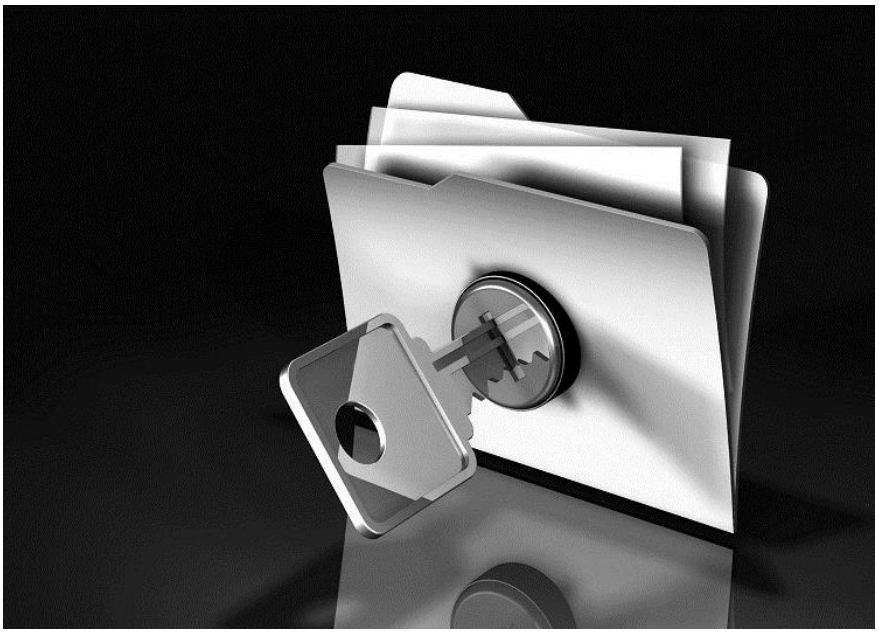
УНИВЕРСИТЕТ ИТМО

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

# ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



**САНКТ-ПЕТЕРБУРГ**
**2016**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

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

# ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## Учебное пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2016

Кармановский Н.С., Михайличенко О.В., Прохожев Н.Н. Организационно-правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: Университет ИТМО, 2016. – 168 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 организации 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 10.04.01 «Информационная безопасность».

Рекомендовано к печати Ученым советом мегафакультета КТиУ,
протокол № 3 от 15 марта 2016 г.

УНИВЕРСИТЕТ ИТМО

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. Дисциплина призвана обеспечить освоение студентами практических навыков работы с нормативно-правовой базой деятельности в области обеспечения информационной безопасности автоматизированных систем.

Целью дисциплины является получение знаний:

– о понятии конфиденциальности информации, объектах защиты, угрозах и нарушителях безопасности предприятия;

– об основных нормативных правовых актах и нормативных методических документах ФСБ России и ФСТЭК России в области защиты информации;

– о государственных стандартах, регламентирующих требования к обеспечению защиты информации, в том числе защиты коммерческой тайны и персональных данных;

– об организации работ по обеспечению безопасности предприятия;

– о функциях и задачах возложенных на службу безопасности и её структурные подразделения;

– о принципах формирования требований по обеспечению безопасности предприятия путем проведения оценки рисков.

После изучения дисциплины студенты должны уметь:

– применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– формировать организационно-административные и технические меры защиты информации.

В результате изучения дисциплины студенты должны приобрести навыки:

– работы с нормативными правовыми актами и нормативными методическими документами в области защиты информации;

– организации и обеспечения режима секретности, в том числе режима коммерческой тайны и защиты персональных данных;

– владения методами организации и управления деятельностью служб безопасности на предприятии;

– методами формирования требований по защите информации.

# 1 КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ. ВИДЫ ТАЙН

В соответствии с Федеральным законом (ФЗ) от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации), циркулирующая в обществе информация подразделяется на общедоступную информацию и информацию ограниченного доступа. Законом также установлено, что ограничения на доступ к информации устанавливаются только ФЗ (ч. 2 ст. 5).

Закон об информации подразделяет информацию в зависимости от порядка ее предоставления или распространения на информацию (ст. 5):

- свободно распространяемую;
- предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- распространение которой в Российской Федерации (РФ) ограничивается или запрещается.

Законодательством РФ установлено, что информация ограниченного доступа может составлять государственную тайну или относиться к конфиденциальной информации.

К государственной тайне относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности РФ, регулируются ФЗ от 21.07.1993 № 5485-1 «О государственной тайне» (в ред. от 01.12.2007).

Определение понятия «конфиденциальность информации» дает Закон об информации: «конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

## 1.1 СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

Перечень сведений конфиденциального характера установлен Указом Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» (в ред. от 23.09.2005, 13.07.2015).

К сведениям конфиденциального характера относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные (ПДн)), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных ФЗ случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с ФЗ принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством РФ такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и ФЗ (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и ФЗ (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и ФЗ (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с ФЗ от 02.10. 2007 г. N 229-ФЗ «Об исполнительном производстве».

## 1.2 ПОНЯТИЕ ТАЙНЫ. ВИДЫ ТАЙН

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

**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 сведений устанавливается законом юридическая ответственность.

Существует большое число охраняемых законом тайн:

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

Государственной и коммерческой тайне, а также защите ПДн будут посвящены отдельные разделы пособия. Далее 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 РФ это право неприкосновенности личной жизни охраняется ст. 23, 24 и 25 Конституции РФ. К нормативным актам, регулирующим защиту права на неприкосновенность частной жизни также относятся ФЗ «О персональных данных», Гражданский кодекс РФ, 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 ст. 26 ФЗ от 02.12.1990 N 395-1 «О банках и банковской деятельности» к банковской тайне относится информация об операциях, счетах и вкладах клиентов и корреспондентов. По законодательству РФ 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. Врачебная тайна является 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 – ст.13 ФЗ от 21.11.2011 №323-ФЗ «Об основах охраны граждан в Российской Федерации».

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 ст. 139 Семейного кодекса РФ, тайна усыновления ребёнка в РФ 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 ст. 155 Уголовного кодекса.

## Тайна связи

В РФ тайна связи гарантируется Конституцией РФ. Часть 2 ст. 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 по охране тайны связи (ст. 63 ФЗ 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 отдель-

ных 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 РФ установлена уголовная ответственность (ст. 138 Уголовного кодекса 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 РФ, о взаимном сотрудничестве между налоговыми (таможенными) 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 министерством РФ по налогам и сборам, органами государственных внебюджетных фондов и федеральной таможенной службой. Утрата документов, содержащих составляющие налоговую тайну сведения, либо разглашение таких сведений влечет ответственность, предусмотренную ФЗ РФ.

## Нотариальная тайна

Нотариальная тайна (тайна нотариальных действий) – разновидность профессиональной тайны. Согласно ст. 16 «Основ законодательства Российской Федерации 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 РФ.

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 Гражданского Кодекса 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 Гражданского Кодекса 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 ПДн, 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).

## Тайна голосования

Принцип тайного голосования – конституционный принцип, гарантирующий гражданам РФ тайну их волеизъявления при голосовании на выборах в органы государственной власти и местного самоуправления и референдуме.

Тайна голосования исключает возможность какого-либо контроля волеизъявления 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 РФ также устанавливаются гарантии соблюдения

тайны волеизъявления при проведении досрочного голосования и голосования вне помещений избирательных комиссий, комиссий референдума.

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 № 125-ФЗ «О свободе совести и о религиозных объединениях» от 26.09. 1997 тайна исповеди охраняется законом. Согласно Гражданского процессуального кодекса РФ (п. 3 ч. 3 ст. 69) священнослужитель не может быть допрошен в качестве свидетеля об обстоятельствах, ставших ему известными из исповеди.

## Выводы

В рамках организации обеспечения безопасности на предприятии разрабатывается и утверждается перечень сведений, относящихся к конфиденциальной информации. Перечень сведений, относящихся к конфиденциальной информации, составляется с учетом требований ФЗ РФ.

С учетом перечня сведений, относящихся к конфиденциальной информации, определяется:

- вид (виды) тайны;
- организационные меры защиты информации;
- технические меры защиты.

Формирование организационных и технических мер защиты сведений, относящихся к конфиденциальной информации, осуществляется с учетом требований законодательства РФ.

# 2 ФОРМИРОВАНИЕ И СТАНДАРТИЗАЦИЯ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

## 2.1 ЗАКОНОДАТЕЛЬНАЯ И НОРМАТИВНАЯ БАЗА РФ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

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

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

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


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

## Конституция Российской Федерации

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

В соответствии со ст. 23 каждый имеет право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а в соответствии со ст. 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 ст. 41 гарантируется право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей и ст. 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 РФ

Уголовный кодекс РФ (в ред. от 27.07.2012) включает в себя главу 28 «Преступления в сфере компьютерной информации», содержащую три статьи:

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

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

Согласно ст. 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 ст. 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.

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

Ст. 13.2 налагает административную ответственность за:

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

Ст. 13.3 налагает административную ответственность за занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с ФЗ обязательно (обязательна).

Ст. 13.14 налагает административную ответственность за разглашение информации, доступ к которой ограничен ФЗ (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 ФЗ в области обеспечения ИБ:

1. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
2. ФЗ РФ от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
3. ФЗ РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных».
5. ФЗ РФ от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
6. ФЗ РФ от № 390-ФЗ от 28.12.2010 «О безопасности».
7. ФЗ РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи».
8. ФЗ РФ от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

## 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 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».
4. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
5. Указ Президента РФ 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 и уполномоченном органе управления атомной энергией».
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 21.11.2006 № 957 «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)».
9. Постановления правительства РФ от 11.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

## Приказы ФСТЭК

В рамках обеспечения технической защиты информации ФСТЭК России 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».

3. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
4. Приказ ФСТЭК России от 11.12.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
5. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

С нормативными правовыми актами, организационно-распорядительными документами, нормативными и методическими документами и подготовленными проектами документов по технической защите информации можно ознакомиться на сайте ФСТЭК России http://fstec.ru/.

## Организационно-распорядительные документы по технической защите информации

К организационно-распорядительным документам по технической защите информации относятся:

1. Доктрина информационной безопасности РФ, утвержденная приказом Президента РФ от 09.09.2000 № Пр-1895.
2. 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 16.04.2012 № 313.
3. 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 РФ ФЗ о техническом регулировании № 184-ФЗ от 27.12.2002 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.

### Российские государственные стандарты серии «Защита информации»

В РФ приняты следующие стандарты серии «Защита информации»:

1. ГОСТ Р 50922-2006 «Основные термины и определения».
2. ГОСТ Р 51188-98 «Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».
3. ГОСТ Р 51275-2006 «Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
4. ГОСТ Р 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

5. ГОСТ Р 51624-2000 «Автоматизированные системы в защищенном исполнении. Общие требования». Документ имеет гриф – для служебного пользования.
6. ГОСТ Р 52447-2005 «Техника защиты информации. Номенклатура ГОСТ Р 52633.0-2006 «Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификацию».
7. ГОСТ Р 5269.0-2013 «Система стандартов. Основные положения».
8. ГОСТ Р 52863-2007 «Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования».
9. ГОСТ Р 53110-2008 «Система обеспечения информационной безопасности сети связи общего пользования. Общие положения».
10. ГОСТ Р 53114-2008 «Обеспечение информационной безопасности в организации. Основные термины и определения».
11. ГОСТ Р 53131-2008 «Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».

