихся файлов.

- Резервные копии. Должны быть сделаны резервные копии всех важных файлов, деловых данных и т.д. Если обнаружена потеря целостности, например, с помощью средств контроля носителей данных или во время тестирования резервных копий, то для восстановления целостности файлов должна использоваться резервная копия или предыдущая генерация резервной копии.

- Защита целостности данных. Для защиты целостности хранящихся данных могут использоваться криптографические средства.

Ошибка технического обслуживания

- Если техническое обслуживание проводится нерегулярно или во время процесса технического обслуживания делаются ошибки, целостность всей связанной с этим информации подвергается опасности. Средства контроля для защиты целостности в данном случае перечисляются ниже.

- Техническое обслуживание. Правильное техническое обслуживание – это наилучший способ избежать ошибок технического обслуживания. Это включает задокументированные и проверенные процедуры технического обслуживания и соответствующий надзор за работой.

- Резервные копии. Если произошли ошибки технического обслуживания, то для восстановления целостности поврежденной информации могут использоваться резервные копии.

- Защита целостности данных. Для защиты целостности информации могут использоваться криптографические средства.

Вредоносное программное обеспечение

Вредоносное программное обеспечение может приводить к потере целостности, например, если данные или файлы изменяются человеком, получающим несанкционированный доступ с помощью вредоносного программного обеспечения, или самим вредоносным программным обеспечением. Средства контроля против этого перечисляются ниже.

- Защита от вредоносного программного обеспечения.

- Менеджмент инцидентов. Своевременное сообщение о необычном инциденте может ограничивать ущерб в случае атак со стороны вредоносного программного обеспечения. Обнаружение вторжения может использоваться для обнаружения попыток проникновения в систему или сеть.

Имитация личности пользователя

Имитация личности пользователя может быть использована, чтобы обойти аутентификацию и все сервисы и функции безопасности, связанные с этим. В итоге это может приводить к проблемам целостности, когда эта имитация дает возможность доступа к информации и ее модификации. Средства контроля в этой сфере перечисляются ниже.

- Идентификация и аутентификация. Имитация значительно затрудняется, если используются средства контроля идентификации и аутентификации, основанные комбинации чего-то известного пользователю, чего-то имеющегося у пользователя, а также неотъемлемых характеристик пользователя.

- Логический контроль доступа и аудит. Средства логического контроля доступа не могут отличить уполномоченного пользователя от лица, выдающего себя за уполномоченного пользователя, но использование механизмов контроля доступа может уменьшить сферу влияния. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность.

- Защита от вредоносного программного обеспечения. Поскольку одним из способов получения паролей является введение вредоносного программного обеспечения для перехвата паролей, должна присутствовать защита против такого программного обеспечения.

- Сетевой менеджмент. Еще один способ несанкционированного доступа состоит в том, чтобы выдать себя за пользователя в трафике, например в электронной почте. ИСО/МЭК работают сейчас над несколькими документами, содержащими дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности.

- Защита целостности данных. Если по некоторым причинам приведенный выше вид защиты невозможен или недостаточен, может быть обеспечена дополнительная защита, использующая криптографические средства, подобные цифровым подписям.

Неправильная маршрутизация/изменение маршрутизации сообщений

Неправильная маршрутизация – это умышленное или случайное неверное направление сообщений, тогда как изменение маршрутизации может происходить как с хорошими, так и с плохими целями. Изменение маршрутизации может, например, осуществляться для поддержки

сохранности доступности. Неправильная маршрутизация и изменение маршрутизации сообщений могут приводить к потере целостности, например, если сообщения изменяются, а затем посылаются исходным получателям. Средства контроля против этого перечисляются ниже.

- Сетевой менеджмент. Средства контроля для защиты от неправильной маршрутизации или изменения маршрутизации можно найти в других документах, над которыми сейчас работают ИСО/МЭК и которые содержат дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности.

- Защита целостности данных. Чтобы избежать несанкционированного изменения в случае неправильной маршрутизации или измерения маршрутизации, могут быть использованы хэш-функции и цифровые подписи.

Неотказуемостъ

Должны быть применены средства контроля неотказуемости, когда важно иметь подтверждение того, что сообщение было послано и/или получено и что сеть передала сообщение. В качестве основы неотказуемости (целостности данных и неотказуемости) существуют специальные криптографические средства контроля.

Сбой программы

Сбой программы может разрушить целостность данных и информации, которые обрабатываются с помощью этого программного средства. Средства контроля для защиты целостности перечисляются ниже.

- Сообщение о неправильном срабатывании программы. Скорейшее возможное сообщение о неправильном срабатывании программы помогает ограничить ущерб в случае сбоев программ.

- Операционные вопросы. Тестирование безопасности может использоваться для обеспечения правильного функционирования

программного обеспечения, а контроль изменений программных средств может помочь избежать проблем, вызванных модернизацией или другими изменениями программного обеспечения.

- Резервные копии. Резервные копии, например предыдущая генерация, могут быть использованы для восстановления целостности данных, которые обрабатывались программным обеспечением, функционирующим неверно.

- Защита целостности данных. Для защиты целостности информации могут использоваться криптографические средства.

Нарушения подачи (электроэнергии, кондиционирования воздуха)

Нарушения подачи могут вызывать проблемы целостности, если из-за них происходят другие сбои. Например, нарушение подачи может приводить к аппаратным сбоям, техническим повреждениям или проблемам с носителями данных. Средства контроля для защиты против этих конкретных проблем можно найти в соответствующих подразделах; средства контроля против нарушения подачи перечислены ниже.

- Энергоснабжение и кондиционирование воздуха. Соответствующие средства контроля энергоснабжения и кондиционирования воздуха, например защита от скачков напряжения, должны использоваться, где это необходимо, чтобы избежать любых проблем, происходящих в результате нарушения подачи.

- Резервные копии. Для восстановления любой поврежденной информации должны использоваться резервные копии.

Техническое повреждение

Технические повреждения, например, в сети, могут разрушать целостность информации, хранящейся или обрабатываемой в этой сети. Средства контроля для защиты против этого перечисляются ниже.

- Операционные вопросы. Менеджмент изменений и конфигурации, а также менеджмент возможностей должны

использоваться, чтобы избежать повреждений любой системы ИКТ или сети. Для обеспечения безотказной работы системы или сети используется документирование и техническое обслуживание.

- Сетевой менеджмент. Операционные процедуры, планирование системы и надлежащая сетевая конфигурация должны использоваться для сведения к минимуму рисков технических повреждений.

- Энергоснабжение и кондиционирование воздуха. Соответствующие средства контроля энергоснабжения и кондиционирования воздуха, например защита от скачков напряжения, должны использоваться, где это необходимо, чтобы избежать любых проблем, происходящих в результате нарушения подачи.

- Резервные копии. Для восстановления любой поврежденной информации должны использоваться резервные копии.

Ошибки передачи

Ошибки передачи могут разрушать целостность передаваемой информации. Средства контроля для защиты целостности перечисляются ниже.

- Прокладка кабелей. Тщательное планирование при прокладке кабелей может помочь избежать ошибок передачи, например, если ошибка вызвана перегрузкой.

- Сетевой менеджмент. Сетевое оборудование должно надлежащим образом управляться и поддерживаться, чтобы избегать ошибок передачи. ИСО/МЭК работают сейчас над несколькими документами, содержащими дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности, которые могут использоваться для защиты от ошибок передачи.

- Защита целостности данных. Для защиты от случайных ошибок передачи могут использоваться контрольные суммы или циклические избыточные коды в протоколах связи. Криптографические средства

могут использоваться для защиты целостности передаваемых данных в случае умышленных атак.

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям может быть угрозой для целостности информации, если возможно несанкционированное изменение. Средства контроля для защиты от несанкционированного доступа включают соответствующую идентификацию и аутентификацию, логический контроль доступа, аудит на уровне системы ИКТ и сетевое разделение на сетевом уровне.

- Идентификация и аутентификация. Соответствующие средства контроля идентификации и аутентификации должны применяться в сочетании с логическим контролем доступа для предотвращения несанкционированного доступа.

- Логический контроль доступа и аудит. Должны применяться средства контроля для обеспечения логического контроля доступа посредством использования механизмов контроля доступа. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность лиц, имеющих права доступа к системе.

- Сетевое разделение. Чтобы затруднить несанкционированный доступ, должно существовать сетевое разделение.

- Физический контроль доступа. Помимо логического контроля доступа, защита может обеспечиваться физическим контролем доступа.

- Средства контроля носителей данных. Если значимые данные хранятся на другом носителе (например, дискете), должны присутствовать средства контроля носителей данных для защиты носителей от несанкционированного доступа.

- Целостность данных. Для защиты целостности хранящейся или передаваемой информации могут использоваться криптографические средства.

Использование несанкционированных программ и данных

Использование несанкционированных программ и данных подвергает опасности целостность информации, хранящейся и обрабатываемой в системе, где это происходит, если программы и данные используются для изменения информации несанкционированным образом или если используемые программы и данные содержат вредоносное программное обеспечение (например, игры). Средства контроля для защиты от этого перечисляются ниже.

- Обучение и повышение осознания безопасности. Все служащие должны сознавать тот факт, что они не должны устанавливать и использовать никакое программное обеспечение без разрешения руководителя безопасности системы ИКТ или лица, отвечающего за безопасность системы.

- Резервные копии. Для восстановления любой поврежденной информации должны использоваться резервные копии.

- Идентификация и аутентификация. Соответствующие средства контроля идентификации и аутентификации должны применяться в сочетании с логическим контролем доступа для предотвращения несанкционированного доступа.

- Логический контроль доступа и аудит. Логический контроль доступа должен обеспечивать, чтобы применение программных средств для обработки и изменения информации осуществлялось только уполномоченными лицами. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность.

- Защита от вредоносного программного обеспечения. Все программы и данные должны проверяться на предмет вредоносного программного обеспечения перед их использованием.

Несанкционированный доступ к носителям данных

Несанкционированный доступ к носителям данных и их использование может подвергать опасности целостность, поскольку это делает возможным несанкционированное изменение информации, хранящейся на этих носителях данных. Средства контроля для защиты целостности перечисляются ниже.

- Операционные вопросы. Средства контроля носителей данных могут применяться, например, для обеспечения физической защиты и учетности носителей данных, чтобы избежать несанкционированного доступа, а верификация целостности – чтобы обнаруживать любую компрометацию целостности информации, хранящейся на носителях данных. Особую заботу следует проявлять для обеспечения защиты сменных носителей, таких как дискеты, резервные магнитные ленты и бумажные носители.

- Физическая безопасность. Соответствующая защита помещений (прочные стены и окна, а также физический контроль доступа) и принадлежности защиты могут обеспечить защиту от несанкционированного доступа.

- Целостность данных. Для защиты целостности информации, хранящейся на носителях данных, могут использоваться криптографические средства.

Ошибки пользователей

Ошибки пользователей могут разрушать целостность информации. Средства контроля для защиты от этого перечисляются ниже.

- Обучение и повышение осознания безопасности. Все пользователи должны быть соответствующим образом обученными,

чтобы избегать ошибок пользователей при обработке информации. Это должно включать обучение определенным процедурам для конкретных действий, таким как операционные процедуры или процедуры безопасности.

- Резервные копии. Резервные копии, например, предыдущая генерация, могут использоваться для восстановления целостности информации, которая была разрушена из-за ошибок пользователей.

Средства контроля доступности

Ниже перечислены виды угроз, которые могут подвергать опасности доступность, вместе с предлагаемыми средствами контроля для защиты от этих угроз. Если это уместно для выбора средств контроля, то должны приниматься в расчет вид и характеристики системы ИКТ.

Следует отметить, что большинство из обсуждающихся средств контроля обеспечивает более «общую» защиту, т.е. они не направлены на конкретные угрозы, а обеспечивают защиту путем поддержки общего эффективного менеджмента информационной безопасности. Поэтому они не перечисляются здесь в деталях, но их эффект не следует недооценивать и они должны реализовываться для обеспечения общей эффективной защиты.

Требования доступности могут колебаться от некритичных в отношении времени данных или систем ИКТ (однако потеря таких данных и недоступность таких систем все же считается критичной) до крайне критичных в отношении времени данных или систем ИКТ. Защита первых может быть обеспечена с помощью резервных копий, тогда как последние могут требовать наличия какой-либо устойчивой системы. Угрозы приводятся в алфавитном порядке.

Разрушительная атака

Информация может быть разрушена путем разрушительных атак. Средства контроля для защиты от этого перечисляются ниже.

- Дисциплинарный процесс. Все служащие должны сознавать последствия в случае разрушения ими информации (намеренно или ненамеренно).

- Средства контроля носителей данных. Все носители данных должны быть соответствующим образом защищены от несанкционированного доступа, используя физическую защиту и учетность всех носителей данных.

- Резервные копии. Должны быть сделаны резервные копии всех важных файлов, деловых данных и т.д. Если файл или какая-либо иная информация недоступны (по каким-либо причинам), то для восстановления информации должна использоваться резервная копия или предыдущая генерация резервной копии.

- Физическая защита. Чтобы избежать любой несанкционированный доступ, который будет способствовать несанкционированному разрушению оборудования ИКТ или информации, должны использоваться физические средства контроля доступа.

- Идентификация и аутентификация. Соответствующие средства контроля идентификации и аутентификации должны применяться в сочетании с логическим контролем доступа для предотвращения несанкционированного доступа.

- Логический контроль доступа и аудит. Логический контроль доступа должен обеспечивать, чтобы не мог произойти никакой несанкционированный доступ к информации, который делает возможным разрушение этой информации. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность.

Ухудшение состояния носителей данных

Ухудшение состояния носителей данных угрожает доступности всего, что хранится на этих носителях. Если доступность важна, должны применяться следующие средства контроля.

