Н.С. Кармановский, О.В. Михайличенко, С.В. Савков

ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

САНКТ-ПЕТЕРБУРГ
2013

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ**

**Н.С. Кармановский, О.В. Михайличенко,
С.В. Савков**

ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Санкт-Петербург

2013

Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.

Пособие охватывает теоретический материал, читаемый в рамках курса «Организационно-правовые механизмы обеспечения информационной безопасности». Материал пособия включает теоретические сведения о видах тайн, основные понятия государственной и коммерческой тайны. Приведена система организационной защиты информации на примере предприятия. Учебное пособие включает обзор современных нормативных и методических документов в области обеспечения безопасности информации.

Пособие адресовано студентам, обучающимся по направлению 090900 «Информационная безопасность».

Рекомендовано к печати Ученым советом факультета КТиУ, протокол №5 от 14.05.2013г.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Учебная дисциплина «Организационно-правовое и методическое обеспечение информационной безопасности» является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Она призвана обеспечить освоение студентами практических навыков работы с нормативно-правовой базой деятельности в области обеспечения информационной безопасности автоматизированных систем.

Целью дисциплины является получение знаний:

– основ организационного и правового обеспечения информационной безопасности;

– основных нормативных правовых актов в области обеспечения информационной безопасности и нормативных методических документов ФСБ России и ФСТЭК России в области защиты информации;

– правовых основ организации защиты государственной тайны и конфиденциальной информации;

– задач органов защиты государственной тайны и служб защиты информации на предприятиях;

– организации работы и нормативных правовых актов и стандартов по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

После изучения дисциплины студенты должны уметь:

– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;

– разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

В результате изучения дисциплины студенты должны приобрести навыки:

– работы с нормативными правовыми актами;

– организации и обеспечения режима секретности;

– владения методами организации и управления деятельностью служб защиты информации на предприятии,

– методами формирования требований по защите информации.

1 ПОНЯТИЕ ТАЙНЫ. ВИДЫ ТАЙН

Государственная безопасность – система гарантий государства от угроз извне и основам конституционного строя внутри страны.

Для реализации этих гарантий в стране создана и функционирует система защищаемых законом тайн.

Под тайной понимается нечто скрываемое от других, известное не всем, секрет.

Существует большое число охраняемых законом тайн:

– государственная тайна;
– коммерческая тайна;
– тайна личной жизни;
– банковская тайна;
– налоговая тайна;
– врачебная тайна;
– тайна усыновления;
– тайна связи;
– налоговая тайна;
– нотариальная тайна;
– адвокатская тайна;
– тайна страхования;
– служебная тайна;
– персональные данные;
– тайна голосования;
– тайна исповеди;
– и другие виды тайн.

Тайна – это, прежде всего, сведения, информация. Признаки тайны:

- сведения должны быть известны или доверены узкому кругу лиц;
- сведения не подлежат разглашению (огласке);
- разглашение сведений (информации) может повлечь наступление негативных последствий (материальный или моральный ущерб ее собственнику, владельцу, пользователю или иному лицу);
- на лицах, которым доверена информация, не подлежащая оглашению, лежит правовая обязанность ее хранить;
- за разглашение этих сведений устанавливается законом юридическая ответственность.

Государственной и Коммерческой тайне будут посвящены отдельные разделы пособия. Здесь остановимся на некоторых других видах тайн.

Тайна личной жизни

Неприкосновенность частной жизни означает охрану законом личной и семейной тайны. Гарантии неприкосновенности частной жизни устанавливают запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

В России это право провозглашается статьями 23, 24 и 25 Конституции Российской Федерации. К нормативным актам, регулирующим защиту права на неприкосновенность частной жизни также относятся Федеральный закон «О персональных данных», Гражданский кодекс, а также ряд международных договоров, прежде всего Всеобщая декларация прав человека, Европейская конвенция о защите прав человека и основных свобод, Международный пакт о гражданских и политических правах.

Право на неприкосновенность частной жизни может быть ограничено только в порядке, предусмотренном законодательством, как правило, только по судебному решению.

Банковская тайна

К основным объектам банковской тайны относятся: тайна банковского счета, тайна операций по банковскому счету, тайна банковского вклада, тайна частной жизни клиента.

Согласно статье 26 закона «О банках и банковской деятельности» к банковской тайне относится информация об операциях, счетах и вкладах клиентов и корреспондентов. По российскому законодательству кредитная организация гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. При разглашении банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, может потребовать от того возмещения причиненных убытков.

Данные, составляющие банковскую тайну, предоставляются клиентам, их представителям, судам, Счетной палате, налоговым, следственным и таможенным органам и др. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом.

Врачебная тайна

Врачебная тайна – это вся информация, касающаяся факта обращения гражданина за медицинской помощью, состояния здоровья гражданина, диагноза его болезни и иные данные, полученные при его обследовании и лечении. Эта информация являются тайной вне зависимости от формы обращения человека к медикам и его результатов.

Медицинским работникам запрещено сообщать третьим лицам информацию о состоянии здоровья пациента, диагнозе, результатах обследования, самом факте обращения за медицинской помощью и сведений о личной жизни, полученных при обследовании и лечении. Соблюдение врачебной тайны распространяется также на всех лиц, которым эта информация стала известна в случаях, предусмотренных законодательством.

Главная правовая норма в отечественном законодательстве, регулирующая врачебную тайну – статья 61 «Основ законодательства РФ об охране здоровья граждан».

Передавать сведения, составляющие врачебную тайну, допускается только с письменного согласия гражданина или его законного представителя другим лицам в интересах обследования и лечения пациента для реализации прав и законных интересов, проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях. При этом не должны разглашаться паспортные данные и сведения, способствующие узнаванию.

В тоже время необходимый обмен информацией специалистами в ходе лечения не рассматривается как нарушение врачебной тайны.

Тайна усыновления

На данный момент, в соответствии со статьей 139 Семейного кодекса РФ, тайна усыновления ребёнка в России охраняется законом.

Тайна усыновления должна соблюдаться лишь по желанию самих усыновителей, и, касается, главным образом, случаев усыновления новорождённых или малолетних детей. Для обеспечения тайны усыновления, по просьбе усыновителей, допускается изменение места рождения, а также даты рождения ребёнка, но не более чем на 3 месяца. Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка.

Лица, разгласившие тайну усыновления ребенка против воли его усыновителей, привлекаются к ответственности в установленном законом порядке. Разглашение тайны усыновления, вопреки воле усыновителя, может повлечь за собой штраф, исправительные работы или другие виды уголовного наказания, в соответствии со статьей 155 Уголовного кодекса.

Тайна связи

В России тайна связи гарантируется Конституцией Российской Федерации. Часть 2 статьи 23 гласит:

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

Правом на тайну связи охватываются личные сообщения, находящиеся в любых каналах связи или в распоряжении оператора связи, от момента отправки сообщения отправителем до момента получения сообщения адресатом. Служебные и рекламные сообщения не защищаются правом на тайну связи, однако это не означает, что служебные каналы связи разрешено негласно контролировать (производить перлюстрацию). Не следует путать право личности на тайну связи с правом лиц на коммерческую тайну, профессиональную тайну (адвокатскую, врачебную и т. д.). Другие виды тайн, также охраняются законом, но термин «тайна связи» относится только к личной жизни.

На всех операторов связи законом возложена обязанность принимать меры к охране тайны связи (ст. 63 закона РФ «О связи»).

Нарушением тайны связи признаётся ознакомление с охраняемым сообщением какого-либо лица кроме отправителя и получателя (или его уполномоченного представителя). В некоторых видах связи, в силу их технических особенностей, допускается ознакомление с сообщением отдельных работников связи, как, например, при передаче телеграммы. В таких случаях нарушением будет считаться не ознакомление, а разглашение содержания сообщения. Наравне с самим сообщением, также охраняются сведения о сообщении; для телефонных переговоров это номера вызывающего и вызываемого абонента, время звонка и его продолжительность.

За нарушение тайны связи в России установлена уголовная ответственность (ст. 138 УК РФ). Также возможна гражданско-правовая ответственность, если нарушение тайны связи повлекло материальный ущерб или моральный вред.

Налоговая тайна

Налоговая тайна – право налогоплательщика на неразглашение информации, предоставленной налоговым органам, гарантированное ст. 102 Налогового Кодекса. Налоговую тайну составляют любые полученные налоговым органом, 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, о взаимном сотрудничестве между налоговыми (таможенны-

ми) или правоохранительными органами (в части сведений, предоставленных этим органам); предоставляемых избирательным комиссиям в соответствии с законодательством о выборах по результатам проверок налоговым органом сведений о размере и об источниках доходов кандидата и его супруга, а также об имуществе, принадлежащем кандидату и его супругу на праве собственности.

Налоговая тайна не подлежит разглашению налоговыми органами, органами государственных внебюджетных фондов и таможенными органами, их должностными лицами и привлекаемыми специалистами, экспертами, за исключением случаев, предусмотренных федеральным законом.

К разглашению налоговой тайны относится, в частности, использование или передача другому лицу производственной или коммерческой тайны налогоплательщика, ставшей известной должностному лицу налогового органа, органа государственного внебюджетного фонда или таможенного органа, привлеченному специалисту или эксперту при исполнении ими своих обязанностей. Поступившие в налоговые органы, органы государственных внебюджетных фондов или таможенные органы сведения, составляющие налоговую тайну, имеют специальный режим хранения и доступа. Доступ к сведениям, составляющим налоговую тайну, имеют должностные лица по перечням, определяемым соответственно МНС, органами государственных внебюджетных фондов и ГТК. Утрата документов, содержащих составляющие налоговую тайну сведения, либо разглашение таких сведений влечет ответственность, предусмотренную федеральными законами.

Нотариальная тайна

Нотариальная тайна (тайна нотариальных действий) – разновидность профессиональной тайны. Согласно ст. 19 Основ законодательства РФ о нотариате нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с его профессиональной деятельностью. Суд может освободить нотариуса от обязанности сохранения тайны, если против него возбуждено уголовное дело в связи с совершением нотариального действия. Поскольку нотариусы предоставляют информацию о совершенных ими нотариальных действиях нотариальным палатам, должностные лица этих палат также обязаны сохранять нотариальную тайну.

Адвокатская тайна

Адвокатская тайна включает в себя те сведения, которые сообщены адвокату в силу носимого им звания и разглашение которых противоречит интересам лица, их сообщившего. Адвокатской тайной являются

любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием. Проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения. Полученные в ходе оперативно-розыскных мероприятий или следственных действий (в том числе после приостановления или прекращения статуса адвоката) сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей. Указанные ограничения не распространяются на орудия преступления, а также на предметы, которые запрещены к обращению или оборот которых ограничен в соответствии с законодательством Российской Федерации.

Соблюдение профессиональной тайны является безусловным приоритетом деятельности адвоката. Срок хранения тайны не ограничен во времени. Адвокат не может быть освобожден от обязанности хранить профессиональную тайну никем, кроме доверителя.

Без согласия доверителя адвокат вправе использовать сообщенные ему доверителем сведения в объеме, который адвокат считает разумно необходимым для обоснования своей позиции при рассмотрении гражданского спора между ним и доверителем или для своей защиты по возбужденному против него дисциплинарному производству или уголовному делу.

Правила сохранения профессиональной тайны распространяются на:

- факт обращения к адвокату, включая имена и названия доверителей;
- все доказательства и документы, собранные адвокатом в ходе подготовки к делу;
- сведения, полученные адвокатом от доверителей;
- информацию о доверителе, ставшую известной адвокату в процессе оказания юридической помощи;
- содержание правовых советов, данных непосредственно доверителю или ему предназначенных;
- все адвокатское производство по делу;
- условия соглашения об оказании юридической помощи, включая денежные расчеты между адвокатом и доверителем;
- любые другие сведения, связанные с оказанием адвокатом юридической помощи.

Тайна страхования

Тайна страхования – разновидность служебной, а также коммерческой тайны. Согласно ст. 946 ГК РФ 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 отвечает по правилам, предусмотренным положением ГК РФ о служебной и коммерческой тайне. Лица, незаконными методами получившие информацию, которая составляет тайну страхования, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших тайну страхования вопреки трудовому договору, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Служебная тайна

Служебная тайна – информация с ограниченным доступом, за исключением сведений, отнесенных к государственной тайне и персональным данным, содержащаяся в государственных (муниципальных) информационных ресурсах, накопленная за счет государственного (муниципального) бюджета и являющаяся собственностью государства, защита которой осуществляется в интересах государства.

Служебная тайна – защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости. Однозначное определение понятия «служебная тайна» в действующем законодательстве РФ отсутствует. Служебная тайна является одним из объектов гражданских прав по гражданскому законодательству РФ. Режим защиты служебной тайны в целом аналогичен режиму защиты коммерческой тайны. В ряде случаев за разглашение служебной тайны закон предусматривает уголовную ответственность (например, за разглашение тайны усыновления, или за разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, лицом, которому такие сведения стали известны по службе).

Персональные данные

Персональные данные (или личные данные) – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Работы по защите персональных данных проводятся на основе требований нормативных документов по защите персональных данных:

- Федерального Закона РФ от 27.07. 2006 № 152 – ФЗ "О персональных данных";
- Постановления правительства РФ от 17.11.2007 г. № 781 об утверждении "Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных";
- Приказа Федеральной службы по техническому и экспортному контролю России (ФСТЭК России), Федеральной службы безопасности российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 № 55/86/20 г. Москва "Об утверждении порядка классификации информационных систем персональных данных".
- Методических документов ФСБ России по защите персональных данных:
    - "Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации";
    - "Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных".
- Методических документов ФСТЭК России в области персональных данных:
    - "Базовая модель угроз безопасности ПДн при их обработке в ИСПДн";
    - "Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн";
    - "Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн";
    - "Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн".

Тайна голосования

Принцип тайного голосования – конституционный принцип, гарантирующий гражданам Российской Федерации тайну их волеизъявления

при голосовании на выборах в органы государственной власти и местного самоуправления и референдуме.

Тайна голосования исключает возможность какого-либо контроля за волеизъявлением гражданина, гарантирует, что результаты его голосования не могут стать известны иным лицам. Данный принцип обеспечивает свободу волеизъявления граждан. Никто не может принудить гражданина голосовать за или против того или иного кандидата, за или против решения, вынесенного на референдум.

Тайна голосования обеспечивается специальными процедурами, предусмотренными законодательством о выборах и референдуме. Гражданин получает бюллетень для голосования, изготовленный по единому образцу, и заполняет его в специально оборудованном месте, обеспечивающем тайну его волеизъявления. В бюллетенях не допускаются какие-либо обозначения и пометки, указывающие на личность лица, его заполнившего. Законодательством также устанавливаются гарантии соблюдения тайны волеизъявления при проведении досрочного голосования и голосования вне помещений избирательных комиссий, комиссий референдума. (См. досрочное голосование, голосование вне помещения для голосования).

Нарушение принципа тайны голосования членами избирательных комиссий, комиссий референдума, должностными лицами влечет привлечение виновных к уголовной и административной ответственности.

Тайна исповеди

Тайна исповеди – самостоятельный вид охраняемых законом тайн, одна из гарантий свободы вероисповедания. В соответствии с п. 7 ст. 3 ФЗ "О свободе совести и о религиозных объединениях" от 26 сентября 1997 г. и охраняется законом. Согласно УПК РФ (п. 4 ч. 3 ст. 56) священнослужитель не может быть допрошен в качестве свидетеля об обстоятельствах, ставших ему известными из исповеди.

2 ОБЩЕСИСТЕМНАЯ КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Задача защиты информации успешно реализуется только при системном подходе к ее решению. С этой целью предложена следующая классификация методов защиты информации.

По классу решаемых задач:
– технические,
– программные,
– организационные,
– криптографические.

По виду решаемых задач:
– резервирование,
– введение избыточности,
– регулирование доступа,
– регулирование использования,
– защитные преобразования,
– контроль,
– регистрация,
– уничтожение,
– сигнализация,
– реагирование.

По функциональному назначению:
– самостоятельное решение средств защиты,
– решение задач защиты в комплексе с другими средствами,
– управление средствами защиты,
– обеспечение функционирования механизмов защиты.

Организационные методы позволяют решать задачи защиты информации как самостоятельно, так и «подкрепляют» и дополняют другие методы защиты. К организационным методам защиты информации относятся организационно-технические и организационно-правовые мероприятия. Вместе с тем в общем комплексе методов и средств защиты информации, организационные методы играют особую роль по следующим причинам:

- повышенное влияние случайных факторов,
- неформальный характер,
- наличие «человеческого фактора».

3 ФОРМИРОВАНИЕ И СТАНДАРТИЗАЦИЯ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Законодательная и нормативная база по информационной безопасности в Российской Федерации

Информационное обеспечение управленческих, финансовых, технологических и производственных бизнес-процессов является основой экономической устойчивости организации, а информация становится важным корпоративным ресурсом, который необходимо защищать.

Для обеспечения конфиденциальности, целостности и доступности информации, а также сохранения устойчивости функционирования информационных систем в условиях угроз, реализуемых посредством целенаправленных деструктивных информационных воздействий на критически важные объекты информационной инфраструктуры, в организации формируются требования к обеспечению ИБ.

Формирование требований к обеспечению ИБ осуществляется с учетом:

- юридических, законодательных, регулирующих и договорных требований, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг;
- результатов оценки рисков организации. Посредством оценки рисков осуществляется выявление актуальных угроз активов организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий;
- принципов и целей в отношении обработки информации, определенных организацией.

Формирование требований к обеспечению ИБ организации и информационных систем осуществляется с учетом нормативных и правовых актов РФ, а также с учетом разработанных стандартов и рекомендаций, апробированных на практике и признанных профессиональными сообществами специалистов в области ИБ.

Законодательную и нормативную базу в области обеспечения ИБ в РФ можно представить как совокупность правовых актов, организационно-распорядительных, нормативных, методических и отраслевых документов по технической защите информации.

Законодательная и нормативная база в области обеспечения ИБ РФ представлена на рисунке 1.

Рисунок 1 – Законодательная и нормативная база в области обеспечения ИБ РФ

Нормативные правовые документы по технической защите информации

Нормативный правовой акт – это письменный официальный документ, принятый (изданный) в определенной форме правотворческим органом в пределах его компетенции и направленный на установление, изменение или отмену правовых норм. В свою очередь, под правовой нормой принято понимать общеобязательное государственное предписание постоянного или временного характера, рассчитанное на многократное применение.

К нормативным правовым документам (актам) РФ по технической защите информации относятся:

1. Конституция РФ.
2. Кодексы РФ

3. Федеральные законы.
4. Указы и распоряжения Президента РФ.
5. Постановления Правительства РФ.
6. Приказы федеральной службы по техническому и экспортному контролю (ФСТЭК).

Конституция Российской Федерации

Основным нормативным правовым документом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 23 каждый имеет право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а в соответствии со статьей 29 каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений подразумевает, в том числе и обеспечение конфиденциальности данных, при их обработке, хранении и передаче по каналам связи, а также использование средств защиты информации.

В соответствии со статьей 41 гарантируется право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей и статьей 42 – право на знание достоверной информации о состоянии окружающей среды. В современных условиях наиболее практичным и удобным источником информации для граждан являются информационные ресурсы (серверы), созданные соответствующими законодательными, исполнительными и судебными органами. Публикуемая информация должна быть защищена с учетом обеспечения её доступности и целостности.

Уголовный кодекс Российской Федерации

Уголовный кодекс Российской Федерации (в ред. от 27.07.2012 г) включает в себя главу 28 "Преступления в сфере компьютерной информации", содержащую три статьи:

1. Статья 272. Неправомерный доступ к компьютерной информации.
2. Статья 273. Создание, использование и распространение вредоносных программ.
3. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Согласно статье 272 под неправомерным доступом к охраняемой законом компьютерной информации, понимается доступ, в результате которого произошло неправомерное уничтожение, блокирование, модификация либо копирование компьютерной информации.

Согласно статье 273 считается уголовно наказуемым создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Согласно статье 273 нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, наступает в случае, если нарушение повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, с причинением крупного ущерба.

Статья 138 Уголовного кодекса РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 Уголовного кодекса РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».

Кодекс РФ об административных правонарушениях

Кодекс РФ об административных правонарушениях, принятый 30.12.2001, содержит главу 13 «Административные правонарушения в области связи и информации», включающую в себя следующие статьи, касающиеся нарушений в области защиты информации:

1. Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).
2. Статья 13.2 Нарушение правил защиты информации.
3. Статья 13.13. Незаконная деятельность в области защиты информации.
4. Статья 13.14. Разглашение информации с ограниченным доступом.

Статья 13.2 налагает административную ответственность за:

- нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации;
- использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации.

Статья 13.3 налагает административную ответственность за занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в уста-

новленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна).

Статья 13.14 налагает административную ответственность за 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.

Федеральные законы по технической защите информации

В РФ разработаны и введены в действие следующие федеральные законы в области обеспечения ИБ:

1. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
2. Федеральный закон РФ от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
3. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи».
4. Федеральный закон РФ от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
5. Федеральный закон РФ от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных».
8. Федеральный закон РФ от № 390-ФЗ от 28.12.2010 «О безопасности».

Указы и распоряжения Президента РФ по технической защите информации

Президентом РФ подписаны следующие указы в области обеспечения ИБ:

1. Указ Президента РФ от 16.08.2004 № 1085 «Вопросы федеральной службы по техническому и экспортному контролю».
2. Указ Президента РФ от 30.11.1995 №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».
3. Указ Президента РФ от 23.09.2005 № 1111 «Об утверждении перечня сведений конфиденциального характера».
4. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при исполь-

зовании информационно-телекоммуникационных сетей международного информационного обмена».
5. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Положение о Федеральной службе по техническому и экспортному контролю».

Постановления Правительства РФ по технической защите информации

К постановлениям Правительства РФ по технической защите информации относятся:

1. Постановление Совета министров-правительства РФ от 15.09.1993 года № 912-51 «Положение о государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам».
2. Постановление Правительства РФ от 03.101994 года № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
3. Постановление Правительства РФ от 15.04.1995 года № 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».
4. Постановление Правительства РФ от 26.06.1995 № 608 "О сертификации средств защиты информации».
5. Постановление Правительства РФ от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности».
6. Постановление Правительства РФ от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».
7. Постановление Правительства РФ от 03.02.2012 № 79 «Лицензировании деятельности по технической защите конфиденциальной информации».
8. Постановление Правительства РФ от 16.04.2012 №313 «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных

систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Приказы ФСТЭК

В рамках обеспечения технической защиты информации ФСТЭК выпустил следующие приказы.

1. Приказ ФСТЭК России от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».
2. Приказ ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

Организационно-распорядительные документы по технической защите информации

К организационно-распорядительным документам по технической защите информации относятся:

1. Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента РФ от 12.05.2009 № 537.
2. Доктрина информационной безопасности Российской Федерации, утвержденная приказом Президента РФ от 09.09.2010.
3. Положение «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств …», утвержденное постановлением Правительства РФ от 16 апреля 2012 г. № 313.
4. Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Государственной технической комиссии при Президенте РФ 25.11.1994.

Нормативные и методические документы по технической защите информации

Государственные стандарты

Стандарт – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

Государственный стандарт – национальный стандарт, принятый федеральным органом исполнительной власти по стандартизации или федеральным органом исполнительной власти по строительству.

В Российской Федерации федеральным законом о техническом регулировании № 184-ФЗ от 27.12.2002 г разделены понятия «технический регламент» и «стандарты» , в связи с чем, все стандарты должны утратить обязательный характер и применяться добровольно. До 1 сентября 2011 года в период до принятия соответствующих технических регламентов закон предусматривал обязательное исполнение требований стандартов 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. С 1 сентября 2011 года все нормативные правовые акты и нормативные документы в области технического регулирования, не включенные в перечень обязательных, имеют добровольное применение.

К нормативным документам по технической защите информации относятся следующие государственные стандарты (ГОСТ):

1. ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».
2. ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
3. ГОСТ Р 51188-98. «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».
4. ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».
5. ГОСТ Р 51583-2000. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования».

6. ГОСТ Р 52447-2005. «Защита информации. Техника защиты информации. Номенклатура показателей качества».
7. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
8. ГОСТ Р 51241-2008. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
9. ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
10. ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
11. ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».
12. ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».
13. ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности».

Российские государственные стандарты серии «Информационная технология»

В РФ приняты следующие стандарты серии «Информационные технологии» аутентичные международным стандартам:

1. ГОСТ Р ИСО/МЭК 27001-2006 «Системы менеджмента информационной безопасности. Требования».
2. ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью (на основе ISO/IEC 17799:2000)».
3. ГОСТ Р ИСО/МЭК 27004-2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
4. ГОСТ Р ИСО/МЭК 27006-2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

5. ГОСТ Р ИСО/МЭК ТО 13335-1-2006 «Информационная технология. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
6. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы менеджмента безопасности информационных технологий».
7. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Выбор защитных мер».
8. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Руководство по менеджменту безопасности сети».
9. ГОСТ Р ИСО/МЭК 15408-2002-1. «Информационная технология. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».
10. ГОСТ Р ИСО/МЭК 15408-2002-2. «Информационная технология. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования».
11. ГОСТ Р ИСО/МЭК 15408-2002-3. «Информационная технология. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия».

Необходимо отметить, что приведенный выше перечень ГОСТ, регулирующих деятельность в области ИБ, является далеко не полным.

Специальные нормативные документы

К специальным нормативным документам относятся следующие руководящие документы (РД) Гостехкомисси:

1. РД. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (1992):

- защита средств вычислительной техники обеспечивается комплексом программно-технических средств, защита автоматизированных систем – комплексом программно-технических средств и поддерживающих их организационных мер.
- защита автоматизированных систем должна включать оценку и контроль эффективности средств защиты

2. РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (1992).

- определено 7 классов защищенности средств вычислительной техники от несанкционированного доступа к информации, разделенных на 4 группы.

3. РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (1992)

– определено 9 классов защищенности автоматизированных систем от несанкционированного доступа к информации, разделенных на 3 группы.

4. РД. Средства вычислительной техники. Межсетевые экраны. Зашита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (1997)

– определено 5 классов защищенности межсетевых экранов.

5. РД. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (1997)

– определено 4 уровня контроля отсутствия недекларированных возможностей.

6. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (2002)

Вышеперечисленные РД на сегодняшний день уже устарели, приведенные в них классификации являются несостоятельными, поскольку разрабатывались без учета сетевой природы современных автоматизированных систем. Например, современные межсетевые экраны существенно превосходят межсетевые экраны 1 класса.

Нельзя обойти вниманием нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» утвержденный приказом Гостехкомиссии России от 30 августа 2002 года.

Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) разработан Гостехкомиссии России для служебного пользования. В свободном доступе в сети Интернет сложно найти СТР-К от 2002 г., но возможно. В тоже время, СТР-К от 2002 г является уже устаревшим, поскольку разработан СТР-К от 2007 г, а на момент написания данного подраздела ходили слухи о начале разработки нового СТР-К.

При проведении работ по защите негосударственных информационных ресурсов, составляющих коммерческую тайну, банковскую тайну и т.п., требования СТР-К носят рекомендательный характер.

СТР-К устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (конфиденциальной информации), на территории РФ.

В СТР-К рассматриваются следующие вопросы, связанные с управлением ИБ:

– Организация работ по защите конфиденциальной информации.
– Защита информации на стадиях жизненного цикла – при создании, на предпроектной стадии, на стадии проектирования, ввода в действие систем защиты информации.
– Защита информации при эксплуатации.
– Защита речевой конфиденциальной информации.
– Защита конфиденциальной информации, обрабатываемой в автоматизированных системах.
– Защита конфиденциальной информации при взаимодействии абонентов с информационными сетями общего пользования.

К специальным документам также относятся документы, регламентирующие требования по защите персональных данных, разработанные Федеральной службой по техническому и экспортному контролю (ФСТЭК) В соответствии с федеральным законом № 152-ФЗ «О персональных данных» разработан комплект руководящих документов по защите персональных данных (см. www. ispdn.ru – «Все об информационных системах персональных данных»).

На момент написания этой главы вносились существенные правки в нормативные документы, регламентирующие требования по защите персональных данных.

Отраслевые нормативные документы по технической защите информации

Стандарты организаций, в том числе коммерческих, общественных, научных организаций, саморегулируемых организаций, объединений юридических лиц, разрабатываются организациями в случаях и на условиях, указанных в статье 17 Федерального закона «О техническом регулировании».

Стандарт организации – стандарт, утвержденный и применяемый организацией для целей стандартизации, а также для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг, а также для распространения и использования полученных в различных областях знаний результатов исследований (испытаний), измерений и разработок.

Стандарты организации не должны противоречить национальным стандартам, обеспечивающим применение международных стандартов ИСО (международной организации по стандартизации), МЭК (Международной электротехнической комиссии) и других международных организаций, к которым присоединилась РФ, а также стандартам, разработанным для обеспечения выполнения международных обязательств РФ.

В качестве организации, разработавшей свои стандарты в области обеспечения ИБ, рассмотрим Центральный банк России.

Центральным банком России разработана серия стандартов в области обеспечения ИБ (данные взяты с www.ib-bank.ru – «Информационная безопасность банков»):

1. СТО БР ИББС-1.0-2010 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
2. СТО БР ИББС-1.1-2007 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности».
3. СТО БР ИББС-1.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации (заменен).
4. РС БР ИББС-2.0-2007 «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».
5. РС БР ИББС-2.1-2007 «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».
6. СТО БР ИББС-1.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы РФ требованиям СТО БР ИББС-1.0-2008».
7. СТО БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».
8. СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

Требования международных и отечественных стандартов к ИБ

Международный и отечественный опыт по формированию требований к ИБ организаций и информационных систем концентрируется в разработанных стандартах и рекомендациях, апробированных на практике, признанных профессиональными сообществами специалистов в области ИБ. Характерными особенностями современных стандартов выступают:

– комплексный подход к обеспечению безопасности, предполагающий реализацию не только программно-технических, но и организационно-административных мер защиты информации;
– возможность формализации проверяемых количественных и качественных показателей ИБ организации;
– наличие базового и повышенных уровней требований, предъявляемых к защищенности информационных ресурсов;
– учет актуальных угроз для уточнения требований базового уровня и анализом рисков для выполнения повышенных требований;
– задание требований ИБ и формализованного описания процедур защиты путем документального оформления политик ИБ, стандартов, руководств, инструкций, регламентов.

Современные стандарты в области защиты информации, описывающие требования по обеспечению ИБ, представлены в таблице 1.

Таблица 1 – Современные стандарты в области защиты информации, описывающие требования по обеспечению ИБ

Стандарт/ Нормативный акт	**Разработчик**	**Статус**
ISO/IEC TR 13335 Information technology – Guidelines for the management of information technology security. Семейство международных стандартов «Информационная технология. Методы и средства обеспечения безопасности»	Международная организация по стандартизации	Международные стандарты
ISO/IEC 15408 Security technigues. Evalution criteria for IT security Безопасность информационных технологий. Критерии оценки безопасности информационных технологий	Международная организация по стандартизации	Международные стандарты
ISO/IEC 19791:2005 Information technology. Security techniques. Security assessment of operational systems Информационные технологии. Методы безопасности. Оценка безопасности автоматизированных систем		
ISO/IEC 2700x Information technology – Security techniques Семейство международных стандартов по управлению информационной безопасностью (разрабатывается подкомитетом ISO/IEC JTC 1/SC 27)		
BSI IT Baseline Protection Manual. Standart security safeguards	Германское информационное	Национальные стандар-

Стандарт/ Нормативный акт	Разработчик	Статус
Руководство по базовому уровню защиты информационных технологий	агентство безопасности	ты
BS-7799 серия стандартов по созданию и сертификации систем управления ИБ	Британский институт стандартизации (BSI)	
NIST SP800-53 Recommended Security Controls for Federal Information Systems. Рекомендуемые меры контроля безопасности для Федеральных информационных систем	Национальный институт по стандартизации и технологиям (NIST)	
COBIT (Control Objectives for Information and related Technology). Цели контроля для информационных и смежных технологий	Ассоциация аудиторов информационных систем (ISACA)	Профессиональный стандарт
FISCAM (Federal Information System Controls Audit Manual) Федеральное руководство по аудиту информационных систем	Главная счетная палата США (GAO)	Отраслевые стандарты
PCI DSS (Payment Card Industry Data Security Standard) Стандарт безопасности данных в индустрии платежных карт	Отраслевая ассоциация платежных карт Payment Card Industry (PCI)	
HIPAA (Health Insurance Portability and Accountability Act) Security Rule / Health Insurance Reform: Security Standards Стандарт безопасности медицинских сведений	Министерство здравоохранения и социального обеспечения США (DHHS)	
SPP ICS (System Protection Profile for Industrial Control Systems) Стандарт обеспечения безопасности АСУ ТП	Национальный институт по стандартизации и технологиям (NIST)	Индустриальный (промышленный) стандарт
СТО БР ИББС-1.0–2010 Обеспечение информационной безопасности организаций банковской системы Российской федерации	Банк России	Стандарт банка России

Стандарт BS-7799 нашел свое развитие в международном стандарте ISO/IEC 17799:2005, который, в свою очередь, на сегодняшний день перешел в серию стандартов ISO/IEC 2700x под номером 27002.

Стандарты SPP ICS, PCI DSS, FISCAM являются отраслевыми стандартами с ограниченной областью применения.

Наибольший интерес с точки зрения анализа вопросов формирования и стандартизации требований к ИБ организаций и информационных систем, представляют:

1. ISO/IEC TR 13335 (ГОСТ Р ИСО/МЭК ТО 13335-4-2007).
2. ISO/IEC 2700x (ГОСТ Р ИСО/МЭК 2700x).
3. NIST SP800-53.
4. COBIT.
5. СТО БР ИББС-1.0–2010.

Требования к информационной безопасности стандартов ИСО/МЭК 13335

Стандарт ГОСТ Р ИСО/МЭК 13335 аутентичен международному документу ISO/IEC TR 13335, разработанному совместно с ИСО и МЭК. Стандарт представлен серией документов «Информационная технология. Методы и средства обеспечения информационной безопасности» (см. подраздел 1.1.3.2).

В документе ГОСТ Р ИСО/МЭК ТО 13335-4–2007 «Выбор защитных мер» задается перечень требований по обеспечению ИБ в организации по 11 направлениям обеспечения ИБ, включающих 59 основных защитных мер. Перечень защитных мер ГОСТ Р ИСО/МЭК ТО 13335-4–2007 приведен в таблице 2.

Таблица 2 – Перечень защитных мер ГОСТ Р ИСО/МЭК ТО 13335-4–2007

Направления обеспечения ИБ	**Категории защитных мер безопасности**
Политика и управление ИБ	1. Политика обеспечения безопасности информационных технологий (ИТ) организации. 2. Политика обеспечения безопасности системы ИТ. 3. Управление безопасностью ИТ. 4. Распределение ответственности и полномочий. 5. Организация безопасности ИТ. 6. Идентификация и определение стоимости активов. 7. Одобрение систем ИТ
Проверка соответствия требованиям	1. Соответствие политики обеспечения безопасности ИТ защитным мерам. 2. Соответствие законодательным и обязательным требованиям. 3. Обработка инцидентов. 4. Отчеты об инцидентах безопасности. 5. Сообщения о слабых местах при обеспечении безо-

Направления обеспечения ИБ	Категории защитных мер безопасности
	пасности. 6. Сообщение о нарушениях в работе программного обеспечения. 7. Управление в случае возникновения инцидента
Работа с персоналом	1. Защитные меры для штатного или временного персонала. 2. Защитные меры для персонала, нанятого по контракту. 3. Обучение и осведомленность о мерах безопасности. 4. Процесс обеспечения исполнительской дисциплины
Организация эксплуатации	1. Управление конфигурацией и изменениями; 2. Управление резервами. 3. Документация. 4. Техническое обслуживание. 5. Мониторинг изменений, связанных с безопасностью. 6. Записи аудита и регистрация. 7. Тестирование безопасности. 8. Управление носителями информации. 9. Обеспечение стирания памяти. 10. Распределение ответственности и полномочий; 11. Корректное использование ПО. 12. Управление изменениями ПО
Планирование непрерывности бизнеса	1. Стратегия непрерывности бизнеса. 2. План непрерывности бизнеса. 3. Проверка и актуализация плана непрерывности бизнеса. 4. Дублирование
Физическая безопасность	1. Материальная защита. 2. Противопожарная защита. 3. Защита от затопления. 4. Защита от стихийных бедствий. 5. Защита от хищения. 6. Энергоснабжение и вентиляция. 7. Прокладка кабелей
Идентификация и аутентификация	1. Идентификация и аутентификация на основе информации, известной пользователю. 2. Идентификация и аутентификация на основе того, чем владеет пользователь. 3. Идентификация и аутентификация на основе использования биометрических характеристик пользователя
Ограничение	1. Политика управления доступом.

Направления обеспечения ИБ	Категории защитных мер безопасности
доступа и аудит доступа	2. Управление доступом пользователя к ЭВМ. 3. Управление доступом пользователя к данным, услугам и приложениям. 4. Анализ и актуализация прав доступа. 5. Контрольные журналы
Антивирусная защита	6. Сканеры. 7. Проверки целостности. 8. Управление обращением съемных носителей. 9. Процедуры организации по защитным мерам
Управление сетью	1. Операционные процедуры. 2. Системное планирование. 3. Конфигурация сети. 4. Разделение сетей. 5. Мониторинг сети. 6. Обнаружение вторжений
Криптография	1. Защита конфиденциальности данных. 2. Защита целостности данных. 3. Неотказуемость. 4. Аутентичность данных. 5. Управление ключами

Требования к информационной безопасности стандартов ISO/IEC 2700x (ГОСТ Р ИСО/МЭК 27001, 17799)

Серия международных стандартов по информационной технологии 2700x разрабатывается подкомитетом ISO/IEC JTC 1/SC 27. Серия стандартов 2700x включает в себя международные стандарты, определяющие требования к управлению ИБ, управлению рисками, метрикам и измерениям, а также руководство по аудиту систем управления информационной безопасности.

Для этой серии стандартов используется последовательная схема нумерации, начиная с 27000 и далее. Перечень международных стандартов по ИБ серии 2700x и отечественных стандартов, аутентичных им представлен в таблице 3.

При составлении перечня использовались данные с http://protect.gost.ru «Федеральное агентство по техническому регулированию и метрологии», http://www.iso27000.ru «Искусство управления информационной безопасностью» и http://www.iso.org/ «International Organization for Standardization».

Таблица 3 – Перечень международных стандартов по ИБ серии 2700х и отечественных стандартов, аутентичных им

Международный стандарт	**Состояние**	**Отечественный стандарт**
ISO27000 Определения и основные принципы. Планируется унификация со стандартами COBIT и ITIL	Выпущен в июле 2009 г.	
ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.	Выпущен в октябре 2005 г.	ГОСТ Р ИСО/МЭК 27001-2006
ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью	Ранее выпущен как ISO/IEC 17799:2005	ГОСТ Р ИСО/МЭК 17799- 2005
ISO/IEC 27003:201 Руководство по внедрению системы управления информационной безопасностью	Выпущен в январе 2010 г.	
ISO/IEC 27004:2009 Измерение эффективности системы управления информационной безопасностью	Выпущен в январе 2010 г.	ГОСТ Р ИСО/МЭК 27004-2011
ISO/IEC 27005:2008 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности. (Разрабатывался на основе BS 7799-3:2006)	Выпущен в июне 2008 г.	ГОСТ Р ИСО/МЭК 27005-2010
ISO/IEC 27006:2007 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью	Выпущен в марте 2007 г.	ГОСТ Р ИСО/МЭК 27006-2008
ISO/IEC 27007:2011 Руководство для аудитора	Выпущен в ноябре 2011 г.	

Международный стандарт	Состояние	Отечественный стандарт
системы управления информационной безопасности		
ISO/IEC 27008:2011 Information technology. Security techniques. Guidance for auditors on ISMS controls (DRAFT) – Руководство по аудиту механизмов контроля системы управления информационной безопасности. Настоящий стандарт будет служить дополнением к стандарту ISO 27007	Выпущен в ноябре 2011 г.	
ISO/IEC 27010:2012 Управление информационной безопасностью при коммуникациях между секторами	Выпущен в марте 2012 г.	
ISO/IEC 27011:2008 Руководство по управлению информационной безопасностью для телекоммуникаций	Выпущен в мае 2009 г.	
ISO/IEC 27013:2012 Руководство по интегрированному внедрению ISO 20000 и ISO 27001	Выпущен в октябре 2012 г.	
ISO/IEC 27014 Базовая структура управления информационной безопасностью.	Проект находится в разработке	
ISO/IEC 27015 Руководство по внедрению систем управления информационной безопасностью в финансовом и страховом секторе	Проект находится в разработке	
ISO/IEC 27031:2011 Руководство по обеспечению готовности информационных и коммуникационных технологий к их использованию для управления непрерывностью бизнеса	Выпущен в марте 2011 г.	

Международный стандарт	Состояние	Отечественный стандарт
ISO/IEC 27033 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Стандарт, возможно, будет включать в себя более 7 частей	Проект в разработке. На 2012 г разработаны первые три части	ГОСТ Р ИСО/МЭК 27033-1-2011
ISO/IEC 27034-1:2011 Безопасность приложений. Часть 1. Общий обзор и концепции	Проекты других частей стандарта ISO 27034 находятся в различной стадии разработки	
ISO/IEC 27035:2011 Управление инцидентами безопасности	Выпущен в августе 2011 г., заменил технический отчет ISO TR 18044	
ISO/IEC 27036 Руководство по аутсорсингу безопасности	Выпуск запланирован на 2012 г.	
ISO/IEC 27037:2011 Руководство по идентификации, сбору и/или получению и обеспечению сохранности цифровых свидетельств. Проект разрабатывался на базе британского стандарта BS 10008:2008 «Evidential weight and legal admissibility of electronic information. Specification»	Выпущен в ноябре 2012 г.	
ISO 27799:2008 Управление информационной безопасностью в сфере здравоохранения	Опубликован в 2008 г.	

Требования ИБ в виде описания рекомендуемых практических мер защиты заданы в ГОСТ Р ИСО/МЭК 17799- 2005 и в согласованным с ним ГОСТ Р ИСО/МЭК 27001-2006 приложении А.

Указанными стандартами задается перечень требований (рекомендаций) в 12 направлениях обеспечения ИБ, включающих 38 основных категорий безопасности, содержащих 133 защитных мер. Перечень защитных мер, реализуемых как организационными, так и программно-техническими средствами приведен в таблице 4.

Таблица 4 – Организационные и программно-технические защитные меры ГОСТ Р ИСО/МЭК 27001-2006

№ п/п	Категория защитных мер	Состав защитных мер
1. Политики безопасности		
1.	Политика ИБ	1. Документирование политики ИБ. 2. Анализ и пересмотр политики ИБ
2. Организация ИБ		
2.	Внутренняя организация	1. Координация вопросов обеспечения ИБ. 2. Распределение обязанностей по обеспечению ИБ. 3. Получение разрешений на использование средств обработки информации. 4. Заключение соглашений о конфиденциальности. 5. Проведение внешнего аудита ИБ
3.	Обеспечение безопасности при доступе сторонних организаций	1. Определение рисков, связанных со сторонними организациями. 2. Соблюдение мер безопасности при работе с клиентами. 3. Соблюдение мер безопасности в соглашениях со сторонними организациями
3. Управление активами		
4.	Обеспечение ответственности за защиту активов	1. Инвентаризация активов. 2. Назначение ответственных за активы. 3. Документирование правил безопасного использования активов
5.	Классификация информации	1. Установление классификации активов. 2. Маркировка и обработка информации

№ п/п	Категория защитных мер	Состав защитных мер
4. Безопасность, связанная с персоналом		
6.	Перед трудоустройством	1. Документирование функциональных обязанностей персонала. 2. Проверка персонала при приеме на работу. 3. Установление ответственности относительно ИБ в трудовом договоре
7.	Во время работы по трудовому договору	1. Проведение руководством ознакомления персонала с требованиями ИБ. 2. Повышение осведомленности, обучение и переподготовка персонала в области ИБ. 3. Дисциплинарная практика
8.	При увольнении или изменении трудового договора	1. Ответственность по окончании трудового договора. 2. Возврат активов. 3. Аннулирование прав доступа
5. Физическая защита		
9.	Охраняемые зоны	1. Периметр охраняемой зоны. 2. Контроль доступа в охраняемую зону. 3. Обеспечение безопасности зданий, помещений и оборудования. 4. Защита от внешних угроз. 5. Выполнение работ в охраняемых зонах. 6. Защита зон приема и отгрузки материальных ценностей

№ п/п	Категория защитных мер	Состав защитных мер
10.	Безопасность оборудования	1. Размещение и защита оборудования. 2. Обеспечивающие подсистемы (электроснабжения, заземления, кондиционирования). 3. Безопасность кабельной сети. 4. Техническое обслуживание оборудования. 5. Обеспечение безопасности внешнего оборудования. 6. Безопасная утилизация или повторное использование оборудования. 7. Разрешение на вынос имущества с территории организации
6. Управление средствами коммуникаций и их функционированием		
11.	Эксплуатация средств и ответственность	1. Документирование процедур эксплуатации средств обработки и обмена данными. 2. Контроль изменений в конфигурациях средств обработки и обмена данными. 3. Разграничение обязанностей по эксплуатации средств обработки и обмена данными. 4. Разграничение средств разработки, тестирования и эксплуатации
12.	Управление услугами, предоставляемыми сторонними организациями	1. Контроль выполнения договорных обязательств. 2. Мониторинг, аудит и анализ аутсорсинговых услуг
13.	Планирование нагрузки и приемка систем	1. Управление производительностью. 2. Проверка новых средств обработки и обмена данными перед приемом в эксплуатацию
14.	Защита от вредоносного программного обеспечения	1. Защита от вредоносного кода. 2. Защита от мобильного кода
15.	Резервное копирование и хранение информации	Резервирование информации и ПО

№ п/п	Категория защитных мер	Состав защитных мер
16.	Безопасное применение носителей информации	1. Контроль доступа к внешним носителям информации и периферийным устройствам, подключаемым к автоматизированным рабочим местам. 2. Утилизация носителей информации. 3. Регламентирование процедур обработки информации
17.	Защищенный обмен информацией	1. Политики и процедуры обмена информацией. 2. Защищенный обмен сообщениями и данными. 3. Защищенное взаимодействие смежных информационных систем
18.	Мониторинг	1. Ведение журналов регистрации действий пользователей и событий безопасности. 2. Мониторинг использования средств обработки и обмена данными. 3. Защита информации журналов регистрации. 4. Журналы регистрации действий администраторов. 5. Регистрация неисправностей. 6. Синхронизация времени
7. Контроль доступа		
19.	Управление доступом в соответствии с требованиями бизнеса	Документирование и выполнение процедур управления доступом
20.	Управление доступом пользователя	1. Регламентирование и выполнение процедур регистрации (снятия с регистрации) пользователей. 2. Управление привилегиями (ролями) пользователей. 3. Управление паролями (аутентификационными данными) пользователей. 4. Пересмотр прав доступа пользователей

№ п/п	Категория защитных мер	Состав защитных мер
21.	Ответственность пользователей	1. Использование паролей. 2. Защита оборудования, оставленного без присмотра. 3. Правила «чистого стола» и «чистого экрана»
22.	Контроль доступа к операционной системе	1. Выполнение процедуры безопасного входа в систему. 2. Идентификация и аутентификация пользователя (субъекта доступа). 3. Управление парольной политикой. 4. Контроль использования системных утилит. 5. Завершение (блокировка) сеанса после определенного времени бездействия. 6. Ограничение времени соединения
23.	Контроль доступа к прикладным системам, СУБД и информации	1. Ограничение доступа к прикладным системам и информации в соответствии с политикой доступа. 2. Выделение (изоляция) вычислительной среды для систем, обрабатывающих важную информацию
24.	Безопасная работа с переносными устройствами и в удаленном режиме	1. Безопасная работа с переносными устройствами. 2. Безопасная работа в удаленном режиме
8. Сетевая безопасность		
25.	Управление безопасностью сетей	1. Безопасное управление сетевым оборудованием. 2. Регламентирование процедур предоставления сетевых сервисов

№ п/п	Категория защитных мер	Состав защитных мер
26.	Контроль сетевого доступа	1. Аутентификация пользователей при доступе к сетевым услугам. 2. Аутентификация удаленных пользователей. 3. Аутентификация удаленного сетевого оборудования. 4. Защита диагностических и конфигурационных портов при удаленном доступе. 5. Сегментирование сетей. 6. Контроль сетевых соединений. 7. Контроль маршрутизации в сети. 8. Обнаружение вторжений
9. Обеспечение ИБ при приобретении, разработке и обслуживании информационных систем		
27.	Задание требований безопасности к разрабатываемым прикладным информационным системам	1. Формирование требований безопасности к прикладным информационным системам. 2. Проверка выполнения требований ИБ при приемке программных средств в эксплуатацию
28.	Проверка корректности обработки данных в прикладных информационных системах	1. Проверка достоверности входных данных. 2. Контроль обработки данных в приложениях. 3. Обеспечение аутентичности и защита целостности содержания сообщений. 4. Подтверждение достоверности выходных данных
29.	Защита информации криптографическими средствами	1. Формализация процедур использования криптографических средств. 2. Управление ключевой информацией. 3. Применение средств криптографической защиты для шифрования информации. 4. Использование электронной цифровой подписи. 5. Использование сервисов неоспоримости

№ п/п	Категория защитных мер	Состав защитных мер
30.	Безопасность системных файлов	1. Контроль целостности эксплуатируемого ПО. 1. Контроль и защита данных при осуществлении тестирования системы. 2. Контроль доступа к исходным кодам программ
31.	Безопасность в процессах разработки и поддержки	1. Контроль изменений прикладного ПО. 2. Анализ функционирования и безопасности ППО после внесения изменений в системное ПО. 3. Формализация процедур контроля изменений в ППО. 4. Предотвращение утечки информации из информационных систем. 5. Формализация процедур разработки ПО с привлечением сторонних организаций
32.	Контроль технических уязвимостей	Обнаружение и устранение технических уязвимостей информационных систем
10. Управление инцидентами ИБ		
33.	Своевременное оповещение о событиях и недостатках информационной безопасности	1. Оповещение о событиях ИБ. 2. Документирование (формализация) административных процедур оповещения о слабых местах (недостатках) ИБ
34.	Управление инцидентами информационной безопасности и улучшениями	1. Формализация ответственности и процедур реагирования на инциденты ИБ. 2. Формализация процедур мониторинга и регистрации инцидентов ИБ. 3. Формализация процедур сбора доказательств об инцидентах ИБ
11. Управление непрерывностью бизнеса		

№ п/п	Категория защитных мер	Состав защитных мер
35.	Обеспечение непрерывности бизнеса	1. Включение ИБ в процесс управления непрерывностью бизнеса. 2. Оценка риска нарушения непрерывности бизнеса. 3. Разработка и внедрение планов непрерывности бизнеса с учетом ИБ. 4. Создание единой структуры планов обеспечения непрерывности бизнеса. 5. Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса
12. Обеспечение соответствия требованиям		
36.	Обеспечение соответствия правовым требованиям	1. Определение и документирование правовых требований. 2. Защита прав на интеллектуальную собственность. 3. Защита персональных данных. 4. Предотвращение злоупотребления средствами обработки информации. 5. Регулирование использования криптографических средств
37.	Обеспечение соответствия политикам и стандартам безопасности, и технического соответствия	1. Обеспечение соответствия политикам и стандартам безопасности. 2. Проверка соответствия техническим требованиям ИБ
38.	Аудит ИБ	1. Управление аудитом ИБ. 2. Защита инструментальных средств аудита

Требования к информационной безопасности стандарта ГОСТ Р ИСО/МЭК 15408-2002

Стандарт ГОСТ Р ИСО/МЭК 15408-2002 аутентичен международному документу ISO/IEC 15408:1999, являющемся одним из наиболее распространенных стандартов в области безопасности. В разработке ISO/IEC 15408:1999 приняли участие организации из США, Канады, Англии, Франции, Германии, Голландии.

Развитие стандарта ISO/IEC 15408:1999 под названием ISO/IEC PDTR 19791:2006 (Информационные технологии. Методы безопасности. Оценка безопасности операционных систем) предусматривает рассмотрение дополнительно административного и процедурного уровней ИБ. Данные меры в значительной степени заимствованы из международного стандарта ISO/IEC 17799.