## Российские государственные стандарты серии «Информационная технология»

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

1. ГОСТ Р ИСО/МЭК 27000-2012 «Системы менеджмента информационной безопасности. Общий обзор и терминология».
2. ГОСТ Р ИСО/МЭК 27001-2006 «Системы менеджмента информационной безопасности. Требования».
3. ГОСТ Р ИСО/МЭК 27002-2012 «Свод норм и правил менеджмента информационной безопасности» (на основе ISO/IEC 27002:2005)».
4. ГОСТ Р ИСО/МЭК 27004-2011 «Менеджмент информационной безопасности. Измерения».
5. ГОСТ Р ИСО/МЭК 27005-2010 «Менеджмент риска информационной безопасности».
6. ГОСТ Р ИСО/МЭК 27006-2008 «Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
7. ГОСТ Р ИСО/МЭК 27007-2014 «Руководства по аудиту систем менеджмента информационной безопасности
8. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».

9. ГОСТ Р ИСО/МЭК ТО 13335-1-2006 «Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
10. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Руководство по менеджменту безопасности сети».
11. ГОСТ Р ИСО/МЭК 15408-1-2012. «Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».
12. ГОСТ Р ИСО/МЭК 15408-2-2013. «Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».
13. ГОСТ Р ИСО/МЭК 15408-3-2013. «Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».
14. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
15. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
16. ГОСТ Р ИСО/МЭК ТО 19791-2009 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».
17. ГОСТ Р ИСО/МЭК ТО 15446-2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».

Необходимо отметить, что приведенный выше перечень ГОСТов, регулирующих деятельность в области ИБ, является далеко не полным. Перечень ГОСТов, регулирующих деятельность в области ИБ, приведен на сайте ФСТЭК России http://fstec.ru – Главная/Техническая защита/Документы/Национальные стандарты.

Доступ к ГОСТам, регулирующим деятельность в области ИБ, а также к их проектам, можно получить на сайте Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru и на сайте Консультант-плюс http://base.consultant.ru.

## Специальные нормативные документы

К специальным нормативным документам относятся следующие руководящие документы (РД)

– ФСТЭК России:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, 2008 г.;

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных 2008 г.

– Гостехкомисси России:

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. Защита 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. РД. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (2002).

Вышеперечисленные РД Гостехкомиссии России 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 конфи-

денциальной 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 Гостехкомиссией России для служебного пользования. В свободном доступе в сети Интернет можно найти СТР-К от 2002 г. 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 об инициировании процедуры утверждения нового СТР-К от 2013 г.

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.

## Отраслевые нормативные документы по технической защите информации

Стандарты организаций (СТО), в том числе коммерческих, общественных, научных организаций, саморегулируемых организаций, объединений юридических лиц, разрабатываются организациями в случаях и на условиях, указанных в ст. 17 ФЗ «О техническом регулировании».

СТО – 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.

СТО 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 ОАО «Газпром».

Под СТО в ОАО «Газпром» понимается стандарт организации, разработанный, утверждённый и введенный в действие в установленном в ОАО «Газпром» порядке, в котором для многократного использования определены:

- характеристики продукции;
- правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации;
- порядок выполнения работ или оказания услуг, учитывающий специфику и условия деятельности ОАО «Газпром».

В соответствии с СТО Газпром 1.0-2009 «Система стандартизации ОАО «Газпром». Основные положения»:

«Стандартизация осуществляется с учётом специфики деятельности ОАО «Газпром» в целях:

- обеспечения единой технической политики в ОАО «Газпром»;
- формирования единого механизма технического регулирования в ОАО «Газпром»;
- технической и информационной совместимости, а также защиты информации;
- сопоставимости результатов измерений и испытаний, технических и экономико-статистических данных на международном, национальном и корпоративном (ОАО «Газпром») уровнях.
- повышения уровня безопасности опасных производственных объектов ОАО «Газпром» с учетом риска возникновения природных и техногенных катастроф и других чрезвычайных ситуаций;
- и др.,

Задачами стандартизации в ОАО «Газпром» являются:

- установление правил, процедур разработки и утверждения стандартов ОАО «Газпром», стандартов его дочерних обществ и организаций, обеспечивающих привлечение всех заинтересованных сторон к работам по стандартизации;
- обеспечение контроля соблюдения требований документов по техническому регулированию в ОАО «Газпром»;
- создание условий для приоритетного использования национальных стандартов и стандартов организаций (ОАО «Газпром», его органи-

заций и дочерних обществ) в интересах ОАО «Газпром» и выполнения его обязательств в РФ и за рубежом;
- повышение уровня гармонизации разрабатываемых и применяемых в ОАО «Газпром» документов по стандартизации с международными документами;
- систематизация и анализ требований к продукции, процессам проектирования (включая изыскания), строительства, производства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, содержащихся в действующих в ОАО «Газпром» документах различного уровня с позиций принципов технического регулирования в ОАО «Газпром»;
- создание информационных ресурсов (баз данных, классификаторов и др.), содержащих полную, достоверную, актуальную информацию, необходимую для обеспечения деятельности структурных подразделений, организаций и дочерних обществ ОАО «Газпром» в сфере технического регулирования;
- и др.

Стандартизация в ОАО «Газпром» с учётом специфики деятельности осуществляется в соответствии с принципами:
- обязательности выполнения требований стандартов ОАО «Газпром» всеми структурными подразделениями, дочерними обществами и организациями ОАО «Газпром», если иное не установлено в конкретном стандарте;
- максимального учета интересов ОАО «Газпром» при разработке документов Системы стандартизации;
- недопустимости установления таких требований в стандартах ОАО «Газпром», которые противоречат требованиям технических регламентов;
- открытости участия в разработке документов системы стандартизации для всех заинтересованных сторонних организаций;
- доступности документов системы стандартизации, в том числе их проектов, а также информации о них;
- централизации направления официальных экземпляров документов системы стандартизации, изменений и поправок к ним в структурные подразделения, дочерние общества и организации ОАО «Газпром»;
- обеспечения условий для единообразного применения документов Системы стандартизации;
- и др.»

В зависимости от объекта стандартизации и аспекта стандартизации, а также содержания устанавливаемых к ним требований в ОАО «Газпром» разрабатываются стандарты следующих видов:
- стандарты основополагающие (организационно-методические и общетехнические);

– стандарты на продукцию;
– стандарты на процессы производства, эксплуатации, хранения, перевозки, реализации и утилизации продукции;
– стандарты на услуги (работы);
– стандарты на методы контроля (испытаний, определений, измерений, анализа);
– стандарты на термины и определения.

В ОАО «Газпром» разработано 56 стандартов серии «Система обеспечения информационной безопасности ОАО «Газпром» и «Система обеспечения безопасности объектов ОАО «Газпром» с использованием инженерно-технических средств охраны» (данные взяты с http://www.gazprom.ru/about/strategy/innovation/tech-regulation – ОАО «Газпром/ Техническое регулирование – «Журнал регистрации стандартов и рекомендаций» по состоянию на 01.10.2015).

В рамках серии «Система обеспечения информационной безопасности ОАО «Газпром» стандартизированы определения, политики, методики, технические требования по защите информации.

Ниже приведен краткий перечень СТО Газпром серии «Система обеспечения информационной безопасности ОАО «Газпром»:

1. СТО Газпром 4.2-1-001-2009 «Основные термины и определения».
2. СТО Газпром 4.2-0-001-2009 «Типовая политика информационной безопасности дочернего общества (организации)».
3. СТО Газпром 4.2-3-002-2009 «Требования по технической защите информации при использовании информационных технологий».
4. СТО Газпром 4.2-2-004-2013 «Требования по обеспечению информационной безопасности при использовании технических решений по IP- телефонии»
5. Рекомендации Газпром 4.2-2-006-2013 «Требования по обеспечению информационной безопасности при использовании средств терминального доступа».
6. СТО Газпром 4.2-3-005-2013 «Управление инцидентами информационной безопасности» (методика).
7. Рекомендации Газпром 4.2-3-002-2015 «Методика классификации объектов защиты».

Полный перечень разработанных СТО Газпром смотрите на сайте ОАО «Газпром» в разделе Техническое регулирование http://www.gazprom.ru/about/strategy/innovation/tech-regulation.

## 2.2 ТРЕБОВАНИЯ МЕЖДУНАРОДНЫХ И ОТЕЧЕСТВЕННЫХ СТАНДАРТОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Международный и отечественный опыт по формированию требований к ИБ организаций и ИС 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.

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

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

| Стандарт / Нормативный акт | Разработчик | Статус |
|---|---|---|
| ISO/IEC 15408 Security techniques. Evolution criteria for IT security. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий | Международная организация по стандартизации | Международные стандарты |
| ISO/IEC 19791:2010 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 ИБ | | |
| BSI IT Baseline Protection Manual. Standard security safeguards | Немецкое 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 Security and Privacy Controls for Federal Information Systems and Organizations.<br>Меры обеспечения безопасности и приватности для Федеральных систем и организаций | Национальный институт по стандартизации и технологиям (NIST) | |
| COBIT (Control Objectives for Information and related Technology).<br>Цели контроля для информационных и смежных технологий | Ассоциация аудиторов ИС (ISACA) | Профессиональный стандарт |
| FISCAM (Federal Information System Controls Audit Manual) Федеральное руководство по аудиту ИС | Главная счетная палата США (GAO) | Отраслевые стандарты |
| PCI DSS (Payment Card Industry Data Security Standard)<br>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<br>Стандарт безопасности медицинских сведений | Министерство здравоохранения и социального обеспечения США (DHHS) | |
| SPP ICS (System Protection Profile for Industrial Control Systems)<br>Стандарт обеспечения безопасности автоматизированных систем управления технологическими процессами | Национальный институт по стандартизации и технологиям (NIST) | Индустриальный (промышленный) стандарт |
| СТО БР ИББС-1.0–2010<br>Обеспечение информационной безопасности организаций банковской системы РФ | 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 ИС, представляют:

1. ISO/IEC 2700x (ГОСТ Р ИСО/МЭК 2700x).
2. ГОСТ Р ИСО/МЭК 15408-2-2013 «Функциональные требования безопасности».
3. NIST SP800-53 «Меры обеспечения безопасности и приватности для Федеральных систем и организаций».
4. COBIT.
5. СТО БР ИББС-1.0–2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

## Требования к информационной безопасности стандартов ISO/IEC 2700x (ГОСТ Р ИСО/МЭК 27001, 27002)

Серия международных стандартов по информационной технологии 2700x разрабатывается ISO/ IEC (Международной организацией по стандартизации (ИСО) и Международной электротехнической комиссией (МЭК)). 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 ИБ.

Для 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 2. При составлении перечня использовались данные с сайта Федерального агентства по техническому регулированию и метрологии» http://protect.gost.ru и ФСТЭК России http://fstec.ru и сайт Международной организации по стандартизации (ISO) www.iso.org.

Требования ИБ в виде описания рекомендуемых практических мер защиты заданы в ГОСТ Р ИСО/МЭК 27002- 2012 и в согласованном с ним ГОСТ Р ИСО/МЭК 27001-2006 (приложение А стандарта).

Стандартами ГОСТ Р ИСО/МЭК 27001-2006 и 27002-2012 задается перечень требований (рекомендаций) в 11 направлениях обеспечения ИБ, включающих 37 основных категорий безопасности, содержащих 133 защитных мер. Организационные и программно-технические защитные меры ГОСТ Р ИСО/МЭК 27001-2006 приведены в таблице 3.