- Средства контроля носителей данных. Регулярное тестирование носителей данных должно обнаруживать любое ухудшение состояния, надо надеяться, до того как информация будет реально недоступна. Носители данных должны храниться таким образом, чтобы любое внешнее влияние, которые может вызвать ухудшение состояния, не могло иметь места.

- Резервные копии. Должны быть сделаны резервные копии всех важных файлов, деловых данных и т.д. Если файл или какая-либо иная информация недоступны (по каким-либо причинам), то для восстановления информации должна использоваться резервная копия или предыдущая генерация резервной копии.

Отказ оборудования и услуг связи

Отказ оборудования и услуг связи угрожает доступности информации, передаваемой с помощью этих услуг. Средства контроля для защиты доступности перечисляются ниже.

- Избыточность и резервные копии. Избыточная реализация компонентов услуг связи может быть использована для снижения вероятности отказа услуг связи. В зависимости от максимально приемлемого времени простоя резервное оборудование тоже может быть использовано для удовлетворения требований. В любом случае должна быть сделана резервная копия данных конфигурации и топологии, чтобы обеспечить доступность в случае чрезвычайной ситуации.

- Сетевой менеджмент. ИСО/МЭК работают сейчас над несколькими документами, содержащими дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности,

которые могут применяться для защиты от отказа оборудования или услуг связи.

- Прокладка кабелей. Тщательное планирование при прокладке кабелей может помочь избежать повреждения; если есть подозрение, что линия может быть повреждена, она должна быть внимательно проверена.

- Неотказуемость. Если нужно подтверждение сетевой доставки, отправки или получения сообщения, должна применяться неотказуемость – тогда сбой связи или пропавшая информация могут быть легко обнаружены.

Пожар, затопление

Информация и оборудование информационно-коммуникационных технологий могут быть разрушены пожаром и/или затоплением. Средства контроля для защиты против пожара и затопления перечисляются ниже.

- Физическая защита. Все строения и помещения, содержащие оборудование информационно-коммуникационных технологий или носители, на которых хранится важная информация, должны быть защищены соответствующим образом от пожара и затопления.

- План обеспечения непрерывности бизнеса. Для обеспечения защиты бизнеса от пагубных эффектов пожара и затопления должен существовать план обеспечения непрерывности бизнеса и должны быть доступны резервные копии всей важной информации.

Ошибка технического обслуживания

Если техническое обслуживание проводится нерегулярно или во время процесса технического обслуживания делаются ошибки, доступность всей связанной с этим информации подвергается опасности. Средства контроля для защиты доступности в данном случае перечисляются ниже.

- Техническое обслуживание. Правильное техническое обслуживание – это наилучший способ избежать ошибок технического обслуживания.

- Резервные копии. Если произошли ошибки технического обслуживания, то для восстановления доступности потерянной информации могут использоваться резервные копии.

Вредоносное программное обеспечение

Вредоносное программное обеспечение может быть использовано, чтобы обойти аутентификацию и все сервисы и функции безопасности, связанные с этим. В итоге это может приводить к потере доступности, например, если данные или файлы разрушаются человеком, получившим несанкционированный доступ с помощью вредоносного программного обеспечения, или самим вредоносным программным обеспечением. Средства контроля против этого перечисляются ниже.

- Защита от вредоносного программного обеспечения.

- Менеджмент инцидентов. Своевременное сообщение о необычном инциденте может ограничивать ущерб в случае атак со стороны вредоносного программного обеспечения. Обнаружение вторжения может использоваться для обнаружения попыток вхождения в систему или сеть.

Имитация личности пользователя

Имитация личности пользователя может быть использована, чтобы обойти аутентификацию и все сервисы и функции безопасности, связанные с этим. В итоге это может приводить к проблемам доступности, когда эта имитация ведет к возможности удаления или разрушения информации. Средства контроля в этой сфере перечисляются ниже.

- Идентификация и аутентификация. Имитация значительно затрудняется, если используются средства контроля идентификации и

аутентификации, основанные на комбинации чего-то известного пользователю, чего-то имеющегося у пользователя, а также неотъемлемых характеристик пользователя.

- Логический контроль доступа и аудит. Средства логического контроля доступа не могут отличить уполномоченного пользователя от лица, выдающего себя за уполномоченного пользователя, но использование механизмов контроля доступа может уменьшить сферу влияния. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность.

- Защита от вредоносного программного обеспечения. Поскольку одним из способов получения паролей является введение вредоносного программного обеспечения для перехвата паролей, должна присутствовать защита против такого программного обеспечения.

- Сетевой менеджмент. Еще один способ несанкционированного доступа состоит в том, чтобы выдать себя за пользователя в трафике, например в электронной почте. ИСО/МЭК работают сейчас над несколькими документами, содержащими дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности.

- Резервное копирование данных. Резервное копирование данных не может защитить от имитации личности пользователя, но уменьшает последствия наносящих ущерб инцидентов, вытекающих из этого.

Неправильная маршрутизация/изменение маршрутизации сообщений

Неправильная маршрутизация - это умышленное или случайное неверное направление сообщений, тогда как изменение маршрутизации может происходить как с хорошими, так и с плохими целями. Изменение маршрутизации может, например, осуществляться для поддержки сохранности доступности. Неправильная маршрутизация сообщений приводит к потере доступности сообщений. Средства контроля против этого перечисляются ниже.

- Сетевой менеджмент. Средства контроля для защиты от неправильной маршрутизации или изменения маршрутизации можно найти в других документах, над которыми сейчас работают ИСО/МЭК и которые содержат дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности.

- Неотказуемость. Если нужно подтверждение сетевой доставки, отправки или получения сообщения, должна применяться неотказуемость.

Злоупотребление ресурсами

Злоупотребление ресурсами может приводить к недоступности информации или услуг. Средства контроля для защиты от этого перечисляются ниже.

- Кадровые. Весь персонал должен сознавать последствия злоупотребления ресурсами; в случае необходимости должны применяться дисциплинарные процессы.

- Операционные вопросы. Использование системы должно подвергаться мониторингу для обнаружения несанкционированной деятельности, а для сведения к минимуму возможностей злоупотребления привилегиями должно применяться разделение обязанностей.

- Идентификация и аутентификация. Соответствующие средства контроля идентификации и аутентификации должны применяться в сочетании с логическим контролем доступа для предотвращения несанкционированного доступа.

- Логический контроль доступа и аудит. Средства контроля должны использоваться для обеспечения логического контроля доступа к ресурсам посредством применения механизмов контроля доступа. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность.

- Сетевой менеджмент. Соответствующая сетевая конфигурация и разделение должны применяться для сведения к минимуму возможности злоупотребления сетевыми ресурсами.

Природные бедствия

Для обеспечения защиты от потери информации и услуг из-за природных бедствий должны существовать следующие средства контроля.

- Защита от природных бедствий. Должна быть обеспечена максимальная возможная защита всех зданий от природных бедствий.

- План обеспечения деловой непрерывности. Для каждого здания должен существовать полностью протестированный план обеспечения деловой непрерывности и должны быть доступны резервные копии всей важной информации, резервы услуг и ресурсов.

Сбой программы

Сбой программы может разрушить доступность данных и информации, которые обрабатываются соответствующим программным обеспечением. Средства контроля для защиты доступности перечисляются ниже.

- Сообщение о неправильном срабатывании программы. Скорейшее возможное сообщение о неправильном срабатывании программы помогает ограничить ущерб в случае сбоев программ.

- Операционные вопросы. Тестирование безопасности может использоваться для обеспечения правильного функционирования программного обеспечения, а контроль изменений программных средств может помочь избежать связанных с программными средствами проблем, которые вызваны модернизацией или другими изменениями программного обеспечения.

- Резервные копии. Резервные копии, например, предыдущая генерация, могут быть использованы для восстановления данных,

которые обрабатывались программным обеспечением, функционирующим неверно.

Нарушения подачи (электроэнергии, кондиционирования воздуха)

Нарушения подачи могут вызывать проблемы доступности, если из-за них происходят другие сбои. Например, нарушение подачи может приводить к аппаратным сбоям, техническим повреждениям или проблемам с носителями данных. Средства контроля для защиты против этих конкретных проблем можно найти в соответствующих подразделах; средства контроля против нарушения подачи перечислены ниже.

- Энергоснабжение и кондиционирование воздуха. Соответствующие средства контроля энергоснабжения и кондиционирования воздуха, например защита от скачков напряжения, должны использоваться, где это необходимо, чтобы избежать любых проблем, происходящих в результате нарушения подачи.

- Резервные копии. Должны быть сделаны резервные копии всех важных файлов, деловых данных и т.д. Если файл или какая-либо иная информация теряются из-за нарушения подачи, то для восстановления информации должны использоваться резервные копии.

Техническое повреждение

Технические повреждения, например, в сети, могут разрушать доступность любой информации, хранящейся или обрабатываемой в этой сети. Средства контроля для защиты против этого перечисляются ниже.

- Операционные вопросы. Менеджмент изменений и конфигурации, а также менеджмент возможностей должны использоваться, чтобы избежать повреждений любой системы ИКТ. Документирование и техническое обслуживание используются для обеспечения безотказного функционирования системы.

- Сетевой менеджмент. Операционные процедуры, планирование системы и надлежащая сетевая конфигурация должны использоваться для сведения к минимуму рисков технических повреждений.

- План обеспечения непрерывности бизнеса. Для обеспечения защиты бизнеса от пагубных эффектов технических повреждений должен существовать план обеспечения деловой непрерывности и должны быть доступны резервные копии всей важной информации, резервы услуг и ресурсов.

Хищение

Очевидно, что хищение подвергает опасности доступность информации и оборудования ИКТ. Средства контроля для защиты против хищения перечисляются ниже.

- Физические средства контроля. Это может быть физическая защита, затрудняющая доступ к строению, сфере или помещению, содержащим оборудование ИКТ и информацию, или специальные средства контроля против хищения.

- Кадровые. Должны существовать средства контроля для персонала (контроль внешнего персонала, соглашения об обеспечении конфиденциальности и т.д.), затрудняющие хищение.

- Средства контроля носителей данных. Любые носители данных, содержащие важный материал, должны быть защищены от хищения.

Перегрузка трафика

Перегрузка трафика угрожает доступности информации, передаваемой с помощью этих служб. Средства контроля для защиты доступности перечисляются ниже.

- Избыточность и резервные копии. Избыточная реализация компонентов служб связи может быть использована для снижения вероятности перегрузки трафика. В зависимости от максимально приемлемого времени простоя резервное оборудование тоже может быть

использовано для удовлетворения требований. В любом случае должна быть сделана резервная копия данных конфигурации и топологии, чтобы обеспечить доступность в случае чрезвычайной ситуации.

- Сетевой менеджмент. Надлежащая конфигурация, менеджмент и администрирование сетей и служб связи должны использоваться, чтобы избежать перегрузки трафика. ИСО/МЭК разрабатывают сейчас документы, содержащие дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности, которые могут применяться для защиты от перегрузки трафика.

Ошибки передачи

Ошибки передачи могут разрушать доступность передаваемой информации. Средства контроля для защиты доступности перечисляются ниже.

- Прокладка кабелей. Тщательное планирование при прокладке кабелей может помочь избежать ошибок передачи, например, если ошибка вызвана перегрузкой.

- Сетевой менеджмент. Сетевой менеджмент не может защитить от ошибок передачи, но может использоваться для распознания проблем, происходящих из-за ошибок передачи и для поднятия тревоги в таких случаях. Это позволяет осуществить своевременное реагирование на эти проблемы. ИСО/МЭК разрабатывают сейчас документы, содержащие дальнейшую информацию о детальных средствах контроля для обеспечения сетевой безопасности, которые могут применяться для защиты от ошибок передачи.

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям может быть угрозой для доступности информации, если возможно несанкционированное разрушение. Средства контроля для

защиты от несанкционированного доступа включают соответствующую идентификацию и аутентификацию, логический контроль доступа, аудит на уровне системы ИКТ и сетевое разделение на сетевом уровне.

- Идентификация и аутентификация. Соответствующие средства контроля идентификации и аутентификации должны применяться в сочетании с логическим контролем доступа для предотвращения несанкционированного доступа.

- Логический контроль доступа и аудит. Должны применяться средства контроля для обеспечения логического контроля доступа посредством использования механизмов контроля доступа. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность лиц, имеющих права доступа к системе.

- Сетевое разделение. Чтобы затруднить несанкционированный доступ, должно существовать сетевое разделение.

- Физический контроль доступа. Помимо логического контроля доступа защита может обеспечиваться физическим контролем доступа.

- Средства контроля носителей данных. Если значимые данные хранятся на других носителях (например, дискете), должны присутствовать средства контроля носителей данных для защиты носителей от несанкционированного доступа.

Использование несанкционированных программ и данных

Использование несанкционированных программ и данных подвергает опасности доступность информации, хранящейся и обрабатываемой в системе, где это происходит, если программы и данные используются для удаления информации или если используемые программы и данные содержат вредоносное программное обеспечение (например, игры). Средства контроля для защиты от этого перечисляются ниже.

- Обучение и повышение осознания безопасности. Все служащие должны сознавать тот факт, что они не должны внедрять никакое программное обеспечение без разрешения руководителя безопасности системы ИКТ или лица, отвечающего за безопасность системы.

- Резервные копии. Для восстановления любой поврежденной или потерянной информации, сервисов или ресурсов должны использоваться резервные копии.

- Идентификация и аутентификация. Соответствующие средства контроля идентификации и аутентификации должны применяться в сочетании с логическим контролем доступа для предотвращения несанкционированного доступа.

- Логический контроль доступа и аудит. Логический контроль доступа должен обеспечивать, чтобы применение программных средств обработки и удаления информации осуществлялось только уполномоченными лицами. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность.

- Защита от вредоносного программного обеспечения. Все программы и данные должны проверяться на предмет вредоносного программного обеспечения перед их использованием.