Важным отличием стандартов ISO/IEC 17799 и ISO/IEC 15408:1999 является то, что первый ориентирован на разработчиков и специалистов по эксплуатации, а второй – в первую очередь на экспертов по оценке.

Российский вариант стандарта ISO/IEC 15408-99 носит название «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий».

Применимость стандарта ГОСТ Р ИСО/МЭК 15408-2002 ограничивается механизмами безопасности программно-технического уровня, однако в нем содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

ГОСТ Р ИСО/МЭК 15408-1 («Введение и общая модель») содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В стандарте вводится понятийный аппарат, определяются принципы формализации предметной области, устанавливается общий подход к формированию требований оценки безопасности.

ГОСТ Р ИСО/МЭК 15408-2 («Функциональные требования безопасности») подробно описывает функциональные требования к безопасности, сгруппированные в 11 классов, 66 семейств, 135 компонентов, и цели безопасности, которые могут быть при этом достигнуты. Данные требования могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в автоматизированных системах (средствах вычислительной техники) функций безопасности.

ГОСТ Р ИСО/МЭК 15408-3 («Требования доверия к безопасности») содержит оценочные уровни доверия, образующие своего рода шкалу для измерения уровня доверия к объекту оценки, и классы требований гарантированности оценки.

Требования к информационной безопасности стандарта NIST SP800-53 «Рекомендуемые меры контроля безопасности для федеральных информационных систем»

Национальный стандарт NIST SP800-53 «Рекомендуемые меры контроля безопасности для федеральных информационных систем» разработан Национальным Институтом Стандартов и Технологии США и определяет требования безопасности и меры контроля (*security controls*) информационных систем.

Минимальные требования безопасности задают тот базовый уровень безопасности, которому должны удовлетворять все информационные системы.

Для каждой меры контроля безопасности установлено три уровня защищенности ИБ информационной системы – низкий, умеренный и высокий.

Необходимым условием выполнения требований безопасности информационных систем являются выбор и реализация соответствующих мер контроля безопасности, то есть экономически оправданных контрмер и средств защиты.

В данном стандарте определены 164 меры контроля безопасности, сгруппированные в три класса и 17 семейств.

Для поддержания базового, среднего или высокого уровня защищенности информационной системы для каждой меры контроля разработаны соответствующие спецификации, содержащие требования ИБ, руководства по выполнению требований и перекрестные ссылки на другие меры контроля безопасности. Для обеспечения удобства использования стандарта NIST SP800-53 каждой мере контроля безопасности присвоен идентификатор, который обычно совпадает с идентификатором соответствующей спецификации.

Требования к информационной безопасности стандарта COBIT

COBIT – результат обобщения мирового опыта, международных и национальных стандартов и руководств в области управления ИТ, аудита и информационной безопасности. Интернациональную команду разработчиков COBIT составили сотрудники госучреждений и коммерческих предприятий, учебных заведений и фирм, специализирующихся на вопросах безопасности и управления ИТ.

Аббревиатура COBIT расшифровывается как Control Objectives for Information and Related Technology – Цели контроля для информационных и смежных технологий.

COBIT представляет собой систематизированный набор принципов и рекомендаций по проведению аудита процессов управления ИТ. Данная модель была впервые предложена профессиональной ассоциацией ISACA (The Information Systems Audit and Control Association) в 1996 году.

Модель COBIT определяет 34 ключевых процесса управления ИТ в организации, которые сгруппированы в 4 основные области (домены). Перечень ключевых процессов управления ИТ приведен в таблице 5.

Таблица 5 – Перечень ключевых процессов управления ИТ

Этап жизненного цикла управления ИТ	**Название процесса управления ИТ**
Планирование и Организация	1. Разработка ИТ-стратегии. 2. Разработка ИТ-архитектуры. 3. Мониторинг технологического развития. 4. Формирование ИТ-службы и определение взаимосвязей. 5. Управление инвестициями в ИТ. 6. Распространение корпоративной информации. 7. Управление персоналом. 8. Обеспечение соответствия внешним требованиям; 9. Управление рисками. 10. Управление проектами. 11. Управление качеством
Приобретение и Реализация	1. Идентификация автоматизируемых решений. 2. Приобретение и поддержка прикладного ПО. 3. Приобретение и поддержка технологической инфраструктуры. 4. Разработка и поддержка процедур. 5. Установка и прием в эксплуатацию систем. 6. Управление изменениями
Предоставление (реализация) и поддержка	1. Определение и управление уровнями обслуживания. 2. Управление услугами третьих сторон; 3. Управление производительностью и мощностью. 4. Обеспечение непрерывности обслуживания. 5. Обеспечение безопасности. 6. Идентификация и управление стоимостью. 7. Обучение пользователей. 8. Помощь клиентам. 9. Управление конфигурациями. 10. Управление проблемами и инцидентами. 11. Управление данными. 12. Управление средствами. 13. Управление операциями
Мониторинг	1. Мониторинг процессов.

Этап жизненного цикла управления ИТ	Название процесса управления ИТ
	2. Обеспечение адекватности внутреннего контроля. 3. Организация независимого контроля. 4. Обеспечение независимого аудита

Требования к информационной безопасности стандарта СТО БР ИББС-1.0 - 2010

Данный стандарт является стандартом банка России, распространяется на организации банковской системы РФ и устанавливает положения (политики, требования и т.п.) по обеспечению ИБ в организациях банковской системы РФ. Этот стандарт ссылается и учитывает требования многих из перечисленных выше стандартов по безопасности (ISO/IEC 27001-2005, ISO/IEC IS 27002, ISO/IEC 13335-1), а также не указанного ранее стандарта ISO TR 13569 «Banking and related financial services. Information security guidelines».

Требования стандарта распространяются на следующие области ИБ:

- Назначение и распределение ролей и доверия к персоналу.
- Стадии жизненного цикла автоматизированной системы.
- Защита от несанкционированного доступа, управление доступом и регистрацией в автоматизированной системе, в телекоммуникационном оборудовании и автоматических телефонных станциях и т.д.
- Антивирусная защита.
- Использование ресурсов Интернет.
- Использование средств криптографической защиты информации.
- Защита банковских платежных и информационных технологических процессов.
- Обеспечение непрерывности.
- Физическая защита.

Сравнительный требований по информационной безопасности защиты, представленных в основных международных стандартах

Формируемые в стандартах требования ИБ представлены в виде перечней правил (защитных мер), позволяющих обеспечивать ИБ в организации. Анализ стандартов ИБ показывает, что наиболее полный охват требований ИБ ко всем направлениям деятельности организации, представлен в стандартах, аутентичных международным стандартам, ГОСТ Р ИСО/МЭК 27001–2006, ГОСТ Р ИСО/МЭК ТО 13335-4 и стандарте США NIST SP800-53. Соотношение охвата требований ИБ в вышеперечисленных стандартах представлено в таблице 6.

Таблица 6 – Соотношение охвата направлений требований ИБ в стандартах ГОСТ Р ИСО/МЭК 27001–2006, ГОСТ Р ИСО/МЭК ТО 13335-4 и стандарте США NIST SP800-53

NIST 800-53	ГОСТ Р ИСО/МЭК ТО 13335-4	ГОСТ Р ИСО/МЭК 27001–2006
Планирование безопасности (политика и процедуры)	Политика и управление ИБ	Политика безопасности
Анализ рисков	–	–
–	–	Управление активами
Закупка систем и сервисов	–	–
Сертификация, аккредитация и оценка безопасности	Проверка соответствия требованиям	Соответствие требованиям
–	–	Организационная безопасность
Кадровая безопасность. Квалификация и обучение персонала.	Работа с персоналом	Безопасность персонала
Физическая защита и защита от внешней среды	Физическая безопасность	Физическая безопасность
Организация бесперебойной работы	Планирование непрерывности бизнеса	Обеспечение непрерывности бизнеса.
Техническое обслуживание (сопровождение)	Организация эксплуатации	Разработка, внедрение и обслуживание информационных систем
Управление конфигурацией системы	–	Эксплуатация средств и ответственность
Целостность систем и информации	Антивирусная защита	Защита от вредоносного кода. Резервирование
Безопасность данных	–	Обращение с носителями информации
Реагирование на инциденты	Обработка инцидентов	Управление инцидентами ИБ
Идентификация и аутентификация. Контроль доступа. Аудит и отчетность (учет)	Идентификация и аутентификация. Ограничение доступа и аудит доступа	Контроль доступа. Мониторинг
Защита систем и средств связи	Управление сетью Криптография	Управление безопасностью сети. Криптографические средства защиты

Выводы по разделу

Формирование требований по обеспечению ИБ необходимо осуществлять с учетом требований законодательной и нормативной базы РФ, регламентирующей требования к ИБ.

Требования по ИБ, рекомендуемые государственными стандартами и международными стандартами, определяют перечень направлений обеспечения ИБ (категорий мер защиты), которые необходимо учесть в рамках обеспечения ИБ организации.

Наиболее полный и адекватный набор требований ИБ представлен в серии стандартов 2700х, в частности ГОСТ Р ИСО/МЭК 27001, 17799 , что позволяет выбрать их за основу для формирования требований обеспечению ИБ организации.

4 ОСНОВНЫЕ ПОНЯТИЯ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Государственная тайна - все защищаемые государством сведения.

Государственная тайна - это сведения политического, экономического, военного и научно-технического характера, утрата или разглашение которых создает угрозу безопасности и независимости государства или наносит ущерб его интересам.

Таким образом, область применения Закона ограничена определенными видами деятельности: военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной. Связывает понятие государственной тайны с понятием безопасности Российской Федерации.

Основные вопросы государственной тайны отражены в Законе РФ о государственной тайне (закон РФ "О государственной тайне" от 21.07.1993г. №5485-1 с изменениями и дополнениями от: 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г., 1 декабря 2007 г., 18 июля 2009 г., 15 ноября 2010 г., 18, 19 июля, 8 ноября 2011 г.).

Действие закона распространяется на территорию Российской Федерации (включая учреждения Российской Федерации за рубежом) и за ее пределами в силу специфичности Закона – его требования обязательны для выполнения должностными лицами и гражданами, осведомленными в государственной тайне, в том числе и при их выездах за границу в служебные командировки или по частным делам.

Субъектами правоотношений закона являются:

- Органы представительной, исполнительной и судебной властей всех уровней, органы местного самоуправления.
- Предприятия, учреждения и организации независимо от их организационно-правовой формы и формы собственности.
- Должностные лица и граждане Российской Федерации, взявшие на себя обязательства либо обязанные по своему статусу исполнять требования настоящего Закона.

В силу ограничительного характера Закона он должен распространяться только на сравнительно небольшую часть населения, **добровольно** вступившую с государством в правоотношения по защите государственной тайны.

Граждане, получившие доступ к государственной тайне в силу сложившихся обстоятельств (нашедшие утраченный носитель сведений, например), не должны ограничиваться из-за этого в своих правах.

Основные понятия

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.

Закон *не рассматривает человека в качестве носителя сведений*, составляющих государственную тайну. Человек рассматривается в качестве субъекта правоотношений, вступающего с государством в договорные отношения.

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;

Степень секретности той или иной информации определяется степенью ущерба (экономического, политического, военного и др.), наносимого в результате утери закрытой информации или передачи ее другим лицам, организациям и государствам. Информация является товаром и имеет конкретную стоимость.

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.

К средствам защиты информации отнесены не только собственно средства, защищающие информацию (от несанкционированного доступа, от утечки по техническим каналам и т.п.), но и защищенные технические средства, то есть технические средства с реализованными в них средствами защиты, а также средства, позволяющие контролировать эффективность защиты информации, то есть эффективность функционирования средств защиты.

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.

Режим секретности – установленный нормами права единый порядок обращения со сведениями, составляющими государственную и служебную тайны в целях предотвращения утечки закрытой информации по различным каналам.

Особенности режима секретности

- единый для всех министерств, ведомств, предприятий, учреждений, организаций порядок обращения с государственными секретами, который определяется высшими органами государственной власти и управления;
- обязательный для всех государственных органов и должностных лиц порядок обращения с государственными секретами;
- персональная ответственность руководителей всех рангов за организацию режима секретности в их учреждениях, организациях и предприятиях, за проведение необходимого комплекса мероприятий, предотвращающих утечку закрытой информации;
- контроль за деятельностью по обеспечению сохранности государственных секретов, соблюдение требований установленного режима секретности, который осуществляется органами государственной безопасности;
- уголовная ответственность лиц, виновных в разглашении секретных сведений, в утрате секретных документов и изделий.

Режим секретности включает в себя

- порядок установления степени секретности сведений, содержащихся в работах, документах и изделиях;
- порядок допуска граждан к работам, документам и изделиям, которые содержат закрытую информацию;
- порядок выполнения должностными лицами своих должностных обязанностей по сохранению государственных и служебных тайн, по соблюдению режима секретности;
- порядок обеспечения секретности при проведении в учреждениях и на предприятиях работ закрытого характера;
- порядок обеспечения секретности при ведении секретного делопроизводства;
- порядок обеспечения секретности при использовании технических средств, передаче, обработке и хранении информации закрытого характера;
- порядок обеспечения секретности при осуществлении предприятиями, учреждениями и организациями, где ведутся закрытые работы, контактов с зарубежными фирмами;
- порядок проведения служебных расследований по фактам разглашения секретных сведений.

5 ПОРЯДОК ЗАСЕКРЕЧИВАНИЯ И РАССЕКРЕЧИВАНИЯ СВЕДЕНИЙ ДОКУМЕНТОВ И ПРОДУКЦИИ

Принципы отнесения сведений к государственной тайне и засекречивания этих сведений

Отнесение сведений к государственной тайне и их засекречивание – введение в предусмотренном Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

Засекречивание конкретных сведений в связи с наличием в них государственных и служебных тайн осуществляется в соответствии с перечнем главнейших сведений, составляющих государственную тайну, и ведомственными перечнями сведений, подлежащих засекречиванию. Единый порядок засекречивания сведений определен положением о порядке установления степени секретности сведений, содержащихся в работах, документах и изделиях.

При засекречивании сведений необходимо руководствуются следующим принципами:

- Решение проблемы засекречивания в целом с позиции государственной значимости этих сведений; при этом необходимо учитывать противоречивость и единство двух тенденций: с одной стороны, стремление обеспечить надежность сохранности государственных и служебных тайн, с другой стороны, не допустить необоснованного массового засекречивания.
- Объективный характер определения степени секретности сведений, который основывается на точном использовании существующих перечней охраняемых сведений.
- Оптимизация объема засекречиваемых сведений.
- Периодический просмотр степени секретности сведений на предмет снятия или снижения грифа секретности.

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с **принципами** законности, обоснованности, своевременности.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений положениям Закона и законодательству Российской Федерации о государственной тайне.

Обоснованность отнесения сведений к государственной тайне и их засекречивание 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 отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Наличие в Законе принципов засекречивания создает базу для создания соответствующих нормативных документов, позволяющих реализовать указанные принципы на практике.

Принцип законности засекречивания дает ориентиры для создания отраслевых, ведомственных или программно-целевых перечней сведений, подлежащих засекречиванию. Статьи Закона выделяют из всего информационного пространства с одной стороны область государственных интересов по обеспечению безопасности Российской Федерации (статья 5), а с другой - область интересов общества и его граждан, информация о которой не подлежит засекречиванию (статья 7). Именно при соблюдении принципа законности засекречивания. Тем самым достигается баланс интересов граждан, общества и государства, положенный в основу Закона Российской Федерации "О безопасности".

Принцип обоснованности засекречивания позволяет из всей области сведений, засекречивание которых законно, выбрать только те, засекречивание которых еще и целесообразно по экономическим и иным причинам. Реализация этого принципа позволяет разработать методику отнесения сведений к соответствующей степени секретности, положив в ее основу экономические и иные критерии экспертной оценки. Это, в свою очередь, позволяет расходовать средства только на защиту тех сведений, распространение которых действительно способно нанести ущерб безопасности страны.

Принцип своевременности засекречивания позволяет реализовать процедуру предварительного засекречивания сведений и их носителей, осуществлять защиту сведений в процессе их производства или разработки.

Перечень сведений, составляющих государственную тайну

Государственную тайну составляют:

1. Сведения в военной области:

– о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегиче-

скому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

- о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
- о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;
- о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
- о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
- о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2. Сведения в области экономики, науки и техники:

- о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;
- об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;
- о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления,

о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;
- о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;
- о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3. Сведения в области внешней политики и экономики:

- о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;
- о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4. Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму:

- о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
- о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

- об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
- о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;
- о методах и средствах защиты секретной информации;
- об организации и о фактическом состоянии защиты государственной тайны;
- о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;
- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;
- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства;
- о мерах по обеспечению защищенности критически важных объектов и потенциально опасных объектов инфраструктуры Российской Федерации от террористических актов;
- о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности.
- Таким образом, в Законе показаны области государственных интересов в соответствии с видами деятельности. Структура перечня не закрепощает набор конкретных сведений путем прямого отнесения их к государственной тайне, а лишь создает законодательную базу для отнесения конкретных сведений к государственной тайне, если для этого имеется соответствующее обоснование. Таким образом, появляется возможность перейти к системе отраслевых, ведомственных и программно-целевых перечней, которые достаточно оперативно могут изменяться в соответствии с происходящими изменениями в экономической и политической жизни страны. Такой подход, позволяет системе засекречивания адаптироваться к изменяющимся обстоятельствам, ввести экономические и качественные показатели обоснованности засекречивания, не поддерживать искусственно секретность, наносящую ущерб экономическим интересам Российской Федерации.

Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- 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 социальных гарантиях, 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.

Определив в статье 5 Закона категории сведений, которые могут быть отнесены к государственной тайне, то есть, выделив область интересов государства по обеспечению своей безопасности, вполне логично было бы предположить, что остальные категории сведений не подлежат засекречиванию. Иными словами можно было бы ограничиться принципом: "Что не запрещено, то разрешено". Вместе с тем, учитывая ограничительный характер Закона и перспективу наращивания его рядом нормативных актов, было признано оправданным включить в Закон статью прямого действия, которая определяла бы, область интересов общества и граждан, засекречивание сведений в которой не допускается. Выделение такой области интересов в явном виде было необходимо еще и потому, что без наличия ее в Законе сложно было бы поставить вопрос об ответственности должностных лиц за умышленное засекречивание сведений, сокрытие которых от общества способно нанести ущерб его гражданам. Правильность этого подхода была позднее подтверждена и Конституцией Российской Федерации, содержащей в части 3 статьи 41 один из основных критериев открытости информации – «сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с Федеральным Зако-

ном». Важное значение для практического применения статьи имеет содержание абзаца, в котором предусмотрена ответственность должностных лиц не только за прямое, но и за косвенное засекречивание перечисленных в статье категорий сведений, а именно за включение их в интересах засекречивания в носители сведений, составляющих государственную тайну. Подобное включение сведений в носители информации преследуется по закону только в том случае, если преследует целью изъять эти сведения из открытого обращения в обществе.

Степени секретности сведений и грифы секретности носителей этих сведений

Установлены **три степени секретности** сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

- особой важности,
- совершенно секретно
- секретно.

К **сведениям особой важности** следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К **совершенно секретным сведениям** следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К **секретным сведениям** следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Все три степени секретности сведений включены в смысловое понятие "государственная тайна. Термин "служебная тайна" вынесен за рамки регулирования Закона и по законопроекту «О государственной службе» описывает несекретные сведения служебного характера.

Закон предполагает разработку **единой** методики определения размеров возможного ущерба, наносимого государству разглашением тех или иных сведений, то есть разработку единой базы качественных и количественных экономических и иных критериев, позволяющих в ходе экспертной оценки обосновывать необходимость и целесообразность отнесения указанных сведений к государственной тайне. Первоначально предполагалось, что создание указанной методики будет осуществлено до разработки ведомственных перечней сведений, подлежащих засекречиванию, и формирования на их основе Перечня сведений, отнесенных к государственной тайне. В настоящий момент единый подход в этой работе задан правилами отнесения сведений к той или иной степени секретности (утверждены постановлением Правительства Российской федерации от 4 сентября 1995 года, №870).

Закон содержит прямое запрещение использования грифов секретности для засекречивания сведений, не отнесенных в установленном Законом порядке к государственной тайне.

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, эти данные указываются в сопроводительной документации на этот носитель.

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий

гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

Помимо перечисленных в настоящей статье реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и порядок проставления дополнительных отметок и других реквизитов определяются нормативными документами, утверждаемыми Правительством Российской Федерации.

Порядок и правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно - целевой принадлежностью и в соответствии с Законом.

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 в соответствии с **Перечнем сведений, составляющих государственную тайну** (ст. 5 Закона о государственной тайне)**.**

Правом отнесения сведений к государственной тайне обладают руководители органов государственной власти в соответствии с **Перечнем должностных лиц, наделенных полномочиями** по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации.

Для осуществления единой государственной политики в области засекречивания сведений создается **межведомственная комиссия по защите государственной тайны (**Указ Президента Российской Федерации «Вопросы межведомственной комиссии по защите государственной тайны» от 6 октября 2004 г. №1286 в ред. Указов Президента РФ от 27.09.2008 № 1410, от 09.12.2008 № 1752, от 26.02.2009 № 228).

Межведомственная комиссия формирует Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом Российской Федерации (Указ Президента Российской Федерации от 11 февраля 2006 г. №

90), подлежит открытому опубликованию и пересматривается по мере необходимости.

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые **Перечни сведений, подлежащих засекречиванию**.

В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности.

В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно - конструкторских и научно - исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться **отдельные перечни сведений, подлежащих засекречиванию.** Эти перечни утверждаются соответствующими руководителями органов государственной власти (Постановление Правительства Российской Федерации от 4 сентября 1995 г. N 870).

Перечни сведений, подлежащих засекречиванию, разрабатываются по отраслевой, ведомственной или программно-целевой принадлежности этих сведений.

Отраслевая принадлежность сведений подразумевает их привязку к отдельной сфере производственной деятельности.

Ведомственная принадлежность означает привязку сведений к определенному органу власти.

Программно-целевая принадлежность означает их привязку к целевым программам научно-исследовательских и опытно-констукторских работ по разработке и модернизации определенных технических устройств или систем главным образом в области вооружения военной техники. Программно-целевые перечни сведений, подлежащих засекречиванию, могут разрабатываться по решению заказчиков НИР и ОКР и утверждаться руководителями органов власти по принадлежности заказчиков.

Перечни сведений, подлежащих засекречиванию, **определяют степень секретности конкретных сведений** (группы сведений), а их структура учитывает ведомственную или отраслевую специфику. Количественные и качественные показатели ущерба безопасности Российской Федерации определяются в соответствии с нормативно-методическими документами, утверждаемыми руководителями органов государственной власти, которые наделены полномочиями по отнесению сведений к государственной тайне, и согласованными с Межведомственной комиссией по защите государственной тайны.

Перечни сведений, подлежащих засекречиванию, доводятся до:

– заинтересованных органов государственной власти в полном объеме либо в части, их касающейся;
– предприятий, учреждений и организаций, действующих в сфере ведения органов государственной власти, в части, их касающейся, по решению должностного лица, утвердившего перечень;
– предприятий, учреждений и организаций, участвующих в проведении совместных работ, в объеме, определяемом заказчиком этих работ.

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию.

При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.

Порядок разработки перечня сведений

Для разработки проекта перечня создается **экспертная комиссия**, в состав которой включаются компетентные специалисты, работающие со сведениями, составляющими государственную тайну.

В ходе подготовки перечня экспертные комиссии проводят анализ всех видов деятельности соответствующих органов государственной власти, предприятий, учреждений и организаций с целью определения сведений, распространение которых может нанести ущерб безопасности Российской Федерации.

Обоснование необходимости отнесения сведений к государственной тайне с указанием соответствующей степени секретности осуществляется **собственниками этих сведений** и оформляется в виде предложений для включения в проект соответствующего перечня. Степень секретности сведений, находящихся в распоряжении нескольких органов государственной власти, устанавливается по взаимному согласованию между ними.

В перечень могут быть включены сведения, которые получены (разработаны) другими органами государственной власти, органами местного самоуправления, предприятиями, учреждениями, организациями или гражданами, не состоящими в отношении подчиненности к руководителю органа государственной власти, утверждающему перечень. Степень секретности таких сведений устанавливается по согласованию между органом государственной власти, разрабатывающим перечень, и собственником сведений.

Проект перечня, разработанный экспертной комиссией, представляется на утверждение руководителю органа государственной власти, наделенному полномочиями по отнесению сведений к государственной тайне, который также решает вопрос о целесообразности засекречивания самого перечня.

Утвержденные перечни в целях координации работ по защите государственной тайны направляются в Межведомственную комиссию.

Перечни пересматриваются в случае необходимости, но не реже, чем через 5 лет. Пересмотр перечней осуществляется в том же порядке, что и их разработка. Предложения по внесению в перечни дополнений и изменений направляются руководителям органов государственной власти, утвердившим эти перечни, которые обязаны в течение трех месяцев организовать проведение экспертизы поступивших предложений и принять соответствующее решение.

Если принятие указанных предложений влечет за собой изменение Перечня сведений, отнесенных к государственной тайне, руководители органов государственной власти направляют проект соответствующего решения с обоснованием в Межведомственную комиссию для проведения экспертной оценки и принятия решения.

Процедура предварительного засекречивания

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить **предварительное засекречивание** полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

Проведение проверки наличия в заявках на выдачу патента на изобретение или полезную модель, сведений, составляющих государственную тайну

Утверждены Постановлением Правительства РФ от 24 декабря 2007 г. N 928 с изменениями и дополнениями от 22 мая 2008 г., 31 марта 2010 г., 7 сентября 2011 г.

Проверке подлежат заявки, поданные в Роспатент российскими юридическими лицами или гражданами РФ, в том числе международные заявки на выдачу патента на изобретение, поданные в соответствии с Договором о патентной кооперации или поданные через Роспатент в соответствии с Евразийской патентной конвенцией.

Проверка заявки осуществляется путем ознакомления с ней имеющих необходимую форму допуска к сведениям, составляющим государственную тайну, представителей федеральных органов исполнительной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне.

В случае выявления представителем компетентного органа обстоятельств, требующих проверки содержания заявки, заявка направляется в соответствующий компетентный орган, о чем уведомляется заявитель. Компетентный орган в двухмесячный срок с даты получения заявки осуществляет ее проверку.