Необходимо отметить, что в стандарте ISO/IEC 27002:2013 приводятся 14 направлений безопасности. По сравнению с ISO/IEC 27002:2005 (и ГОСТ Р ИСО/МЭК 27001-2006) добавилось два новых направления обеспечения ИБ «Криптография» и «Взаимодействие с поставщиками» (ранее требования этих направлений входили в состав других направлений), а также направление «Управление коммуникациями и их функционирование» было разделено на два направления: «Безопасность операций»

и «Безопасность коммуникаций». В ISO/IEC 27002:2013 приводятся 113 защитных мер (раньше было 133). Ряд защитных мер был логически объединен между собой, ряд мер был удален, поскольку разработчики признали эти меры неактуальными, дублирующими требования обновленных основных разделов стандарта, либо слишком узконаправленными (другие меры включают их в себя). Всего было удалено 26 защитных мер.

Таблица 2 – Перечень международных стандартов по ИБ серии 2700х и отечественных стандартов, аутентичных им

| **Международные стандарты серии 2700х** | **Отечественные стандарты серии 2700х** |
|---|---|
| ISO 27000 «Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы» | ГОСТ Р ИСО/МЭК 27000-2012 «Общий обзор и терминология» |
| ISO/IEC 27001:2013 «Системы управления информационной безопасностью» | ГОСТ Р ИСО/МЭК 27001-2006 «Системы менеджмента информационной безопасности. Требования» (стандарт идентичен ISO/IEC 27001:2005) |
| ISO/IEC 27002:2013 «Практические правила управления информационной безопасностью « | ГОСТ Р ИСО/МЭК 27002-2012 «Свод норм и правил менеджмента безопасности» |
| ISO/IEC 27003:2010 «Руководство по внедрению системы управления информационной безопасностью» | ГОСТ Р ИСО/МЭК 27003-2012 «Руководство по реализации системы менеджмента информационной безопасности» |
| ISO/IEC 27004:2014 «Метрики информационной безопасности» | ГОСТ Р ИСО/МЭК 27004-2011 «Менеджмент информационной безопасности. Измерения» |
| ISO/IEC 27005:2011 «Управление рисками информационной безопасности» | ГОСТ Р ИСО/МЭК 27005-2010 «Менеджмент риска информационной безопасности» |
| ISO/IEC 27006:2015 «Требования к органам аудита и сертификации систем управления информационной безопасностью» | ГОСТ Р ИСО/МЭК 27006-2008 «Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» |
| ISO/IEC 27007:2011 «Руководство для аудитора системы управления информационной безопасности» | – |
| ISO/IEC 27008:2011 «Руководство по аудиту механизмов контроля системы управления информационной безопасности» | – |
| ISO/IEC 27010:2015 «Управление информационной без-опасностью при коммуникациях между секторами» | – |

| Международные стандарты серии 2700х | Отечественные стандарты серии 2700х |
|---|---|
| ISO/IEC 27011:2008 «Руководство по управлению информационной безопасностью для телекоммуникаций» | – |
| ISO/IEC 27013:2015 «Руководство по интегрированному внедрению ISO 20000 и ISO 27001» | ГОСТ Р ИСО/МЭК 27013-2014 «Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1» |
| ISO/IEC 27014:2014 «Базовая структура управления информационной безопасностью» | – |
| ISO/IEC 27015:2012 «Руководство по внедрению систем управления информационной безопасностью в финансовом и страховом секторе» | – |
| ISO/IEC 27031:2011 «Руководство по обеспечению готовности информационных и коммуникационных технологий к их использованию для управления непрерывностью бизнеса» | – |
| ISO/IEC 27032:2012 «Руководство по кибербезопасности» | – |
| ISO/IEC 27033-1:2015 «Сетевая безопасность. Часть 1. Обзор и концепции».<br>ISO/IEC 27033-2:2012 «Сетевая безопасность. Часть 2. Методические рекомендации по проектированию и реализации сетевой безопасности».<br>ISO/IEC 27033-3:2010 «Сетевая безопасность. Часть 3. Угрозы, методы проектирования и вопросы управления».<br>ISO/IEC 27033-4:2014 «Сетевая безопасность. Часть 4. Обеспечение связи между сетями с использованием шлюзов безопасности».<br>ISO/IEC 27033-5:2013 «Сетевая безопасность. Часть 5. | ГОСТ Р ИСО/МЭК 27033-1-2011 «Безопасность сетей. Часть 1. Обзор и концепции».<br>ГОСТ Р ИСО/МЭК 27033-3-2014 «Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления» |

| Международные стандарты серии 2700х | Отечественные стандарты серии 2700х |
|---|---|
| Обеспечение связи через сети с использованием виртуальных частных сетей» | |
| ISO/IEC 27034-1:2011 «Безопасность приложений. Часть 1. Общий обзор и концепции».<br>ISO/IEC 27034-2:2015 «Безопасность приложений. Часть 2. Организация нормативной базы». | ГОСТ Р ИСО/МЭК 27034-1-2014 «Безопасность приложений. Часть 1. Обзор и общие понятия» |
| ISO/IEC 27035:2011 «Управление инцидентами безопасности» | – |
| ISO/IEC 27036-1:2014 «Защита информации для связей с поставщиками. Часть 1. Общий обзор и концепции».<br>ISO/IEC 27036-2:2014 «Защита информации для связей с поставщиками Часть 2. Требования».<br>ISO/IEC 27036.-3:2013 «Защита информации для связей с поставщиками. Часть 3. Руководящие указания по защите цепей поставки информационных и коммуникационных технологий».<br>ISO/IEC 27036-4:2013 «Защита информации для связей с поставщиками. Часть 4. Рекомендации по безопасности облачных сервисов» | – |
| ISO/IEC 27037:2012 «Руководство по идентификации, сбору и/или получению и обеспечению сохранности цифровых свидетельств» | ГОСТ Р ИСО/МЭК 27037-2014 «Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме» |

Таблица 3 – Организационные и программно-технические защитные меры ГОСТ Р ИСО/МЭК 27001-2006

| № | Категория защитных мер | Состав защитных мер |
|---|---|---|
| 1. Политики безопасности | | |
| 1. | Политика ИБ | 1. Документирование политики ИБ.<br>2. Анализ и пересмотр политики ИБ |
| 2. Организация ИБ | | |
| 2. | Внутренняя организация | 1. Обязанности руководства по обеспечению ИБ.<br>2. Координация вопросов обеспечения ИБ.<br>3. Распределение обязанностей по обеспечению ИБ.<br>4. Получение разрешений на использование средств обработки информации.<br>5. Заключение соглашений о конфиденциальности.<br>6. Проведение внешнего аудита ИБ.<br>7. Взаимодействие с компетентными органами.<br>8. Взаимодействие с организациями и профессиональными группами. |
| 3. | Обеспечение безопасности при доступе сторонних организаций | 1. Определение рисков, связанных со сторонними организациями.<br>2. Соблюдение мер безопасности при работе с клиентами.<br>3. Соблюдение мер безопасности в соглашениях со сторонними организациями |
| 3. Управление активами | | |
| 4. | Обеспечение ответственности за защиту активов | 1. Инвентаризация активов.<br>2. Назначение ответственных за активы.<br>3. Документирование правил безопасного использования активов |

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

| № | Категория защитных мер | Состав защитных мер |
|---|---|---|
| 10. | Безопасность оборудования | 1. Размещение и защита оборудования.<br>2. Обеспечивающие подсистемы (электроснабжения, заземления, кондиционирования).<br>3. Безопасность кабельной сети.<br>4. Техническое обслуживание оборудования.<br>5. Обеспечение безопасности внешнего оборудования.<br>6. Безопасная утилизация или повторное использование оборудования.<br>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.<br>2. Контроль изменений в конфигурациях средств обработки и обмена данными.<br>3. Разграничение обязанностей по эксплуатации средств обработки и обмена данными.<br>4. Разграничение средств разработки, тестирования и эксплуатации |
| 12. | Управление услугами, предоставляемыми сторонними организациями | 1. Оказание услуг.<br>2. Контроль выполнения договорных обязательств.<br>3. Мониторинг, аудит и анализ аутсорсинговых услуг |
| 13. | Планирование нагрузки и приемка систем | 1. Управление производительностью.<br>2. Проверка новых средств обработки и обмена данными перед приемом в эксплуатацию |
| 14. | Защита от вредоносного программного обеспечения (ПО) | 1. Защита от вредоносного кода.<br>2. Защита от мобильного кода |

| № | Категория защитных мер | Состав защитных мер |
|---|---|---|
| 15. | Резервное копирование и хранение информации | Резервирование информации и ПО |
| 16. | Управление безопасностью сети | 1. Средства контроля сети.<br>2. Безопасность сетевых сервисов. |
| 17. | Безопасное применение носителей информации | 1. Контроль доступа к внешним носителям информации и периферийным устройствам, подключаемым к автоматизированным рабочим местам.<br>2. Утилизация носителей информации.<br>3. Регламентирование процедур обработки информации.<br>4. Безопасность системной документации. |
| 18. | Защищенный обмен информацией | 1. Политики и процедуры обмена информацией.<br>2. Соглашение по обмену информацией.<br>3. Защищенный обмен сообщениями и данными.<br>4. Защита физических носителей информации при транспортировке.<br>5. Защищенное взаимодействие смежных ИС |
| 19. | Услуги электронной торговле | 1. Обеспечение защиты электронной торговли.<br>2. Защита от модификации общедоступной информации.<br>3. Защита транзакции в режиме реального времени |
| 20. | Мониторинг | 1. Ведение журналов регистрации действий пользователей и событий безопасности.<br>2. Мониторинг использования средств обработки и обмена данными.<br>3. Защита информации журналов регистрации.<br>4. Журналы регистрации действий администраторов.<br>5. Регистрация неисправностей.<br>6. Синхронизация времени |

| № | Категория защитных мер | Состав защитных мер |
|---|---|---|
| 7. Контроль доступа | | |
| 21. | Управление доступом в соответствии с требованиями бизнеса | Политика контроля доступа |
| 22. | Управление доступом пользователя | 1. Регламентирование и выполнение процедур регистрации (снятия с регистрации) пользователей.<br>2. Управление привилегиями (ролями) пользователей.<br>3. Управление паролями (аутентификационными данными) пользователей.<br>4. Пересмотр прав доступа пользователей |
| 23. | Ответственность пользователей | 1. Использование паролей.<br>2. Защита оборудования, оставленного без присмотра.<br>3. Правила «чистого стола» и «чистого экрана» |
| 24. | Контроль сетевого доступа | 1. Политика в отношении использования сетевых услуг.<br>2. Аутентификация пользователей для внешних соединений.<br>3. Идентификация оборудования в сетях.<br>4. Защита портов при удаленном доступе.<br>5. Разделение сетей.<br>6. Контроль сетевых соединений.<br>7. Контроль маршрутизации в сети |

| № | Категория защитных мер | Состав защитных мер |
|---|---|---|
| 25. | Контроль доступа к операционной системе | 1. Выполнение процедуры безопасного входа в систему.<br>2. Идентификация и аутентификация пользователя (субъекта доступа).<br>3. Управление парольной политикой.<br>4. Контроль использования системных утилит.<br>5. Завершение (блокировка) сеанса после определенного времени бездействия.<br>6. Ограничение времени соединения |
| 26. | Контроль доступа к прикладным системам, системам управления базами данных, информации | 1. Ограничение доступа к прикладным системам и информации в соответствии с политикой доступа.<br>2. Выделение (изоляция) вычислительной среды для систем, обрабатывающих важную информацию |
| 27. | Безопасная работа с переносными устройствами и в удаленном режиме | 1. Безопасная работа с переносными устройствами.<br>2. Безопасная работа в удаленном режиме |
| 8. Обеспечение ИБ при приобретении, разработке и обслуживании ИС | | |
| 28. | Задание требований безопасности к разрабатываемым прикладным ИС | Формирование требований безопасности к прикладным ИС |
| 29. | Проверка корректности обработки данных в прикладных ИС | 1. Проверка достоверности входных данных.<br>2. Контроль обработки данных в приложениях.<br>3. Обеспечение аутентичности и защита целостности содержания сообщений.<br>4. Подтверждение достоверности выходных данных |