Несанкционированный доступ к носителям данных

Несанкционированный доступ к носителям данных и их использование могут подвергать опасности доступность, поскольку это может приводить к несанкционированному разрушению информации, хранящейся на этих носителях данных. Средства контроля для защиты доступности перечисляются ниже.

- Операционные вопросы. Средства контроля носителей данных могут применяться, например, для обеспечения физической защиты и учетности носителей данных, чтобы избежать несанкционированного доступа к информации, хранящейся на носителях данных. Особую заботу

следует проявлять для обеспечения защиты сменных носителей, таких как дискеты, резервные магнитные ленты и бумажные носители.

- Физическая безопасность. Соответствующая защита комнат (прочные стены и окна, а также физический контроль доступа) и принадлежности защиты могут обеспечить защиту от несанкционированного доступа.

Ошибки пользователей

Ошибки пользователей могут разрушать доступность информации. Средства контроля для защиты от этого перечисляются ниже.

- Обучение и повышение осознания безопасности. Все пользователи должны быть соответствующим образом обученными, чтобы избегать ошибок пользователей при обработке информации. Это должно включать обучение определенным процедурам для конкретных действий, таким как операционные процедуры или процедуры безопасности.

- Резервные копии: Резервные копии, например, предыдущая генерация, могут использоваться для восстановления информации, которая была разрушена из-за ошибок пользователей.

Средства контроля учетности, подлинности и надежности

Рамки учетности, подлинности и доступности широко различаются в разных сферах. Эти различия означают, что может применяться множество различных средств контроля. Поэтому ниже может быть дано лишь общее руководство.

Средства контроля, обсуждавшиеся выше, обеспечивают более «общую» защиту, т.е. они направлены на целый диапазон угроз и обеспечивают защиту путем поддержки общего эффективного менеджмента информационной безопасности. Поэтому они не перечисляются здесь, но их эффект не следует недооценивать, и они должны реализовываться для обеспечения общей эффективной защиты.

Учетностъ

Для обеспечения защиты учетности должны рассматриваться любые угрозы, которые могут приводить к предпринимаемым действиям, которые не могут быть приписаны конкретной сущности или субъекту. Примерами таких угроз являются коллективное использование учетной записи, отсутствие прослеживаемости действий, имитация личности пользователя, сбой программы, несанкционированный доступ к компьютерам, данным, сервисам и приложениям и слабая аутентификация.

Существуют два вида учетности, которые следует рассматривать. Один из них имеет дело с идентификацией пользователя, ответственного за определенные действия по отношению к информации и системам ИКТ. Это могут обеспечивать контрольные журналы. Другой вид связан с учетностью между пользователями в системе. Услуги неотказуемости, разделенное знание или двойной контроль могут достигать этого.

Многие средства контроля могут использоваться для осуществления учетности или могут способствовать ее осуществлению. Могут быть применимы средства контроля, простирающиеся от таких вещей, как политики безопасности, повышение осознания безопасности, логический контроль доступа и аудит, до одноразовых паролей и средств контроля носителей данных. Реализация политики в отношения владения информацией является необходимым условием учетности. Выбор определенных средств контроля будет зависеть от конкретного использования учетности в рамках данной сферы.

Подлинность

Уверенность в подлинности может быть снижена любой угрозой, которая может приводить к неуверенности человека, системы или процесса в том, что объект является таким, как подразумевается. Некоторые примеры, которые могут приводить к возникновению такой

ситуации, включают не контролируемые изменения данных, не проверяемый источник данных, не поддерживаемый источник данных.

Многие средства контроля могут использоваться для обеспечения подлинности или могут способствовать ее обеспечению. Могут быть применимы средства контроля, простирающиеся от использования данных с помеченной ссылкой, логического контроля доступа и аудита до использования цифровых подписей. Выбор определенных средств контроля будет зависеть от конкретного использования подлинности в рамках данной сферы.

Надежность

Любая угроза, которая может приводить к несоответствующему поведению систем или процессов, будет давать в результате снижение надежности. Некоторыми примерами таких угроз являются несоответствующее функционирование системы и ненадежные поставщики. Потеря надежности может приводить к плохому обслуживанию клиентов или утрате доверия клиентов.

Многие средства контроля могут использоваться для обеспечения надежности или могут способствовать ее обеспечению. Могут быть применимы средства контроля, простирающиеся от таких вещей, как планы обеспечения деловой непрерывности, введение избыточности в физическую архитектуру и техническое обслуживание системы до идентификации и аутентификации и логического контроля доступа и аудита. Выбор определенных средств контроля будет зависеть от конкретного использования надежности в рамках данной сферы.

Выбор средств контроля (мер защиты) в соответствии с проектом стандарта ГОСТ Р ИСО/МЭК 13335-4-2007

Стандарт рассматривает два существующих главных подходов к выбору защитных мер: использование базового подхода и выполнение детального анализа риска.

При базовом подходе, чтобы выбрать подходящие защитные меры, необходимо определить базовые оценки безопасности систем ИТ вне зависимости от того, будет ли затем проводиться детальный анализ рисков. Для этого надо рассмотреть следующие вопросы: для какого типа системы ИТ предполагается выбор защитных мер (например, автономный или подсоединенный к сети персональный компьютер); где находятся системы ИТ, каковы условия окружающей среды в месте расположения этих систем; какие защитные меры уже приняты и/или планируются; насколько полученные оценки предоставляют достаточную информацию для выбора базовых защитных мер для системы ИТ.

Раздел 8 Стандарта содержит обзор возможных защитных мер, которые предполагается реализовать для повышения уровня безопасности. Они разделены на организационные, технические (т.е. выборка проведена в соответствии с потребностями и нарушениями обеспечения безопасности, а также с учетом ограничений) и на специальные защитные меры систем ИТ. Все защитные меры сгруппированы по категориям. Для каждой категории защитных мер приведено описание наиболее типичных защитных мер, включая краткое описание уровня безопасности, которую они должны обеспечивать. Специальные защитные меры в рамках установленных категорий и их подробное описание можно найти в документах по базовой безопасности (ссылки в приложениях A – H).

Использование каталогов защитных мер

Существует несколько известных каталогов с защитными мерами. Самый большой из них, по-видимому, содержится в германском стандарте **IT-Grundschutz**

Каталог, доступный по адресу http://www.bsi.bund.de/gshb/english/menue.htm, содержит следующие группы контрмер для обеспечения безопасности:

- поддерживающей инфраструктуры;

- на организационном уровне;
- на кадровом уровне;
- программного обеспечения и вычислительной техники;
- коммуникаций;
- непрерывности бизнеса.

Детальное описание контрмер на английском языке можно найти на сайте http://www.bsi.bund.de/ gshb/english/s/s1000.htm .

На практике можно встретить коммерческие продукты, реализующие защитные меры в некотором наборе. Приведем наиболее встречающиеся средства защиты, большинство из которых относятся к сетевой безопасности.

Средства обнаружения атак (IDS).

Средства предотвращения атак (IPS).

Виртуальные частные сети (VPN).

Межсетевые экраны (Firewalls).

Антивирусные средства.

Антишпионское ПО.

Средства фильтрации спама.

Биометрические средства защиты.

Средства мониторинга и фильтрации содержимого электронной почты и веб-ресурсов.

Средства криптографии.

Системы централизованного управления средствами защиты информации.

Средства защиты от НСД.

PKI-решения.

Средства защиты от утечки по техническим каналам.

Средства защиты телефонных систем.

Системы мониторинга событий безопасности.

Средства аутентификации.

Системы резервного копирования и системы их защиты.

Средства гарантированного уничтожения информации и носителей.

Системы защиты от инсайдеров.

Системы слежения за пользователем.

Системы защиты электронного документооборота.

Системы защиты жестких дисков и каталогов.

Средства защиты операционных систем (ОС).

Средства поиска уязвимостей в сетях.

Средства противодействия электромагнитным излучениям и наводкам (ПЭМИН).

Средства защиты от USB-флешек.

Системы видео- и аудионаблюдения.

Некоторые из приведенных выше мер защиты будут подробно изучаться в других смежных курсах по информационной безопасности («Современная прикладная криптография», «Технические средства защиты информации», «Защита информации с использованием интеллектуальных карт»), другие требуют изучения большого дополнительного материала (например, по сетевым технологиям) и при изучении основ информационной безопасности могут рассматриваться только при выполнении курсовых работ и дополнительных заданий.

ЛИТЕРАТУРА

Литература расположена по годам выпуска. Многие из приведенных источников использовались при подготовке данного пособия. Те разделы курса по информационной безопасности, которые не удалось рассмотреть или рассмотрены недостаточно подробно, можно найти в приводимых ниже источниках или в их списках литературы.

1. Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике. – М.: ИЛ, 1963.

2. Хоффман Л.Д. Современные методы защиты информации. – М.: Сов.радио, 1980.

3. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ. – М.: Мир, 1982.

4. Denning D. Cryptography and data security. Addison- Weslay Publishing Company. 1982. – 400 p.

5. ТИИЭР т. 76, № 5. Защита информации. Малый тематический выпуск. – М.: Мир, 1988.

6. Russel D., G.T.Gangemi Sr. Computer Security Basics. – O`Reilli & Associates, Inc., 1991. – 448 p.

7. Jackson K., Hruska J. (Ed.) Computer Security Reference Book. Butterworth-Heinemann Ltd., 1992. – 932 p.

8. Спесивцев А.В., Вегнер В.А. и др. Защита информации в персональных ЭВМ. – М.: Радио и связь, 1992. – 191 с.

9. Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 1993.

10. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. – М.: Яхтсмен, 1993. – 188 с.

11. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994, Кн. 1 и 2.

12. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Единая Европа, 1994.

13. Михайлов С.Ф., Петров В.А., Тимофеев Ю.А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие. – М.: МИФИ, 1995. – 112 с.

14. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: Учебное пособие. – М.: МИФИ, 1995.

15. Горохов П.К. Информацинная безопасность. Англо-русский словарь. – М.: Радио и связь, 1995. – 224 с.

16. Garfinkel S. PGP: Pretly Good Privacy. – O'Reilly and Associates, Inc., 1995.

17. Stinson D. Cryptography: theory and practice. CRC Press, 1995.

18. Hoffman L. (Ed.) Building in big Brother: the cryptography policy debate. Springer-Verlag NewYork. Inc., 1995. – 560 p.

19. Kaufman C., Pelman R., Speciner M. Network Security – PRIVATE Communication in a PUBLIC World, Prentice-Hall, Inc.,1995.

20. Варфоломеев А.А., Пеленицин М.Б. Методы криптографии и их применение в банковских технологиях. – М.: МИФИ, 1995. – 116 стр.

21. Варфоломеев А.А., Гаврилкевич М.В., Устюжанин Д.Д., Фомичев В.М. Методические указания к выполнению лабораторного практикума «Информационная безопасность. Криптографические методы защиты информации», ч. 1, 2. – М.: МИФИ, 1995. – 44 с.

22. Schneier B. Applied cryptography, second edition: protocols, algorithms, and source code in C. J. Wiley & sons, Inc. 1996. – 758 pp.

Русский перевод: Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

23. Menezes A., Van Oorschot P., Vanstone S. Handbook of Applied cryptography. CRC Press, 1996. – 816 с.

24. Теория и практика обеспечения информационной безопасности. Под ред. Зегжды П.Д. – М.: Яхтсмен, 1996.

25. Грушо А.А., Тимонина Е.Е. Основы защиты информации. – М.: Яхтсмен, 1996. – 192 с.

26. Тайли Э. Безопасность персонального компьютера. – Мн.: ООО Попурри, 1997. – 480 с.

27. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 1997. – 538 с.

28. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. – СПб.: НПО Мир и семья, 1997.

29. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Ось-89, 1998. – 336 с.

30. Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. – СПб: СПбГУ, 1998. – 328 с.

31. Варфоломеев А.А., Жуков А.Е. и др. Блочные криптосистемы. Основные свойства и методы анализа стойкости. – М.: МИФИ, 1998. – 198 стр.

32. Эдвардс М.Дж. Безопасность в Интернете на основе Windows NT. – М.: ТОО Channel Trading Ltd. – 1999. – 656 с.

33. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328 с.

34. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб: СПбГУ, 1999. – 368 с.

35. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности, – М: Радио и связь, 2000. – 192 с.

36. Зегжда Д., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

37. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: Учебное пособие. – М.: ЮНИТИ-ДАНА, 2000. – 527 с.

38. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах, – М: Радио и связь, 2000. – 168 с.

39. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.: СИНТЕГ, 2000. – 248 с.

40. Ярочкин В.И. Информационная безопасность. – М.: Международные отношения, 2000. – 400 с.

41. Анин Б. Защита компьютерной информации. – СПб.: БХВ-Санкт-Петербург, 2000. – 384 с.

42. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.

43. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.

44. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРБ, 2001. – 480 с.

45. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия – Телеком, 2001. – 148 с.

46. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. – М.: Юрист, 2001. – 415 с.

47. Голдовский И. Безопасность платежей в Интернете. – СПб: Питер, 2001. – 240 с.

48. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. – Мн.: БГУ, 2001. – 190 с.

49. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий. – М.: Издательство СИП РИА, 2001. – 356 с.

50. Стрельцов А.А. Обеспечение информационной безопасности России. – М.: МЦНМО, 2002. – 296.

51. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2002. – 432 с.

52. Бармен С. Разработка правил информационной безопасности. – М.: Вильямс, 2002. – 208 с.

53. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб.: Питер, 2002. – 848 с.

54. Смит Р. Аутентификация: от паролей до открытых ключей. – М.: Вильямс, 2002. – 432 с.

55. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки: Учебное пособие. – М.: РГГУ, 2002. – 399 с.

56. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. – М.: Бином-Пресс, 2002. – 384 с.

57. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер. – М.: Гелиос АРБ, 2002. – 256 с.

58. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие. – М.: Радио и связь. 2003. – 296 с.