Если по результатам проверки не установлено наличие в заявке сведений, составляющих государственную тайну, она возвращается в Роспатент с соответствующим заключением. Если по результатам проверки установлено наличие в заявке сведений, составляющих государственную тайну, принимается решение о засекречивании заявки и присвоении ей соответствующего грифа секретности. Заявитель уведомляется о засекречивании его заявки до истечения 6 месяцев с даты подачи заявки в Роспатент.

В случае засекречивания заявки на изобретение компетентный орган возвращает заявку в Роспатент либо направляет ее в федеральный орган исполнительной власти, уполномоченный рассматривать заявки на выдачу патента на изобретение, сведения которого составляют государственную тайну, либо рассматривает заявку. В случае засекречивания заявки на полезную модель, заявка возвращается в Роспатент.

Порядок рассекречивания сведений

Рассекречивание сведений и их носителей - снятие ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основания для рассекречивания сведений:

1. Взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;
2. Изменение международной обстановки;
3. Изменение перечней сведений, подлежащих засекречиванию;
4. Окончание срока действия грифа;
5. Появление новых достижений в науке и технике;
6. Продажа или передаче вооружения другим странам;
7. Снятие оружия или боевой техники с вооружения.
8. Изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Срок засекречивания сведений, составляющих государственную тайну, **не должен превышать 30 лет.** В исключительных случаях этот **срок может быть продлен по заключению межведомственной комиссии** по защите государственной тайны.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности.

Правом изменения действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, наделяются утвердившие их руководители органов государственной власти.

Носители сведений, составляющих государственную тайну, **рассекречиваются не позднее сроков**, установленных при их засекречивании.

До истечения этих сроков носители подлежат рассекречиванию, если изменены положения действующего в данном органе государственной власти, на предприятии, в учреждении и организации перечня, на основании которых они были засекречены.

В исключительных случаях **право продления** первоначально установленных сроков засекречивания носителей сведений, составляющих государственную тайну, предоставляется руководителям государственных органов, наделенным полномочиями по отнесению соответствующих сведений к государственной тайне, на основании заключения назначенной ими в установленном порядке экспертной комиссии.

Руководители государственных архивов Российской Федерации наделяются полномочиями по рассекречиванию носителей сведений, составляющих государственную тайну, находящихся на хранении в закрытых фондах этих архивов, в случае делегирования им таких полномочий организацией - фондообразователем или ее правопреемником.

В случае ликвидации организации - фондообразователя и отсутствия ее правопреемника вопрос о порядке рассекречивания носителей сведений, составляющих государственную тайну, рассматривается межведомственной комиссией по защите государственной тайны.

При таком подходе носители сведений, на которых указаны условия рассекречивания сведений либо событие, после наступления которого сведения могут быть рассекречены, защищены от процедуры произвольного, без согласования с фондообразователем, рассекречивания, предусмотренного в ряде действующих документов по линии архивной службы, например. В качестве условия для рассекречивания может быть указана, например, процедура обязательного согласования с органом государственной власти, предприятием, учреждением, организацией или их правопреемниками. Это позволяет поставить процедуру рассекречивания носителей, независимо от места их хранения, под контроль должностных лиц, обосновавших в свое время необходимость их засекречивания. Законом установлены полномочия руководителей государственных архивов Российской Федерации по рассекречиванию материалов, находящихся на хранении в закрытых фондах архивов.

Сохранены права фондообразователей по принятию решения на рассекречивание архивных материалов, что обеспечивает контроль за этим процессом со стороны должностных лиц, несущих персональную ответственность перед государством за реализацию требований Закона. Вместе с этим предусматривается возможность делегирования организациями-фондообразователями полномочий по рассекречиванию носителей сведений руководителям государственных архивов. Это положение призвано упростить рассекречивание архивных носителей, в отношении утраты которыми секретности у организации-фондообразователя не имеется сомнений.

6 ДОПУСК И ДОСТУП ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ

Общие положения

Допуск - это официальное разрешение руководителя предприятия на право выполнения закрытых работ, на право ознакомления с секретными работами и документами.

К секретным работам и документам могут быть допущены только граждане России, которые по своим деловым, политическим и моральным качествам способны обеспечить сохранность доверенных им тайн.

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 (Постановление Правительства РФ от 06.02.2010 №63 «Об утверждении инструкции о порядке допуска должностных лиц и граждан российской федерации к государственной тайне»).

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется **в добровольном порядке**.

Допуск граждан к государственной тайне на территории Российской Федерации и за ее пределами осуществляется руководителями соответствующих организаций.

Граждане, которым по характеру занимаемой ими должности необходим доступ к государственной тайне, могут быть назначены на эти должности только после оформления допуска по соответствующей форме в установленном порядке.

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;
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных 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.

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий.

Основания для отказа должностному лицу или гражданину в допуске к государственной тайне

– признание его судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;
– наличие медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения Российской Федерации;
– постоянное проживание его самого или его близких родственников за границей или оформление указанными лицами документов для выезда на постоянное жительство в другие государства; постоянный контакт с лицами (родственниками) за границей.
– выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;
– уклонение его от проверочных мероприятий или сообщение заведомо ложных анкетных данных.

Решение об отказе гражданину в допуске к государственной тайне принимается руководителем организации в индивидуальном порядке с учетом результатов проверочных мероприятий.

На каждое лицо, допускаемое к секретным работам и документам, оформляется **допуск** - официальное разрешение руководителя предприятия на право выполнения закрытых работ, на право ознакомления с секретными работами и документами.

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска:

– **первая форма** - для граждан, допускаемых к сведениям особой важности;

- **вторая форма** - для граждан, допускаемых к совершенно секретным сведениям;
- **третья форма** - для граждан, допускаемых к секретным сведениям.

Наличие у должностных лиц и граждан **допуска** к сведениям более высокой степени секретности является основанием для **доступа** их к сведениям более низкой степени секретности.

Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности Российской Федерации и ее территориальными органами (далее именуются – органы безопасности) во взаимодействии с органами, осуществляющими оперативно-розыскную деятельность.

Допуск граждан по третьей форме осуществляется руководителем организации без проведения проверочных мероприятий органами безопасности.

Органы безопасности во взаимодействии с заинтересованными организациями имеют право определять те организации, на которых допуск к секретным сведениям осуществляется только после проведения проверочных мероприятий органами безопасности.

Руководители организаций допускаются к секретным сведениям (по третьей форме) только после проведения проверочных мероприятий органами безопасности.

Граждане, принимаемые на временную работу или не достигшие 18-летнего возраста, как правило, не подлежат оформлению на допуск к особой важности и совершенно секретным сведениям.

Граждане, принимаемые на работу в подразделения по защите государственной тайны, а также для ведения секретного делопроизводства в организациях, где штатным расписанием не предусмотрено наличие таких подразделений, оформляются на допуск по второй форме, если по характеру выполняемой работы им не требуется допуск по первой форме.

Перечень должностей, при назначении на которые граждане обязаны оформлять допуск к сведениям, составляющим государственную тайну, определяется **номенклатурой должностей**, утверждаемой руководителем организации или его заместителем, занимающимся вопросами защиты государственной тайны, после согласования ее с органом безопасности. В номенклатуру включаются только те должности, по которым допуск граждан к указанным сведениям действительно необходим для выполнения ими должностных (функциональных) обязанностей. Изменения и дополнения в номенклатуру должностей вносятся по мере необходимости, согласовываются и утверждаются в установленном порядке. Номенклатура должностей пересматривается не реже одного раза в 5 лет.

При несоответствии формы допуска гражданина степени секретности сведений, к которым он фактически имеет доступ, форма допуска должна быть изменена.

Снижение формы допуска с первой на вторую (третью) или со второй на третью оформляется распоряжением руководителя организации.

В случае производственной необходимости руководитель, ранее снизивший форму допуска работнику, может восстановить ее без проведения проверочных мероприятий органами безопасности.

О фактах снижения и восстановления ранее имевшейся формы допуска информируется территориальный орган государственной безопасности.

Повышение в случае необходимости формы допуска производится в установленном порядке.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, **устанавливаются льготы:**

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Взаимные обязательства администрации и оформляемого лица отражаются в трудовом договоре (контракте). **Заключение трудового договора (контракта) до окончания проверки компетентными органами не допускается.**

Допуск должностного лица или гражданина к государственной тайне может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

- расторжения с ним трудового договора (контракта) в связи с проведением организационных или штатных мероприятий;
- однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны;
- возникновения обстоятельств, являющихся основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

В случае отстранения гражданина от работы со сведениями, составляющими государственную тайну, оформляется письменное заключение, подготовленное подразделением по защите государственной тайны и структурным подразделением, в котором указанный гражданин работает.

Заключение утверждается руководителем организации. Об этом факте письменно сообщается в орган безопасности.

Прекращение допуска должностного лица или гражданина к государственной тайне является **дополнительным основанием для расторжения с ним трудового договора** (контракта), если такие условия предусмотрены в трудовом договоре (контракте).

Прекращение допуска к государственной тайне **не освобождает должностное лицо или гражданина от взятых ими обязательств** по неразглашению сведений, составляющих государственную тайну.

Подразделение по защите государственной тайны организации ведет учет фактической степени осведомленности граждан, работающих в данной организации и допущенных к особой важности, совершенно секретным и секретным сведениям.

Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть **временно ограничены в своих правах.** Ограничения могут касаться:

- права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;
- права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;
- права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Подготовка материалов на граждан, оформляемых (переоформляемых) на допуск к особой важности, совершенно секретным и секретным сведениям, **осуществляется управлениями (отделами) кадров**, а в случае их отсутствия - работниками, ведущими кадровую работу в организации (кадровый аппарат). **Направлять граждан в подразделения по защите государственной тайны и органы безопасности по вопросам оформления допуска запрещается.**

Граждане, оформляемые на допуск к государственной тайне, заполняют анкету, в которой обязаны указывать достоверные данные.

Работники кадрового аппарата в ходе беседы с оформляемым на работу (службу) гражданином сверяют указанные в анкете данные с его личными документами (паспорт, военный билет, трудовая книжка, диплом об образовании, свидетельство о рождении и т. д.), уточняют отдельные вопросы анкеты, выявляют представляющие интерес сведения, не предусмотренные вопро-

сами анкеты, выясняют у гражданина, имел ли он за последний год отношение к секретным работам, документам и изделиям, давал ли он обязательство по неразглашению сведений, составляющих государственную тайну, работал ли (служил) на режимных объектах, запрашивают необходимые справки и документы, знакомят гражданина с содержанием договора (контракта) об оформлении допуска к государственной тайне.

Если в ходе беседы или в анкетных данных выявлены обстоятельства, влияющие на принятие решения о допуске гражданина к государственной тайне, или установлено, что он ранее работал с особой важности или совершенно секретными сведениями, то о результатах беседы работники кадрового аппарата обязаны информировать в устной или письменной форме руководителя подразделения по защите государственной тайны соответствующей организации.

Подразделения по защите государственной тайны:

- разрабатывают рекомендации для кадровых аппаратов по оформлению на работу граждан, подлежащих допуску;
- запрашивают при необходимости из подразделений по защите государственной тайны организаций, где оформляемый гражданин в течение последнего года работал,
- дают оценку первичным материалам, представляемым кадровыми аппаратами на оформляемых (переоформляемых) граждан или получаемым из подразделений по защите государственной тайны с прежних мест работы указанных граждан, в целях определения целесообразности проведения проверочных мероприятий органами безопасности;
- оформляют и хранят учетные материалы по допуску,
- осуществляют контроль за исполнением требований по допуску.

Данные положения Закона описывают одну из основных форм отношений – отношения между государством в лице органов государственной власти, предприятий, учреждений и организаций и должностными лицами и гражданами, допускаемыми к государственной тайне. Статьи Закона и напрямую затрагивают права и свободы граждан.

Основой допуска является его добровольность на условиях, оговариваемых в трудовом договоре (контракте). Выделение из, безусловно, более широкой категории "граждан" категории "должностных лиц" связано с положениями статьи 1 Закона, в соответствии с которой принцип добровольности рассматривается как бы с двух позиций: для граждан - в качестве условия при поступлении на работу или при привлечении их к работам, связанным с использованием сведений, составляющих государственную тайну, а для должностных лиц – в качестве условия для занятия определенных должностей,

статус которых, предполагает ознакомление со сведениями, составляющими государственную тайну.

Положения, касающиеся проведения проверочных мероприятий, согласуются с положениями Закона Российской Федерации "Об оперативно-розыскной деятельности". В законе есть существующее положение о том, что **до окончания проверочных мероприятий администрация не имеет права вступать с допускаемым лицом в договорные отношения.**

Для должностных лиц и граждан, допускаемых к государственной тайне на постоянной основе, Законом предусмотрены льготы, направленные на стабилизацию контингента допущенных лиц. Для работников структурных подразделений по защите государственной тайны предусмотрены дополнительные льготы, увязанные со стажем их работы в указанных подразделениях. Такая мера способствует уменьшению текучести кадров в режимно-секретных и других органах, непосредственно связанных с защитой государственной тайны. Данная норма реализована постановлением Правительства Российской Федерации от 18 сентября 2006 г. № 573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны» (в ред. Постановлений Правительства РФ от 06.06.2008 № 440, от 31.01.2012 № 60.

Допуск предприятий, учреждений и организаций

Допуск предприятий, учреждений и организаций (далее – предприятия) 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, регламентируется Положением 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 (утв. постановлением Правительства РФ от 15 апреля 1995 г. № 333 с изменениями и дополнениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г., 3 октября 2002 г., 17 декабря 2004 г., 26 января 2007 г., 22 мая 2008 г., 31 марта, 24 сентября 2010 г., 3 ноября 2011 г., 5 мая 2012 г)

Лицензии выдаются на конкретный вид деятельности:

– на допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну;

– на право проведения работ, связанных с созданием средств защиты информации;
– на правоосуществление мероприятий и (или) оказания услуг в области защиты государственной тайны.

Лицензия является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока, в зависимости от специфики вида деятельности, но не более чем на 5 лет. Действует на всей территории Российской Федерации.

Лицензии выдаются 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.

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, – Федеральная служба по техническому и экспортному контролю, 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, Федеральная служба по техническому и экспортному контролю, Служба внешней разведки Российской Федерации (в пределах их компетенции).

Работа органов, уполномоченных на ведение лицензионной деятельности, координируется Межведомственной комиссией по защите государственной тайны.

Для получения лицензии заявитель представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности, следующие документы:

а) заявление о выдаче лицензии с указанием:
– наименования, организационно-правовой формы и местонахождения предприятия;

– идентификационного номера налогоплательщика;
– даты уплаты предприятием государственной пошлины за предоставление лицензии;
– сведений о наличии допуска к государственной тайне у руководителя предприятия;
– адресов мест осуществления лицензируемого вида деятельности;
– реквизитов правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;
– вида деятельности, на осуществление которого должна быть выдана лицензия;
– срока действия лицензии;
– степени секретности сведений, составляющих государственную тайну, с которыми заявитель предполагает осуществлять работы, подтвержденной органом государственной власти или организацией, наделенными полномочиями по распоряжению указанными сведениями;
– формы предоставления лицензии (на бумажном носителе или в электронной форме (в форме электронного документа, подписанного электронной подписью));

б) копии учредительных документов юридического лица;

в) копии правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

г) копия договора об оказании услуг (в случае использования заявителем услуг структурного подразделения по защите государственной тайны другой организации).

Орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии в течение 30 дней со дня получения заявления со всеми необходимыми документами.

В случае необходимости проведения дополнительной экспертизы предприятия решение принимается в 15-дневный срок после получения заключения экспертизы, но не позднее чем через 60 дней со дня подачи заявления о выдаче лицензии и необходимых для этого документов.

В зависимости от сложности и объема подлежащих специальной экспертизе материалов руководитель органа, уполномоченного на ведение лицензионной деятельности, может продлить срок принятия решения о выдаче или об отказе в выдаче лицензии до 30 дней.

Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (руководители предприятий), 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.

В лицензии указываются:

- наименование органа, выдавшего лицензию;
- наименование, место нахождения предприятия, адреса мест осуществления лицензируемого вида деятельности (при необходимости), в том числе адреса мест осуществления лицензируемого вида деятельности подразделениями предприятия;
- идентификационный номер налогоплательщика;
- вид деятельности, на осуществление которого выдана лицензия;
- условия осуществления вида деятельности, на который выдана лицензия;
- степень секретности разрешенных к использованию сведений, составляющих государственную тайну, для лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну;
- срок действия лицензии;
- регистрационный номер и дата выдачи лицензии.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не более чем на 5 лет. По просьбе заявителя лицензия может выдаваться на срок менее 5 лет. Срок действия лицензии, выданной предприятию, не может превышать срока действия лицензии предприятия, структурное подразделение по защите государственной тайны которого оказывает услуги по защите государственной тайны.

Продление срока действия лицензии производится в порядке, установленном для ее получения.

Предприятие может иметь несколько лицензий.

Лицензия подписывается руководителем органа, уполномоченного на ведение лицензионной деятельности, либо лицом, им уполномоченным, и заверяется печатью этого органа. Копия лицензии хранится в органе, уполномоченном на ведение лицензионной деятельности.

В случае изменений условий ведения лицензируемого вида деятельности, изменения степени секретности сведений, с которыми осуществляется (предполагается осуществлять) деятельность, а также в отношении которых лицензиат предполагает проводить мероприятия и (или) оказывать услуги, смены организационно-правовой формы или реорганизации лицензиата, изменения его наименования, места нахождения, адресов мест осуществления лицензируемого вида деятельности лицензиат или его правопреемник обязаны в 15-дневный срок подать в орган, уполномоченный на ведение лицензионной деятельности, заявление о переоформлении лицензии в связи с изменением условий деятельности с приложением документов, подтверждающих соответствующие изменения. В указанных случаях орган, уполномоченный на ведение лицензионной деятельности, по результатам рассмотрения заявления и проведения проверки соответствия предприятия лицензионным требованиям и условиям принимает решение о необходимости проведения специальной экспертизы и уведомляет о своем решении заявителя. В случае принятия решения о необходимости проведения специальной экспертизы выдача лицензии производится с учетом ее результатов.

Орган, уполномоченный на ведение лицензионной деятельности, вправе отказать в выдаче лицензии. Письменное уведомление об отказе в выдаче лицензии с указанием причин отказа направляется заявителю в 3-дневный срок после принятия соответствующего решения.

Основанием для отказа в выдаче лицензии является:

- наличие в документах, представленных заявителем, недостоверной или искаженной информации;
- отрицательное заключение экспертизы, установившей несоответствие необходимым для осуществления заявленного вида деятельности условиям.
- отрицательное заключение по результатам государственной аттестации руководителя предприятия.

Специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Организация и порядок проведения специальных экспертиз предприятий определяются инструкциями, которые разрабатываются уполномочен-

ными государственными органами и согласовываются с Межведомственной комиссией.

Государственная аттестация руководителей предприятий

Организуется органами, уполномоченными на ведение лицензионной деятельности, а также министерствами и ведомствами Российской Федерации, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий. Методические рекомендации по организации и проведению государственной аттестации руководителей предприятий разрабатываются Межведомственной комиссией.

Органы, уполномоченные на ведение лицензионной деятельности, приостанавливают действие лицензии или аннулируют ее в случае:

- предоставления лицензиатом соответствующего заявления;
- обнаружения недостоверных данных в документах, представленных для получения лицензии;
- нарушения лицензиатом условий действия лицензии;
- невыполнения лицензиатом предписаний или распоряжений государственных органов или приостановления этими государственными органами деятельности предприятия в соответствии с законодательством Российской Федерации;
- ликвидации предприятия.

Организация доступа к сведениям, составляющим государственную тайну

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия, учреждения или организации, а также на их структурные подразделения по защите государственной тайны.

Порядок доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, устанавливается нормативными документами, утверждаемыми Правительством Российской Федерации (Постановление Правительства РФ от 06.02.2010 №63 «Об утверждении инструкции о порядке допуска должностных лиц и граждан российской федерации к государственной тайне»).

Руководители органов государственной власти, предприятий, учреждений и организаций несут персональную ответственность за создание таких условий, при которых должностное лицо или **гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей**.

Таким образом, организация доступа к сведениям, составляющим государственную тайну, возлагается на руководителей соответствующих органов государственной власти, предприятий, учреждений и организаций, а также на их структурные подразделения по защите государственной тайны, непосредственно реализующих процедуру доступа. Сама процедура доступа в Законе не описывается в предположении сделать это в нормативных документах, утверждаемых Правительством Российской Федерации. Такой подход представляется оправданным, поскольку процедура доступа довольно объемна по содержанию, предполагает определенную инвариантность, связанную со спецификой осуществляемой деятельности и, кроме того, должна сохранять способность оперативно реагировать на изменения внешних условий.

Доступ граждан к особой важности, совершенно секретным и секретным сведениям в организациях, куда они командируются по служебным делам, осуществляется после предъявления ими документов, удостоверяющих личность, справок о допуске и предписаний на выполнение заданий.

В случае отсутствия в организации режимно-секретного подразделения или работника, исполняющего функции режимно-секретного подразделения, справка о допуске выдается командированному лицу режимно-секретным подразделением организации, оказывающей услуги в области защиты государственной тайны.

Справка о допуске по соответствующей форме подписывается руководителем режимно-секретного подразделения и заверяется печатью организации. Справка регистрируется в журнале учета выдачи справок о допуске и выдается командируемому на время разовой командировки или на период выполнения задания, но не более чем на год, под расписку. По окончании срока действия справка возвращается по месту ее выдачи.

Предписание на выполнение задания подписывается руководителем организации, а в органах государственной власти - должностным лицом, уполномоченным руководителем соответствующего органа, заверяется печатью организации (органа) и регистрируется в журнале учета выдачи предписаний на выполнение заданий. В предписании на выполнение задания указывается основание для командирования (номер и дата постановления, решения, договора, совместного плана научно-исследовательских и опытно-конструкторских работ и т. п.). Предписание на выполнение задания, в кото-

ром содержатся сведения, составляющие государственную тайну, пересылается в установленном порядке.

Предписание на выполнение задания выдается для посещения только одной организации.

Командированный гражданин может иметь доступ в присутствии работников принимающей организации, ответственных за прием командированных лиц, только к тем сведениям, составляющим государственную тайну, которые ему необходимы для выполнения задания, указанного в предписании на выполнение задания.

Доступ командированных граждан к сведениям, составляющим государственную тайну, осуществляется по письменному разрешению руководителя принимающей организации, а в органах государственной власти - должностного лица, уполномоченного руководителем соответствующего органа. Разрешение оформляется на предписании на выполнение задания с указанием конкретных носителей сведений, составляющих государственную тайну, с которыми можно ознакомить командированного гражданина.

Предписание на выполнение задания и справка о допуске по соответствующей форме регистрируются в журнале учета командированных. После регистрации справка о допуске остается в режимно-секретном подразделении принимающей организации, а предписание на выполнение задания с отметкой о форме допуска командированного гражданина передается принимающему его должностному лицу. Указанное должностное лицо заполняет на оборотной стороне предписания на выполнение задания справку, после чего данное предписание передается в режимно-секретное подразделение принимающей организации, где хранится в отдельном деле не менее 5 лет. Справка о допуске возвращается командированному гражданину для сдачи в выдавшее ее режимно-секретное подразделение. На обороте справки о допуске по соответствующей форме делается запись с указанием степени секретности сведений, с которыми ознакомился командированный гражданин, и даты ознакомления, которая заверяется подписью руководителя режимно-секретного подразделения принимающей организации и печатью этой организации.

7 ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ КАК ОБЪЕКТ ЗАЩИТЫ

Структура предприятия

Под предприятием будем понимать любой объект, обрабатывающий материальные или информационные потоки. Вариант структуры предприятия представлен на рисунке 2.

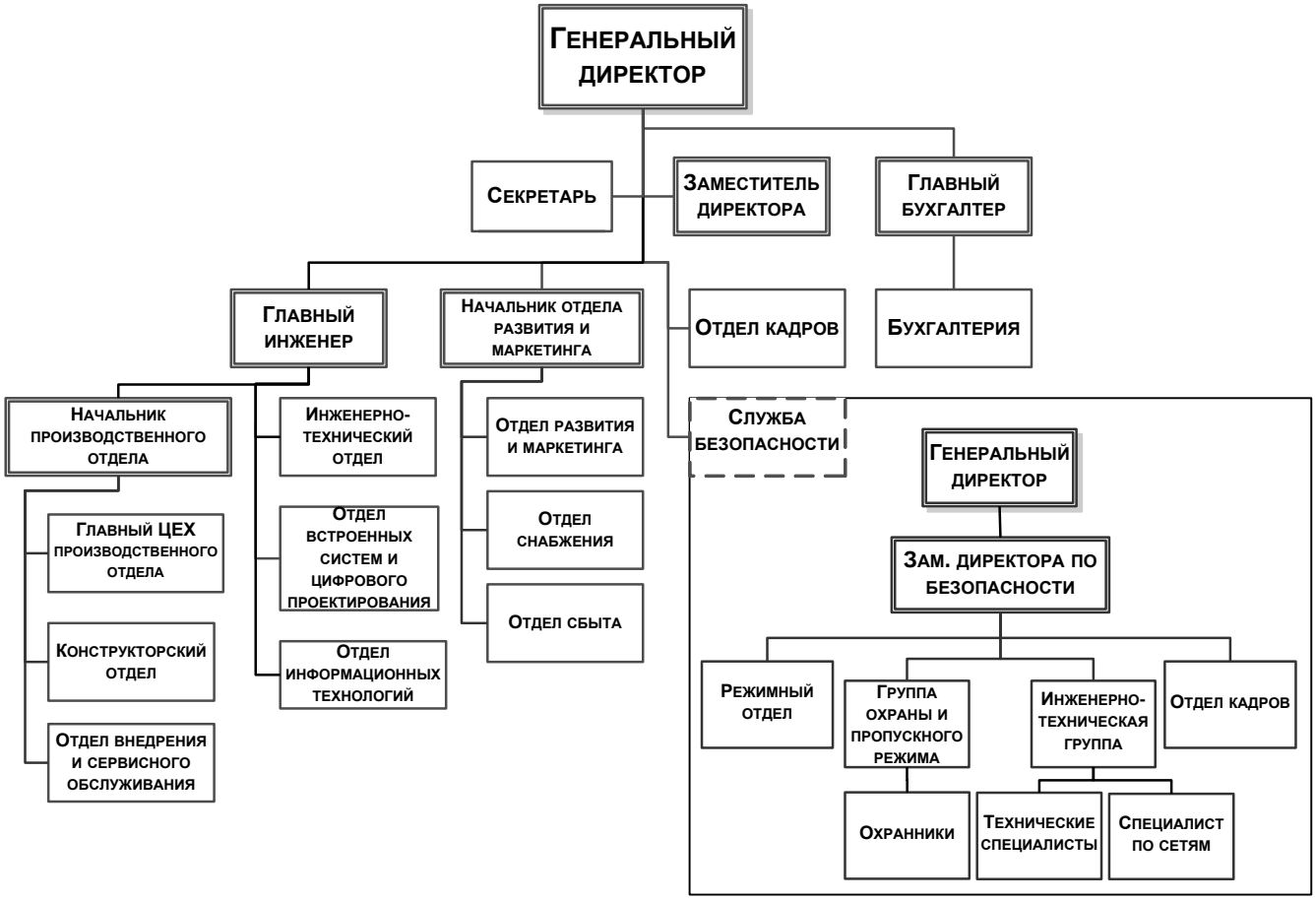


Рисунок 2 – Вариант структуры предприятия

В общем случае предприятие включает в себя здания и прилегающие к ним территории. Границы этой территории могут быть обозначены физической преградой или просто зафиксированы законодательно.