| № | Категория защитных мер | Состав защитных мер |
|---|---|---|
| 30. | Защита информации криптографическими средствами | 1. Формализация процедур использования криптографических средств.<br>2. Управление ключевой информацией. |
| 31. | Безопасность системных файлов | 1. Контроль целостности эксплуатируемого ПО.<br>2. Контроль и защита данных при осуществлении тестирования системы.<br>3. Контроль доступа к исходным кодам программ |
| 32. | Безопасность в процессах разработки и поддержки | 1. Контроль изменений прикладного программного обеспечения.<br>2. Анализ функционирования и безопасности прикладного ПО после внесения изменений в системное ПО.<br>3. Формализация процедур контроля изменений в прикладное ПО.<br>4. Предотвращение утечки информации из ИС.<br>5. Формализация процедур разработки ПО с привлечением сторонних организаций |
| 33. | Контроль технических уязвимостей | Обнаружение и устранение технических уязвимостей ИС |
| 9. Управление инцидентами ИБ | | |
| 34. | Своевременное оповещение о событиях и недостатках информационной безопасности | 1. Оповещение о событиях ИБ.<br>2. Документирование (формализация) административных процедур оповещения о слабых местах (недостатках) ИБ |
| 35. | Управление инцидентами информационной безопасности и улучшениями | 1. Формализация ответственности и процедур реагирования на инциденты ИБ.<br>2. Формализация процедур мониторинга и регистрации инцидентов ИБ.<br>3. Формализация процедур сбора доказательств об инцидентах ИБ |

| № | Категория защитных мер | Состав защитных мер |
|---|---|---|
| 10. Управление непрерывностью бизнеса | | |
| 36. | Обеспечение непрерывности бизнеса | 1. Включение ИБ в процесс управления непрерывностью бизнеса.<br>2. Оценка риска нарушения непрерывности бизнеса.<br>3. Разработка и внедрение планов непрерывности бизнеса с учетом ИБ.<br>4. Создание единой структуры планов непрерывности бизнеса.<br>5. Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса |
| 11. Обеспечение соответствия требованиям | | |
| 37. | Обеспечение соответствия правовым требованиям | 1. Определение и документирование правовых требований.<br>2. Защита прав на интеллектуальную собственность.<br>3. Защита учетных данных.<br>4. Защита ПДн.<br>5. Предотвращение злоупотребления средствами обработки информации.<br>6. Регулирование использования криптографических средств |
| 38. | Обеспечение соответствия политикам и стандартам безопасности, и технического соответствия | 1. Обеспечение соответствия политикам и стандартам безопасности.<br>2. Проверка соответствия техническим требованиям ИБ |
| 39. | Аудит ИБ | 1. Управление аудитом ИБ.<br>2. Защита инструментальных средств аудита |

## Требования к информационной безопасности стандарта ГОСТ Р ИСО/МЭК 15408-2-2013 «Функциональные требования безопасности»

Стандарт ГОСТ Р ИСО/МЭК 15408-2-2013 аутентичен международному стандарту ISO/IEC 15408-2:2008, который является одним из распространенных стандартов в области безопасности. В разработке ISO/IEC 15408-2:2008 приняли участие правительственные организации из США, Канады, Англии, Франции, Германии, Голландии, Японии, Австралии.

Важным отличием стандартов ISO/IEC 27002:2013 и ISO/IEC 15408-2:2008 является то, что первый ориентирован на разработчиков и специалистов по эксплуатации, а второй – на экспертов по оценке безопасности.

ИСО/МЭК 15408 не содержит критериев оценки безопасности, касающихся административных мер безопасности, непосредственно не относящихся к мерам безопасности информационных технологий (ИТ).

В ИСО/МЭК 15408 не рассматривается ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки. Тем не менее, ИСО/МЭК 15408 может использоваться для целей оценки в контексте такой структуры и такой методологии

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 (определения), 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. Под компонентами понимается совокупность элементов (неделимых требований безопасности), которая может быть включена в профиль защиты или задание по безопасности.

Соответствие классов и семейств требований безопасности в ГОСТ Р ИСО/МЭК 15408-2-2006 приведено в таблице 4.

Таблица 4 – Соответствие классов и семейств требований безопасности в ГОСТ Р ИСО/МЭК 15408-2-2006

| № п/п | Класс требований безопасности | Семейство требований безопасности |
|---|---|---|
| 1. | Аудит безопасности | 1. Автоматическая реакция аудита безопасности. |

| № п/п | Класс требований безопасности | Семейство требований безопасности |
|---|---|---|
| | | 2. Генерация данных аудита.<br>3. Анализ данных аудита.<br>4. Просмотр аудита.<br>5. Выбор событий аудита безопасности.<br>6. Хранение данных аудита |
| 2. | Связь | 1. Неотказуемость отправления.<br>2. Неотказуемость получения |
| 3. | Криптографическая поддержка | 1. Управление криптографическими ключами.<br>2. Криптографические операции |
| 4. | Защита данных пользователя | 1. Политика управления доступом.<br>2. Функции управления доступом.<br>3. Аутентификация данных.<br>4. Экспорт данных за пределы действия.<br>5. Политика управления информационными потоками.<br>6. Функции управления информационными потоками.<br>7. Импорт данных из-за пределов действий.<br>8. Защита остаточной информации.<br>9. Передача данных в пределах объекта оценки.<br>10. Откат.<br>11. Защита конфиденциальности.<br>12. Защита целостности.<br>13. Целостность хранимых данных |
| 5. | Идентификация и аутентификация | 1. Отказы аутентификации.<br>2. Определение атрибутов аутентификации.<br>3. Спецификация секретов.<br>4. Аутентификация пользователя.<br>5. Идентификация пользователя.<br>6. Связывание пользователя-субъект |
| 6. | Управление безопасностью | 1. Управление отдельными функциями.<br>2. Управление атрибутами безопасности.<br>3. Управление данными.<br>4. Отмена.<br>5. Срок действия атрибутов безопасности.<br>6. Роли управления безопасность |

| № п/п | Класс требований безопасности | Семейство требований безопасности |
|---|---|---|
| 7. | Приватность | 1. Анонимность.<br>2. Псевдонимность.<br>3. Невозможность ассоциации.<br>4. Скрытность |
| 8. | Защита функций безопасности объекта оценки (ФБО) | 1. Тестирование базовой абстрактной машины.<br>2. Безопасность при сбое.<br>3. Доступность экспортируемых данных.<br>4. Передача ФБО в пределах объекта оценки.<br>5. Физическая защиты ФБО.<br>6. Надежное восстановление.<br>7. Обнаружение повторного использования.<br>8. Разделение домена.<br>9. Протокол синхронизации состояний.<br>10. Метки времени.<br>11. Согласованность данных ФБО между ФБО.<br>12. Согласованность данных ФБО при дублировании в пределах объекта оценки.<br>13. Самотестирование ФБО. |
| 9. | Использование ресурсов | 1. Отказоустойчивость.<br>2. Приоритет обслуживания.<br>3. Распределение ресурсов |
| 10. | Доступ к объекту оценки | 1. Ограничение области выбираемых атрибутов.<br>2. Ограничение на параллельные сеансы.<br>3. Блокирование сеанса.<br>4. Предупреждение перед предоставлением доступа к объекту оценки |
| 11. | Доверенный маршрут/канал | 1. Доверенный канал передачи.<br>2. Доверенный маршрут |

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 «Меры обеспечения безопасности и приватности для Федеральных систем и организаций»

Национальный стандарт NIST SP800-53 «Меры обеспечения безопасности и приватности для Федеральных систем и организаций» разработан Национальным Институтом Стандартов и Технологии США и определяет требования безопасности и меры контроля (security controls) ИС.

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

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

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

В NIST SP800-53 меры контроля безопасности разбиты на три класса: технические, операционные, управленческие. Всего в стандарте определено 240 мер контроля, сгруппированных в 17 семейств, таких как:

- осведомлённость и обучение;
- аудит и отчётность;
- авторизация и оценка безопасности;
- управление конфигурацией;
- планирование непрерывности бизнеса;
- идентификация и аутентификация;
- реагирование на инциденты;
- обслуживание/техническая поддержка;
- защита носителей информации;
- физическая защита и защита от стихийных бедствий;
- планирование;
- безопасность персонала;
- оценка рисков;
- приобретение систем и сервисов;
- защита систем и коммуникаций;
- целостность систем и информации;
- управление программой ИБ.

Для поддержания базового, среднего или высокого уровня защищенности ИС 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 работники 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.<br>2. Разработка ИТ-архитектуры.<br>3. Мониторинг технологического развития.<br>4. Формирование ИТ-службы и определение взаимосвязей.<br>5. Управление инвестициями в ИТ.<br>6. Распространение корпоративной информации.<br>7. Управление персоналом.<br>8. Обеспечение соответствия внешним требованиям.<br>9. Управление рисками.<br>10. Управление проектами.<br>11. Управление качеством |
| Приобретение и реализация | 1. Идентификация автоматизируемых решений.<br>2. Приобретение и поддержка прикладного ПО.<br>3. Приобретение и поддержка технологической |

| Этап жизненного цикла управления ИТ | Название процесса управления ИТ |
|---|---|
| | инфраструктуры.<br>4. Разработка и поддержка процедур.<br>5. Установка и прием в эксплуатацию систем.<br>6. Управление изменениями |
| Предоставление (реализация) и поддержка | 1. Определение и управление уровнями обслуживания.<br>2. Управление услугами третьих сторон;<br>3. Управление производительностью и мощностью.<br>4. Обеспечение непрерывности обслуживания.<br>5. Обеспечение безопасности.<br>6. Идентификация и управление стоимостью.<br>7. Обучение пользователей.<br>8. Помощь клиентам.<br>9. Управление конфигурациями.<br>10. Управление проблемами и инцидентами.<br>11. Управление данными.<br>12. Управление средствами.<br>13. Управление операциями |
| Мониторинг | 1. Мониторинг процессов.<br>2. Обеспечение адекватности внутреннего контроля.<br>3. Организация независимого контроля.<br>4. Обеспечение независимого аудита |

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

СТО БР ИББС -1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» 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. Стандарт ссылается и учитывает требования из перечисленных выше стандартов по безопасности (ISO/IEC 27001-2005, ISO/IEC IS 27002), а также не указанного ранее стандарта ISO TR 13569 «Banking and related financial services. Information security guidelines».

Требования СТО БР ИББС-1.0-2010 распространяются на следующие области ИБ:

- назначение и распределение ролей и доверия к персоналу;
- стадии жизненного цикла автоматизированной системы;
- защита от несанкционированного доступа (НСД), 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.

## ВЫВОДЫ

Для обеспечения конфиденциальности, целостности и доступности информации, а также сохранения устойчивого функционирования ИС 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 для 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 ИС 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.

Требования по ИБ, рекомендуемые государственными и международными стандартами, определяют перечень направлений обеспечения ИБ (кате-

горий мер защиты), которые необходимо учитывать в рамках обеспечения ИБ организации.

Наиболее полный и адекватный набор требований ИБ представлен в серии стандартов 2700х, в частности ГОСТ Р ИСО/МЭК 27001 и 27002, что позволяет выбрать их за основу для формирования требований по обеспечению ИБ организации.

# 3 ОРГАНИЗАЦИЯ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Основные вопросы государственной тайны отражены в Законе РФ «О государственной тайне» (далее – Закон).

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. Закон связывает понятие государственной тайны с понятием безопасности РФ.