59. Конеев И., Беляев А. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752с.

60. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб, 2003. http://lib.aldebaran.ru/author/shnaier_bryus/shnaier_bryus_sekrety_i_lozh_bezopasnost_dannyh_v_cifrovom_mire/

61. Парфенов В.И. Защита информации: Словарь. – Воронеж.: НП РЦИБ Факел, 2003. – 292 с.

62. Царегородцев А.В. Информационная безопасность в распределенных управляющих системах. – М.: РУДН, 2003.

63. Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2003. – 192 с.

64. Скляров Д.В., Искусство защиты и взлома информации. – СПб.: БХВ – Петербург, 2004. – 288 с.

65. Галатенко В.А. Стандарты информационной безопасности: Курс лекций. –М.: ИНТУИТ. РУ, 2004. – 328 с.

66. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности: Учебное пособие. – М.: Гелиос АРВ, 2004. – 144 с.

67. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – 432 с.

68. Гринберг А.С., Горбачев Н.Н., Бондаренко А.С. Информационные технологии управления: Учебное пособие для вузов. – М.: ЮНИТИ-ДАНА, 2004. – 479 с. (8.10. Технологии обеспечения информационной безопасности. – С. 358–37).

69. Государственная тайна и ее защита. Собрание законодательных и нормативных правовых актов. – М.: Ось-89, 2004. – 160 с.

70. Максим М., Полино Д. Безопасность беспроводных сетей. – М.: Компания АйТи, ДМК Пресс, 2004. – 288 с. (пер. книги 2002 изд.)

71. Вус М.А., Гусев В.С. и др. Информатика: введение в информационную безопасность. – СПб.: Юридический центр Пресс, 2004. – 204 с.

72. Деднев М.А., Дыльнов Д.В., Иванов М.А. Защита информации в банковском деле и электронном бизнесе. – М.: КУДИЦ-ОБРАЗ, 2004. – 512 с.

73. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М., Белов Е.Б., Полникова С.В. Правовое обеспечение информационной безопасности: Учебное пособие. – М.: Издательский центр «Академия», 2005. – 240 с.

74. Информационные технологии управления: Учебное пособие для вузов / Под ред. проф. Г.А. Титоренко. – М.: ЮНИТИ-ДАНА, 2005. – 439 с. (6. Защита информации в ИС и ИТ управления организацией. – С. 192-221).

75. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М.: Гелиос АРВ, 2005. – 192 с.

76. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск.: БЕЛЛІТФОНД, 2005. –304 с.

77. Венбо Мао. Современная криптография: теория и практика.: Пер. с англ. – М.: Вильямс, 2005. – 768 с.

78. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная информация. – Компания АйТи; ДМК Пресс, 2005. – 384 с.

79. Фисун А.П., Касилов А.Н., Глоба Ю.А., Савин В.И., Белевская Ю.А. Право и информационная безопасность: Учебное пособие. – М.: Приор-издат, 2005. – 272 с.

80. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: Учебное пособие. – М.: Гелиос АРВ, 2005. – 224 с.

81. Смарт Н. Криптография. –М.: Техносфера, 2005. – 528 с.

82. Курило А.П. и др. Обеспечение информационной безопасности бизнеса. – М.: БДЦ-пресс, 2005. – 512 с.

83. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. – М.: Интернет-Ун-т Информ. Технологий, 2005. – 608 с.

84. Фергюсон Н., Шнайер Б. Практическая криптография. – М.: Издательский дом «Вильямс», 2005. – 424 с.

85. Асанович В.Я., Маньшин Г.Г. Информационная безопасность: анализ и прогноз информационного взаимодействия. – Мн.: Амалфея, 2006. – 204 с.

86. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006. – 544 с.

87. Филин С.А. Информационная безопасность: Учебное пособие. – М.: Альфа-Пресс, 2006. – 412с.

88. Петренко С.А., Курбатов В.А. Политики информационной безопасности. –М.: Компания АйТи, 2006. – 400 с.

89. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия – Телеком, 2006. – 536 с.

90. Галатенко В.А. Основы информационной безопасности: Курс лекций. – М.: ИНТУИТ. РУ, 2006. – 205 с.

91. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие. – М.: ФОРУМ: ИНФРА-М, 2006. – 368 с.

92. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. – М.: Гелиос АРВ, 2006. – 528 стр.

93. Земор Ж. Курс криптографии. – М.: Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2006. – 256 с.

94. Тилборг Ван Х.К.А. Основы криптологии: Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.

95. Сердюк В.А. Новое в защите от взлома корпоративных систем. – М.: Техносфера, 2007. – 360 с.

96. Доля А.А. Внутренние ИТ – угрозы в России – 2006. «Защита информации. Инсайд», № 2 март–апрель 2007. – 60–69 с.

97. Зубов А.Ю. Математика кодов аутентификации. – М.: Гелиос АРБ, 2007. – 480 с.

98. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.

99. Сазыкин Б.В. Управление операционным риском в коммерческом банке. – М.: Вершина, 2008. – 272 с.

100. Цирлов В.Л. Основы информационной безопасности: Краткий курс. – Ростов-на-Дону: Феникс, 2008. – 253 с.

101. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.

ОПИСАНИЕ КУРСА И ПРОГРАММА

1.1. Цели и задачи курса.

Основная цель курса:

обеспечить комплексность и полноту подготовки бакалавриата по направлениям «Информационные технологии», «Прикладная математика и информатика», «Математика. Прикладная математика», «Автоматизация и управление» путем формирования у студентов знаний и навыков по вопросам информационной безопасности и защите информации.

Задачи курса:

ознакомить студентов с основными проблемами в области информационной безопасности, а также с методами и средствами их решения; обеспечить необходимыми сведениями и навыками для последующего обучения по направлениям «Информационные технологии», «Прикладная математика и информатика», «Математика. Прикладная математика», "Автоматизация и управление".

1.2. Профессиональные знания, умения и навыки, приобретаемые в результате изучения курса

Знания

Студент должен знать:

общие проблемы информационной безопасности информационных систем;

методы и средства защиты информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение);

организационно- правовое обеспечение информационной безопасности;

методы и средства защиты информации от несанкционированного доступа;

основные криптографические и методические средства защиты информации;

компьютерные средства реализации защиты в информационных системах;

программу информационной безопасности России и пути ее реализации.

Навыки и умения

Студент должен уметь:

анализировать риски информационной безопасности информационных систем;

оценивать существующие современные средства защиты информации;

выбирать и разрабатывать меры защиты информации при реализации информационных процессов;

осуществлять организационно- правовое обеспечение информационной безопасности;

1.3. Инновационность курса по содержанию, методике преподавания, литературе, организации учебного процесса.

Инновационность курса по содержанию обеспечена высокой динамикой развития информационных технологий, и большой зависимостью их от обеспечения информационной безопасности. Инновационность курса также основывается на необходимости осознанного выбора достаточного материала для введения студентов в

данную проблематику из многочисленных публикаций с подходами разных организаций и исследователей к проблемам информационной безопасности.

Автор данного курса имел желание построить курс в соответствии с содержанием одной из доступных и качественных книг на русском языке с соответствующей тематикой. Это позволило бы облегчить как преподавание курса, так и обучение. Сделать это оказалось невозможно по причине быстрого устаревания материалов этих книг и большого числа направлений исследований в данной области. Все проблемы информационной безопасности и их решения являются комплексными. В качестве основы были выбраны книги, приведенные в списке обязательной литературы для студентов.

Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия-телеком, 2001г.,-148 с.

Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006.- 544 с.

Галатенко В.А. Основы информационной безопасности. Курс лекций. - М.: ИНТУИТ. РУ, 2006г. – 205 с.

Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учеб. пособие. – М.: Гелиос АРВ, 2006.- 528 стр.

Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебн. Пособие.- М.: ИД «ФОРУМ»: ИНФРА-М,2008.-416 с.

Все книги написаны известными специалистами в области информационной безопасности и во многом основаны на передовом зарубежном и отечественном опыте. Однако, даже за прошедшее с их выхода время произошли существенные изменения в данной области,

например, вышли новые стандарты и рекомендации по вопросам информационной безопасности и новым технологиям, приняты новые законы и другие акты. В связи с этим должно быть переработано и дополнено содержание всех этих книг и курса на их основе. По-видимому, в последующем также надо будет учесть и процесс гармонизации международных и отечественных стандартов, особенности новых отраслевых стандартов. Также новизна содержания курса должна определяться выбором перспективных технологий для демонстрации решения проблем.

При разработке курса было необходимо ознакомиться с лучшими практиками преподавания данной тематики, чтобы критически их переработав создать собственный курс, адаптированный к конкретным условиям преподавания на Инженерном факультете РУДН.

В настоящее время приобрело популярность получение международных сертификатов путем сдачи соответствующих квалификационных экзаменов, которые проводятся в виде тестов. Одними из наиболее признанных являются сертификаты CISA и CISSP, выдаваемые Международным Информационным Консорциумом по Сертификации Защиты Систем (Information Security Certification Consortium (ISC)2 - www.isc2.org). Программа курса должна учитывать требования и соответствующие разделы программ этих экзаменов, чтобы в последующем позволить студентам сдать данные экзамены без больших дополнительных усилий.

Следует обратить внимание на согласование содержания данного курса и курсов УМК «Современная прикладная криптография», «Управление информационными рисками» и «Защита информации с использованием интеллектуальных карт», где должны быть расширены и углублены соответствующие разделы данного основного курса.

Отличительной особенностью данного курса должно явиться привлечение банковской тематики для демонстрации основных понятий и

положений информационной безопасности. В настоящее время в России идет процесс формирования системы требований информационной безопасности для организаций банковской системы России, созданы несколько стандартов, система сертификации, методика проверки требований. Конечно, при этом использовался зарубежный опыт, но отечественные разработчики и специалисты по ИБ внесли много нового в этот процесс.

Особенностью методики преподавания является не только выбор и компановка материала, но и направления в его изучении. В данном курсе изучение вопросов информационной безопасности идет на основе первоначального изучения стандартов и нормативно правовой базы передовых в технологическом плане стран (США, Канада, Великобритания, Германия, Австралия, Россия, …) и доходит до международной практики(ISO, EC, …). Такой подход диктуется не совсем устоявшейся практикой и научно-методической базой в данной области, которая продолжает изменяться и совершенствоваться в настоящее время. Разные страны по разному развиваются, лучшие практики меняются, и наблюдение и изучение этого процесса является основой для изучения студентами этой области. Активно будут использоваться и источники из сети Интернет, прошедшие рецензирование специалистами в данной предметной области и рекомендованные ими.

1.4. Структура курса

Виды учебных работ	Объем работ (2 кредита)	
	Всего	**7 сем.**
Выделено на дисциплину	74	74
Аудиторная работа:	64	64
- лекции	54	54
- семинары	-	-
- лабораторные занятия	-10	-10
Самостоятельная работа:	-	-
- курсовой проект	-	-
- курсовая работа	-10	-10
- домашнее задание	-	-
- самостоятельная проработка курса и подготовка к контрольным работам	-	-
Виды отчетности по дисциплине:		
- зачет	-	-
- экзамен	-	Экз.

Темы лекций

Тема 1. Основные задачи и проблемы информационной безопасности

Тема 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.

Тема 4. Угрозы информационной безопасности и управление рисками.

Тема 5. Причины, виды, каналы утечки и искажения информации.

Тема 6. Технические каналы утечки информации.

Тема 7. Технические средства обеспечения безопасности объекта.

Тема 8. Программно-аппаратные средства обеспечения информационной безопасности.

Тема 9. Методы контроля доступа к информации.

Тема 10. Вредоносные программы.

Тема 11. Основы криптографической защиты информации.

Тема 12.Обеспечение информационной безопасности операционных систем

Тема 13. Основы безопасности сетевых технологий.

Тема 14. Организационно-правовое обеспечение защиты информации.

Тема 15. Стандарты информационной безопасности

Тема 16. Сертификация и аттестация в области информационной безопасности

Некоторые темы лабораторных работ

1. Изучение и применение пакета программ PGP.(и/или аналогичных программ КриптоАРМ, STCLite, Articsoft FileAssurity OpenPGP…).

2. Изучение цели нападения. Предварительный сбор данных о цели.

3. Изучение работы эксплойтов, используемых для получения административного контроля над системой.

4. Изучение и использование сканеров уязвимостей (XSpider)/

5. Практическое восстановление пароля к:
-ZIP/RAR архиву,
- файлу PGP.

6 Практическое восстановление пароля к предоставленному серверу ftp.

7. Обоснование выбора и установка firewall, настройка и тестирование(Например, Atelier web firewall tester).

8. Подписание цифрового изображения или наложение на него водяных знаков для защиты от НСД (Visual watermark).

9. Проведение оценки PC и настройка безопасности не меньше заданного уровня (например, при помощи pcAudit)

10. Стеганография и шифрование файлов в фомате jpeg/bmp или gif или mp3.

11. Обнаружение и изучение вредоносных ПО после запуска предоставленных файлов. Методы борьбы.

ПРОГРАММА КУРСА УМК

2.1. Аннотированное содержание курса

Изучение данного курса обеспечивает студента сведениями о современном состоянии в области информационной безопасности. Курс является основой для последующего изучения вопросов безопасности в курсах «Современная прикладная криптография», « Управление информационными рисками» и «Защита информации с использованием интеллектуальных карт». Материал курса основан на последних достижениях зарубежных и отечественных специалистов, а также на материалах известных признанных учебных пособиях.

Существенное место в курсе уделено и стандартным методам и рекомендациям защиты информации, позволяющим существенно ускорить разработку и внедрение новых систем.