Предприятие включает в себя помещения и участки различного назначения, в том числе:

- кабинет руководящего состава и совещательные комнаты;
- кабинеты сотрудников и основных служб;
- представительские и переговорные помещения;
- помещения технических служб, а именно: узлы энергоснабжения, водоснабжения, газоснабжения, телефонный узел, склады и т.д.;
- производственные помещения с оборудованием;
- хранилища ценностей, оружия, вредных и опасных веществ;
- хранилища различных носителей информации.

Между помещениями и внутри них циркулируют материальные потоки, ценности и информация (документы, телефонные, телефаксные, компьютерные и радиоканалы связи), энергоносители.

Аналогичные потоки, а также транспорт перемещаются и через границу предприятий.

Обработку и транспортировку перечисленных потоков выполняет персонал предприятия.

Кроме того, на любом предприятии присутствуют посетители, наличие которых также нужно учитывать при формировании системы защиты информации.

Порядок перемещения и обработки входящих и выходящих из каждого подразделения информационных потоков устанавливается правилами внутреннего распорядка и должностными инструкциями. Пример формирования информационных потоков показан на рисунках 3 и 4. Информационные потоки могут быть как открытые, так и закрытые.

Документами, определяющими размещение подразделений и служб предприятия являются генеральные планы территорий и поэтажные планы зданий.

На планах должны быть обозначены каналы связи, линии энергоснабжения, потоки движения ценностей и материальные потоки.

Для анализа и упорядочивания информационных потоков составляется схема документооборота. Таким образом, в систему анализа информационной безопасности необходимо включать:

- персонал предприятия,
- посетителей,
- материальные ценности,
- энергоносители,
- информацию в различных ее видах.

Рисунок 3 – Пример формирования внешних информационных потоков

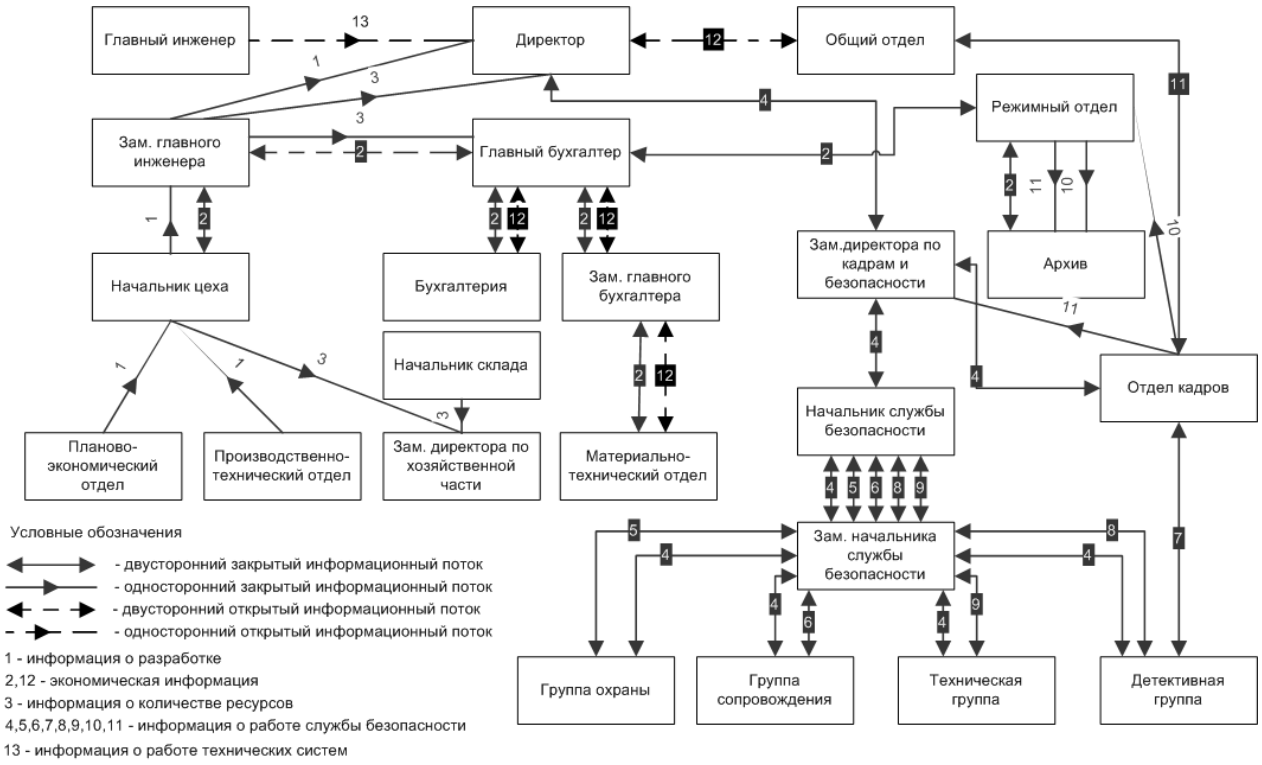


Рисунок 4 – Пример формирования внутренних информационных потоков

Основные виды угроз безопасности

Все виды угроз безопасности можно разделить на естественные и искусственные.

Естественные угрозы – угрозы, не связанные с деятельностью человека (пожар, ураган, наводнение и т.д.).

Искусственные угрозы - угрозы, вызванные деятельностью человека. Искусственные угрозы, в свою очередь, можно разделить на:

- Непреднамеренные угрозы – несознательно наносимый вред. Субъекта таких угроз называют нарушителем.
- Преднамеренные или умышленные угрозы (угрозы, при которых человек сознательно искажает, портит, крадет информацию и т.д.). Субъекта таких угроз называют злоумышленником

Умышленные угрозы могут проявляться путем:

- внедрения злоумышленника в персонал предприятия,
- вербовки персонала, при этом завербованный сотрудник приравнивается к злоумышленнику,
- несанкционированного проникновения на территорию объекта,
- дистанционного воздействия и наблюдения.

Среди всех видов угроз отдельно выделим несанкционированный съем информации. Съем информации может осуществляться путем:

- контроля каналов связи,
- негласной установки специальных технических средств,
- анализа и контроля побочных излучений (электромагнитные звуковые, видео, тепловые излучения),
- негласной фото- и видеосъемки,
- хищения документов,
- хищения магнитных и других носителей,
- хищения бумажных отходов, а именно: распечатки, копировальная бумага и т.д.

Об основных видах и субъектах угроз можно получить информацию из таблицы 7.

Классификация средств защиты

По функциональному значению средства защиты делятся на 3 группы:

1. средства обнаружения угрозы,
2. средства отражения угрозы,
3. средства ликвидации угрозы.

Таблица 7 – Виды и субъекты угроз (+ существование угрозы)

Приоритет	Виды угроз	Субъекты угроз			
		Стихия	Нарушитель	Злоумышленник	
				На территории	Вне территории
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудование, техники	+	+	+	+
3	Повреждение систем жизнеобеспечения	+	+	+	+
4	Несанкционированное изменение технологического процесса		+	+	
5	Использование нерегламентированных технических и программных средств		+	+	
6	Дезорганизация функционирования предприятия	+		+	
7	Хищение материальных ценностей			+	
8	Уничтожение или перехват данных путем хищения носителей информации			+	
9	Устное разглашение конфиденциальной информации		+		
10	Несанкционированный съем информации			+	+
11	Нарушение правил эксплуатации средств защиты		+	+	

Средства обнаружения угрозы – это технические средства и организационные мероприятия, позволяющие обнаружить факт наличия злоумышленника или разрушающего воздействия.

Основу группы составляют средства сигнализации и оповещения, проверка входящих и выходящих потоков информации и персонала. По режиму работы эти средства делятся на средства постоянного (непрерывного) и периодического воздействия.

Средства отражения угрозы – это средства, препятствующие самой угрозе, а именно:

- ограждение территорий,
- специальная планировка помещений,
- замки, решетки, ограждения,
- средства защиты коммуникаций,
- средства защиты данных.

Средства ликвидации угрозы – это средства, обеспечивающие устранение источников угрозы:

- оружие, охрана,
- средства связи с милицией, охранными структурами и т.д.

Кроме того, все средства защиты можно разделить на:

- основные,
- дополнительные (для повышения эффективности защиты)
- специальные (средства, предназначенные для безопасности с учетом специфики функционирование предприятия).

Границы пространства, защищаемого от угрозы, называются **рубежами защиты.** Таких рубежей может быть несколько. Область пространства внутри замкнутого рубежа называется **зоной безопасности.**

Выделение рубежей защиты и грамотное формирование зон безопасности позволяет не только снизить затраты на охрану объекта, но и повысить эффективность самой защиты. При грамотном формировании зон безопасности зоны с ограниченным доступом должны располагаться в зонах с меньшими требованиями к безопасности (рис. 5).

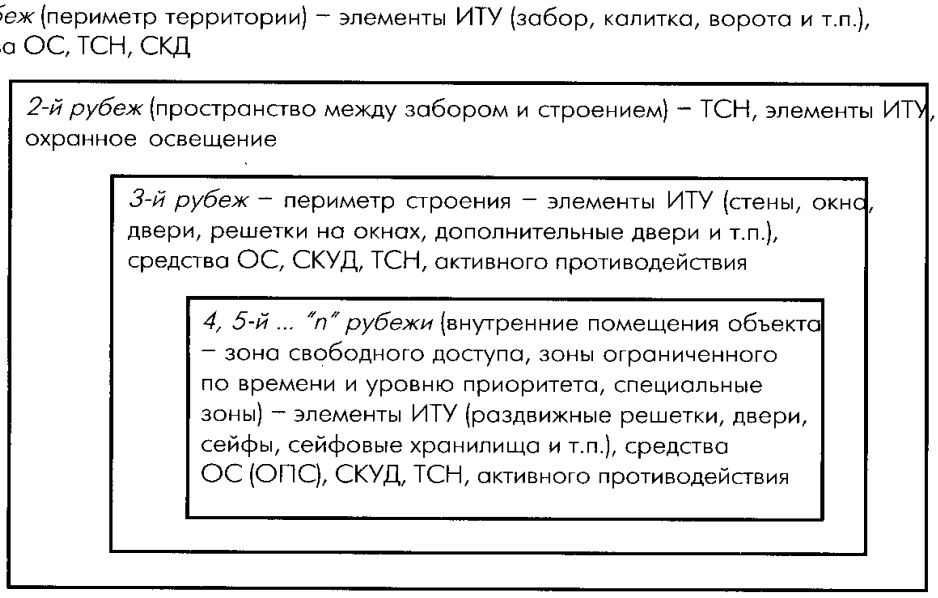


Рисунок 5 – Принцип формирования зон безопасности

Последнее особенно актуально для предприятий, занимающих большую территорию, имеющих большое количество сотрудников, а также в случае, когда предприятие не имеет физической границы Пример формирования зон безопасности конкретного предприятия показан на рисунках 6 и 7.

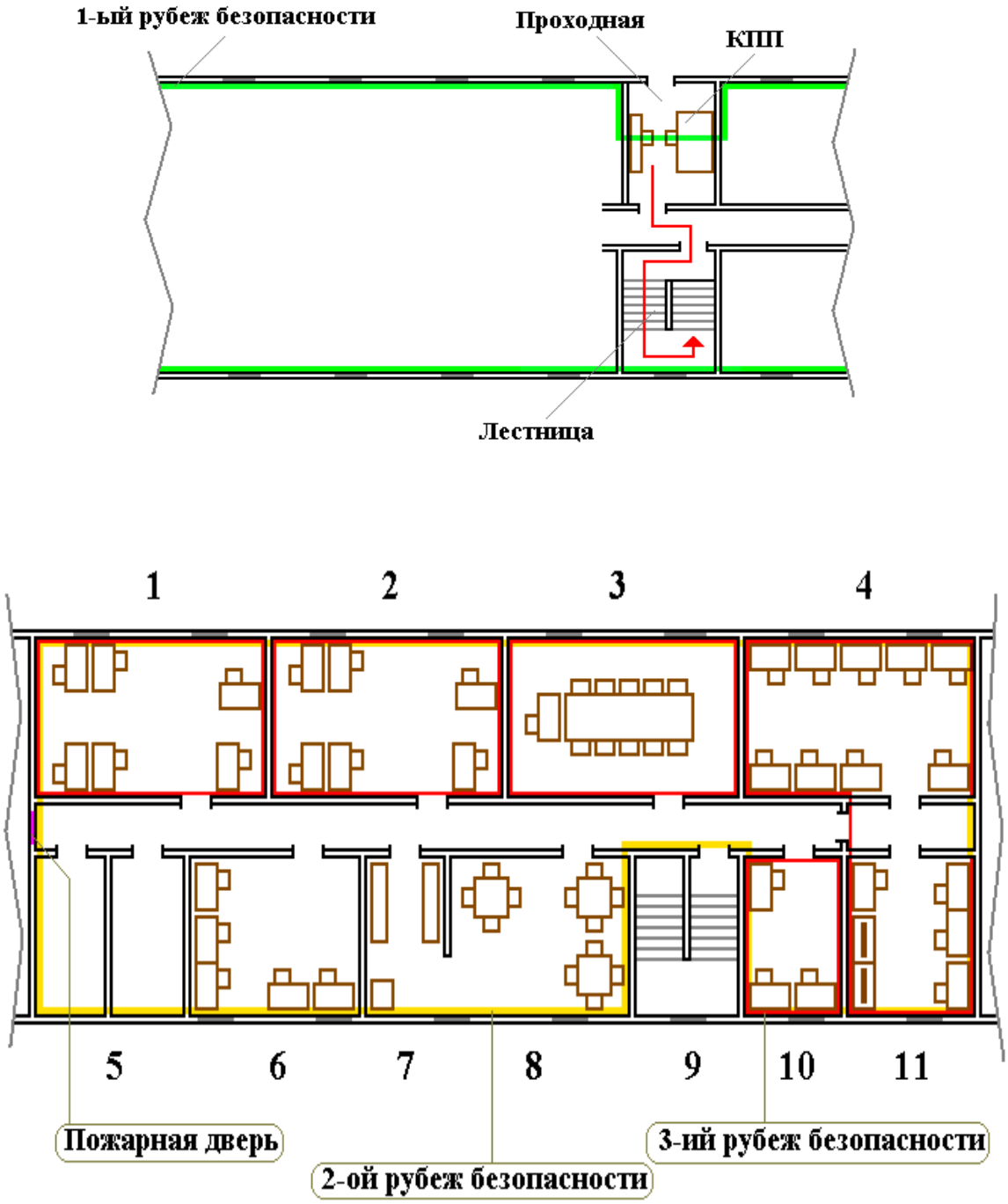
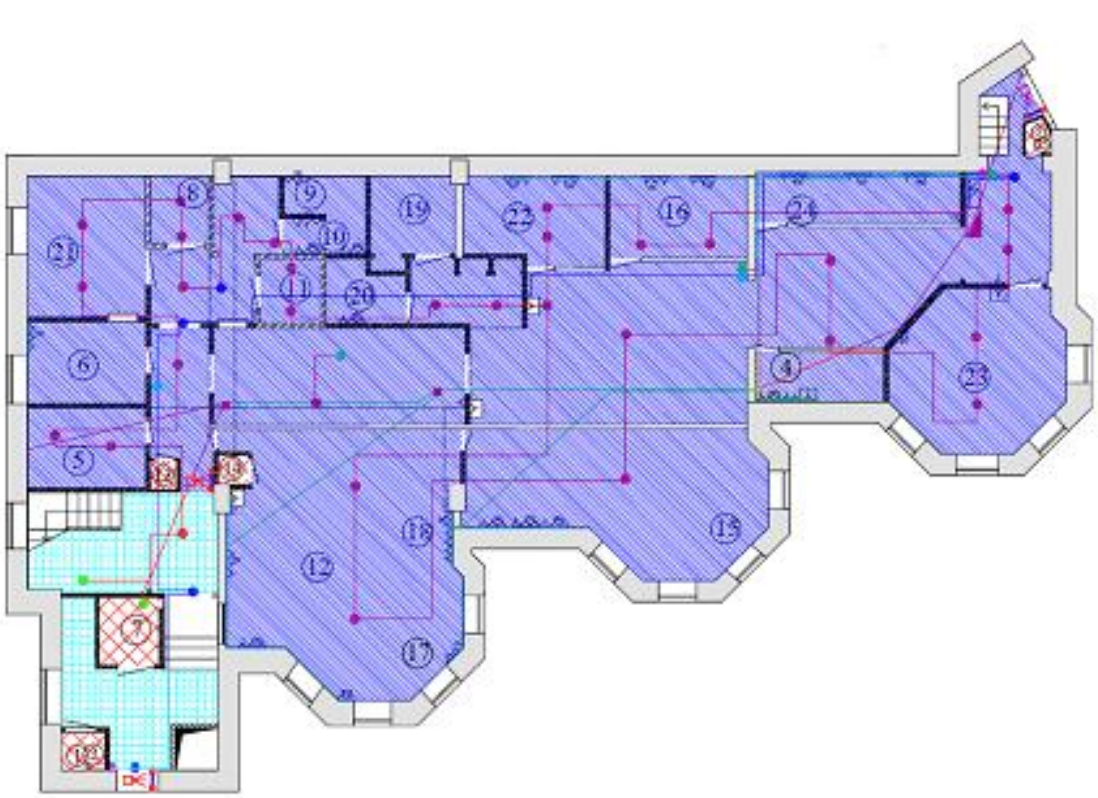


Рисунок 6 – Пример формирования зон безопасности офиса, расположенного на арендуемых площадях (1-й и 2-й этажи)

Экспликация помещений

N	Наименование	Площ кв. м
1	Пост охраны	3.00
2	Проходная	3.40
3	Пост охраны	3.00
4	Кабинет нач. делопроизводства	14.70
5	Охрана	11.00
6	Кабинет нач. бюро пропусков	9.80
7	Дежурный бюро пропусков	3.30
8	Кабинет директора по безопасности	8.40
9	Нач. отдела защиты информации	8.00
10	Отдел защиты информации	12.60
11	Нач. отдела физической защиты	12.80
12	Производственные помещения	220.80
13	Пост охраны	3.20
14	Пост охраны	3.00
15	Склад продукции	150.20
16	Главный инженер	12.20
17	Заместитель инженера	12.20
	по производству	
18	Отдел производства	50.20
19	Главный конструктор	14.40
20	Главный технолог	9.80
21	Конструкторское бюро	20.80
22	Отдел качества	10.80
23	Кабинет директора	20.80
	по делопроизводству	
24	Отдел делопроизводства	30.80
25	Проходная	3.20



УСЛОВНЫЕ ОБОЗНАЧЕНИЯ:

- Компьютер
- Телефон
- Принтер
- металлорукав
- гофрированная труба d=32
- гофрированная труба d=40
- кабельный канал 32х16
- коробка разветвительная
- извещатель пожарный дымовой
- извещатель ручной пожарный
- видеокамера
- оповещатель световой
- оповещатель звуковой
- зона безопасности категории А
- зона безопасности категории В
- зона безопасности категории С

Рисунок 7 – Пример формирования зон безопасности в здании офиса

8 СЛУЖБА БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

К организационным методам защиты информации относят организационно-технические и организационно-правовые меры, которые регламентируют процесс функционирования объекта, а также обеспечивающие запрет доступа или затрудняющие несанкционированный доступ к информации.

Адекватный уровень информационной безопасности в организации может быть обеспечен только на основе комплексного подхода, предполагающего использование как технических, так и организационных мер защиты.

Причем, по мнению большинства отечественных и западных специалистов, организационные меры играют существенную роль в этом направлении.

Эффективность любых самых сложных и дорогостоящих технических механизмов защиты может быть сведена к нулю, в случае игнорирования элементарных правил безопасности.

Основой организационных мер является политика информационной безопасности, под которой понимается совокупность нормативных и организационно-распорядительных документов предприятия по защите информации и ассоциированных с ней ресурсов.

Для планирования и практической реализации этих мер на крупных предприятиях создается служба безопасности. Рассмотрим ее структуру и задачи.

На небольших предприятия функции службы безопасности могут исполнять один или несколько человек, либо подобные функции возлагаются на какого-либо сотрудника предприятия.

Задачи службы безопасности

Служба безопасности выполняет следующие задачи:

- определение основных направлений работы по обеспечению безопасности деятельности объекта и его персонала, а также соблюдение сохранности информации;
- организация системы защиты объекта, разработка системы защиты на предпроектной стадии, участие в разработке технического проекта и его реализации, приемка всех элементов защиты, поддержание системы защиты в работоспособном состоянии;
- разработка нормативов работы с информацией всех категорий, контроль за соблюдением правил обработки, хранения и пересылки конфиденциальной информации;

– разработка мер безопасности и правил обработки, хранения и транспортировки материальных ценностей и ценных бумаг, контроль за выполнением соответствующих нормативов;
– организация и обучение персонала объекта правилам соблюдения и поддержания режима безопасности, проведение квалифицированные тестов;
– организация и проведение совместно с другими подразделениями объекта мероприятий по защите;
– взаимодействие с правоохранительными органами по вопросам безопасности.

Типовая структура Службы безопасности и ее вариант приведены на рисунках 8 и 9.

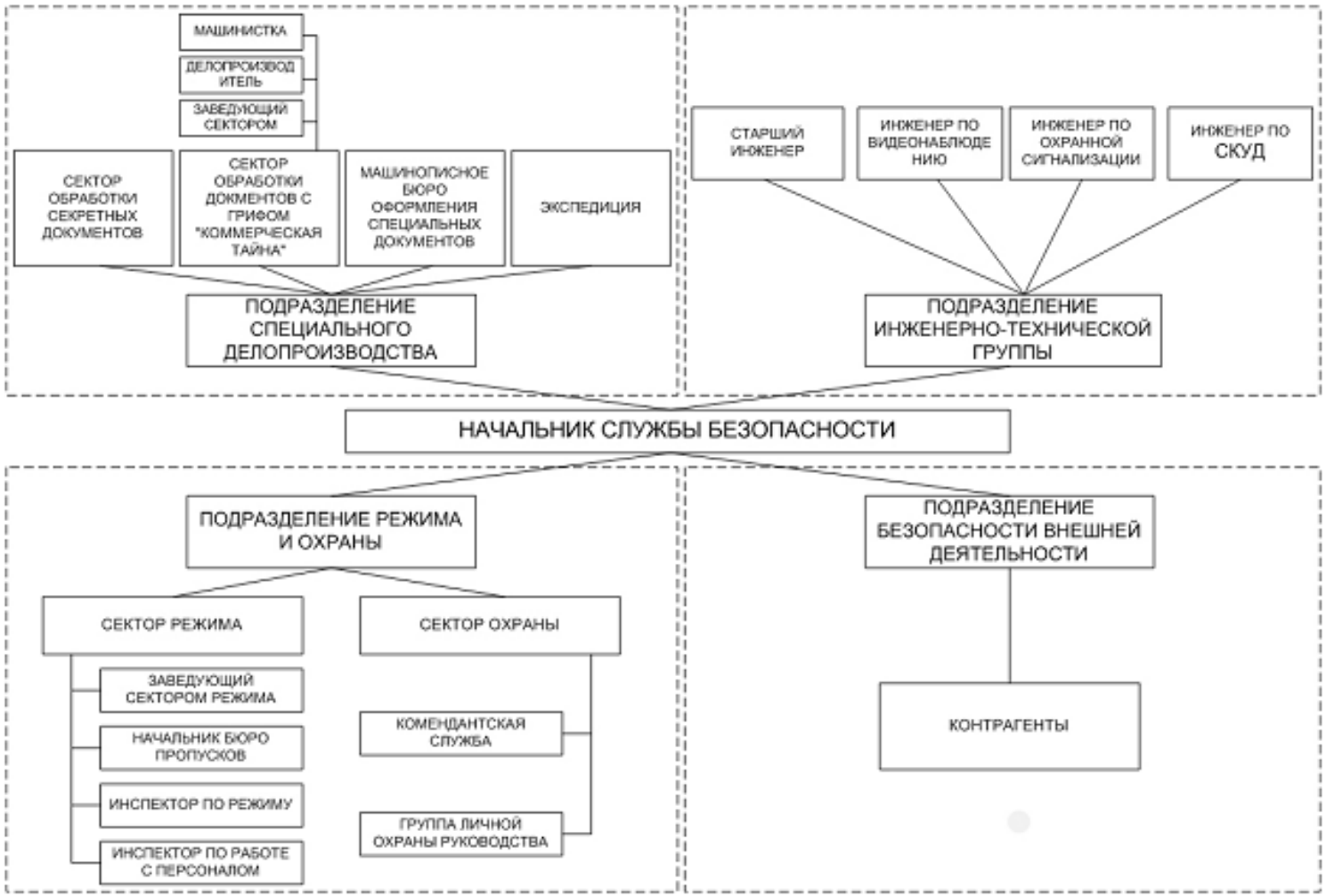


Рисунок 9 – Вариант структуры службы безопасности

Функции основных групп службы безопасности

В состав основных групп службы безопасности входя следующие группы:

1. группа режима;
2. группа охраны и сопровождения;
3. техническая группа;
4. группа режима;
5. детективная группа (группа разведки).