Действие Закона распространяется на всю территорию РФ (включая учреждения РФ 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 РФ, 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.

## 3.1 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 НСД, 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.

## 3.2 РЕЖИМ СЕКРЕТНОСТИ

Особенностями режима секретности являются:

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

## 3.3 СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ

### 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 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. 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 РФ 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 РФ (ст. 5), а с другой – область интересов общества и его граждан, информация в которой не подлежит засекречиванию (ст. 7). Именно при соблюдении принципа законности засекречивания. Тем самым достигается баланс интересов граждан, общества и государства, положенный в основу Закона РФ «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

В перечень сведений, составляющих государственную тайну, входят:

**1. Сведения в военной области о:**

- содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил РФ, других войск, воинских формирований и органов, предусмотренных ФЗ «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
- планах строительства Вооруженных Сил РФ, других войск РФ, 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;

- 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;
- 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;
- 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;
- 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 РФ 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;
- использовании инфраструктуры РФ в целях обеспечения обороноспособности и безопасности государства;
- 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 РФ в целях обеспечения безопасности государства;
- 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;

– достижениях науки и техники, о научно-исследовательских работах (НИР), об опытно-конструкторских работах (ОКР), о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;
– запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней РФ, Центральном банке РФ, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых РФ (по списку, определяемому Правительством РФ).

**3. Сведения в области внешней политики и экономики о:**

– внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства;
– 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 РФ, исключительной экономической зоны и континентального шельфа РФ;
- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в РФ;
- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства;
- о мерах по обеспечению защищенности критически важных объектов и потенциально опасных объектов инфраструктуры РФ 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. В силу выше сказанного, 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 РФ.

## 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;
- состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

- привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- фактах нарушения прав и свобод человека и гражданина;
- размерах золотого запаса и государственных валютных резервах РФ;
- состоянии здоровья высших должностных лиц РФ;
- фактах нарушения законности органами государственной власти и их должностными лицами.

Определив в ст. 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 котором 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 РФ, содержащей в части 3 ст. 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 ФЗ». Большое 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.

## 3.4 ПОРЯДОК ЗАСЕКРЕЧИВАНИЯ И РАССЕКРЕЧИВАНИЯ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

### Степени секретности сведений и грифы секретности

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 РФ 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 РФ в одной или нескольких из перечисленных областей.

К **секретным сведениям** следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности РФ 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 РФ вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством РФ.

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 РФ №870 от 04.09.1995).

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

## 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)**.**

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 РФ.

Для осуществления единой государственной политики в области засекречивания сведений создается **межведомственная комиссия по защите государственной тайны (**Указ Президента РФ «Вопросы межведомственной комиссии по защите государственной тайны» №1286).

**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 РФ (Указ Пре-

зидента РФ № 90 от 11.02.2006 г.), 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, ОКР и НИР по решению заказчиков указанных образцов и работ могут разрабатываться **отдельные перечни сведений, подлежащих засекречиванию.** Перечни утверждаются соответствующими руководителями органов государственной власти (Постановление Правительства РФ N 870 от 04.09.1995).

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 НИР и ОКР 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 РФ 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 РФ.

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, наде-

ленному 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.

### Порядок предварительного засекречивания сведений

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.

### 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 государствен-

ной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;
- органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
- регистрационном номере;
- 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 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 РФ.

## 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:
- взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну;
- изменение международной обстановки;
- изменение перечней сведений, подлежащих засекречиванию;
- окончание срока действия грифа;
- появление новых достижений в науке и технике;
- продажа или передаче вооружения другим странам;
- снятие оружия или боевой техники с вооружения;

– 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** РФ 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 РФ по рассекречиванию материалов, находящихся на хранении в закрытых фондах архивов.

Сохранены права фондообразователей по принятию решения на рассекречивание архивных материалов, что обеспечивает контроль процесса 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.

## 3.5 ДОПУСК И ДОСТУП К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ ГОСУДАРСТВЕННУЮ ТАЙНУ

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

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

Допуск граждан к государственной тайне на территории РФ 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 РФ 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.

## Организация доступа должностного лица или гражданина 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 РФ (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 РФ. 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.

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

Основанием для отказа должностному лицу или гражданину в допуске к государственной тайне является:

- 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 РФ;
- 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 РФ;
- 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.

## Порядок предоставления допуска должностного лица или гражданина к государственной тайне

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 (ФСБ) РФ 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 органи-

зациях, 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.**

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 вопросами 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 исполнения требований по допуску.

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 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 ст. 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 РФ «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 государ-

ственной тайны. Данная норма реализована постановлением Правительства РФ от 18.09.2006 г. № 573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и работникам структурных подразделений по защите государственной тайны».

## Допуск командированного лица к сведениям, составляющим государственную тайну

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 НИР и ОКР и т. п.). Предписание на выполнение задания, в котором 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.

## Порядок прекращения допуска должностного лица или гражданина к государственной тайне

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, под-

готовленное 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.

### 3.6 ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ПРОВЕДЕНИЮ РАБОТ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

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 № 333 от 15.04.1995 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 те-

чение установленного срока, в зависимости от специфики вида деятельности, но не более чем на 5 лет. Лицензия действует на всей территории РФ.

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, – ФСБ и ее территориальные органы (на территории РФ), Служба внешней разведки РФ (за рубежом);
- на право проведения работ, связанных с созданием средств защиты информации, – ФСТЭК России, Служба внешней разведки РФ, Министерство обороны РФ, ФСБ РФ (в пределах их компетенции);
- на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – ФСБ РФ и ее территориальные органы, ФСТЭК, Служба внешней разведки РФ (в пределах их компетенции).

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

## Порядок получения лицензии на ведение лицензионной деятельности

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 РФ 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 работников 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-х 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 уполномоченными государственными органами и согласовываются с Межведомственной комиссией.

## Государственная аттестация руководителей предприятий

Государственная аттестация руководителей предприятия организуется органами, уполномоченными на ведение лицензионной деятельности, а также министерствами и ведомствами РФ, руководители которых наделены полно-

мочиями 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 РФ;
- ликвидации предприятия.

### 3.7 ПРОВЕРКА НАЛИЧИЯ В ЗАЯВКАХ НА ВЫДАЧУ ПАТЕНТА НА ИЗОБРЕТЕНИЕ ИЛИ ПОЛЕЗНУЮ МОДЕЛЬ, СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

Правила проведения проверки наличия в заявках на выдачу патента на изобретение или полезную модель, сведений, составляющих государственную тайну, утверждены Постановлением Правительства РФ № 928 от 24.12.2007 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.

# 4 ОРГАНИЗАЦИЯ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ

ФЗ «О коммерческой тайне» № 98-ФЗ принят 29.07.2004 года (последняя редакция от 12.03.2014 г.).

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

Положения ФЗ №98 распространяются на информацию, составляющую КТ, независимо от вида носителя, на котором она зафиксирована.

Положения ФЗ №98 не распространяется на сведения, отнесенные в установленном порядке к государственной тайне.

## 4.1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В ФЗ «О коммерческой тайне» даны определения следующим терминам:

**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 КТ (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 КТ.

**Обладатель информации**, составляющей КТ – лицо, которое владеет информацией, составляющей КТ, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим КТ.

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

**Передача информации,** составляющей КТ – передача информации, составляющей КТ 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.

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

**Разглашение информации**, составляющей КТ – действие или бездействие, в результате которых информация, составляющая КТ, 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 К**Т**,** и на определение перечня и состава такой информации принадлежит обладателю такой информации

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

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

## 4.2 СВЕДЕНИЯ, КОТОРЫЕ НЕ МОГУТ БЫТЬ ОТНЕСЕНЫ К КОММЕРЧЕСКОЙ ТАЙНЕ

**Режим КТ 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 РФ 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 ФЗ.

## 4.3 ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ТРЕТЬИМ ЛИЦАМ

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

В случае отказа обладателя информации, составляющей КТ, предоставить ее органу государственной власти, иному государственному органу, ор-

гану местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

Обладатель информации, составляющей к КТ, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию, 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 РФ.

На документах, предоставляемых указанным выше органам и содержащих информацию, составляющую КТ, должен быть нанесен гриф «Коммерческая тайна» с указанием ее обладателя.

Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с ФЗ «О коммерческой тайне» и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей КТ, 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 ФЗ «О коммерческой тайне», а также не вправе использовать эту информацию в корыстных или иных личных целях.

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 РФ.

### 4.4 МЕРЫ ПО ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Меры по обеспечению конфиденциальности информации должны включать в себя:

- определение перечня информации, составляющей КТ;
- ограничение доступа к информации, составляющей КТ, путем установления порядка обращения с этой информацией и контроля соблюдения такого порядка;

– учет лиц, получивших доступ к информации, составляющей КТ, и (или) лиц, которым такая информация была предоставлена или передана;
– регулирование отношений по использованию информации, составляющей КТ, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
– нанесение на материальные носители, содержащие информацию, составляющую КТ, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации.

**Режим КТ считается установленным** после принятия обладателем информации, составляющей КТ, мер, указанных выше.

Обладатель информации, составляющей КТ, вправе применять методы технической защиты конфиденциальности этой информации, другие меры, не противоречащие законодательству РФ.

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

– исключается доступ к информации, составляющей КТ, любых лиц без согласия ее обладателя;
– обеспечивается возможность использования информации, составляющей КТ, работниками и передачи ее контрагентам без нарушения режима КТ.

### 4.5 ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В РАМКАХ ТРУДОВЫХ ОТНОШЕНИЙ

В целях обеспечения конфиденциальности информации работодатель обязан:

– ознакомить под расписку работника, доступ которого к информации, составляющей КТ, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей КТ, обладателями которой являются работодатель и его контрагенты;
– ознакомить под расписку работника с установленным работодателем режимом КТ и с мерами ответственности за его нарушение;
– создать работнику необходимые условия для соблюдения им установленного работодателем режима КТ.

Доступ работника к информации, составляющей КТ, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

В целях обеспечения конфиденциальности информации работник обязан:

– выполнять установленный работодателем режим КТ;

– не разглашать информацию, составляющую КТ, 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 КТ, либо уничтожить такую информацию или удалить ее с этих материальных носителей под контролем работодателя.

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.

Работник имеет право обжаловать в судебном порядке незаконное установление режима КТ в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

## 4.6 ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

Нарушение требований ФЗ «О коммерческой тайне» влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

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 РФ.

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.

Лицо, которое использовало информацию, составляющую КТ, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может быть привлечено к ответственности.

По требованию обладателя информации, составляющей коммерческую тайну, лицо, получившее доступ к информации, составляющей коммерческую тайну, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей КТ, вправе требовать в судебном порядке защиты своих прав.

# 5 ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ФЗ «О персональных данных» № 152-ФЗ принят 27.07.2006 г. (последняя редакция 21.07.2014 г.).

ФЗ «О персональных данных» регулирует отношения, связанные с обработкой ПДн государственными и муниципальными органами юридическими лицами и физическими лицами с использованием средств автоматизации и без использования таких средств.

Положения ФЗ «О персональных данных» не распространяются на отношения, возникающие при:

- обработке ПДн физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов ПДн;
- организации хранения, комплектования, учета и использования содержащих ПДн документов Архивного фонда РФ и других архивных документов в соответствии с законодательством об архивном деле в РФ;
- обработке ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;
- предоставлении уполномоченными органами информации о деятельности судов в РФ.

Целью ФЗ «О персональных данных» является обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайн.