В читаемой дисциплине излагаются:

- основные задачи и проблемы информационной безопасности;
- важнейшие документы международной, национальной и ведомственных нормативных правовых баз в области информационной безопасности;
- типовые угрозы информационной безопасности и методы управления информационными рисками;
- каналы утечки и искажения информации;
- типовые технические средства обеспечения безопасности объектов;
- типовые программно-аппаратные средства обеспечения информационной безопасности;
- методы контроля доступа к информации;
- вредоносные программы, в том числе компьютерные вирусы;
- основы криптографической защиты информации;

- основы обеспечения информационной безопасности операционных систем;
- основы безопасности сетевых технологий;
- организационно-правовое обеспечение защиты информации;
- основные стандарты информационной безопасности;
- вопросы сертификации и аттестации в области информационной безопасности.

Для самостоятельной работы студентов, подготовки рефератов и курсовых проектов выбираются темы из перечня тем известных отечественных и международных конференций и семинаров по информационной безопасности (information security).

Курс предполагает выполнение студентами серии лабораторных работ по актуальным и практическим методам информационной безопасности и защите информации.

2.2. Список обязательной и дополнительной литературы для преподавателей.

При составлении списка учитывалась доступность литературы. По крайней мере, авторам курса она доступна или в бумажном виде или в электронном. Конечно, главный критерий выбора источника - это его качество. При выборе приходится искать компромисс между классическими и новейшими источниками, которые актуальны на определенный момент и еще не прошли проверку временем и практикой.

Приводимый ниже список литературы достаточно обширен и предназначен прежде всего для преподавателей. Даже деление его на обязательный и дополнительный довольно условно. Конечно, для студентов эти списки должны быть достаточно небольшими, чтобы в отведенное время можно было реально познакомиться с этой литературой.

Особо в Приложение 1 выделена нормативная правовая база информационной безопасности, без которой немыслимо освоение данного курса. Возможно, со временем это будет предметом рассмотрения отдельного курса, настолько важными и особыми являются рассматриваемые при этом вопросы.

Обязательная:

1. Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике. – М.: ИЛ, 1963.

2. Hoffman L. Modern methods for computer security and privacy. Prentice-Hall,Inc.,1977.

Русский перевод: Хоффман Л.Д.Современные методы защиты информации.-М.:Сов.радио, 1980.

3. Hsiao D., Kerr D., Mednick S. Computer security. Academic Press, 1979.

Русский перевод: Сяо Д., Керр Д., Мэдник С. Защита ЭВМ. - М.:Мир,1982.

4. Jackson K., Hruska J. (Ed.) Computer Security Reference Book. Butterworth-Heinemann Ltd., 1992. - 932 pp.

5. Muftic S. Security Mechanisms for Computer Networks. Halsted Press.

Русский перевод: Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 1993.

6. Спесивцев А.В., Вегнер В.А. и др. Защита информации в персональных ЭВМ.- М.: Радио и связь, 1992.- 191 стр.

7. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. –М.: Яхтсмен, 1993.- 188 с.

8. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоатомиздат, 1994, Кн. 1 и 2.

9. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Единая Европа, 1994.

10. Михайлов С.Ф., Петров В.А., Тимофеев Ю.А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции. Учеб. пособие. - М.: МИФИ, 1995.- 112 с.

11. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. Учебное пособие. - М.: МИФИ, 1995.

12. Schneier B. Applied cryptography, second edition: protocols, algorithms, and source code in C. J. Wiley & sons, Inc. 1996.- 758 pp.

Русский перевод: Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Триумф, 2002. – 816 с.

13. Tiley E., Personal Computer Security, IDG Books Worldwide, 1996.

Русский перевод: Тайли Э. Безопасность персонального компьютера. – Мн.: ООО Попурри. 1997. – 480 с.

14. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 1997 г., - 538 с.

15. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. – СПб.: НПО Мир и семья, 1997.

16. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Ось-89, 1998.-336 с.

17. Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. – СПб: СПбГУ, 1998. – 328 с.

18. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.:Радио и связь, 1999. – 328 с.

19. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб: СПбГУ, 1999. – 368 с.

20. Stallings W. Network and Internetwork Security: principles and practice, Second Edition, Prentice-Hall, Inc., 1999.- 459 pp.

Русский перевод: Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.

21. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю., Теоретические основы компьютерной безопасности, – М: Радио и связь, 2000. -192 с.

22. Зегжда Д., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телекомю 2000. – 452 с.

23. Милославская Н.Г., Толстой А.И. Интрасети:доступ в Internet, защита: Учебное пособие. – М.: ЮНИТИ-ДАНА, 2000. – 527 с.

24. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах, – М: Радио и связь, 2000. -168 с.

25. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. М.: СИНТЕГ, 2000, -248 с.

26. Ярочкин В.И. Информационная безопасность. – М.: Международные отношения, 2000г., - 400 с.

27. Безопасность сети на основе Windows 2000. Учебный курс MCSE. – М.: ИТД Русская Редакция. 2001. –912 с.

28. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРБ, 2001. –480 с.

29. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия-телеком, 2001г.,-148 с.

30. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. – М.: Юрист, 2001 г., - 415 с.

31. Стрельцов А.А. Обеспечение информационной безопасности России. - М.: МЦНМО, 2002.-296.

32. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2002. – 432 с.

33. Barman S. Writing Information Security Policies. 2001.

Русский перевод: Бармен С. Разработка правил информационной безопасности. – М.: Вильямс, 2002.- 208 с.

34. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб.: Питер, 2002. – 848 с.

35. Smith R. Authenticaton: From Passwords to Public Keys. – NY: Addison-Wesley Publishing Company, Inc., 2002.

Русский перевод: Смит Р. Аутентификация: от паролей до открытых ключей. – М.: Вильямс, 2002. – 432 с.

36. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. Учеб. пособие. –М.: РГГУ, 2002.-399 с.

37. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учеб. пособие. – М.: Радио и связь. 2003.- 296 с.

38. Конеев И., Беляев А. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003.-752с.

39. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. - СПб: 2003. http://lib.aldebaran.ru/author/shnaier_bryus/shnaier_bryus_sekrety_i_lozh_bezopasnost_dannyh_v_cifrovom_mire/

40. Скляров Д.В., Искусство защиты и взлома информации.- СПб.: БХВ - Петербург, 2004.-288 с.

41. Галатенко В.А. Стандарты информационной безопасности. Курс лекций. М.: ИНТУИТ. РУ, 2004. – 328 с.

42. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности: Учебное пособие. – М.: Гелиос АРВ, 2004.- 144 с.

43. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография.- М.: Норма, 2004. – 432 с.

44. Гринберг А.С., Горбачев Н.Н., Бондаренко А.С. Информационные технологии управления: Учеб. Пособие для вузов. – М.:

ЮНИТИ - ДАНА, 2004.-479с.(8.10. Технологии обеспечения информационной безопасности. 358-371стр.)

45. Государственная тайна и ее защита. Собрание законодательных и нормативных правовых актов. – М.: «Ось-89», 2004.-160 с.

46. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М., Белов Е.Б., Полникова С.В. Правовое обеспечение информационной безопасности: Учеб. пособие.- М.: Издательский центр «Академия», 2005.-240 с.

47. Информационные технологии управления: Учеб. Пособие для вузов/ Под ред.проф. Г.А. Титоренко. – М.: ЮНИТИ-ДАНА, 2005.-439с. (6. Защита информации в ИС и ИТ управления организацией, 192-221 стр.)

48. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособие. – М.: Гелиос АРВ, 2005.- 192 с.

49. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск.: БЕЛЛІТФОНД, 2005.-304 с.

50. Венбо Мао. Современная криптография: теория и практика.: Пер. с англ.- М.: Вильямс, 2005. 768 с.

51. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная информация. Компания АйТи; ДМК Пресс, 2005.-384 с.

52. Фисун А.П., Касилов А.Н., Глоба Ю.А., Савин В.И., Белевская ю.А. Право и информационная безопасность: Учебное пособие// -М.: Приор-издат, 2005.-272 с.

53. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: Учеб. пособие. – М.: Гелиос АРВ, 2005.- 224 с.

54. Асанович В.Я., Маньшин Г.Г. Информационная безопасность: анализ и прогноз информационного взаимодействия. – Мн.: Амалфея, 2006.-204 с.

55. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006.- 544 с.

56. Филин С.А. Информационная безопасность: Уч. Пособие. - М.: Альфа-Пресс, 2006.-412с.

57. Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи, 2006. – 400 с.

58. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем: Уч. Для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая линия – Телеком, 2006. – 536 с.

59. Галатенко В.А. Основы информационной безопасности. Курс лекций. - М.: ИНТУИТ. РУ, 2006г. – 205 с.

60. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие. – М.: ФОРУМ: ИНФРА-М. 2006. – 368 с.

61. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учеб. пособие. – М.: Гелиос АРВ, 2006.- 528 стр.

62. Сердюк В.А. Новое в защите от взлома корпоративных систем. М.: Техносфера, 2007.- 360 с.

63. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебн. Пособие.- М.: ИД «ФОРУМ»: ИНФРА-М,2008. – 416 с.

Дополнительная литература

64. Denning D. Cryptography and data security. Addison- Weslay Publishing Company. 1982,- 400 pp.

65. ТИИЭР т.76, №5. Защита информации. Малый тематический выпуск. – М.: Мир, 1988.

66. Russel D., G.T.Gangemi Sr. Computer Security Basics. –O`Reilli & Associates, Inc., 1991. – 448 pp.

67. Горохов П.К. Информацинная безопасность. Англо-русский словарь. – М.: Радио и связь, 1995. 224 с.-

68. Garfinkel S. PGP: Pretly Good Privacy. – O'Reilly and Associates, Inc., 1995.

69. Stinson D. Cryptography: theory and practice. CRC Press, 1995.

70. Hoffman L. (Ed.) Building in big Brother: the cryptography policy debate. Springer-Verlag NewYork. Inc. , 1995.- 560 pp.

71. Kaufman C., Pelman R., Speciner M. Network Security – PRIVATE Communication in a PUBLIC World, Prentice-Hall, Inc.,1995.

72. Wayner P. Digital Cash, AP Professional, 1995.

73. Варфоломеев А.А., Пеленицин М.Б. Методы криптографии и их применение в банковских технологиях. – М.: МИФИ, 1995.- 116 стр.

74. Варфоломеев А.А., Гаврилкевич М.В., Устюжанин Д.Д., Фомичев В.М. Методические указания к выполнению лабораторного практикума "Информационная безопасность. Криптографические методы защиты информации", ч.1 ,ч.2. – М.: МИФИ, 1995. – 44 с., - 38с.

75. Menezes A., Van Oorschot P., Vanstone S. Handbook of Applied cryptography. CRC Press, 1996.- 816 стр.

76. Теория и практика обеспечения информационной безопасности. Под ред. Зегжды П.Д. – М.: Яхтсмен, 1996.

77. Варфоломеев А.А., Жуков А.Е. и др. Блочные криптосистемы. Основные свойства и методы анализа стойкости. М.: МИФИ, 1998.- 198 стр.

78. Edvards M.J. Internet security with Windows NT.- DUKE PRESS, 1998.

Русский перевод: Эдвардс М.Дж. Безопасность в Интернете на основе Windows NT. – М.: ТОО Channel Trading Ltd. – 1999. –656 с.

79. Анин Б. Защита компьютерной информации. – СПб.: БХВ-Санкт-Петербург, 2000.- 384 с.

80. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.:ДМК, 2000. – 448 с.

81. Burnet S., Paine S. RSA Security`s Official Guide to Cryptography.- NY.: The McGraw-Hill Companies, 2001.

Русский перевод: Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security.- М.: Бином-Пресс, 2002. –384 с.

82. Голдовский И. Безопасность платежей в Интернете. – СПб : Питер, 2001. – 240 с.

83. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. – Мн.:БГУ, 2001. – 190 с.

84. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий. _ М.: Издательство СИП РИА, 2001. – 356 с.

85. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер. – М.: Гелиос АРБ, 2002. – 256 с.

86. Парфенов В.И. Защита информации. Словарь. Воронеж.: НП РЦИБ Факел. 2003, - 292 с.

87. Царегородцев А.В. Информационная безопасность в распределенных управляющих системах. – М.: РУДН, 2003.

88. Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2003.- 192 с.

89. Максим М., Полино Д. Безопасность беспроводных сетей. – М.: Компания АйТи, ДМК Пресс, 2004. – 288 с.(пер. книги 2002 изд.)

90. Смарт Н. Криптография. М.: Техносфера, 2005.- 528 с.

91. Земор Ж. Курс криптографии.- М.-Ижевск: НИЦ”Регулярная и хаотическая динамика”; Институт компьютерных исследований, 2006.-256.

92. Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.; Мир, 2006, 471 с.

93. Зубов А.Ю. Математика кодов аутентификации. – М.: Гелиос АРБ, 2007.- 480с.

2.3. Список обязательной и дополнительной литературы для студентов.

Далее сохранена нумерация списка для преподавателей.

Обязательная литература:

10. Михайлов С.Ф., Петров В.А., Тимофеев Ю.А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции. Учеб. пособие. - М.: МИФИ, 1995.- 112 с.

29. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.: Горячая линия-телеком, 2001г.,-148 с.

55. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006.- 544 с.

57. Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи, 2006. – 400 с.

59. Галатенко В.А. Основы информационной безопасности. Курс лекций. - М.: ИНТУИТ. РУ, 2006г. – 205 с.

61. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учеб. пособие. – М.: Гелиос АРВ, 2006.- 528 стр.

63. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебн. Пособие.- М.: ИД «ФОРУМ»: ИНФРА-М,2008.- 416 с.

Дополнительная литература:

9. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Единая Европа, 1994.

16. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Ось-89, 1998.-336 с.

18. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.:Радио и связь, 1999. – 328 с.

22. Зегжда Д., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телекомю 2000. – 452 с.

24. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах, – М: Радио и связь, 2000. -168 с.

30. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. – М.: Юрист, 2001 г., - 415 с.

31. Стрельцов А.А. Обеспечение информационной безопасности России. - М.: МЦНМО, 2002.-296.

32. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. – М.: Гелиос АРБ, 2002. – 432 с.

38. Конеев И., Беляев А. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003.-752с.

39. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. - СПб: 2003.

2.4. Темы рефератов, курсовых работ, эссе

Темы для самостоятельной работы студентов при подготовке рефератов и курсовых работ определяются на основе тематики известных признанных научных конференций и семинаров, рассматривающих вопросы безопасности ИТ систем. Среди таких мероприятий выделим следующие.

USENIX Security Symposium.

IEEE Symposium on Security and Privacy.

ACM Conference on Computer and Communications Security (CCS).

ISOC Network and Distributed System Security Symposium (NDSS).

International Symposium on Recent Advances in Intrusion Detection (RAID).

GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA).

Annual EICAR Conference.

Annual Computer Security Applications Conference (ACSAC).

International Conference on Applied Cryptography and Network Security (ACNS).

ACM Symposium on Information, Computer and Communications Security (ASIACCS).

European Symposium on Research in Computer Security (ESORICS).

Financial Cryptography and Data Security (FC).

ACM Workshop on Recurring Malcode (WORM).

DEFCON.

BlackHat.

The Virus Bulletin International Conference.

AVAR International Conference.

CanSecWest and EuSecWest Conferences.

Hack In The Box (HITB) Conference.

RSA Conference.

Chaos Communication Congress (CCC).

Труды большинства этих конференций и семинаров доступны для образовательных учреждений в сети Интернет на сайте http://www.springerlink.com/ .

Примеры тем.

1. О некоторых атаках на схемы типа Бонеха-Франклина для обнаружения внутренних нарушителей. (Traitor Tracing)

2. Различные подходы построения безопасных служб установки точного времени в электронном документообороте. (Timestamping)

3. О механизмах электронных водяных знаков. (Watermarking)

4. О новых схемах электронных платежных систем и методах их защиты.

5. Вопросы информационной безопасности аутсорсинга.

6. Модели внутреннего нарушителя информационной безопасности.

7. Вопросы безопасности в беспроводных сетях.

8. Особенности сбора исходной информации системами обнаружения атак.

9. Коммерческие средства аутентификации пользователей телекоммуникационных сетей.

10. Методология разработки политики информационной безопасности предприятия.

2.5. Учебный тематический план курса

Раздел 1. Сущность, задачи и проблемы информационной безопасности (3часа)

Введение. Роль информации в жизнедеятельности современного общества. Развитие информационной индустрии. Объективная необходимость информационной безопасности и защиты информации. Определение информации. Документированная информация. Электронное сообщение. Активы. Ресурсы. Различные определения информационной безопасности и защиты информации. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.

Современная постановка задачи защиты информации. Комплексность целевая и инструментальная.

Назначение и структура курса. Рекомендуемая основная и дополнительная литература. Интернет-источники.

Раздел 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ. (3 часа)

Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной политики государств и ведомств. Государственная тайна.

Раздел 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности. (3часа)

Общие положения. Концептуальные документы в области информационной безопасности. Важнейшие федеральные нормативные правовые акты. Законы, касающиеся охраны интеллектуальной собственности. Положения Гражданского кодекса РФ по защите информации. Международное сотрудничество. Кодекс об административных правонарушениях. Уголовный кодекс и защита информации. Основные подзаконные акты в области информационной безопасности. Указы Президента РФ, постановления Правительства РФ, ведомственная нормативная база.

Раздел 4. Угрозы информационной безопасности. Управление рисками. (3часа)

Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные

Общая характеристика анализа и управления рисками. Логарифмическая шкала. Оценка по верхним и нижним значениям. Оценка на основе выявления слабого звена. Оценка рисков на основе рассмотрения этапов вторжения. Программные средства, используемые для анализа

рисков: CRAMM, RiskWatch, COBRA, Buddy System, RA Software Tool, ПО «Авнгард».

Раздел 5. Методы нарушения конфиденциальности, целостности и доступности информации. (3часа)

Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные.

Потенциально возможные злоумышленные действий в автоматизированных системах обработки данных. Функции защиты информации. Стратегии защиты информации: оборонительная стратегия, наступательная стратегия, упреждающая стратегия. Архитектура систем защиты информации. Модели защиты информации

Раздел 6. Причины, виды, каналы утечки и искажения информации. (3часа)

Подходы к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Модель затрат фирмы IBM. Модель защиты - модель системы с полным перекрытием. Последовательность решения задачи защиты информации. Фундаментальные требования для вычислительных систем обработки конфиденциальной информации. Три группы требований. Стратегия, подотчетность, гарантии. Факторы, влияющие на требуемый уровень защиты информации

Раздел 7. Функции и задачи защиты информации. Проблемы региональной информационной безопасности. (2часа)

Методы формирования функций защиты. Сокрытие информации о средствах, комплексах, объектах и системах обработки информации. Дезинформация противника. Введение избыточности элементов системы. Резервирование элементов системы. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на психику человека.

Региональные компоненты защиты информации. Защита информации предприятия. Проведение анализа защищенности локального объекта

Раздел 8. Информационные и автоматизированные системы (2 часа)

Определения информационной (ИС) и автоматизированной системы (АС) обработки информации. ГОСТы на АС. Типовые виды структуры АС. Виды воздействия на информацию в ИС и АС. Угрозы безопасности АС и их классификация. Меры противодействия угрозам безопасности АС. Уязвимости АС. Принципы построения системы защиты АС.

Раздел 9. Технические каналы утечки информации (2 часа)

Технические каналы утечки информации (ТКУИ) и способы их перекрытия. Пассивная и активная защита от утечки информации по техническим каналам. Определение, классификация и общая характеристика ТКУИ. Визуальные и акустические каналы. Защита информации в телефонных каналах. Защита от побочных электромагнитных излучений и наводок (ПЭМИН). Технические закладки. Способы обнаружения ТКУИ. Способы и методы перекрытия ТКУИ. Требования к выбору и оборудованию помещений для АС обработки данных по условиям защиты от ТКУИ. Понятие контролируемой территории и методы определения ее размеров. Общие сведения о защищенных средствах ЭВТ. Особенности защиты персональной вычислительной техники от утечки информации по техническим каналам.

Раздел 10. Технические средства обеспечения безопасности объекта. (3 часа)

Определение и основные цели защиты современных объектов. Технические средства обеспечения защиты объекта: определение, системная классификация, общий анализ. Технические средства и системы охраны территории, зданий и помещений. Технические средства наблюдения и контроля за перемещением людей и предметов. Технические средства и системы опознавания людей. Технические средства и системы управления доступом на территорию, в здания и помещения, к средствам обработки и хранения информации. Методы выбора технических средств, общие сведения о рынке технических средств обеспечения безопасности.

Раздел 11. Программно-аппаратные средства обеспечения информационной безопасности. (3 часа)

Программно-аппаратные средства (ПАС) обеспечения защиты информации от несанкционированного доступа (НСД). СЗИ НСД “Аккорд”. Угрозы безопасности НСД. Основные концепции обеспечения защиты от НСД. Принципы программно-аппаратной защиты информации.

Раздел 12. Методы контроля доступа к информации (3 часа)

Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. Метод паролей. Биометрическая аутентификация. Способы разграничения доступа, методы и средства их реализации. Краткая характеристика современных средств разграничения доступа. Дискреционный и мандатный методы доступа.

Математические модели управления доступом к информации. Субъектно-объектная модель доступа. Потоковая модель доступа. Политика безопасности и модель доступа. Способы анализа моделей доступа и политик безопасности. Механизмы разграничения доступа в современных операционных системах.

Электронные ключи. Идентификационные карточки, брелоки. Назначение, принципы устройства, возможности. Типы карточек. Принципы и методы использования. Программно-аппаратное обеспечение использования карточек.

Раздел 13. Вредоносные программы (3 часа)

Вредоносные закладки (ВЗ): определение, разновидности. Разрушающие действия закладок. Особенности взаимодействия с программно-аппаратными средствами защиты. Методика применения

средств борьбы с вредоносными закладками на этапе эксплуатации систем. Системы разграничения доступа и защиты от ВЗ. Предупреждение и минимизация последствий воздействия ВЗ. Краткая характеристика мер защиты: юридические, административные и организационные, аппаратно-программные.

Компьютерные вирусы. Классификация. Жизненный цикл. Основные каналы распространения вирусов и других вредоносных программ. Средства борьбы с вирусами: краткая характеристика популярных антивирусных программ.

Средства защиты от копирования. Примеры средств и технологий. Вопросы правовой защиты.

Раздел 14. Основы криптографической защиты информации. (3 часа)

Основные понятия и задачи криптологии (криптографии). Цели и задачи криптологии. Секретность, целостность, аутентичность, неотказуемость, неотслеживаемость, анонимность. Понятие о криптографических примитивах и протоколах.

Криптография с секретным и открытым ключом, плюсы и минусы. Причины и предпосылки появления новых направлений в криптографии.

Введение в криптосистемы с секретным ключом (симметричные). Теоретическая и практическая стойкость. Блочные криптосистемы. Краткая характеристика стандартов DES, AES(Rijndael), ГОСТ 28147-89. Генераторы псевдослучайных чисел и последовательностей. Поточные криптосистемы.

Математические основы современной криптологии. Односторонние функции. Односторонние функции с секретом. Криптосистемы с открытым ключом (ассиметричные). Система RSA.

Понятие о цифровой подпись. Краткая характеристика стандартов на цифровую подпись DSS, ГОСТ Р 34,10-94, ГОСТ Р 34.10-2001.

Криптографические функции хэширования. Основные характеристики. Практические применения.

Проблемы управления криптографическими ключами. Открытое распределение ключей. Инфраструктуры открытых ключей и стандарт X.509.

Защита электронного документооборота с использованием электронной цифровой подписи.

Примеры программно-аппаратных средств криптографической защиты: пакет PGP, пакет Криптон, СКЗИ «Верба-О», ПК «Inter-PRO», … .

Раздел 15.Обеспечение информационной безопасности операционных систем (3 часа)

Проблемы обеспечения ИБ ОС. Угрозы безопасности ОС. Понятие защищенной ОС. Архитектура подсистемы защиты ОС. Основные функции подсистемы защиты ОС. Разграничение доступа к объектам ОС. Аудит.

Раздел 16.Основы безопасности сетевых технологий (4 часа)

Введение в Internet и Intranet. Способы нападения на сети и защита от межсетевого доступа. Особенности для различных уровней модели ISO/OSI.

Технологии межсетевых экранов. Функции МЭ. Формирование политики межсетевого взаимодействия. Основные схемы подключения МЭ. Персональные и распределенные сетевые экраны. Проблемы безопасности МЭ. Критерии оценки межсетевых экранов.

Построение защищенных виртуальных сетей VPN. Варианты построения. Средства обеспечения безопасности VPN.

Защита на канальном и сеансовом уровнях. Протоколы PPTP, L2TP, SSL/TLS, SOCKS.

Защита на сетевом уровне. Протокол IPSEC. Основные схемы применения, преимущества средств безопасности IPSEC.

Безопасность удаленного доступа к локальной сети. Централизованный контроль. Управление доступом по схеме однократного входа с авторизацией.

Технологии обнаружения атак. Классификация систем обнаружения атак IDS. Компоненты и архитектура IDS. Методы реагирования.

Угрозы и уязвимости беспроводных сетей.

Раздел 17. Организационно-правовое обеспечение защиты информации (3 часов)

Сущность и роль организационно-правовых аспектов информационной безопасности. Человек как главное звено в системе защиты информации и как злоумышленник. Нормативная правовая база информационной безопасности. Закон РФ “Об информации, информационных технологиях и о защите информации”.

Виды и категории информации ограниченного доступа: государственная и другие виды тайн. Закон РФ “О государственной тайне”. Государственная система лицензирования и сертификации деятельности в области защиты информации. Указ Президента РФ “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации”. Закон РФ “Об электронной цифровой подписи”. Уголовно- правовое регулирование защиты информации.

Раздел 18. Стандарты информационной безопасности (3 часа)

Исторический очерк развития зарубежных стандартов информационной безопасности. Критерии безопасности компьтерных систем Министерства обороны США – «Оранжевая книга». Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности. Канадские критерии безопасности компьютерных систем. ГОСТ Р ИСО/МЭК 15408-2002, как аутентичный вариант общих критериев безопасности ИТ.Функциональные требования безопасности. Требования доверия к безопасности. Стандарты ISO/IEC 17799: 2002 (BS 7799:2000). ISO/IEC 27001. Германский стандарт BSI. Стандарты SysTrust, SCORE, GIAC.

Стандарты для беспроводных сетей. Отечественные стандарты информационной безопасности. Стандарты обеспечение информационной безопасности организаций банковской системы Российской Федерации.

Стандарты информационной безопасности в Интернете.

Раздел 19. Сертификация и аттестация в области информационной безопасности (2 часа)

Назначение и общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия. Декларирование соответствия. Обязательная сертификация. Проведение сертификационных испытаний: принципы проведения испытаний, документы сертификационных испытаний. Сертификация продукции, ввозимой из-за границы РФ. Сертификация на региональном и международном уровнях: страны СНГ, Евросоюз, … .

Приложение 1.

Нормативно-правовые акты и другие документы РФ в области информационной безопасности

Почти все документы доступны в электронном виде, например, по адресам:
www.kremlin.ru , www.duma.gov.ru, www.cryptopro.ru , www.infotex.ru
Вопросами информационной безопасности в Государственной думе занимаются 3 комитета: Комитет по безопасности, Комитет по информационной политике. Комитет по энергетике, транспорту и связи.