Функции группы режима

В ведении сотрудников этой группы находятся все вопросы, связанные с регламентацией деятельности персонала объекта и его посетителями.

Основные функции группы режима.

1. Определение перечня сведений, составляющих коммерческую или служебную тайну, если таковые сведения не упомянуты в общегосударственных документах.

2. Разработка положений и инструкций о порядке работы с конфиденциальной информацией и сведениями, составляющими тайну.

3. Организация и ведение закрытого делопроизводства, учет пользования, хранение и размножение документов и других носителей конфиденциальной информации.

4. Допуск персонала объекта к работе с конфиденциальной информацией, проверка выполнения сотрудниками работы с такой информацией.

5. Изучение кандидатов для приема на работу, связанную с допуском к информации различных категорий конфиденциальности.

Функции группы охраны и сопровождения

Основные функции группы режима охраны и сопровождения.

1. Обеспечение физической охраны объекта и помещений внутри предприятия.

2. Выявление угроз безопасности объекта, защита от угроз и их ликвидация.

3. Организация прохода персонала и посетителей в различные зоны безопасности.

4. Наблюдение за обстановкой на территории объекта и вокруг него.

5. Участие в экстренных действиях при чрезвычайных обстоятельствах.

6. Контроль работоспособности элементов системы защиты.

7. Обеспечение безопасности транспортировки ценных грузов и документов.

В исключительных случаях эта группа обеспечивает охрану отдельных лиц из числа персонала объекта.

Охрана предприятия может осуществляться силами самого предприятия (ведомственная охрана) либо с привлечением по договору соответствующих организаций (МВД, вневедомственная охрана, охранные группы).

Функции технической группы

Взаимодействует с группой охраны по обеспечению безопасности деятельности объекта с помощью технических средств, а именно:

- системы сигнализации,
- системы наблюдения,
- системы связи и т.п.

Сотрудники группы отвечают за бесперебойную работу всех технических средств, ремонтируют и настраивают аппаратуру, совершенствуют технические средства. Сотрудники этой группы особенно тщательно проверяются и отбираются при приеме на работу, т.к. сотрудники группы имеют доступ практически во все помещения предприятия.

Функции детективной группы (группа разведки)

Это специализированное подразделение, которое проводит мероприятия по изучению отдельных лиц из числа персонала, посетителей и клиентов фирм, иногда жителей ближайшего к объекту окружения, в действиях которых содержится угроза безопасности объекта; кроме этого сотрудники группы могут проверять кандидатов для приема на работу.

По заданию руководства разрабатывают и проводят специальные мероприятия в отношении фирм-конкурентов, поддерживают контакт с правоохранительными органами.

Для средних объектов создаются группы безопасности, состоящие из сотрудников охраны и техников по настройке и ремонту аппаратуры.

Небольшие предприятия могут размещаться в одном здании с другими предприятиями. В этом случае возможно создание единой службы безопасности.

В случае аренды помещения у крупного предприятия более мелким предприятием вступают в силу договорные отношения. Чаще всего в таких случаях охрана всего объекта осуществляется арендодателем.

Организация аналитической работы на предприятии по изучению возможных путей утечки информации

(Разведывательная деятельность службы безопасности предприятия)

Направления этого вида деятельности Службы безопасности можно условно разделить на внешнюю разведку и внутреннюю разведку (или контрразведку).

Вся разведывательная или контрразведывательная деятельность должна **строго следовать закону.** Перед службой безопасности ставится одна общая цель: своевременное выявление и предоставление руководству предприятия информации о реальных и потенциальных угрозах его функционирования.

Для достижения данных целей решаются следующие задачи:

- Выявление правонарушений, затрагивающих экономические интересы предприятия.
- Своевременное информирование о методах, способах и лицах, имеющих намерение нанести ущерб предприятию или его персоналу.
- Содействие правоохранительным, судебным и контрольно-надзорным органам в привлечении к ответственности юридических и физических лиц, действия которых затрагивают интересы предприятия.

Пути решения поставленных задач:

- Изучение криминальных аспектов рынка.
- Определение степени надежности деловых партнеров.
- Предоставление руководству предприятия необходимой информации до и во время проведения деловых переговоров.
- Изучение негативных аспектов теневой экономики.
- Выявление предприятий, занимающихся недобросовестной конкуренцией.
- Сбор сведений о лицах, не работающих на предприятии, и замышляющих, либо совершивших преступление против его персонала или имущества.
- Проверка лиц, заключивших с предприятием коммерческий контракт.
- Проверка кредитоспособности деловых партнеров.
- Выявление и документирование фактов нарушения прав владельцев товарного знака.
- Сбор сведений по гражданским делам в отношении юридических или гражданских лиц, ранее работавших на предприятии.
- Выявление среди работающих на предприятии лиц, занимающихся экономическим шпионажем против предприятия-учредителя.

Структура разведки, обычно, включает в себя добывающие и информационные подразделения (группы). На добывающие подразделения приходится 80% финансирования, и 20% - на информационные.

Добывающие подразделения.

Задача добывающих подразделений состоит в получении всеми доступными, но не противоречащими законодательству средствами и методами, сведений, документов, предметов и других материалов, которые могут представлять разведывательный интерес. Добывающие подразделения должны

быть ориентированы на то, что необходимые сведения могут быть в первую очередь перехвачены у людей, которые причастны к процессу сбора, передачи, накопления, хранения, поиска, переработки информации (т. е. все виды работы с информацией) и выдачи ее для использования.

Информационные подразделения.

Задача информационных подразделений – оценка, классификация, анализ и предоставление руководству предприятия разведывательной информации.

Источники информации:

1. Люди:
   - сотрудники своего предприятия, контактирующие в силу своего служебного положения с внешними источниками;
   - персонал других предприятий и учреждений, имеющий доступ к закрытой информации;
   - лица свободных профессий или не работающие, имеющие контакты с сотрудниками других предприятий, общественных организаций, общественных движений, партий;
   - сотрудники разведывательного подразделения службы безопасности, внедрившиеся по заданию своего руководства на другие предприятия с целью сбора информации.
2. Документы – наибольшей доказательностью является оригинал документа. При его отсутствии прибегают к получению копии.
3. Изделия – промышленный образец рассматривается как важнейший элемент доказательства.

Полученную информацию принято делить на укрупненные категории:

- сигнальная (предупреждающая);
- тактическая (требующая немедленных действий);
- стратегическая (собирается длительное время и подвергается анализу);
- доказательная (информация в виде документов, предметов, предоставляемых в правоохранительные органы).

Конечным результатом разведывательной деятельности является:

- информирование руководства;
- долгосрочное планирование и анализ;
- сбор вещественных доказательств для правосудия.

9 ОРГАНИЗАЦИЯ ПРОПУСКНОГО И ВНУТРИОБЪЕКТОВОГО РЕЖИМА НА ПРЕДПРИЯТИИ

Организация пропускного и внутриобъктового режима является важнейшей составной частью организационной защиты информации, определяется Правилами внутреннего распорядка и соответствующими инструкциями.

Задачами пропускного и внутриобъектового режима являются:

- организация входа и выхода сотрудников, посетителей, транспорта,
- контроль за перемещением через границу предприятия материальных и финансовых ценностей;
- поддержание соответствующего режима и состояния территории внутри предприятия.

Организация охраны. Общие положения

Организация охраны – составная часть общей системы защиты конфиденциальной информации предприятия. Вопросы обеспечения надежной охраны территории предприятия и его объектов неразрывно связаны с задачами организации пропускного режима на предприятии.

Силы и средства, участвующие в решении этих задач, являются составными элементами системы охраны предприятия. От эффективности функционирования системы охраны в полной мере зависят возможность и уровень решения задач пропускного и внутриобъектового режимов. Системы пропускного и внутриобъектового режимов образуют следующие после системы охраны рубежи безопасности, предотвращающие доступ злоумышленника к охраняемой предприятием информации.

Объекты охраны:

- территория предприятия;
- расположенные на территории предприятия объекты (здания, сооружения);
- носители конфиденциальной информации (документы, изделия);
- материальные ценности (грузы).
- руководство предприятия персонал, допущенный к конфиденциальной информации.

Организация охраны руководства и персонала предприятия регулируются отдельным положением (инструкцией), которое утверждается руководи-

телем предприятия, и, в необходимых случаях согласовывается с территориальными органами внутренних дел и органами безопасности. Основные цели охраны руководства предприятия — обеспечение их личной безопасности в повседневных условиях и при возникновении чрезвычайных ситуаций, предотвращение возможных попыток завладения злоумышленниками защищаемой информацией путем физического и иного насильственного воздействия на этих лиц, выработка рекомендаций охраняемым лицам по особенностям поведения в различных ситуациях

Главные цели охраны предприятия:

- предотвращение попыток проникновения посторонних лиц (злоумышленников) на территорию (объекты) предприятия;
- своевременное обнаружение и задержание лиц, противоправно проникших (пытающихся проникнуть) на охраняемую территорию;
- обеспечение сохранности находящихся на охраняемой территории носителей конфиденциальной информации и материальных средств и исключение, таким образом, нанесения ущерба предприятию;
- предупреждение происшествий на охраняемом объекте и ликвидация их последствий.

Основные задачи охраны:

- контроль объекта и охраняемой территории, в том числе территории с особым режимом пропуска, в целях обнаружения и предотвращения попыток несанкционированного проникновения на них посторонних лиц (злоумышленников);
- обеспечение конфиденциальности и сохранения в тайне фактов проведения закрытых мероприятий на предприятии (его объектах), обсуждаемых или рассматриваемых на них вопросов;
- сопровождение и охрана носителей конфиденциальной информации, в том числе служебных документов предприятия, материальных ценностей и грузов при их транспортировке и перевозке (доставке);
- защита объектов и территорий с особым режимом пропуска т насильственных действий и вооруженных нападений, которые могут нанести ущерб предприятию;
- выполнение в необходимых случаях специальных задач по обеспечению личной охраны руководства предприятия и персонала предприятия, допущенного к конфиденциальной информации;

– участие в обеспечении пропускного режима для посетителей, транспортных средств и грузов на охраняемой территории (объектах предприятия) в целях установления личности и учета посетителей, контроля за ввозом, вывозом носителей конфиденциальной информации, грузов, материальных ценностей, предотвращения их несанкционированного перемещения, а также фиксации следов скрытых и открытых попыток хищения иного имущества предприятия;
– систематический анализ эффективности системы охраны, принимаемых должностными лицами мер по охране объектов предприятия и обеспечению сохранности носителей конфиденциальной информации, материальных ценностей и грузов, и выработка предложений по совершенствованию системы охраны.

Система охраны предприятия – совокупность используемых для охраны предприятия сил и средств, а также способов и методов охраны предприятия и его объектов. Она включает:

– личный состав подразделений охраны (караулов);
– технические средства охраны;
– места размещения личного состава, выполняющего задачи охраны, и используемых технических средств;
– методы охраны объектов.

Одним из основных элементов системы организации пропускного режима является **контрольно-пропускной пункт.**

Используемые при охране предприятий **технические средства** охраны делятся на две группы:

– средства обнаружения (пожарная и охранная сигнализация, «тревожное» оповещение, охранное телевидение, охранное освещение, аппаратура проверки почтовой корреспонденции, радиосвязь, прямая внутренняя связь, прямая телефонная связь с милицией и др.);
– средства обнаружения и ликвидации (средства пожаротушения, средства индивидуальной защиты, газовые ловушки, автотранспорт, оружие, инженерно-технические средства и др.).

Для охраны предприятий и их объектов создаются штатные подразделения охраны, которые организационно могут быть объединены в службу охраны. Служба охраны включает посты охраны, группы (подразделения) сотрудников охраны (в том числе подразделение личной охраны руководства и персонала), группу охраны и сопровождения материальных ценностей и грузов, «тревожную» группу (группу быстрого реагирования), а также подразделения сторожевых собак (при необходимости).

Часто подразделения охраны наряду с другими подразделениями, решающими задачи по различным направлениям защиты информации, объединяются в службу безопасности предприятия.

В своей деятельности по выполнению задач охраны предприятия сотрудники подразделения охраны руководствуются должностными обязанностями (инструкциями), которые разрабатываются совместно со службой безопасности предприятия, а в некоторых случаях – во взаимодействии с другими заинтересованными должностными лицами, и утверждаются руководителем предприятия (его заместителем).

Основными обязанностями сотрудников подразделений охраны являются:

- обеспечение защиты охраняемых объектов от противоправных посягательств (действий злоумышленников и нарушителей);
- осуществление мероприятий по предупреждению нарушений пропускного и внутриобъектового режимов, установленных на предприятии;
- пресечение преступлений и административных правонарушений на охраняемых объектах предприятия;
- поиск и задержание лиц, незаконно проникших на охраняемые объекты;
- участие в установленном порядке в осуществлении контроля соблюдением противопожарного режима, тушении пожаров, а также в ликвидации последствий аварий, катастроф, стихийных действий и других чрезвычайных ситуаций на охраняемых объектах;
- участие в пределах компетенции в проведении мероприятий по обеспечению защиты информации и сохранности носителей конфиденциальной информации;
- оказание в пределах компетенции содействия правоохранительным органам в решении возложенных на них задач.

Сотрудники подразделений охраны имеют право при выполнении возложенных задач в пределах охраняемых объектов:

- требовать от работников, должностных лиц охраняемых объектов и других граждан соблюдения пропускного и внутриобъектового режимов;
- проверять на охраняемых объектах у лиц документы, удостоверяющие их личность, а также документы, дающие право на вход, въезд транспортных средств, внос (ввоз) имущества на охраняемые объекты, а также на выход этих лиц, выезд транспортных средств, вынос (вывоз) имущества с охраняемых объектов;
- производить досмотр транспортных средств при их въезде на охраняемые объекты и выезде с охраняемых объектов;

- проверять условия хранения материальных ценностей (имущества) и носителей конфиденциальной информации на охраняемых объектах, состояние инженерно-технических средств охраны (охранное видеонаблюдение, пожарная сигнализация, охранная сигнализация), при выявлении нарушений, способствующих хищениям материальных ценностей (имущества) или носителей конфиденциальной информации, а также условий, которые могут привести к возникновению пожаров на охраняемых объектах и создают угрозы безопасности людей, принимать меры по пресечению указанных нарушений и ликвидации указанных условий;
- производить административное задержание и доставлять в служебное помещение охраны или орган внутренних дел лиц, совершивших преступления или административные правонарушения на охраняемых объектах, производить личный досмотр, досмотр вещей, изъятие вещей и документов, являющихся орудием или непосредственным объектом правонарушения, обеспечивать охрану места происшествия и сохранность указанных вещей и документов;
- беспрепятственно входить в помещения охраняемых объектов и осматривать их при преследовании лиц, незаконно проникших на охраняемые объекты, а также для задержания лиц, подозреваемых в совершении преступлений или административных правонарушений;
- использовать транспортные средства собственников охраняемых объектов для преследования лиц, совершивших преступления или административные правонарушения на охраняемых объектах, и доставления их в орган внутренних дел;
- при необходимости в порядке, установленном законодательством Российской Федерации, применять физическую силу, специальные средства и огнестрельное оружие.

Права и обязанности сотрудников подразделения личной охраны руководства и персонала предприятия отражаются в утверждаемом руководителем предприятия положении (инструкции), которое определяет организацию и порядок охраны указанных лиц. На предприятиях, входящих в структуру федеральных органов исполнительной власти, для защиты охраняемых объектов, являющихся государственной собственностью и находящихся в сфере ведения данных органов, в соответствии с Федеральным законом «О ведомственной охране» создаются и функционируют подразделения ведомственной охраны.

Охрана предприятия может обеспечиваться не только путем создания перечисленных подразделений охраны, но и путем использования услуг частных охранных предприятий, имеющих право в соответствии с законодатель-

ством осуществлять этот вид деятельности. Порядок оказания услуг такими предприятиями, права и обязанности их сотрудников при выполнении задач охраны объектов определены Законом РФ «О частной детективной и охранной деятельности в Российской Федерации».

Для организации охраны предприятия могут быть также использованы силы и средства подразделений вневедомственной охраны при органах внутренних дел. В этом случае применяются следующие основные способы охраны объектов предприятия:

- использование технических средств охраны (сигнализации), оконечные устройства которых выведены на пульты централизованного наблюдения в подразделения вневедомственной охраны;
- несение дежурства сотрудниками подразделений вневедомственной охраны непосредственно на объекте охраны. Функции, возлагаемые на подразделения вневедомственной охраны, и порядок их деятельности определяются Положением о вневедомственной охране при органах внутренних дел Российской Федерации.

Создание надежной системы охраны предприятия определяется принятием правильного решения на основе анализа потенциальных угроз безопасности охраняемого объекта и реальной оценки возможностей для создания эффективной системы охраны с учетом имеющегося выбора сил и средств. Организация системы охраны предприятия и его объектов устанавливается решением руководителя предприятия. Подготовку такого решения осуществляют структурные подразделения, отвечающие за защиту конфиденциальной информации и безопасность предприятия.

При организации системы охраны определяют:

- способы охраны территории предприятия и его объектов;
- количество постов, мест несения дежурства по охране объектов, участки (зоны, территории) охраны;
- количество и виды контрольно-пропускных пунктов, порядок и особенности несения дежурства на этих пунктах сотрудниками охраны;
- порядок и особенности действий личного состава охраны во всех случаях (в том числе в экстренных ситуациях);
- порядок и особенности применения (использования) технических средств обнаружения и охраны на каждом участке (зоне, территории) охраны.

В целях определения задач, основных направлений охраны, используемых для осуществления охраны сил, средств, способов и методов на предприятии разрабатывается инструкция по организации охраны предприятия, его территории и объектов.

Одной из важных задач, решаемых подразделениями охраны, является сопровождение и охрана носителей конфиденциальной информации, материальных ценностей и грузов при их транспортировке и перевозке (доставке) на другие предприятия (объекты). В этом случае сотрудники подразделений охраны обеспечивают защиту лиц, доставляющих (перевозящих) носители конфиденциальной информации, иные материальные ценности и грузы в пункт назначения (на другие предприятия), и охрану перечисленного имущества в порядке, определенном специально разрабатываемой на предприятии инструкцией (положением), либо отдельным разделом ранее упоминавшейся инструкции по организации охраны предприятия, его территории и объектов.

Для выполнения задач перевозки (доставки) носителей конфиденциальной информации, материальных ценностей и грузов приказом руководителя предприятия назначаются наиболее подготовленные сотрудники предприятия, способные в любых условиях обеспечить сохранность перевозимого имущества. Сотрудники подразделения охраны при этом обеспечивают охрану и защиту от хищения, кражи или иных преднамеренных действий посторонних лиц, направленных на овладение носителями конфиденциальной информации, материальными ценностями и грузами. Подготовка сотрудников охраны к выполнению указанных задач осуществляется с учетом выбора маршрута движения, способа доставки (автомобильным, железнодорожным или авиационным транспортом) и времени прибытия в пункт назначения.

При охране имущества и защите перевозящих (доставляющих) его лиц сотрудники охраны обязаны путем применения всех имеющихся средств и способов охраны обеспечить защиту указанных лиц, исключить хищение имущества или завладение им посторонними лицами (злоумышленниками).

Руководство организацией охраны предприятия

Возлагается на заместителя руководителя предприятия по безопасности, или начальника службы безопасности (рис. 10). В текущей работе по поддержанию внутриобъектового режима ему подчиняются руководители подразделений– в части полномочий по обеспечению безопасности. Для обеспечения охраны предприятия выделяется специальная группа во главе начальника охраны. Во внерабочее время принятие оперативных мер по организации деятельности предприятия и обеспечению его безопасности возлагается на ответственного дежурного. Ответственным дежурным может быть назначен специально выделенный сотрудник, либо по графику дежурство возлагается на заместителей руководителя предприятия или руководителей крупных структурных подразделений.

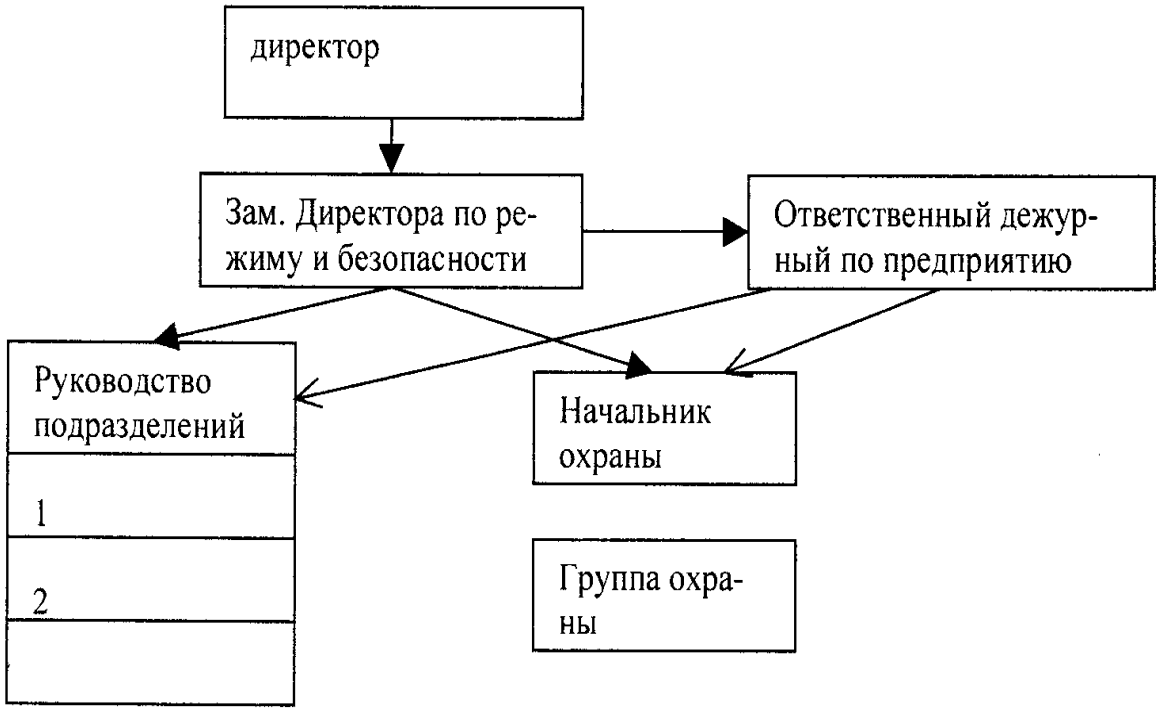


Рисунок 10 - Организация пропускного и внутриобъектового режима на предприятии

Организация пропускного режима

Пропускной режим устанавливается на предприятиях в целях недопущения бесконтрольного прохода на территорию, а также бесконтрольного вноса, выноса материальных ценностей, ввоза и вывоза материальных ценностей, технической и другой служебной документации.

Пропускной режим распространяется как на сотрудников предприятия, так и на посетителей и на автотранспорт.

Пропускной режим может устанавливаться как для прохода на территорию предприятия в целом, так и в отдельные зоны безопасности; под наблюдением непосредственно сотрудников охраны, либо через автоматизированные посты, оборудованные соответствующими техническими средствами.

Пропуск - документ, удостоверяющий право прохода на территорию и нахождение на этой территории.

В отсутствие сотрудника на территории предприятия все пропуска могут храниться на специально оборудованном контрольно-пропускном пункте (КПП) в специальных ячейках. В ряде случаев допускается нахождение пропуска на руках сотрудника.

На пропуске могут устанавливаться специальные шифры, которые определяют график работы, право свободного прохода, входа и выхода, право прохода на режимные территории на предприятии (зоны ограниченного доступа), содержат иную служебную информацию.

Необходимо следить, чтобы проход осуществлялся строго по документам, и исключить допуск на предприятие по устным заявлениям.

На период длительного отсутствия сотрудника пропуск должен сдаваться в службу безопасности.

Существуют 3 вида пропусков:

- постоянный;
- временный;
- разовый.

Постоянные пропуска оформляются на сотрудников, постоянно работающих на предприятии, и только после выхода соответствующего приказа.

При выдаче пропуска сотрудник обязательно знакомится под расписку с правилами внутреннего распорядка.

При утере пропуска проводится служебное расследование. На период проведения служебного расследования сотруднику может быть выдан временный, а по его результатам принято решение о списании старого пропуска и выдачи нового.

Временные пропуска выдаются при выполнении определенного вида работ (производственная необходимость) либо на период замещения временно отсутствующего сотрудника (длительная командировка, болезнь).

Временные пропуска выдаются по заявкам руководителей структурных подразделений с обязательной визой заместителя директора по режиму (начальника Службы безопасности). Максимальный срок действия временного пропуска устанавливается 6 месяцев с возможностью дальнейшего продления еще на 6 месяцев, после чего временный пропуск оформляется заново.

Краткосрочные пропуска могут не иметь фотографии. В этом случае проход на территорию осуществляется при одновременном предъявлении паспорта.

Разовые пропуска оформляются на каждое лицо в отдельности только на данный день и время. Для получения разового пропуска необходимо иметь:

- предписание на выполнение конкретного вида работ;
- справку о допуске;
- паспорт или другое удостоверение личности.

Разрешение на проход по разовым пропускам выдается по заявке руководителя структурного подразделения, подписанной заместителем руководителя предприятия.

Проход на территорию предприятия по разовому пропуску разрешается, как правило, только в сопровождении сотрудника подразделения, куда прибыл посетитель.

На контрольно-пропускном пункте делается отметка о времени прохода. По окончании работы руководитель подразделения делает отметку о времени выхода, в предписании указывается характер предоставленных сведений и степень их секретности. Справка о допуске регистрируется в службе безопасности.

Для участия в массовых мероприятиях (общих собраниях, конференциях и т. д.) допускается проход на территорию по спискам с предъявлением паспорта. При этом должен быть назначен ответственный за проведение мероприятия. Руководством предприятия принимаются меры по ограничению доступа участников на неоговоренные планом мероприятия территории.

Въезд и выезд автотранспорта на территорию предприятия осуществляется по пропускам на машину с конкретным номером.

Сотрудники, сопровождающие машину (например, грузчики, экспедиторы), должны проходить на территорию в установленном порядке, т.е. по пропускам.