## 5.1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В ФЗ «О персональных данных» используются следующие термины и определения:

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

**Обработка ПДн** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение,

использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

**Распространение ПДн** – действия, направленные на раскрытие ПДн неопределенному кругу лиц;

**Обезличивание ПДн** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

### 5.2 УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка ПДн допускается в следующих случаях:

- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;
- обработка ПДн необходима для осуществления правосудия, исполнения судебного акта;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно
- обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн;
- и др.

### 5.3 КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с ФЗ «О персональных данных» определены четыре категории ПДн:

*Специальные категории ПДн* – данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

*Биометрические ПДн* – данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн.

*Общедоступные ПДн* – ПДн субъектов ПДн, полученные только из общедоступных источников ПДн, созданных в соответствии со ст. 8 ФЗ «О персональных данных».

*Иные ПДн* – ПДн субъектов ПДн, не попадающие в выше перечисленные категории ПДн.

Обработка специальных категорий ПДн допускается в случаях, если:

- субъект ПДн дал согласие в письменной форме на обработку своих ПДн;
- ПДн, сделанные общедоступными субъектом ПДн;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн;
- обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг
- обработка ПДн осуществляется в соответствии с законодательством РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством РФ;
- и др.

### 5.4 СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн оператор вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований и в соответствии с ФЗ.

Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;
- цель обработки ПДн;

– перечень ПДн, на обработку которых дает согласие субъекта ПДн;
– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;
– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
– срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;
– подпись субъекта ПДн.

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

– подтверждение факта обработки ПДн оператором;
– правовые основания и цели обработки ПДн;
– цели и применяемые оператором способы обработки ПДн;
– наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании ФЗ;
– обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен ФЗ;
– сроки обработки ПДн, в том числе сроки их хранения;
– порядок осуществления субъектом ПДн прав, предусмотренных ФЗ «О персональных данных»;
– и др.

## 5.5 МЕРЫ, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОПЕРАТОРОМ ОБЯЗАННОСТЕЙ

Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных ФЗ. К таким мерам могут, в частности, относиться:

– назначение оператором ответственного за организацию обработки ПДн;
– издание оператором документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн;

– применение правовых, организационных и технических мер по обеспечению безопасности ПДн;
– осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ;
– оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ;
– ознакомление работников оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о ПДн.

Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн о реализуемых требованиях к защите ПДн.

## 5.6 МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

Оператор при обработке ПДн обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Обеспечение безопасности ПДн достигается, в частности:
– определением угроз безопасности ПДн при их обработке в информационных системах ПДн (ИСПДн);
– применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн;
– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
– оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
– учетом машинных носителей ПДн;
– обнаружением фактов НСД к ПДн и принятием мер;
– восстановлением ПДн, модифицированных или уничтоженных вследствие НСД к ним;
– установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– контролем принимаемых мер по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Правительство РФ с учетом возможного вреда субъекту ПДн, объема и содержания обрабатываемых ПДн, вида деятельности, при осуществлении которого обрабатываются ПДн, актуальности угроз безопасности ПДн устанавливает:

– уровни защищенности ПДн при их обработке в ИСПДн в зависимости от угроз безопасности этих данных;
– требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;
– требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн.

## Уровни защищенности персональных данных

В соответствии с Постановлением Правительства № 1119 от 01.10.2012 г. «Требования к защите персональных данных при их обработке в информационных системах персональных данных» при обработке ПДн в ИС устанавливаются 4 уровня защищенности ПДн.

При определении уровня защищенности ПДн учитываются:

1) тип актуальных угроз для ИСПДн;
2) категория ПДн, обрабатываемых в ИСПДн;
3) количество субъектов, ПДн которых обрабатываются в ИСПДн.

В Постановлении Правительства №1119 определены три типа актуальных угроз для ИС:

– угрозы 1-го типа – угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном ПО;
– угрозы 2-го типа – угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном ПО;
– угрозы 3-го типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО.

Актуальные угрозы определяются по результатам разработки модели угроз ПДн, обрабатываемых в ИСПДн. Модель угроз ПДн разрабатывается с учетом документа ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Категория ПДн и количество субъектов, ПДн которых обрабатываются в ИСПДн, определяются по результатам обследования ИСПДн.

## Требования к защите персональных данных при их обработке в информационных системах

Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, осуществляющее обработку ПДн по поручению оператора в соответствии с законодательством РФ.

Меры по обеспечению безопасности ПДн реализуются в рамках системы защиты ПДн и должны быть направлены на нейтрализацию актуальных угроз безопасности ПДн.

В состав мер по обеспечению безопасности ПДн, реализуемых в рамках системы защиты ПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности ПДн;
- обеспечение целостности ИС и ПДн;
- обеспечение доступности ПДн;
- защита среды виртуализации;
- защита ТС;
- защита ИС, ее средств, систем связи и передачи данных;
- выявление инцидентов ИБ;
- управление конфигурацией ИС и системы защиты ПДн.

Состав и содержание мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, приведены в приказе ФСТЭК № 21 от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

# 6 РАСПРЕДЕЛЕНИЕ ОБЯЗАННОСТЕЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

## 6.1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

Под предприятием будет пониматься любой объект, обрабатывающий материальные или информационные потоки. Вариант организационной структуры предприятия представлен на рисунке 2.

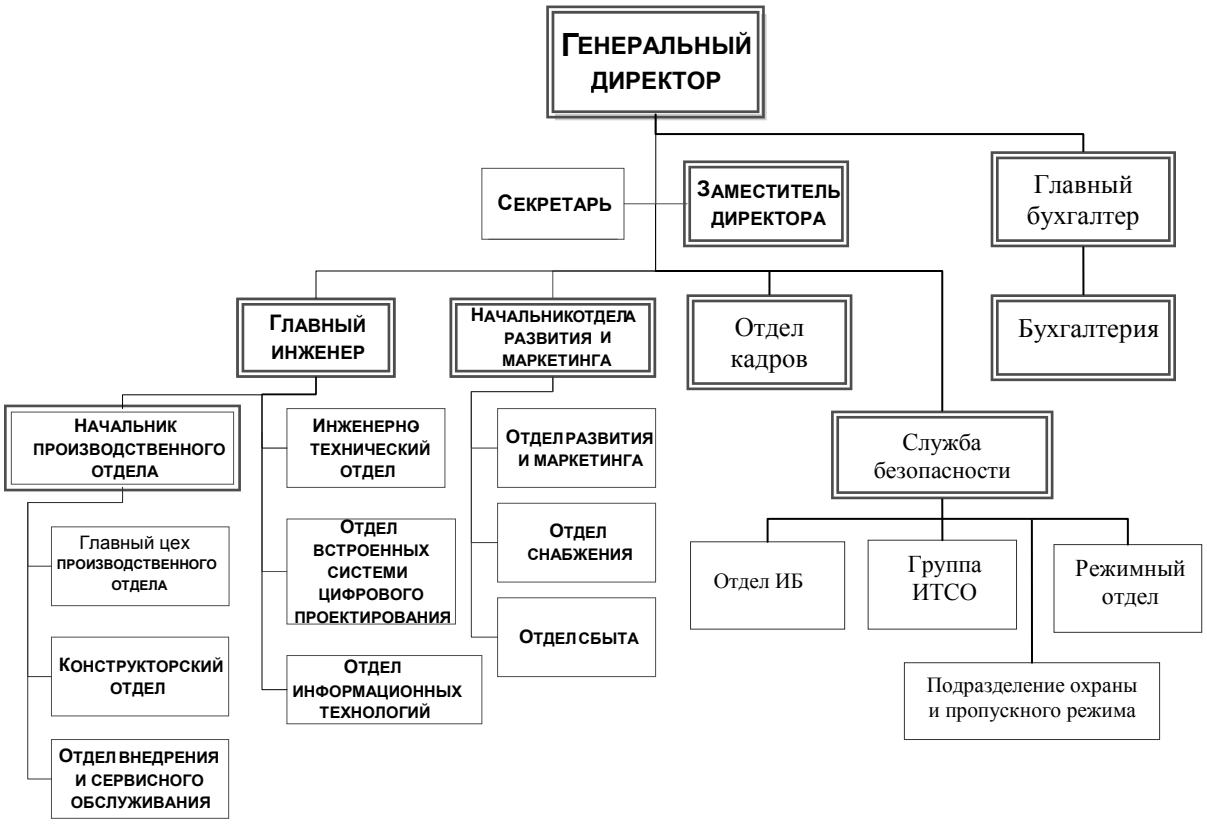



Рисунок 2 – Вариант организационной структуры предприятия

## 6.2 СТРУКТУРА СЛУЖБЫ БЕЗОПАСНОСТИ

Служба безопасности должна быть самостоятельным подразделением и подчиняться напрямую первому лицу на предприятии – генеральному директору или зам. генерального директора.

Структура Службы безопасности зависит от структуры и вида деятельности предприятия, численности персонала, защищаемой информации, активов (объектов защиты) и т.п.

При организации Службы безопасности разделяют подразделения, отвечающие за физическую безопасность и ИБ.

В большинстве случаев специалисты по защите информации не обладают должными знаниями в области обеспечения физической защиты объекта (предприятия) и, наоборот, подразделение охраны не занимается вопросами обеспечения ИБ в силу специфики последней. В тоже время подразделения охраны и ИБ должны работать скоординировано, что позволить повысить эффективность защиты предприятия в целом.

На небольших предприятиях (например, на предприятии численностью 50-100 человек и занимающем офисные помещения в бизнес-центре) функции Службы безопасности могут исполнять один или несколько человек, или подобные функции возлагаются на какого-либо работника предприятия.

Типовая структура Службы безопасности и ее варианты приведены на рисунках 3 и 4.