Международные нормативно-правовые акты

94. Хартия глобального информационного общества, (Окинава, 22 июля 2000 года).
95. Совет Европы «Конвенция о преступности в сфере компьютерной информации», (ETS № 185) (Будапешт, 23 ноября 2001 г.)
96. Совет Европы «Конвенция о защите физических лиц в отношении автоматизированной обработки данных личного характера» (ETS N 108) (Страсбург, 28 января 1981 года),
97. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R 12 декабря 2003 года «Декларация принципов построение информационного общества – глобальная задача в новом тысячелетии»,
98. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/5-R 12 декабря 2003 года «План действий»,
99. Соглашение об организации информационного взаимодействия в объединенных вооруженных силах Содружества Независимых Государств и вооруженных силах государств - участников Соглашения. Заключено в г. Москве 13 ноября 1992 г.,
100. Декларация совещания министров «Восьмерки» в Оттаве по борьбе с терроризмом. Принята в г.Оттаве 12 декабря 1995 г.,
101. Заявление лидеров АТЭС по борьбе с терроризмом. Подписано в г. Лос-Кабосе 26 октября 2002 – 27 октября 2002 г.,
102. Рекомендация N 26 Европейской экономической комиссии ООН «Коммерческое использование соглашений об обмене для электронного обмена данными» (ECE/TRADE/208; ECE/TRADE/WP.4/R.1133/Rev.l) вместе с «Типовым соглашением об обмене для международного коммерческого использования электронного обмена данными»). Принята в г. Женеве в марте 1995 г. Рабочей группой по упрощению процедур международной торговли,
103. Рекомендация NR(92)16 Комитета министров Совета Европы «О европейских правилах по общим санкциям и мерам». Принята 19 октября 1992 г.;
104. Стокгольмская Конвенция «О стойких органических загрязнителях (вместе с «Ликвидацией», «Ограничением», «Непреднамеренным производством», «Требованиями в отношении информации и критериями отбора», «Информацией о социально-экономических соображениях» и «Требованиями в отношении информации, необходимой для характеристики рисков»). Заключена в г. Стокгольме 22 мая 2001 г.,
105. Хартия Шанхайской Организации Сотрудничества. Принята в г. Санкт-Петербурге 07.06.2002 г.

106. Соглашение между Правительством Российской Федерации и Правительством Малайзии «О сотрудничестве в области информационных и коммуникационных технологий». Заключено в г. Путраджайе 5 августа 2003 г.,
107. Совместное заявление Российской Федерации и Соединенных Штатов Америки «Об общих вызовах безопасности на рубеже XXI века». Подписано в г. Москве 2 сентября 1998 г.,
108. Совет Европы «Конвенция о противодействии терроризму», (ETS № 196) (1.06.07.).

Нормативно-правовые акты, заключенные между странами СНГ, а также Латвией, Литвой и Эстонией

109. Модельный закон о международном информационном обмене. Принят в г.Санкт-Петербурге 26 марта 2002 г. Постановлением 19-7 на 19-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ,
110. Модельный закон о персональных данных. Принят в г.Санкт- Петербурге 16 октября 1999 г. Постановлением 14-19 на 14-ом пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ,
111. Постановление № 7 Совета Министров Союзного государства «О ходе выполнения программы Союзного Государства «Защита общих информационных ресурсов Беларуси и России» и продлении срока ее реализации». Принято 29 апреля 2003 г.,
112. Программа развития межгосударственной информационно-вычислительной сети железных дорог государств - участников СНГ, Латвии, Литвы, Эстонии (вместе с «Целями и предметом деятельности межгосударственного вычислительного центра...», «Межгосударственной информационной системой»). Утверждена 28 мая 1999 г. на 24 заседании Совета по железнодорожному транспорту;
113. Программа Союзного Государства «Защита общих информационных ресурсов Беларуси и России». Утверждена 29 апреля 2003 Постановлением № 7 Совета Министров Союзного государства,
114. Решение Совета глав государств СНГ «О предложениях республики Молдова по развитию отдельных направлений концепции формирования информационного пространства Содружества Независимых Государств». Принято в г. Кишиневе 7 октября 2002 г.;
115. Решение Совета глав правительств СНГ «О Концепции информационной безопасности государств - участников Содружества Независимых Государств в военной сфере». Принято в г. Минске 4 июня 1999 г.;
116. Решение Совета глав правительств СНГ «О концепции межгосударственной подсистемы информационного обмена между пограничными войсками государств - участников Содружества Независимых Государств». Принято в г. Москве 18 октября 1996 г.;
117. Решение Совета глав правительств СНГ «О Концепции межгосударственной подсистемы информационного обмена между органами внутренних дел государств - участников Содружества Независимых Государств». Принято в г. Минске 04 июня 1999 г.;
118. Решение Совета глав правительств СНГ «О концепции межгосударственной подсистемы информационного обмена между пограничными войсками государств - участников Содружества Независимых Государств». Принято в г. Москве 18 октября 1996 г.;
119. Решение Совета глав правительств СНГ «О концепции создания совместной (объединенной) системы связи вооруженных сил государств-участников Содружества Независимых Государств». принято в г. Ялте 18 сентября 2003 г.,

120. Решение Совета глав правительств СНГ «О Концепции формирования информационного пространства Содружества Независимых Государств». Принято в г. Москве 18 октября 1996 г.,
121. Решение Совета глав правительств СНГ «О межгосударственной Программе создания сети информационно-маркетинговых центров для продвижения товаров и услуг на национальные рынки государств - участников Содружества Независимых Государств на период до 2005 года» (вместе с «Планом мероприятий...», Таблицами расчетных финансовых затрат и расчета бюджетных и внебюджетных средств, «Описанием и основными задачами пилотного проекта...» и «Технологией международной торговой сделки»). Принято в г. Москве 29 ноября 2001 г.,
122. Решение Совета глав правительств СНГ «О перспективном плане подготовки документов и мероприятий по реализации концепции формирования информационного пространства Содружества Независимых Государств». Принято в г. Москве 25 ноября 1998 г.,
123. Решение Совета глав правительств СНГ «О положении о координационном совете государств-участников СНГ по информатизации при региональном содружестве в области связи». Принято в г. Кишиневе 7 октября 2002 г.,
124. Решение Совета глав правительств СНГ «О создании информационно-аналитической системы в штабе по координации военного сотрудничества государств - участников Содружества Независимых Государств и министерствах обороны государств - участников Содружества Независимых Государств и порядке ее финансирования (ОКР «Дистанция») (вместе с «Положением о порядке финансирования...», «Планом выделения ассигнований...», «Тактико-техническим заданием...»). Принято в г. Кишиневе 7 октября 2002 г.,
125. Совместное заявление стран СНГ по развитию информационного общества (Санкт-Петербургская Декларация). Принято в г. Санкт-Петербурге 1 июля 2003 г. на заседании Координационного совета государств-участников СНГ по информатизации при Региональном содружестве в области связи,
126. Соглашение между Российской Федерацией и Киргизской Республикой «О сотрудничестве в области безопасности». Заключено в г. Бишкек 5 декабря 2002 г.,
127. Соглашение «О правовом режиме информационных ресурсов пограничных войск государств - участников Содружества Независимых Государств». Заключено в г. Москве 25 ноября 1998 г.,
128. Соглашение между железнодорожными администрациями стран СНГ, а также Литовской Республики, Латвийской Республики и Эстонской Республики «О принципах обмена информацией на основе программно-технических комплексов и международных стандартов». Заключено в г. Алма-Ате 30 января 1998 г.;
129. Соглашение «О создании межгосударственной системы документальной шифрованной связи Содружества Независимых Государств». Заключено в г. Москве 18 октября 1996 г.,
130. Соглашение между правительствами Армении, Белоруссии, Казахстана, Киргизии, Молдавии, России, Таджикистана, Туркмении, Узбекистана и Украины «О сотрудничестве в области информации». Заключено в г. Бишкеке 9 октября 1992 г.,
131. Соглашение «О сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств - участников Содружества Независимых Государств в сфере информатизации» (вместе с «Базовым перечнем приоритетных направлений...», «Порядком формирования и реализации межгосударственных программ...»). Заключено в г. Москве 24 декабря 1999 г. Утверждено Постановлением Правительства РФ от 28 мая 2002 г. № 356,
132. Соглашение «Об информационном взаимодействии государств-членов Евразийского экономического Сообщества по пограничным вопросам (вместе с

«Перечнем видов документированной информации для межгосударственного обмена информационными ресурсами...»). Заключено в г. Алма-Ате 14 сентября 2001 г.,
133. Решение Совета глав государств СНГ "О дальнейшем развитии сотрудничества государств-участников Содружества в противодействии международному терроризму, а также иным вызовам и угрозам безопасности и стабильности на современном этапе в свете принятых документов в рамках СНГ, ОБСЕ и ООН" (Вместе с "Заявлением глав государств-участников Содружества Независимых Государств о борьбе с международным терроризмом") Принято в г. Астане 16 сентября 2004 г.

Нормативно-правовые акты Российской Федерации

Конституция Российской Федерации, Федеральные конституционные законы, доктрины и декларации

134. Конституция Российской Федерации от 12 декабря 1993 г. (с изменениями от 9 июня 2001 г.),
Федеральный Конституционный Закон РФ от 21 июля 1994 г. № 1-ФКЗ «О конституционном суде Российской Федерации»,
135. Декларация прав и свобод человека и гражданина (принята Верховным Советом РСФСР 22 ноября 1991 г.),

Кодексы

136. Уголовный Кодекс РФ (введен в действие Федеральным Законом от 13 июня 1996 г. N 63-ФЗ),
Гражданский Кодекс РФ (введен в действие федеральными законами: от 30 ноября 1994 г. № 51-ФЗ 1 часть; от 26 января 1996 г. № 14-ФЗ 2 часть; от 26 ноября 2001 г. № 146-ФЗ 3 часть, от 18.12.2006 № 230-ФЗ 4 часть-358 стр.),
137. Гражданский процессуальный кодекс РФ (введен в действие Федеральным законом от 14 ноября 2002 г. № 138-ФЗ),
138. Арбитражный процессуальный кодекс РФ (введен в действие Федеральным законом от 24 июля 2002 г. № 95-ФЗ),
139. Уголовно-процессуальный кодекс РФ (введен в действие Федеральным законом от 18 декабря 2001 г. № 174-ФЗ),
140. Таможенный кодекс Российской Федерации (введен в действие Законом РФ от 18 июня 1993 г. № 5221-1),
141. Налоговый кодекс Российской Федерации (Часть 1, введена в действие Федеральным Законом № 146-ФЗ от 31 июля 1998 г., Часть 2, введена в действие Федеральным Законом № 118-ФЗ от 5 августа 2000 г.),
142. Кодекс Российской Федерации об административных правонарушениях (введен в действие Федеральным Законом от 30 декабря 2001 г. № 195-ФЗ),
143. Трудовой Кодекс Российской Федерации» (введён в действие Федеральным Законом от 30.12.2001г. №197-ФЗ),

Законы

144. Федеральный Закон РФ от 3 апреля 1995 г. № 40-ФЗ «О Федеральной Службе безопасности» (с изменениями),
145. Федеральный Закон РФ от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»,

146. Федеральный Закон РФ от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»,
147. Федеральный Закон РФ от 3 февраля 1996 г. № 17-ФЗ «О банках и банковской деятельности»,
148. Закон РФ от 27 декабря 1991 г. № 2124-I «О средствах массовой информации»,
149. Закон РФ от 9 июля 1993 г. № 5351-I «Об авторском праве и смежных правах»,
150. Закон РФ от 18 апреля 1991 г. № 1026-I «О милиции» (с изменениями),
151. Федеральный Закон РФ от 13 января 1995 г. № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»,
152. Федеральный Закон от 29 декабря 1994 г. РФ № 77-ФЗ "Об обязательном экземпляре документов",
153. Закон РФ от 23 сентября 1992 г. № 3517-1 «Патентный закон Российской Федерации»,
154. Закон РФ от 23 сентября 1992 г. № 3520-1 «О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров»,
155. Закон РФ от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»,
156. Федеральный Закон от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»,
157. Федеральный Закон РФ от 29.07.2004г. № 98-ФЗ "О коммерческой тайне",
158. Федеральный Закон РФ от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи",
159. Федеральный Закон РФ от 8 августа 2001г. № 128-ФЗ "О лицензировании отдельных видов деятельности",
160. Федеральный Закон РФ от 23 августа 1996 г. № 127-ФЗ "О науке и государственной научно-технической политике",
161. Федеральный Закон РФ от 4 июля 1996 г. № 85-ФЗ "Об участии в международном информационном обмене", (утратил силу)
162. Федеральный Закон РФ от 24 ноября 1995 г. № 213-ФЗ "О государственном оборонном заказе",
163. Федеральный Закон РФ от 27.07.2006 № 149-ФЗ “Об информации, информационных технологиях и о защите информации”(Взамен ФЗ от 20 февраля 1995 г. № 24-ФЗ "Об информации, информатизации и защите информации"),
164. Федеральный Закон РФ от 7 июля 2003 г. № 126-ФЗ "О связи",
165. Закон РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне",
166. Федеральный закон от 10 января 1996 г. № 5-ФЗ «О внешней разведке»,
167. Федеральный Закон РФ от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»,
168. Федеральный Закон РФ от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»,
169. Закон РФ от 23 сентября 1992 г. № 3526-1 "О правовой охране топологий интегральных микросхем",
170. Закон РФ от 5 марта 1992 г. № 2446-1 «О безопасности»,
171. Федеральный Закон РФ от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг»,
172. Федеральный Закон РФ от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и религиозных объединений»,

173. Федеральный Закон РФ от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре»,
174. Закон РФ от 22 декабря 1992 г. № 4180-1 «О трансплантации органов и (или) тканей человека»,
175. Закон РФ от 27 ноября 1992 г. № 4015-1 «Об организации страхового дела в Российской Федерации»,
176. Закон РСФСР от 22 марта 1991 г. № 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках» (с изменениями),
177. Федеральный Закон РФ от 18 июля 1995 г. № 108-ФЗ «О рекламе»,
178. Закон Российской Федерации «О защите прав потребителей» от 07.02.1992г. №2300-1 (вред. 30.12.2001г.);
179. Основы законодательства Российской Федерации «Об охране здоровья граждан» (утверждены Верховным Советом РСФСР 22 июля 1993 г. № 5487-1), (с изменениями),
180. Основы законодательства Российской Федерации о нотариате (утверждены Верховным Советом РСФСР 11 февраля 1993 г. № 4462-1), (с изменениями),
181. Федеральный Закон РФ от 30.12.2004 г. № 218-ФЗ «О кредитных историях»,
182. Федеральный Закон РФ от 21.07.2005 г. № 110-ФЗ «О внесении изменений в 183. Федеральный Закон «О кредитных историях»,
184. Федеральный Закон РФ от 06 марта 2006 г. № 35-ФЗ «О противодействии терроризму»,
185. Федеральный Закон РФ от 27 июля 2006 г. № 153-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием 186. Федерального закона «О ратификации Конвенции Совета Европы о предупреждении терроризма» и Федерального закона «О противодействии терроризму»,
187. Федеральный Закон РФ от 09 февраля 2007 г. № 16-ФЗ «О транспортной безопасности».