Охрана обязана осуществлять досмотр ввозимого и вывозимого груза. На весь груз должно быть оформлено разрешение в виде материальных накладных.

Сотрудники МЧС, скорой помощи проезжают на собственной машине в сопровождении сотрудников службы безопасности.

Внос и вынос материальных ценностей и документов производится при наличии товарно-транспортной накладной или **материального пропуска.**

Материальный пропуск подписывается:

- руководителем или заместителем руководителя предприятия;
- начальником финансово-бухгалтерского отдела или его заместителем (главным бухгалтером).

Оформление на вынос или вывоз **специальных изделий** осуществляется в том же порядке, но с обязательной визой начальника Службы безопасности.

Допускается ввоз и вывоз материальных ценностей на опломбированных машинах. В этом случае сотрудники службы безопасности проверяют только наличие пломб и разрешение на выезд.

Мусор, снег, старый лом, отходы производства вывозятся по специальным накладным, а погрузка осуществляется в присутствии специально назначенных лиц.

Внос или вынос несекретной документации (литературы) осуществляется после просмотра в Службе безопасности. Внос и вынос секретных доку-

ментов производится в установленном порядке с разрешения заместителя руководителя предприятия (начальника службы безопасности).

Проход на территорию предприятий разрешается, как правило, с личными вещами небольшого размера.

Работникам охраны разрешается в ряде случаев досмотр личных вещей (последнее должно быть особо оговорено Правилами внутреннего распорядка). При обнаружении подозрительных вещей должен составляется протокол и проводиться служебное расследование.

В связи с тем, что на большинстве режимных предприятий ограничен пронос личный вещей, то при входе, на нережимной территории, оборудуются специальные камеры хранения.

Для ведения переговоров с сотрудниками других предприятий рекомендуется оборудовать специальные изолированные комнаты переговоров, расположенные на нережимной территории предприятия.

Организация внутриобъектового режима

Обязательной составляющей частью организации внутриобъектового режима является учет посещений предприятия, отдельных подразделений, зон безопасности, а также учет нахождения сотрудников в подразделениях.

Такой учет можно осуществить разнообразными методами:

- применение автоматизированных постов прохода;
- выдача и сдача служебных пропусков, хранящихся в бюро пропусков;
- выдача и сдача под расписку ключей от служебных помещений;
- введение при проходе соответствующих личных кодов;
- ведение табелей учета рабочего времени (строго говоря, табель является бухгалтерским документом для начисления заработной платы);
- ведение журналов прихода и ухода с работы на контрольно-пропускном пункте или в подразделении и т.п.

Сотрудники и посетители должны находиться на территории предприятия в строго определенное время. Для нахождения в нерабочее время требуется разрешение руководителя или заместителя руководителя предприятия. Особо оговаривается нахождение сотрудников в выходные и праздничные дни. Такое нахождение допускается в исключительных случаях по производственной необходимости и строго индивидуально по предварительному согласованию.

Отдельно Правилами должен быть оговорен пронос на территорию предприятия (без соответствующего разрешения) личной кино- и фотосъемочной аппаратуры, звуко- и видеозаписывающей аппаратуры, множитель-

ной, копировальной техники, персональных ЭВМ и блоков к ним, мобильных телефонов.

Режимные, складские помещения, хранилища ценностей и носителей информации, архивы должны обладать надежными стенами и перекрытиями, иметь прочные двери и обладать охранной сигнализацией. Окна нижних этажей помещений, выходящих на неохраняемую территорию, а также окна режимных и складских помещений, выходящих на охраняемую территорию, должны иметь соответствующие решетки.

По окончании работы в помещениях, заблокированных сигнализацией, двери запираются и опечатываются. Ключи под расписку сдаются в охрану.

Включение сигнализации производится начальником охраны или его заместителем в присутствии сотрудника, сдающего помещение. О времени включения сигнализации делается отметка в соответствующем журнале.

Получение ключей, вскрытие заблокированных помещений осуществляется лицами, работающими на данном предприятии, при предъявлении соответствующего пропуска и только в том случае, если эти лица включены в соответствующий список. Место хранения и порядок выдачи дубликатов ключей заранее оговариваются.

Уборка режимных помещений должна производиться в присутствии сотрудника, работающего в данном помещении. Во время уборки помещения все служебные документы должны быть убраны с рабочих мест.

Помещения, в которых ведутся секретные работы, должны быть постоянно закрыты на замок. В таких помещениях должны находиться только лица, которые имеют отношение к работе в данном помещении. Список лиц, допущенных к работе в режимном помещении, составляется руководителем подразделения, согласовывается со Службой безопасности и утверждается руководителем предприятия или его заместителем.

Режимные помещения аттестуются. Вид аттестации определяется степенью конфиденциальности информации, представленной в данном помещении. На случай пожара или других стихийных бедствий должны быть разработаны специальные инструкции, в которых определяется порядок вывода сотрудников, вскрытие помещений, спасение документов и изделий.

10 НАПРАВЛЕНИЯ И МЕТОДЫ РАБОТЫ С ПЕРСОНАЛОМ

По данным социологических исследований, проведенных за рубежом, 65% утечки конфиденциальной информации происходит через сотрудников и только 35% - через технические средства.

Только 25% сотрудников являются абсолютно честными, 25% готовы продать конфиденциальную информацию всегда, 50% готовы ее продать при определенных обстоятельствах.

Работа с персоналом ведется по двум основным направлениям:

- проверка персонала при приеме на работу;
- работа с постоянными сотрудниками.

Проверка персонала при приеме на работу

В приеме на работу новых сотрудников участвуют несколько подразделений. От их взаимодействия во многом зависит грамотная работа по приему на работу нового персонала, обладающего как необходимыми деловыми качествами, так и способного обеспечить сохранность доверенной информации. Как уже отмечалось, при приеме на работу, связанную с государственной тайной, заключение контракта до окончания проверочных мероприятий не допускается. Подготовка документов на оформление допуска к государственной тайне возложена на отдел кадров (управление кадров). Отдел кадров также отвечает за правильность оформления документов при приеме сотрудника на работу, обеспечивает проверку соответствия сотрудника квалификационным требованиям, предусмотренным должностными инструкциями, проверяет наличие соответствующих документов.

Начальник подразделения, в котором принимаемый сотрудник будет работать, проверяет профессиональные качества кандидата и его личные качества (подходит ли он по своим личным качествам для работы в коллективе).

Специальная проверка, если это не связано с допуском к государственной тайне, может быть возложена на службу безопасности предприятия. При этом проверяются кандидаты, способные нанести реальный ущерб.

Виды угроз от потенциального кандидата:

- кража материальных ценностей;
- разглашение конфиденциальной информации;
- сбор конфиденциальной информации в пользу одной из конкурирующих фирм, криминальных структур и т. д.;

– скрытое обучение сотрудника тому или иному виду деятельности;
– скрытые психические расстройства кандидата, либо плохое состояние его здоровья.

Направления проверки:

– проверка достоверности сообщенной кандидатом информации;
– проверка подлинности предоставленных кандидатом документов (паспорт, диплом, трудовая книжка);
– проверка достоверности всех записей в документе.

Глубина проверки определяется реальным ущербом, который может нанести кандидат в случае его приема на работу.

Существуют **три уровня проверки**:

– поверхностный;
– средний;
– глубокий.

Поверхностный уровень проверки предполагает проверку информации, предоставленной самим кандидатом, и визуальную проверку правильности оформления документов. К достоинствам данного вида проверки можно отнести оперативность получения информации и то, что в ходе проверки кандидат получает минимальные сведения о предприятии.

Вместе с тем не представляется возможным выявить негативные факты биографии, представляет сложность выявления поддельных сведений в документах, имеющих достоверные и нефальсифицированные сведения.

Средний уровень проверки предполагает проверку сведений, сообщенных кандидатом. На этом уровне сведения проверяются с привлечением независимых источников. Эта проверка осуществляется по двум направлениям: проверка подлинности документов, получение подробной информации о человеке, на чье имя документы официально выданы.

Глубинный уровень проверки предусматривает изучение окружающей кандидата обстановки с целью выявления его истинного облика, а не того образа, который он пытается продемонстрировать. Существует два типа людей: завышающие и занижающие свои успехи.

Приемы проверки

Собеседование

Обычно первым с кандидатом беседует представитель кадровой службы организации; его задачей является проверка соответствия кандидата формальному набору признаков (стаж работы, уровень образования, возраст и т. д.). При соответствии кандидата формальному набору требований он направляется на собеседование в подразделение, где предполагается его работа. При

необходимости собеседование может проводиться собеседование с представителем службы безопасности.

Успех собеседования во многом определяется подготовкой должностных лиц. При собеседовании существуют различные способы выявления недостоверной информации: наблюдение за невербальными сигналами тела (жесты, мимика, взгляд), за интонацией, голосом; просьба более детального повторения отдельных эпизодов, повторения сообщенной ранее сказанной информации.

Информацию о человеке можно получить из анализа стиля его одежды, поведения, манеры говорить.

Проверка предоставленных кандидатом документов.

Наиболее распространенными видами подделки являются переклейка фотографии, покупка чистых бланков, покупка бланков, имеющих подлинные подписи, печати и прочие атрибуты.

Проверка рекомендаций и резюме.

Последние проверяются особенно тщательно, так как часто являются существенными аргументами при приеме на работу. По данным зарубежных исследований около 20% рекомендаций оказываются фальшивыми.

В резюме же, обычно, представлена только выгодная для кандидата информация.

Тестирование.

При всей кажущейся привлекательности и простоте тестирования достоверность сведений по нему не превышает 50% . Успех тестирования во многом определятся качеством составленного теста. Вопросы, предлагаемые для тестирования, не должны наводить тестируемого на какой либо запрограммированный ответ, предоставлять возможности альтернативных ответов, в том числе – нейтральных (к примеру: «затрудняюсь ответить»).

Проверка сообщенной кандидатом информации.

В идеальном варианте вся информация, сообщенная кандидатом, должна быть подтверждена независимым источником: документами, фактами биографии и пр. Проверяется информация с предыдущего места работы кандидата: истинные причины увольнения, реально выполнявшиеся трудовые обязанности, взаимодействие с коллегами по работе и т.п. Важной информацией могут стать сведения о политических пристрастиях (к примеру, приверженность экстремистским группировкам), вероисповедании (к примеру, сектантство).

При проверке сведений о кандидате служба безопасности должна строго руководствоваться законодательством. Так же, как и в случае допуска к государственной тайне, необходимо составить письменное соглашение о про-

верке личных сведений о кандидате. Все сведения, полученные при проверке, должны носить конфиденциальный характер и не подлежать разглашению.

Методы работы с постоянными сотрудниками

Следует учитывать, за время работы на предприятии могут измениться материальное положение сотрудника, отношения его с руководством, сослуживцами. Появляются факторы, которые могут изменить отношение сотрудника предприятия к вопросам сохранения конфиденциальной информации. К ним относятся:

- изменение психологии сотрудников в процессе работы;
- возможное увольнение;
- наличие у сотрудника преступных намерений или агентурных заданий;
- воздействие на сотрудника со стороны преступных группировок,
- отрицательное влияние других сотрудников;
- увольнение или уход из коллектива лиц, обладающих конфиденциальной информацией;
- плохая организация внутриобъектового режима и конфиденциального делопроизводства;
- плохие взаимоотношения сотрудников;
- заинтересованность в разглашении;
- плохое материальное положение; материальное положение сотрудника может измениться даже в случае изменения соотношения оплаты труда различных работников;
- отсутствие постоянной работы с сотрудниками по вопросам сохранения конфиденциальности информации; отсутствие необходимого контроля.

Весь комплекс мероприятий по предотвращению разглашения и утечки информации через постоянных сотрудников можно разделить на следующие категории:

1. Проверка. Сюда следует отнести тестирование, сбор информации, анкетирование, проверочные мероприятия, оперативные и оперативно-технические мероприятия, проверку профессиональной пригодности, проверку на полиграфе, наблюдение, прослушивание внутри предприятия, внедрение информатора, внутренний аудит и др.
2. Улучшение организации пропускного и внутриобъектового режима.
3. Защита от утечки информации по техническим каналам, разработка соответствующих нормативов работы с техническими средствами.
4. Улучшение организации и ведения конфиденциального делопроизводства, разработка соответствующих инструкций.
5. Более качественный подбор и изучение кандидатов при приеме на работу.

11 ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ КОНФИДЕНЦИАЛЬНЫХ СОВЕЩАНИЙ

В процессе хозяйственной, финансовой, научной, организационной деятельности возникает необходимость проведения совещаний по закрытой тематике. Примеры совещаний:

- рабочее совещание, проводимое руководителем предприятия или руководителем структурного подразделения;
- научно-технические советы по закрытой тематике;
- конференции и симпозиумы по закрытой тематике;
- защиты диссертаций, дипломных проектов;
- лекции по закрытой тематике.

Совещания могут проводиться как среди сотрудников данного предприятия (внутренние совещания), так и с привлечением сотрудников других предприятий или даже сотрудников предприятий других стран (международные совещания).

При проведении совещаний с участием представителей сторонних организаций вниманию участников совещания предоставляются в полном объеме материалы информации, составляющие информационную базу, на основании которой принимаются конкретные решения. В зависимости от вида совещаний на них могут быть представлены сведения, которые могут составлять коммерческую тайну какой-либо из участвующих организаций.

Источниками информации при проведении совещания являются выступающие люди, документы, задокументированные материалы совещания, презентации, модели.

Основная часть информации на совещании передается посредством речи как сотрудников организации, проводящей совещание, так и сторонних организаций. Под речевой информацией понимается то, что произносится участниками совещаний (доклады, выступления, обсуждения, замечания, ремарки). Речевая информация несет в себе основную информационную нагрузку.

Защита информации при проведении совещаний имеет ряд особенностей, вызванных следующими факторами:

- большим ущербом от утечки сведений по комплексным работам, особенно при участии различных организаций;
- присутствием на совещании представителей сторонних организаций с различным отношением к требованиям по обеспечению безопасности информации;

- стремлением части сотрудников к регистрации информации, в том числе записи на диктофон, с целью последующей обработки хода и результатов совещания, в том числе для предоставления их своему руководству;
- стремлением некоторых сотрудников связаться со своим руководством во время совещания для принятия оперативных решений,
- возможным выполнением участниками совещания агентурных заданий;
- высоким уровнем концентрации и обобщения закрытых сведений в докладах выступающих, отображаемых в презентациях, на плакатах и в раздаточных материалах, находящихся у участников;
- большой продолжительностью совещаний по комплексным работам,
- сам факт совещания и состав его участников являются информативным признаком хода совещания и его повестки дня.

Эти обстоятельства усложняют задачи и ужесточают требования по защите информации, прежде всего требования по защите помещения перед проведением совещания, предотвращению утечки информации в ходе совещания по различным каналам.

При проведении подобных мероприятий следует руководствоваться следующими рекомендациями.

Решение о проведении закрытого совещания принимается руководителем предприятия или по согласованию с ним. Список участников совещания утверждается руководителем и согласовывается с подразделением, отвечающим за соблюдение конфиденциальности.

К совещанию допускаются (привлекаются) только лица, имеющие допуск, соответствующий степени конфиденциальности обсуждаемых вопросов. Представители других предприятий обязаны представить справку о режиме допуска установленной формы.

Совещания должны проводиться в специально оборудованном помещении. Помещение аттестуется для данного вида деятельности. Вид аттестации зависит от формы проведения совещания

В ряде случаев при необходимости во время проведения совещания около входа в помещение может быть выставлена охрана.

Допускается ведение рабочих записей только на учтенной бумаге или блокнотах. По окончании совещания все записи сдаются на хранение в службу безопасности, если заранее не было оговорено иное.

Регистрация с использованием технических средств должна быть оговорена заранее; при этом съемные носители информации должны регистрироваться. Целесообразно исключить возможность использования во время совещания мобильных средств связи, с этой целью следует предусмотреть наличие соответствующего хранилища на период совещания. Для исключения

проноса на совещание нерегламентированных технических средств возможна установка при входе соответствующих детекторов, а участники совещания предупреждаются о запрете на использование технических средств регистрации.

Очередность рассмотрения вопросов ставится такой, чтобы при рассмотрении очередного закрытого вопроса сотрудники, не имеющие на него допуск, могли покинуть помещение.

За соблюдением режима конфиденциальности при проведении совещания отвечает специально назначенный сотрудник. Это может быть специально назначенный сотрудник службы безопасности, или эта работа поручается кому либо из участников совещания.

12 ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРЕДСТАВЛЕНИИ ЕЕ В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

Одним из направлений утечки конфиденциальной информации может служить ее публикация в средствах массовой информации (СМИ). Это могут быть статьи, реклама, интервью и т. д. Сбором и систематизацией подобной информации занимаются в первую очередь разведывательные центры иностранных государств, а в последнее время – и группы анализа и разведки конкурирующих фирм и организаций. Существуют определенные аналитические центры, группы, собирающие опубликованные сведения, и анализирующие их с целью получения прибыли в конкурентной борьбе.

Электронные средства массовой информации, печать традиционно являются самыми емкими и наиболее используемыми каналами получения информации. При грамотно организованном поиске в средствах массовой информации можно получить информацию по очень широкому кругу вопросов, интересующих разведывательные подразделения конкурирующих фирм.

Качественная работа профессиональных журналистов по духу во многом близка к работе спецслужб. Журналиста, который постоянно пишет о каких-то однотипных проблемах, вполне можно рассматривать как эксперта в той или иной области. Кроме того, СМИ дают представление о ситуации не просто на цифрах, а на понятном языке. При постоянно мониторинге СМИ многое можно почерпнуть даже из факта исчезновения публикаций по определенной тематике.

Во многом анализу СМИ помогает приблизительное знание принадлежности средств массовой информации к конкретным финансово-промышленным группировкам. Не следует преувеличивать «независимость» журналистов: СМИ подстраиваются под своего владельца. Материал, подготовленный журналистом, подвергается редакторской правке и может сильно отличаться от первоначального варианта.

Материалы СМИ позволяют сопоставлять, уточнять и снабжать новыми подробностями данные, полученные оперативным путем, а также давать новые направления для текущей информационно-поисковой работы.

Деятельность средств массовой информации регламентируется соответствующим **Федеральным законом о СМИ**. К сожалению, вопросы защиты государственной и иной защищаемой законом тайны прописаны в законе декларативно.

В соответствии этим законом не допускается использование средств массовой информации для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну.

Журналисту может быть отказано в предоставлении запрашиваемой информации если она содержит сведения, составляющие государственную, коммерческую или иную специально охраняемую законом тайну.

Уведомление об отказе вручается представителю редакции в трехдневный срок со дня получения письменного запроса информации. В уведомлении должны быть указаны:

- причины, по которым запрашиваемая информация не может быть отделена от сведений, составляющих специально охраняемую законом тайну;
- должностное лицо, отказывающее в предоставлении информации;
- дата принятия решения об отказе.

Законом определено, что редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные ей с условием сохранения их в тайне, а также сохранять конфиденциальность информации или ее источника.

Сбор и обработка информации, представленной в материалах СМИ целесообразно проводить по заранее определенному перечню изданий. Большое значение играет постоянство и регулярность мониторинга СМИ, грамотно организованная классификация поступающей информации и ее хранение.

При наличии финансовых возможностей сбор информации можно производить силами службы безопасности предприятия. Эту же работу можно качественно выполнить и с привлечением сторонних фирм, специализирующихся на сборе информации.

Сбор информации силами предприятия

Все материалы СМИ, поступающие на предприятие, могут обрабатываться ответственным за это лицом и, согласно разработанному классификатору, соответствующим образом сортироваться и храниться, в том числе и информация, поступающая в электронном виде.

При невозможности выделения отдельной штатной единицы для работы с прессой, эта работа может быть распределена между сотрудниками службы безопасности. При этом за каждым из них закрепляется по два-три периодических издания. В процессе сбора и обмена мнениями выделяются ключевые вопросы для наблюдения. Особое внимание уделяется публикациям, которые

могут затрагивать экономические интересы предприятия. Наиболее интересные материалы могут переводиться в электронную форму и заноситься в базу данных. Некоторые информационные материалы можно бесплатно скачать из интернета.

Сбор информации с привлечением сторонних фирм

В ряде случаев информация может приобретаться на стороне. Эту работу целесообразно поручить специально подготовленным сотрудникам, так как сам факт сбора информации является «демаскирующим» признаком.

Часто функции первичной обработки материалов СМИ дешевле передать сторонним лицам, нежели проводить ее силами собственных сотрудников.

За относительно невысокую плату можно приобрести информацию в редакциях изданий. Сегодня при газетах, службах новостей очень часто имеются подразделения, где можно получить досье на фирмы или людей по совокупности событий, публикации о них. Многие газеты, журналы имеют свои сайты в сети Интернет, где наряду с представлением материалов в электронном виде можно организовать грамотный поиск нужной информации.

В первичной обработке прессы значительную помощь могут оказать работники библиотек, которые дешево и достаточно профессионально выполнят мониторинг требуемых изданий, в том числе и иностранных.

Важное значение имеет при сборе информации соблюдение режима конспирации для того, чтобы исполнители не имели представления, для кого и с какой целью они это делают. Здесь, к примеру, возможно использование «надомников».

Методология обработки материалов СМИ выделяет следующие **категории данных**:

- базовая информация (для дальнейшей аналитической обработки);
- текущая информация о фактах;
- субъективно-оценочные категории, содержащие оценки и предупреждения.

Средства массовой информации регистрируются в соответствующих государственных органах. В зависимости от территории распространения СМИ регистрируются Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), либо ее территориальными органами в соответствии с Административным регламентом предоставления Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной услу-

ги по регистрации средств массовой информации (приказ Министерства связи и массовых коммуникаций РФ от 29 декабря 2011 г. № 362).

Учредителем (соучредителем) СМИ могут быть гражданин, объединение граждан, организация, государственный орган, орган местного самоуправления.

В соответствии с Законом Российской Федерации от 27 декабря 1991 г. № 2124-I «О средствах массовой информации» (Закон о СМИ) не требуется регистрация:

- средств массовой информации, учреждаемых органами государственной власти и органами местного самоуправления исключительно для издания их официальных сообщений и материалов, нормативных и иных актов;
- периодических печатных изданий тиражом менее одной тысячи экземпляров;
- радио- и телепрограмм, распространяемых по кабельным сетям, ограниченным помещением и территорией одного государственного учреждения, учебного заведения или промышленного предприятия, либо имеющим не более десяти абонентов;
- аудио- и видеопрограмм, распространяемых в записи тиражом не более десяти экземпляров.

Таким образом, государственному контролю в сфере СМИ не подлежат многие малотиражные печатные издания, такие как научные и другие ведомственные издания, научные и прочие издания предприятий, материалы конференций, симпозиумов, съездов (издателями последних могут выступать организационные комитеты, предприятия-организаторы, группы предприятий). Проведение основных мероприятий по предотвращению утечки конфиденциальной информации в этом случае лежит на предприятиях, предоставляющих информацию в СМИ, и на сотрудников этих предприятий.

Ниже остановимся на основных правилах предоставления результатов научной, производственной иной деятельности информации в СМИ, позволяющих исключить или уменьшить вероятность попадания в средства массовой информации материалов конфиденциального характера.

В зависимости от правил, утвержденных на предприятии, и требований редакций набор требований может варьироваться.

Каждая публикация должна подписывается лично автором или группой авторов. Автором (авторами) по требованию редакции может запрашиваться справка, что в публикации не использованы материалы других авторов, незаконченных научно-исследовательских работ или работ, проводимых коллективом авторов.

Ряд предприятий требуют направлять материалы с сопроводительным письмом, подписываемым его руководителем.

В редакцию представляются экспертное заключение и Лицензионное соглашение. Лицензионное соглашение — договор о передаче прав на использование лицензий, ноу-хау, товарных знаков, технических знаний, инжиниринговых услуг. В нем оговариваются условия передачи информации, содержащейся в рукописи, как продукта интеллектуальной собственности, редакции (печать, передача подписчикам, публикация в сети Интернет и др.).

Экспертное заключение составляется специально назначенной экспертной комиссией (советом) в целях

- оценки научной новизны представляемых результатов;
- отсутствия в них сведений, содержащих государственную, коммерческую или иную охраняемую законом тайну;
- оценки патентоспособности материалов.

В состав комиссии включаются представители профильных подразделений по данному научному направлению (эксперт, эксперты), представители отдела интеллектуальной собственности (патентного отдела). По решению руководителя предприятия в экспертную комиссию могут включаться сотрудники службы безопасности.

Экспертное заключение утверждается руководителем предприятия.

Отметим, что перечисленные мероприятия должны дополняться постоянной разъяснительной работой с сотрудниками и анализом имеющихся публикаций.

13 ЗАЩИТА ИНФОРМАЦИИ ПРИ РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ

Защита информации при рекламной деятельности очень схожа с мероприятиями по защите конфиденциальной информации в СМИ. Особенностью рекламы является желание рекламодателя представить свои разработки, продукцию в наиболее выгодном для себя свете, наиболее привлекательной для потребителей.

Рекламная деятельность регламентируется Федеральным Законом «О рекламе» от 13.03.2006 № 38-ФЗ.

В соответствии со статьей 26 (Реклама продукции военного назначения и оружия):

1. Не допускается реклама:

- продукции военного назначения, за исключением рекламы такой продукции в целях осуществления военно-технического сотрудничества Российской Федерации с иностранными государствами;
- оружия, не указанного в частях 3 - 5 статьи.

2. Производство, размещение и распространение рекламы продукции военного назначения в целях осуществления военно-технического сотрудничества Российской Федерации с иностранными государствами осуществляется в соответствии с законодательством Российской Федерации о военно-техническом сотрудничестве Российской Федерации.

3. Реклама служебного оружия и патронов к нему допускается только в специализированных печатных изданиях для пользователей такого оружия, в местах производства, реализации и экспонирования такого оружия, а также в местах, отведенных для стрельбы из оружия.

4. Реклама боевого ручного стрелкового оружия, патронов к нему, холодного оружия допускается в специализированных печатных изданиях, в местах производства, реализации и экспонирования такого оружия, а также в местах, отведенных для стрельбы из оружия.

5. Реклама гражданского оружия, в том числе оружия самообороны, спортивного, охотничьего и сигнального оружия, допускается только:

- в периодических печатных изданиях, на обложках и в выходных данных которых содержится информация о специализации указанных изданий на сообщениях и материалах рекламного характера, а также в специализированных печатных изданиях для пользователей гражданского оружия;
- в местах производства, реализации и экспонирования такого оружия, а также в местах, отведенных для стрельбы из оружия;

– в теле- и радиопрограммах с 22 до 7 часов местного времени.