Рисунок 3 – Вариант организационно-штатной структуры Службы безопасности

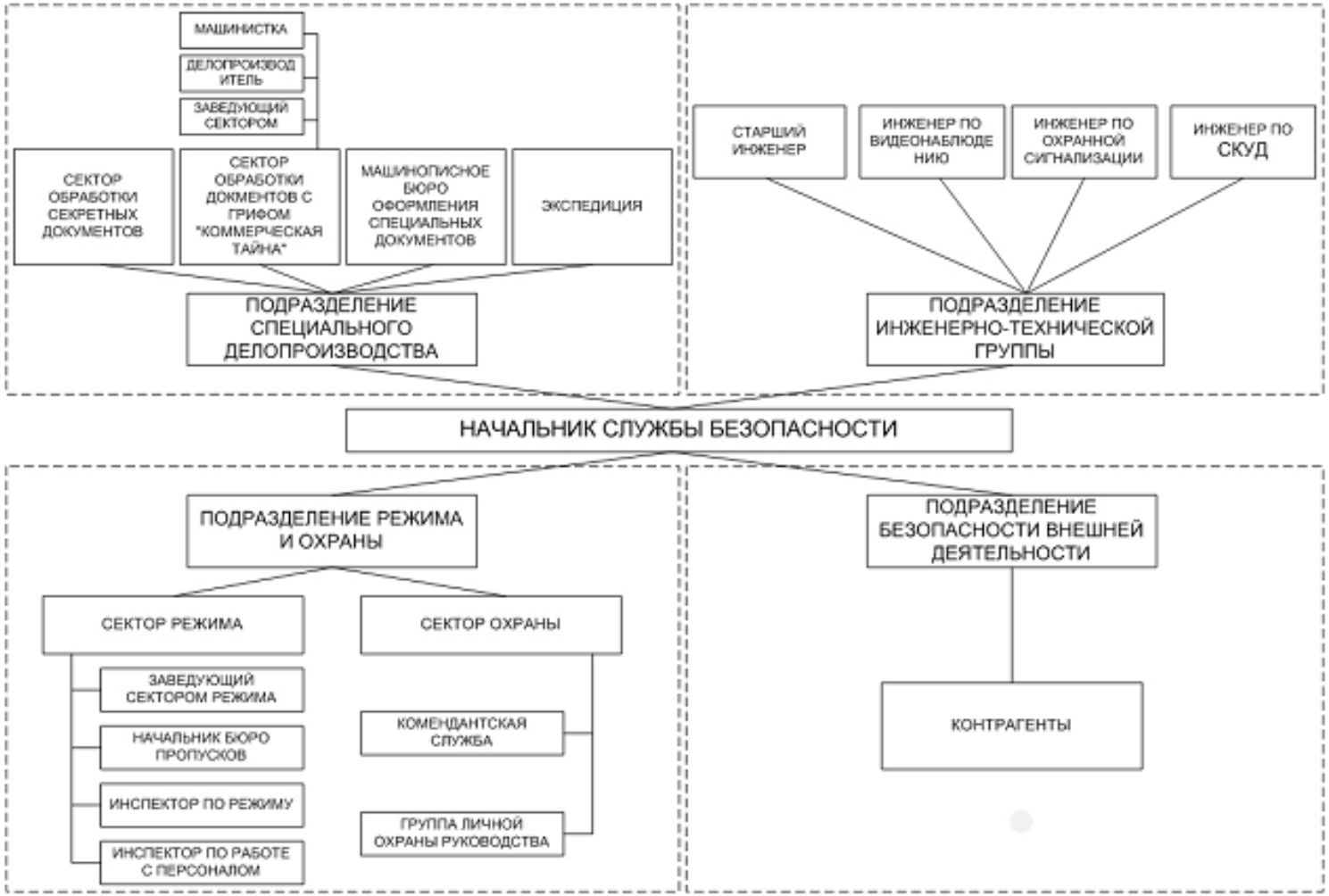



Рисунок 4 – Вариант организационно-штатной структуры Службы безопасности

### Задачи службы безопасности

На Службу безопасности предприятия возлагается выполнение следующих задач:

- определение основных направлений работы по обеспечению безопасности деятельности объекта и его персонала, а также соблюдение требований обеспечения информационной безопасности;
- организация мероприятий и координация работ всех подразделений и служб по обеспечению безопасности, контроль выполнения ими нормативных и организационно-распорядительных документов по защите информации.
- контроль и оценка эффективности принятых мер и средств защиты, применяемых для обеспечения непрерывности бизнес-процессов предприятия;
- организация системы защиты объекта (как физической, так и системы защиты информации), 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 организационно-распорядительной документации по обеспечению ИБ, физической безопасности;
- разработка мер безопасности и правил обработки, хранения и транспортировки материальных ценностей и ценных бумаг, контроль выполнения соответствующих нормативов;
- организация и обучение персонала объекта правилам соблюдения и поддержания режима безопасности, проведение квалифицированные тестов;
- расследование инцидентов, связанных с нарушением требований безопасности;
- организация и проведение совместно с другими подразделениями объекта мероприятий по обеспечению защиты;
- взаимодействие с правоохранительными органами по вопросам безопасности.

## 6.3 ФУНКЦИИ ОСНОВНЫХ ПОДРАЗДЕЛЕНИЙ СЛУЖБЫ БЕЗОПАСНОСТИ

В состав основных подразделений Службы безопасности входят:

1. подразделение специального делопроизводства (режима);
2. подразделение ИБ;

3. подразделение ИТСО и САЗ;
4. подразделение охраны и пропускного режима;
5. подразделение безопасности внешней деятельности.

***Функции подразделения специального делопроизводства (режим*а):**

- обработка поступающей и отправляемой корреспонденции, доставка ее по назначению;
- осуществление контроля сроков исполнения документов и соблюдения установленного порядка работы с секретными документами.
- организация работы по регистрации, учету и хранению документальных материалов текущего пользования;
- разработка номенклатуры дел, осуществление контроля правильного формирования дел в подразделениях и подготовкой материалов к своевременной сдаче в архив;
- разработка и внедрение предложений по совершенствованию системы делопроизводства;
- печать и размножение секретных документов и документов с грифом «Коммерческая тайна»;
- участие в подготовке созываемых и проводимых руководством закрытых совещаний и организация их технического обслуживания;
- и др.

Специальный отдел в части обеспечения обработки секретных документов руководствуется соответствующими документами, в части ведения делопроизводства с грифом «Коммерческая тайна» выполняет требования документов «Инструкция по защите коммерческой тайны».

***Функции подразделения ИБ::***

- разработка нормативных и организационно-распорядительных документов в области обеспечения ИБ с учетом требований законодательства РФ;
- организация и участие в работе по отнесению сведений к различным категориям информации ограниченного доступа, разработке перечней такой информации;
- организация и проведение процедуры оценки рисков ИБ;
- формирование требований к комплексной системе защиты информации, средствам управления и защиты информации;
- участие в проектировании, внедрении и вводе в эксплуатацию систем защиты информации;
- инициирование и проведение внешнего и/или внутреннего аудит ИБ предприятия;

– настройка и администрирование средств защиты информации (в случае если эти функции не возложены на отдел ИТ);
– контроль параметров настройки средств защиты информации;
– контроль ввода/вывода в/из эксплуатации объектов защиты с учетом требований ИБ;
– анализ журналов событий ИБ;
– расследование инцидентов ИБ;
– консультирование и проведение обучения работников предприятия по вопросам ИБ;
– и др.

***Функции подразделения ИТСО и САЗ***

Подразделение ИТСО и САЗ взаимодействует с группой охраны в рамках обеспечения безопасности предприятия.

В функции отдела ИТСО и САЗ входят:

– определение границ охраняемой (контролируемой) территории (зоны) с учетом возможностей технических средств, наблюдения злоумышленников;
– определение опасных, с точки зрения возможности образования каналов утечки, технических средств;
– формирование требований к ИТСО и САЗ, внедряемых на предприятие;
– локализация возможных каналов утечки организационными, организационно-техническими или техническими средствами и мероприятиями.
– организация наблюдения за возможным неконтролируемым излучением за счет побочных электромагнитных излучений и наводок;
– организация контроля наличия, проноса каких-либо предметов (устройств, средств, механизмов) в контролируемую зону, способных представлять собой технические средства несанкционированного получения конфиденциальной информации;
– участие в проектировании, наладке и вводе в эксплуатацию системы ИТСО и САЗ;
– настройка и администрирование ИТСО и САЗ;
– контроль выполнения требований предъявляемых в рамках обеспечения защиты с использованием ИТСО;
– обеспечение бесперебойной работы ИТСО и САЗ;
– разработка нормативной и организационно-распорядительной документации по использованию ИТСО и САЗ на предприятии;
– участие в расследованиях инцидентов, связанных с использованием ИТСО и САЗ.
– и др.

***Функции подразделения охраны и пропускного режима:***

- организация и поддержание пропускного и внутри объектного режима;
- выявление угроз безопасности объекта, защита от угроз и их ликвидация;
- организация и контроль прохода работников и посетителей в различные зоны безопасности;
- учет, контроль и наблюдение за охраняемыми зонами, помещениями, хранилищами, а также за обстановкой на территории объекта и вокруг него;
- прием под охрану и сдачу в эксплуатацию охраняемых помещений, проверяя при этом надежное срабатывание средств охраны, делая соответствующую запись в журнале приема и сдачи под охрану;
- выполнение мер по ликвидации возможных пожаров и других аварийных ситуаций в зонах безопасности предприятия.
- контроль работоспособности элементов ИТСО;
- обеспечение безопасности транспортировки ценных грузов и документов;
- участие в расследовании инцидентов связанных с нарушением безопасности объектов защиты.

В исключительных случаях подразделение 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).

Небольшие предприятия могут размещаться в одном здании с другими предприятиями. В этом случае возможно создание единого подразделения охраны и пропускного режима.

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

***Функции подразделения безопасности внешней деятельности:***

- изучение торгово-конъюнктурных ситуаций в пространстве деятельности учредителей, партнеров, клиентов и потенциально возможных конкурентов;
- ситуационный анализ текущего состояния финансово-торговой деятельности с точки зрения прогнозирования возможных последствий, могущих привести к неправомерным действиям со стороны конкурирующих организаций и предприятий;
- выявление платежеспособности юридических и физических лиц, их возможности по своевременному выполнению платежных обязательств.

– установление антагонистических конкурентов, выявление их методов ведения конкурентной борьбы и способов достижения своих целей;
– определение возможных направлений и характера злоумышленных действий со стороны специальных служб промышленного шпионажа против предприятия, его партнеров и клиентов.

## 6.4 РАЗГРАНИЧЕНИЕ ФУНКЦИЙ ПОДРАЗДЕЛЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Для понимания логики разделения функций по обеспечению ИБ подразделений ИБ и ИТ необходимо определить уровни (области) ответственности этих подразделений.

В организационную структуру подразделения ИТ входят:
– программисты;
– группа внедрения и сопровождения ПО (группа техподдержки);
– группа эксплуатации (обслуживания и ремонта) технических средств (ТС);
– администраторы прикладного и системного ПО, средств защиты.

В организационно-штатную структуру подразделения ИБ входят:
– аналитики;
– администраторы дополнительных средств защиты;
– специалисты по безопасности ИТ.

Организационную структуру системы обеспечения ИБ автоматизированной системы предприятия можно представить в виде совокупности следующих уровней:
– уровень 1 – Руководство организации.
– уровень 2 – Подразделение ИБ.
– уровень 3 – Администраторы штатных и дополнительных средств защиты.
– уровень 4 – Ответственные за обеспечение ИБ в подразделениях (на технологических участках).
– уровень 5 – Конечные пользователи и обслуживающий персонал.

Разграничение ответственности подразделений ИБ и ИТ в соответствии с уровнями ИБ представлено на рисунке 5.

**1. Уровень принятия решений**

Ответственные – руководство организации, руководители подразделений ИБ и ИТ.

Руководство организации – принимает стратегические решения по вопросам автоматизации и обеспечения ИБ, утверждает основные документы, регламентирующие порядок функционирования и развития ИС,

обеспечивающий безопасную обработку и использование защищаемой информации.

Руководители организации и подразделений ИБ и ИТ определяют критичность процессов, ресурсов и требуемую степень их защиты, а также координируют управление и распределение обязанностей подразделений ИБ и ИТ.