Указы, распоряжения и иные акты Президента Российской Федерации

188. Доктрина Информационной Безопасности Российской Федерации, (утверждена Президентом РФ 9 сентября 2000 № Пр-1895),
189. Указ Президента РФ от 28 июня 1993 г. № 966 «О концепции правовой информатизации России»,
190. Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, составляющих государственную тайну»,
191. Указ Президента РФ от 24 января 1998 г. № 61 «О перечне сведений, составляющих государственную тайну»,
192. Указ Президента РФ от 12 мая 2004 г. № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена»,
193. Указ Президента РФ от 14 января 1992 г. № 20 «О защите государственных секретов Российской Федерации»,
194. Указ президента РФ от 8 ноября 1995 года № 1108 «О Межведомственной комиссии по защите государственной тайны»,
195. Указ Президента РФ от 20 января 1996 года № 71 «Вопросы Межведомственной комиссии по защите государственной тайны», с прилагаемым «Положением о Межведомственной комиссии по защите государственной тайны»,
196. Указ Президента Российской Федерации от 1 ноября 1999 г. № 1467 «О составе Межведомственной комиссии по защите государственной тайны по

должностям» (в редакции от 5 октября 2001 г.), с прилагаемым «Составом Межведомственной комиссии по защите государственной тайны по должностям»
197. Указ Президента РФ от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»,
198. Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации»,
199. Указ Президента Российской Федерации от 8 мая 1993 г. № 644 «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам»,
200. Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (в редакции 30.12.2000г.)
201. Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной Службы по техническому и экспортному контролю»,
202. Указ Президента РФ от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях права граждан на информацию»,
203. Указ Президента РФ от 10 января 2000 г. № 24 «О концепции национальной безопасности Российской Федерации»,
204. Указ Президента РФ от 17 декабря 1997 г. № 1300 "Об утверждении Концепции национальной безопасности Российской Федерации",
205. Указ Президента РФ от 20 января 1996 г. № 71 «Вопросы межведомственной комиссии по защите государственной тайны»,
206. Указ Президента РФ от 20 мая 2004 г. № 649 «Вопросы структуры федеральных органов исполнительной власти»,
207. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»,
208. Распоряжение Президента РФ от 16 апреля 2005 г. № 151-рп «Об утверждении перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне» с приложением «Перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне».

Постановления и распоряжения Правительства Российской Федерации

209. Постановление Правительства РФ от 30 августа 2001 г. № 647 «Об утверждении Порядка разработки списка продукции военного назначения, разрешенной к передаче иностранным заказчикам, и Порядка разработки списка государств, в которые разрешена передача продукции военного назначения, указанной в списке продукции военного назначения, разрешенной к передаче иностранным заказчикам»,
210. Постановление Правительства РФ от 29 августа 2001 г. № 633 «О порядке размещения и использования на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации иностранных технических средств наблюдения и контроля»,
211. Постановление Правительства РФ от 11 февраля 2002 г. № 135 «О лицензировании отдельных видов деятельности»,

212. Постановление Правительства РФ от 23 сентября 2002 г. № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»,
213. Постановление Правительства РФ от 13 декабря 1999 г. № 1384 «Об утверждении Положения об участии российских организаций в проведении выставок и показов продукции военного назначения»,
214. Постановление Правительства РФ от 28 февраля 1996 г. № 226 «О государственном учете и регистрации баз и банков данных»,
215. Постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»,
216. Постановление Правительства РФ от 30 апреля 2002 г. № 290 «О лицензировании деятельности по технической защите конфиденциальной информации»,
217. Постановление Правительства РФ от 26 июня 2004 г. № 311 «Об утверждении Положения о Министерстве информационных технологий и связи Российской Федерации»,
218. Постановление Правительства РФ от 30 июня 2004 г. № 319 «Об утверждении Положения о Федеральном агентстве по информационным технологиям»,
219. Постановление Правительства РФ от 28 января 2002 г. № 65 «О Федеральной целевой программе «Электронная Россия (2002-2010 годы)»,
220. Постановление Правительства РФ от 12 февраля 2003 г. № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»,
221. Постановление Правительства РФ от 18 февраля 2005 г. № 87 "Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий",
222. Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»,
223. Постановление Правительства РФ от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»,
224. Постановление Правительства РФ от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности»,
225. Постановление Правительства РФ от 9 июня 1995 г. № 578 «Об утверждении правил охраны линий и сооружений связи Российской Федерации»,

226. Постановление Правительства РФ от 30 июня 2004 г. № 318 «Об утверждении Положения о Федеральной службе по надзору в сфере связи»,
227. Распоряжение Правительства РФ от 27 августа 2005 г. № 1314-Р «Об одобрении Концепции Федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов»,
228. Постановление Правительства РФ от 28 октября 1995г. № 1050 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» с прилагаемой «Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне»,
229. Постановление Правительства РФ от 15 сентября 1993 г. № 912-51 «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам»
230. Постановление Правительства РФ от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» с прилагаемыми «Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности»,
231. Постановление Правительства РФ от 27 мая 2002 г. № 348 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации» с прилагаемым «Положением о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»,
232. Постановление Правительства РФ от 17 июня 2004 г. № 301 «О Федеральной Службе по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия»,
233. Постановление Правительства РФ от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»,
234. Постановление Правительства РФ от 27.04.2005 № 260 "О мерах по государственной поддержке молодых российских ученых - кандидатов наук и их научных руководителей, молодых российских ученых - докторов наук и ведущих научных школ Российской Федерации" (вместе с "Положением о совете по грантам Президента Российской Федерации для государственной поддержки молодых российских ученых и по государственной поддержке ведущих научных школ Российской Федерации", "Положением о выделении грантов Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук и их научных руководителей, молодых российских ученых - докторов наук и средств для государственной поддержки ведущих научных школ Российской Федерации").

Акты Федеральной Службы безопасности Российской Федерации, а также Федерального Агентства правительственной связи и информации при Президенте Российской Федерации

235. Федеральная Служба безопасности Российской Федерации. Приказ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005).
236. Федеральная Служба безопасности Российской Федерации. Приказ от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений,

составляющих государственную тайну, и о ее знаках соответствия» (Система сертификации СЗИ-ГТ),

237. Федеральная Служба безопасности Российской Федерации. «Инструкция о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну» (утверждена Директором ФСБ РФ 23 августа 1995 г. № 28),

238. «Положение о государственном лицензировании деятельности в области защиты информации». Утверждено решением Гостехкомиссии при Президенте Российской Федерации и Федерального Агентства правительственной связи и информации при Президенте Российской Федерации от 24 апреля 1994 г. № 10 (в редакции решения от 24 июня 1997 г. № 60);

239. «Система сертификации средств криптографической защиты информации» (N РОСС RU.0001.03001). Утверждена Генеральным директором Федерального Агентства правительственной связи и информации при Президенте Российской Федерации 28 октября 1993 г., регистрационный номер Госстандарта присвоен 15 ноября 1993 г.

240. Приказ Федерального Агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 (зарегистрирован в Минюсте 6 августа 2001 г. под № 2848) «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» с прилагаемой «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической зашиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»,

Акты Федеральной Службы по техническому и экспортному контролю(ФСТЭК), включая акты Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России)

241. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации». Руководящий документ Гостехкомиссии России,

242. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Руководящий документ Гостехкомиссии России,

243. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Руководящий документ Гостехкомиссии России,

244. «Защита информации. Специальные защитные знаки. Классификация и общие требования». Руководящий документ Гостехкомиссии России,

245. «Защита от несанкционированного доступа к информации. Термины и определения». Руководящий документ Гостехкомиссии России,

246. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Руководящий документ Гостехкомиссии России,

247. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1. Часть 2. Часть 3. Руководящий документ Гостехкомиссии России,
248. «Инструкция о порядке проведения специальных экспертиз предприятий, учреждений и организаций на право осуществления мероприятий и (или) оказания услуг в области противодействия иностранной технической разведке». Утверждена Председателем Гостехкомиссии 17 октября 1995 г.
249. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России,
250. Решение Гостехкомиссии от 3 октября 1995 г. № 42 «О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте»,
251. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Председателем Гостехкомиссии России 25 ноября 1994 г.
252. Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации. Утверждено Председателем Гостехкомиссии России 25 ноября 1994 г.
253. Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3,
254. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3,
255. Типовое положение об испытательной лаборатории. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3,
256. «Перечень средств защиты информации, подлежащих сертификации в системе сертификации Гостехкомиссии России» (N РОСС RU.0001.01БИ00);
257. «Положение о государственном лицензировании деятельности в области защиты информации». Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27.04.1994г. №10;
258. «Положение о сертификации средств защиты информации по требованиям безопасности информации». Введено в действие Приказом Председателя Гостехкомиссии России от 27.10.1995г. №199;
259. «Положение по аттестации объектов информатизации по требованиям безопасности информации». Утверждено Председателем Гостехкомиссии при Президенте Российской Федерации 25 ноября 1994 г.,
260. «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР-97)» от 23 мая 1997 г. № 55,
261. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России,
262. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Руководящий документ Гостехкомиссии России.

263. «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации». Руководящий документ Гостехкомиссии России;
264. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР — К)»,
265. Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам. Руководящий документ Гостехкомиссии России,
266. «Положение о государственном лицензировании деятельности в области защиты информации». Утверждено решением Гостехкомиссии при Президенте Российской Федерации и ФАПСИ при Президенте Российской Федерации от 24 апреля 1994 г. № 10 (в редакции решения от 24 июня 1997 г. № 60);

Акты других ведомств

267. «Концепция информатизации Министерства юстиции РФ», утверждена приказом Министерства юстиции РФ от 21 января 2000 г. № 10,
Проект документа «Концепция информационной безопасности сетей связи общего пользования Взаимоувязанной сети связи Российской Федерации»,
268. ОТТ 1.1.8-90 Система общих технических требований к видам вооружения и военной техники. Системы и комплексы (образцы) вооружения и военной техники. Общие требования по защите от иностранной технической разведки,

Судебные акты

269. Инструктивные указания Государственного Арбитража СССР от 29 июня 1979 г. № И-1-4 «Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники»,
270. Письмо Высшего Арбитражного суда Российской Федерации от 19 августа 1994 г. № С1-7/ОП-587 (в редакции 12 сентября 1996 г.) «Об отдельных рекомендациях, принятых на совещаниях по судебно-арбитражной практике. Раздел IV. Могут ли подтверждаться обстоятельства дела доказательствами, изготовленными и подписанными с помощью средств электронно-вычислительной техники, в которых использована система цифровой (электронной) подписи»
271. Письмо Высшего Арбитражного суда Российской Федерации от 7 июня 1995 г. №С1-7/03-316 «О Федеральном законе «Об информации, информатизации и защите информации»,

Стандарты, действующие на территории Российской Федерации

272. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
273. ГОСТ Р 50922-96 Защита информации. Основные термины и определения,
274. ГОСТ Р 51000.5 Общие требования к органам по сертификации продукции и услуг,
275. ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения»,
276. ГОСТ Р 51188-98 Испытания программных средств на наличие компьютерных вирусов. Типовое руководство,

277. ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищённом исполнении,
278. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищённом исполнении,
279. ГОСТ Р 51275-99 Защита информации. Объекты информатизации. Факторы, воздействующие на информацию. Общие положения,
280. ГОСТ Р 34.10-94 Системы обработки информации. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма,
281. ГОСТ Р 34.11-94 Информационная технология. Криптографическая обработка информации. Функция хэширования,
282. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования,
283. ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты,
284. ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения,
285. ГОСТ 26883-86. Внешние воздействующие факторы. Термины и определения,
286. ГОСТ 15971-90 «Системы обработки информации. Термины и определения»,
287. ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель,
288. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации,
289. ГОСТ Р ИСО/МЭК 15408-1-2000 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель,
290. ГОСТ Р ИСО/МЭК 15408-2-2000 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности,
291. ГОСТ Р ИСО/МЭК 15408-3-2000 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности,
292. ГОСТ Р ИСО/МЭК 27001: 2005. «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
293. Стандарт Банка России СТО БР ИББС-1.0-2004 «Обеспечение информационной безопасности организаций банковской системы российской федерации общие положения»,
294. ОСТ 45.127-99 Система обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации. Термины и определения,
295. ОСТ В1 00464-97. Защита информации об авиационной технике и вооружении от иностранных технических разведок. Термины и определения.

Стандарты и рекомендации Банка России
http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd

296. Стандарт Банка России:"Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности" (СТО БР ИББС-1.1-2007)

297. Стандарт Банка России:"Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0-2006" (СТО БР ИББС-1.2-2007)

298. Обеспечение информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС-1.0-2006)

299. Обеспечение информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС-1.0-2004)