6. Реклама оружия и реклама продукции военного назначения, распространяемая в соответствии с законодательством Российской Федерации о военно-техническом сотрудничестве Российской Федерации, не должна:

– прямо или косвенно раскрывать сведения, составляющие государственную тайну, в том числе сведения, относящиеся к технологии производства, способам боевого и иного применения этого оружия;
– обращаться к несовершеннолетним;
– использовать образы несовершеннолетних.

Примечание: подпункт 1 пункта 6 статьи 26 прямо указывает на запрет в рекламе сведений, прямо или косвенно раскрывающих **государственную тайну.**

В соответствии со статьей 7 (Товары, реклама которых не допускается) не допускается реклама:

– товаров, производство и (или) реализация которых запрещены законодательством Российской Федерации;
– взрывчатых веществ и материалов, за исключением пиротехнических изделий;
– товаров, подлежащих государственной регистрации, в случае отсутствия такой регистрации;
– товаров, подлежащих обязательной сертификации или иному обязательному подтверждению соответствия требованиям технических регламентов, в случае отсутствия такой сертификации или подтверждения такого соответствия;
– товаров, на производство и (или) реализацию которых требуется получение лицензий или иных специальных разрешений, в случае отсутствия таких разрешений.

14 КОММЕРЧЕСКАЯ ТАЙНА

Закон о коммерческой тайне принят 29 июля 2004 года (в ред. Федеральных законов от 02.02.2006 № 19-ФЗ, от 18.12.2006 № 231-ФЗ, от 24.07.2007 № 214-ФЗ, от 11.07.2011 № 200-ФЗ)

Закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).

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

Закон не распространяются на сведения, отнесенные в установленном порядке к государственной тайне.

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.

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 тайны.

Доступ к информации, составляющей коммерческую тайн, - 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, 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.

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, **считается полученной законным способом.**

Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, **считается полученной незаконно**, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также, если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- 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;
- 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;
- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- 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;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Предоставление информации, составляющей коммерческую тайну

1. Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

2. В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

3. Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию в соответствии с частью 1 настоящей статьи, обязаны предоставить эту информацию по запросу судов, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

4. На документах, предоставляемых указанным в частях 1 и 3 настоящей статьи органам и содержащих информацию, составляющую коммерческую тайну, должен быть **нанесен гриф "Коммерческая тайна"** с указанием ее обладателя (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Меры по охране конфиденциальности информации должны включать в себя:

1. определение перечня информации, составляющей коммерческую тайну;

2. ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

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

4. регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5. нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

Обладатель информации, составляющей коммерческую тайну, вправе применять методы технической защиты конфиденциальности этой информации, другие меры, не противоречащие законодательству Российской Федерации.

Меры по охране конфиденциальности информации признаются **разумно достаточными,** если:

- исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
- обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Охрана конфиденциальности информации в рамках трудовых отношений

1. В целях охраны конфиденциальности информации работодатель обязан:
   - ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;
   - ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;
   - создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

2. **Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия,** если это не предусмотрено его трудовыми обязанностями.

3. В целях охраны конфиденциальности информации работник обязан:
   - выполнять установленный работодателем режим коммерческой тайны;
   - не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;
   - передать работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую

тайну, либо уничтожить такую информацию или удалить ее с этих материальных носителей под контролем работодателя.

4. 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.

5. 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.

Охрана конфиденциальности информации при ее предоставлении

1. Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с данным Федеральным законом и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

2. Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей коммерческую тайну, не вправе разглашать или передавать другим лицам, органам государственной власти, иным государственным органам, органам местного самоуправления ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных настоящим Федеральным законом, а также не вправе использовать эту информацию в корыстных или иных личных целях.

3. В случае нарушения конфиденциальности информации должностными лицами органов государственной власти, иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством Российской Федерации.

Ответственность за нарушение настоящего Федерального закона

1. Нарушение настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. 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.

3. Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.

4. **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.

5. По требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное в части 4 настоящей статьи, обязано принять меры по охране конфиденциальности информации. **При отказе такого лица принять указанные меры** обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

Грифы, нанесенные до вступления в силу Федерального закона на материальные носители и указывающие на содержание в них информации, составляющей коммерческую тайну, сохраняют свое действие при условии, если меры по охране конфиденциальности указанной информации будут приведены в соответствие с требованиями Федерального закона.

15 МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Моделирование – это исследование объектов познания на их моделях; построение и изучение моделей реально существующих объектов, процессов или явлений с целью получения объяснений этих явлений, а также для предсказания явлений, интересующих исследователя. Моделирование какой-либо системы заключается в построении некоторого ее образа, адекватного (с точностью до целей моделирования) исследуемой системе, и получения с помощью построенной модели необходимых характеристик реальной системы.

В информационной безопасности моделирование часто применяется для изучения поведения потенциального нарушителя (модель нарушителя), либо для анализа безопасности информационной системы (модель угроз).

Существует множество различных определений модели угроз. Согласно ГОСТ Р 50922-2006, Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Под угрозами безопасности здесь понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение данных, а также иных несанкционированных действий при их обработке.

Нормативный подход к построению модели угроз

Модель угроз (или как ее еще называют "Частная модель угроз") может разрабатываться ответственными за информационную безопасность в организации. Также могут привлекаться сторонние эксперты. Разработчики модели угроз должны владеть полной информацией об информационной системе персональных данных (ПД), знать нормативную базу по защите информации.

Порядок разработки модели угроз определен в следующих документах ФСТЭК:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

«**Базовая модель**» содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн). Появление угроз безопасности

может быть связано как с преднамеренными действиями злоумышленников, так и с непреднамеренными действиями персонала или пользователей ИСПД.

Угрозы безопасности могут быть реализованы двумя путями:

– через технические каналы утечки;
– путем несанкционированного доступа.

Обобщенная схема реализации канала угроз ПД показана на рисунке 11.

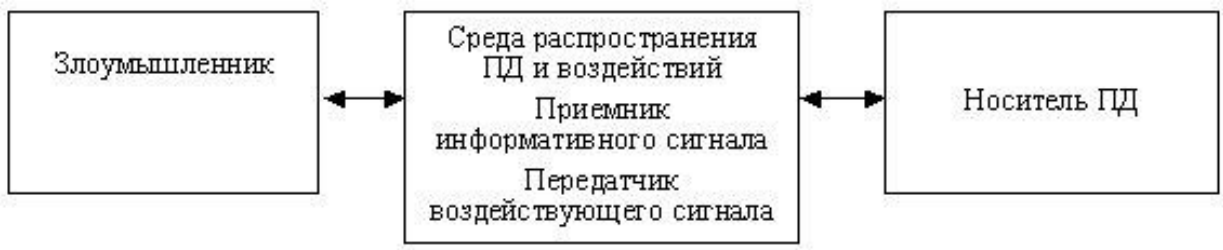


Рисунок 11 – Обобщенная схема канала реализации угроз безопасности персональных данных.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация. Среда распространения бывает однородной, например, только воздух при распространении электромагнитного излучения, или неоднородной, когда сигнал переходит из одной среды в другую. Носителями ПД могут быть люди, работающие с ИСПДн, технические средства, вспомогательные средства и т.д. Главное, что информация при этом отображается в виде полей, сигналов, образов, количественных характеристиках физических величин.

Как правило, выделяют следующие угрозы за счет реализации технических каналов утечки:

– угрозы утечки речевой информации. Фактически злоумышленник перехватывает информацию с помощью специальной аппаратуры в виде акустических, виброакустических волн, а также электромагнитного излучения, модулированного акустическим сигналом. В качестве средств могут использоваться различного рода электронные устройства, подключаемые либо к каналам связи, либо к техническим средствам обработки ПД.
– угрозы утечки видовой информации. В этом случае речь идет о непосредственном просмотре ПД при наличии прямой видимости между средством наблюдения и носителем ПД. В качестве средств наблюдения используются оптические средства и видеозакладки;

– угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН). Речь идет о перехвате побочных (не связанных с прямым функциональным значением элементов ИСПД) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПД. Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПД. Наводки электромагнитных излучений возникают при излучении элементами технических средств ИСПДн информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПДн и различных вспомогательных устройств.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПДн правила разграничения доступа к информации. Этими субъектами могут быть:

– нарушитель;
– носитель вредоносной программы;
– аппаратная закладка.

Под нарушителем здесь и далее понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПД при их обработке техническими средствами в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на два типа:

– нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;
– нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – внутренние нарушители.

Для ИСПДн, предоставляющих информационные услуги удаленным пользователям, внешними нарушителями могут являться лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий, алгоритмических или

программных закладок через автоматизированные рабочие места, терминальные устройства ИСПДн, подключенные к сетям общего пользования.

Документ «**Методика определения актуальных угроз**» содержит алгоритм оценки угрозы. Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПД.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под ***уровнем исходной защищенности*** ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 8.

Таблица 8 – Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению: распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования: ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных: чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн: интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной	+	–	–

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	**Средний**	**Низкий**
ИСПДн			
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

Исходная степень защищенности определяется следующим образом:

- ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).
- ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.
- ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:

- 0 – для высокой степени исходной защищенности;
- 5 – для средней степени исходной защищенности;
- 10 – для низкой степени исходной защищенности.

Под ***частотой (вероятностью) реализации угрозы*** понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПД недостаточны;
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПД не приняты.

При составлении перечня актуальных угроз безопасности ПД каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2, а именно:

– 0 – для маловероятной угрозы;
– 2 – для низкой вероятности угрозы;
– 5 – для средней вероятности угрозы;
– 10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы *Y* будет определяться соотношением

$$Y = (Y_1 + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы *Y* формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если $0 \le Y \le 0,3$, то возможность реализации угрозы признается низкой;

– если $0,3 < Y \le 0,6$, то возможность реализации угрозы признается средней;

– если $0,6 < Y \le 0,8$, то возможность реализации угрозы признается высокой;

– если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

Далее оценивается ***опасность*** каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к ***актуальным*** для данной ИСПДн, в соответствии с правилами, приведенными в таблице 9.

Таблица 9 – Правила отнесения угрозы безопасности ПД к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Риск-подход к моделированию угроз ИБ

Принципиальным отличием риск-модели от указанных выше базовых моделей угроз и аналогичных им нормативных моделей безопасности, является объединение факторов риска в связную причинно-обусловленную структуру. Все факторы (угрозы), явно указанные в базовой модели, включаются в набор факторов риск-модели, как подмножество, тем самым обеспечивая непротиворечивость последней по отношению к базовой. При этом для соблюдения методической строгости и логической полноты риск-модели некоторые исходные факторы определенным образом модифицируются: переформулируются без искажения смысла в том случае, когда исходные формулировки не вполне четкие; разбиваются на несколько факторов, если исходные формулировки обозначают сложные факторы. Кроме того добавляются факторы, включенные в базовую модель контекстуально, а также необходимые для соблюдения полноты и связности, но явным образом не указываемые в базовой модели, что не создает противоречий с ней.

Таким образом, набор факторов в риск-модели состоит из трех подмножеств: факторы, обозначение которых полностью совпадают с формулировками угроз из базовой модели; несколько видоизмененные, но по смыслу также совпадающие, в том числе, полученные разбиением исходного понятия на части (возможна и обратная операция — объединение нескольких угроз в одну); введённые дополнительно. Последнее подмножество, в свою очередь, состоит из трёх частей: контекстуально присутствующие в базовой модели источники угроз, информационные компоненты объекта защиты (ПД в различных состояниях на материальных носителях), угрозы, которые обеспечивают структурную связность основного набора факторов.

В разработанной системе в качестве структурной основы использовалась метамодель, допускающая различные содержательные и алгоритмические интерпретации. Она построена на дихотомической оппозиции: «защищаемый объект» - потенциально враждебная «среда» в широком смысле этих слов. Подчеркивается необходимость фиксации «границы объекта», или, функционально, - «границы ответственности», и «внешней границы среды», ограничивающей зону досягаемости для противодействия факторам риска.

Элементы модели определяются в терминах трех категорий: субъектов, объектов и воздействий первых на вторые. Соответственно категориям выделяются три непересекающихся непустых подмножества множества $M_0 = M_s \cup M_e \cup M_c$ элементов модели (факторов риска):

- независимые активные субъекты, «источники угроз» - множество M_s (threat sources);
- проводники воздействий, события, порождаемые источниками угроз, «угрозы» нарушения безопасности - множество M_e (threat events), в котором выделяется подмножество так называемых «событий риска» - угроз, наносящих непосредственно ущерб объекту;
- «компоненты» объекта - множество M_c (components).

На множестве M_0 определяется хотя бы один тип отношений: бинарное отношение причинности R со свойством транзитивности, к которому можно свести многие связи, имеющие импликативный характер. R упорядочивает M_0 и задает на нем структуру, фиксирующую каналы распространения потоков угроз от источников до объекта, и порождает квадратную матрицу отношений $\mathbf{W}_0$.

Цель реализует «система защиты информации» - СЗИ, которая представима в виде множества элементов S, каждый из которых осуществляет воздействие на элементы из M_0. Между элементами множеств S и M_0 устанавливается отношение, формально сводимое к R, порождающее прямоугольную матрицу отношений R_0.

На рисунке 12 показана простая иллюстрация данного представления метамодели.

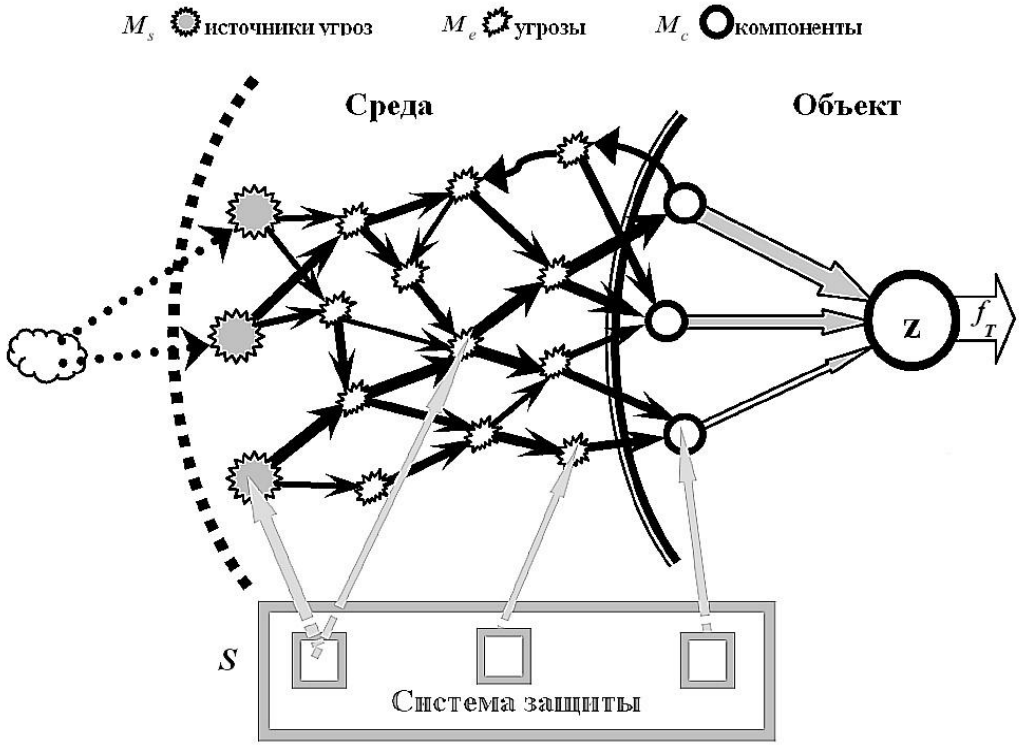


Рисунок 12 – Структурная схема метамодели анализа рисков.

Источники угроз из M_s считаются генераторами потока событий (угроз), распространяющегося по каналам, заданным отношением R на M_0 Элементы M_e рассматриваются как функциональные преобразователи, перераспределяющие потоки событий. На выходе элементов M_e, представляющих события риска, формируется поток угроз, непосредственно воздействующий на объект в составе M_c .Тогда средства защиты из S можно интерпретировать как линейные фильтры.

Роль условного элемента z, соответствующего состоянию объекта в целом, как преобразователя, ограничивается функцией сумматора-интегратора. Тогда на выходе z можно фиксировать результирующий поток f_T, интеграл от которого по некоторому интервалу времени, является, по сути, мерой риска для объекта, измеряемого ущербом, наносимым ему за это время.

Простейшая количественная интерпретация метамодели, предполагающая линейный характер отношений в $\mathbf{W}_0$, отображает ее в арифметическую

матрицу $W=(w_{ij})$, элементы которой можно рассматривать как весовые коэффициенты, имеющие смысл меры влияния i-го элемента на j-ый. Она содержит все исходные данные для расчетов на модели, полученные тем или иным способом.

Далее рассчитываются показатели v_{ij}, аналогичные по смыслу w_{ij}, но уже с учетом транзитивности отношений, прежде всего на z. В результате определяется матрица V, структурно эквивалентная W. При отсутствии рефлексии элементов, если W считать взвешенной матрицей смежности некоторого графа, они легко рассчитываются на графе в соответствующих терминах, как суммы по всем путям из i-ой в j-ую вершину произведений оценок дуг каждого пути, что равносильно матричному преобразованию $\mathbf{V}=(\mathbf{I}-\mathbf{W})^{-1}-\mathbf{I}$.

Однако в общем случае такой расчет не возможен, и тогда V рассчитывается с использованием аппарата марковских цепей следующим образом. Из W исключается левый блок нулевых столбцов, соответствующих множеству M_s, выделяются верхний горизонтальный блок в виде матрицы W_s и остальная нижняя часть, квадратная матрица W_e. Тогда, обозначив $I-W_e=D_e$, определяются соответствующие блоки V: $V_s=W_sD_e^{-1}$ и $V_e=\det(D_e)(D_e^{-1})$.

Последний, всегда не нулевой, z-ый столбец v_z матрицы V содержит искомые показатели $\{v_{iz}\}$ влияния любого i-го фактора риска на состояние защищенности объекта. Эти показатели должны целенаправленно ориентировать создание СЗИ на противодействие наиболее значимым факторам риска.

Факторы риска можно также связать с физическими объектами, задав множество P, представляющее оборудование, физические среды, персонал и т.д., и отношение $\rho_p \subset P\times M_0$. Тогда нетрудно оценки факторов риска отобразить на элементы множества P, что может быть полезно на практике.

Для получения количественной оценки результативности СЗИ матрица $\mathbf{R}_0$ также арифметизируется, а соответствующая матрица $\mathbf{R}=(r_{kj})$ содержит оценки воздействия k-го элемента СЗИ на j-ый фактор риска. Далее она преобразуется в вектор $\mathbf{r}=[r_j]$, где $r_j=1-\prod_k(1-r_{kj})$, или дополняющий его $\mathbf{u}=[u_j]$, $u_j=1-r_j$, $r_j\le 1, u_j\ge 0$, представляющие совместное действие элементов СЗИ. Тогда общий показатель результативности СЗИ r_z рассчитывается следующим образом. Во-первых, определяется вектор $v_s=u_sW_s(I-diag(u_e)W_e)^{-1}$, где u_s, u_e – части вектора u, с компонентами, относящимися, соответственно, к элементам множества M_s и остальным элементам из M_e, далее, используя композицию $v=\{e_s;v_s\}$, где e_s – вектор, состоя-

щий из единиц, порядка, равного количеству элементов в M_s, определяется r_z: $r_z = (\mathbf{v} * \mathbf{r}) \cdot \mathbf{v}_z$, где символ * обозначает операцию поэлементного умножения векторов.

Оценка r_z отображает сложное взаимодействие элементов моделируемой системы, учитывая трудно предсказуемые мультипликативные эффекты удаленных косвенных влияний и циклических связей, являясь одновременно относительной оценкой изменения интегральной характеристики результирующего потока угроз.

Сопоставление подходов. Выводы

Сложившаяся практика исполнения Закона о персональных данных, базируется на нормативном подходе, подразумевающем формальное следование требованиям инструкций и руководящих документов. Полное выполнение требований зачастую невозможно, так как многие организации, являющиеся операторами ПДн, не обладают для этого достаточными ресурсами. Такая практика, безусловно, приносит определенную пользу с точки зрения повышения безопасности ПДн, однако она не позволяет учесть особенности каждой конкретной организации. Поэтому полезно наряду с нормативным подходом использовать риск-подход, который позволит, не уходя от требований нормативов, обеспечить более адекватные оценки факторов риска, что позволит построить более эффективную систему противодействия угрозам информационной безопасности.

Готовая модель угроз должна стать отправной точкой для проектирования будущих систем защиты конфиденциальной информации ее владельцем. С другой стороны, плохо или поверхностно составленная модель угроз сделает всю дальнейшую работу бесполезной, не позволит правильно составить техническое задание на разработку системы защиты информации и приведет к необоснованным тратам на средства защиты.

ЛИТЕРАТУРА

1. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. Учебное пособие, М.: Горячая линия-Телеком, 2001. - 148 с.
2. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа, М: РадиоСофт, 2010. – 232 с.
3. И. А. Баймакова, А. В. Новиков, А. И. Рогачев, А. Х. Хыдыров, М: 1С-Паблишинг, 2010 – 270 с.
4. Савков С. В., Шишкин В. М. Разработка системы интервального оценивания информационных рисков, Известия вузов. Приборостроение, Вып. №09/2011, СПбГУИТМО, 2011, С. 38-43
5. Гатчин Ю.А., Савков С.В., Шишкин В.М. Риск-модель угроз безопасности персональных данных // Труды конгресса по интеллектуальным системам и информационным технологиям IS&IT'11. Научное издание в 4-х томах. – М.: Физматлит, 2011. – Т. 2. – С. 344-350.

НОРМАТИВНЫЕ ДОКУМЕНТЫ

1. Конституция Российской Федерации от 25.12.1993
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ
3. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ
4. Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон Российской Федерации от 27.12.2002 №184-фз «О техническом регулировании».
6. Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».
7. Федеральный закон Российской Федерации от 29.07.2004 №98-ФЗ «О коммерческой тайне».
8. ГОСТ Р 1.4-2004. Стандартизация в Российской Федерации. Стандарты организаций. Общие положения. – Введ. 01.06.2005. – М: Стандартинформ. – 6 с.
9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 27.12.2006. – М: Стандартинформ. – 12 с.

10. ГОСТ Р 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. – Введ. 29.12.2005.– М: Стандартинформ. – 55 с.
11. ГОСТ Р ИСО/МЭК ТО 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – Введ. 19.12.2007. – М. Стандартинформ. – 23 с.
12. ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий». – Введ. 07.06.2007. – М. Стандартинформ. – 45 с.
13. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» утвержденный приказом Гостехкомиссии России от 30.08.2002 г. № 282.
14. Приказ Министерства юстиции Российской Федерации от 4 мая 2007 г. N 88 г. Москва «Об утверждении разъяснений о применении правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации».
15. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008г.
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА ПРОЕКТИРОВАНИЯ И БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

РЛПУ (1945 – 1966)

Решением Правительства в августе 1945 года в ЛИТМО был открыт факультет электроприборостроения. Приказом по Институту от 17 сентября 1945 года на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Организатором и первым заведующим кафедрой был д.т.н. профессор Зилинткевич С.И. (до 1951 года). Выпускникам кафедры присваивалась квалификация «инженер – радиомеханик», а с 1956 года – «радиоинженер» (специальность 0705). В разные годы заведовали кафедрой доцент Мишин Б.С., доцент Захаров И.П., доцент Иванов А.Н.

КиПРЭА 1966 – 1970 (Кафедра конструирования и производства радиоэлектронной аппаратуры)

Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско – технологической направленностью. Оканчивающим институт по этой специальности присваивалась

квалификация «инженер – конструктор – технолог РЭА». Заведовал кафедрой доцент Иванов А.Н.

КиПЭВА 1970 – 1988 (Кафедра конструирования и производства электронно-вычислительной аппаратуры)

Бурное развитие электронной вычислительной техники и внедрение ее во все отрасли народного хозяйства потребовали от отечественной радиоэлектронной промышленности решения новых ответственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям: автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА. Заведовали кафедрой д.т.н. проф. Новиков В.В. (до 1976 г.), затем проф. Петухов Г.А.

Кафедра МАП 1988 – 1997 (Кафедра микроэлектроники и автоматизации проектирования) выпускала инженеров – конструкторов – технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205). Выпускники этой кафедры имели хорошую технологическую подготовку и успешно работали как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования.

Инженеры специальности 2205 требовались микроэлектронной промышленности и предприятиям – разработчикам вычислительных систем.

Кафедрой с 1988 по 1992 год руководил профессор Арустамов С.А., затем снова профессор Петухов Г.А.

Кафедра ПКС 1997-2011 (Кафедра проектирования компьютерных систем) выпускает инженеров по специальности 210202 «Проектирование и технология электронных средств». Область профессиональной деятельности выпускников включает в себя проектирование, конструирование и технологию электронных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации. Кроме того, кафедра готовит специалистов по специальности 090104 «Комплексная защита объектов информатизации», причем основное внимание уделяется программно – аппаратной защите информации компьютерных систем. С 1996 года кафедрой заведует профессор Гатчин Ю.А.

В 2009 и 2010 кафедра заняла второе, а в 2011 году – почетное первое место на конкурсе среди кафедр Университета.

С 2011 года ПБКС (кафедра проектирования и безопасности компьютерных систем). Готовит бакалавров и магистров по направлениям 211000 «Конструирование и технология электронных средств» и 090900 «Информационная безопасность».

Николай Сергеевич КАРМАНОВСКИЙ
Ольга Викторовна МИХАЙЛИЧЕНКО
Сергей Витальевич САВКОВ

Организационно-правовое и методическое обеспечение информационной безопасности

Учебное пособие

В авторской редакции
Редакционно-издательский отдел НИУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати 17.05.13
Заказ № 2990
Тираж 100 экз.
Отпечатано на ризографе

Редакционно-издательский отдел
Санкт-Петербургского национального исследовательского университета информационных технологий, механики
и оптики
197101, Санкт-Петербург, Кронверкский пр., 49