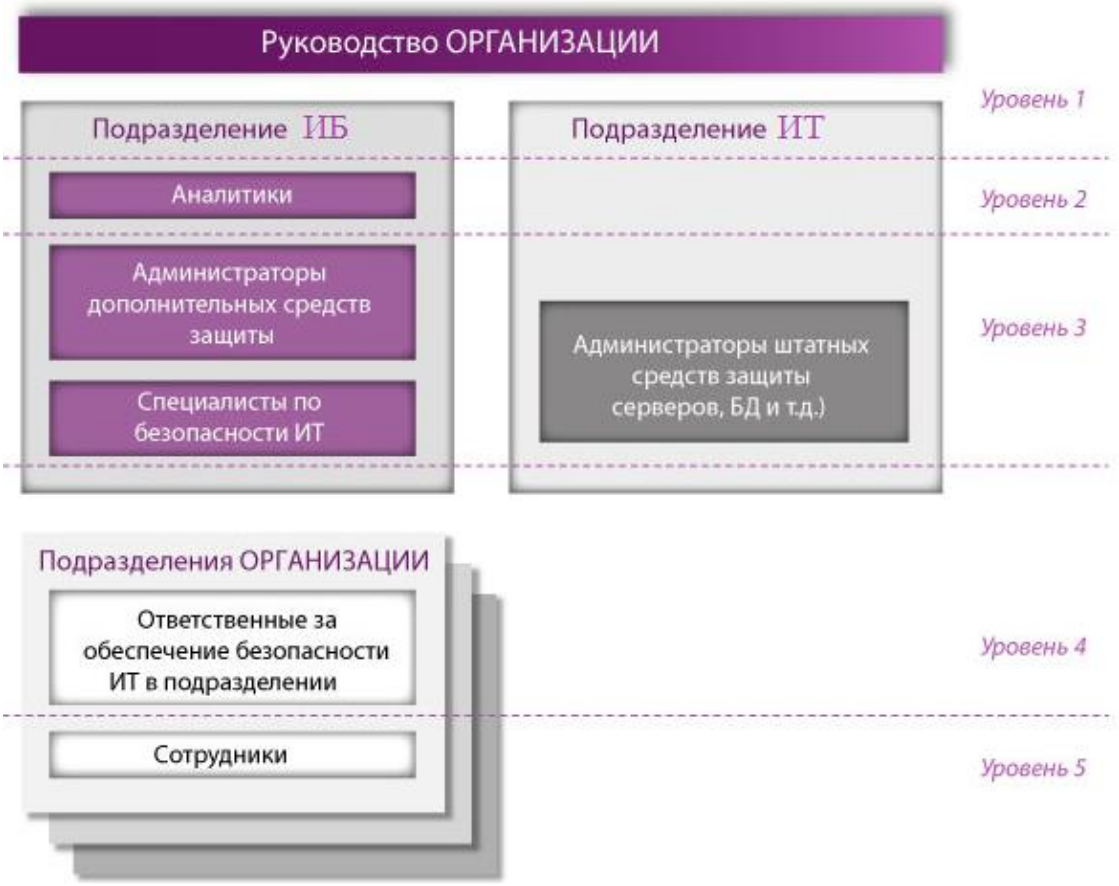



Рисунок 5 – Разграничение ответственности подразделений ИБ и ИТ в соответствии с уровнями по управлению ИБ

**2. Уровень подготовки информации для принятия решений.**

Ответственные – аналитики по вопросам безопасности ИТ.

Аналитики подразделений ИБ отвечают за анализ состояния безопасности ИТ, определение требований к защищенности различных подсистем ИС и выбор методов и средств защиты, разрабатывают регламенты (политики ИБ).

**3. Уровень организации и контроля исполнения решений.**

Ответственные:

– подразделение ИБ – администраторы дополнительных средств защиты, специалисты по безопасности ИТ;

– подразделение ИТ – системные и сетевые администраторы, администраторы серверов, приложений, баз данных.

Администраторы дополнительных средств защиты, контроля и управления безопасностью отвечают за эффективное применение специализированных средств защиты (влияют на безопасность и персонал через средства защиты).

Системные и сетевые администраторы, администраторы серверов, приложений, баз данных и т.п. отвечают за эффективное применение штатных (встроенных) средств защиты и разграничение доступа ко всем используемым ОС и СУБД.

**4. Уровень поддержки исполнения политики ИБ**

Ответственные – ответственные за обеспечение безопасности ИТ в подразделениях (на технологических участках).

Ответственные за обеспечение безопасности ИТ в подразделениях (на технологических участках) – это роль, возлагаемая на работника конкретного подразделения. Основные функции ответственных за обеспечение безопасности ИТ – доведение до работников подразделения требований ИБ, изложенных в регламентах, разработанных подразделением ИБ и утверждённых руководством.

**5. Уровень исполнения политики ИБ (работники)**

Ответственные – работники структурных подразделений (конечные пользователи системы и обслуживающий персонал, работающие со средствами автоматизированной обработки информации), которые решают свои функциональные задачи с применением средств автоматизации.

Работники структурных подразделений выполняют свои должностные и функциональные обязанности с учетом требований нормативных и организационно-распорядительных документах предприятия в области ИБ.

Сравнение функций по обеспечению ИБ подразделений ИБ и ИТ представлено в таблице 6.

Таблица 6 – Сравнение функций по обеспечению ИБ подразделений ИБ и ИТ

| **Подразделение ИБ** | **Подразделение ИТ** |
|---|---|
| Разработка нормативной и организационно-распорядительной документации по обеспечению ИБ | Участие в разработке нормативной и организационно-распорядительной документации по обеспечению ИБ |
| Оценка рисков ИБ | Участие в проведение оценки рисков ИБ |
| Формирование требований по обеспечению ИБ | Участие в формировании требований по обеспечению ИБ |
| Контроль выполнения требований по обеспечению ИБ | Выполнение требований по обеспечению ИБ |

| Подразделение ИБ | Подразделение ИТ |
|---|---|
| Контроль параметров настройки средств защиты информации, анализ журналов событий ИБ | Настройка и администрирование средств защиты информации |
| Настройка и администрирование *дополнительных* средств защиты информации (криптографические средства защиты, системы автоматизации процессов управления ИБ и др.) | |
| Организация и участие в расследованиях инцидентов ИБ | Участие в расследовании инцидентов ИБ |

Как видно из таблицы 6 подразделение ИТ должно выполнять требования по обеспечению ИБ, в то время как на подразделение ИБ возлагаются функции по формированию требований по обеспечению ИБ и контролю их выполнения.

## 6.5 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:
   – работники 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 работниками других предприятий, общественных организаций, общественных движений, партий;

– работники 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.

## ВЫВОДЫ

Распределение функций и обязанностей по обеспечению безопасности позволяет организовать эффективную систему защиты предприятия.

Цели, задачи и функции подразделений, участвующих в обеспечении безопасности, должны быть прописаны в положениях о подразделениях и утверждены руководством предприятия.

Должно быть четкое распределение обязанностей по выполнению и контролю выполнения требований безопасности между работниками подразделений. Не допускается возложение этих обязанностей на одного работника в рамках одного процесса обеспечения безопасности (например, настройка политик безопасности антивирусного ПО и контроль выполнения требований по защите от вредоносного ПО осуществляется разными работниками). Обязанности по выполнению требований безопасности должны быть прописаны в соответствующих инструкциях, например в должностных инструкциях, инструкции администратора безопасности, инструкции администратора средств защиты и т.д.

# 7 ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛОМ

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

Только 25% работников являются 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 работниками.

## 7.1 ПРОВЕРКА ПЕРСОНАЛА ПРИ ПРИЕМЕ НА РАБОТУ

В приеме на работу новых работников 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 работника на работу, обеспечивает проверку соответствия работника квалификационным требованиям, предусмотренным должностными инструкциями, проверяет наличие соответствующих документов.

Начальник подразделения, в котором принимаемый работник 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 работником 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 предоставленных кандидатом документах.

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 п**редполагает 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.***

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

## 7.2 РАБОТА С РАБОТНИКАМИ ПРЕДПРИЯТИЯ

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

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

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

1. Проверка – 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. Качественный подбор и изучение кандидатов при приеме на работу.

# 8 ОРГАНИЗАЦИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

## 8.1 ЗОНЫ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В соответствии с ГОСТ Р ИСО/МЭК 27002-2012 «Методы и средства обеспечения информационной безопасности. Свод норм и правил менеджмента информационной безопасности» целью обеспечения физической безопасности предприятия является предотвращение неавторизированного физического доступа, повреждения и воздействия в отношении помещений и информации 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.

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

При формировании зон безопасности необходимо учитывать:

- помещения и участки разного значения;
- материальные потоки, информацию (документы, телефонные, телефаксные, компьютерные и радиоканалы связи), циркулирующие между помещениями и внутри них;
- транспорт, перемещающийся через границу предприятий;
- наличие посетителей.

В понятие помещения и участки различного назначения входят:

- кабинет руководящего состава и совещательные комнаты;
- кабинеты работников 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.

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.

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. 6).

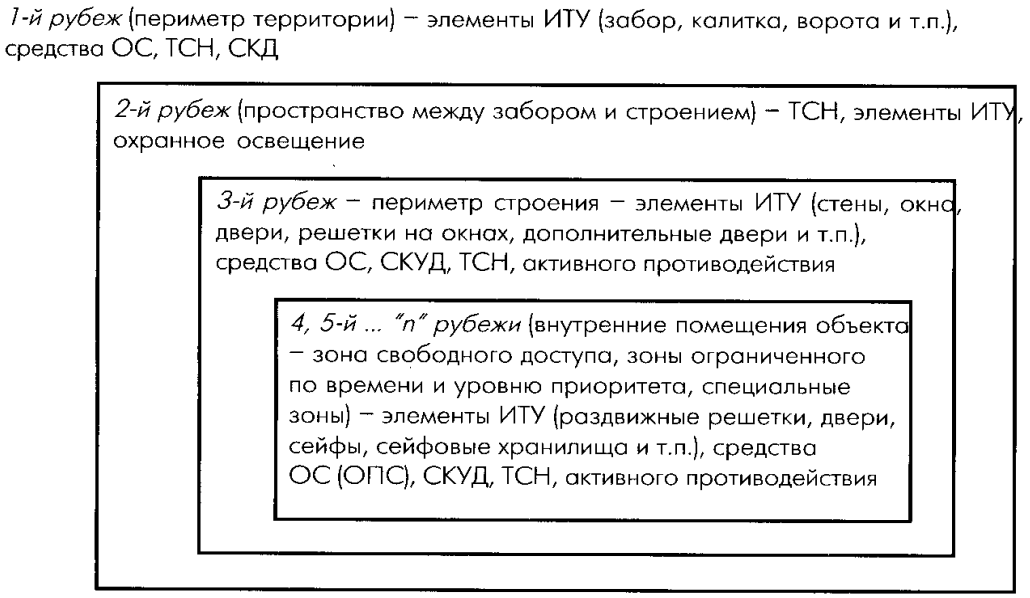



Рисунок 6 – Принцип формирования зон безопасности

Последнее особенно актуально для предприятий, занимающих большую территорию, имеющих большое количество работников, а также в случае, когда предприятие не имеет физической границы. Пример формирования зон безопасности конкретного предприятия показан на рисунках 7 и 8.

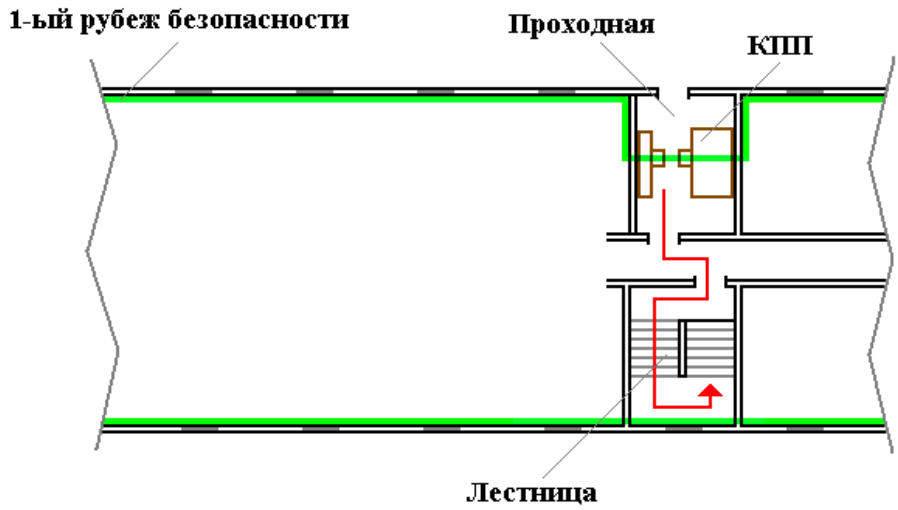



Рисунок 7.1 – Пример формирования зон безопасности офиса, расположенного на арендуемых площадях (1-й этаж)

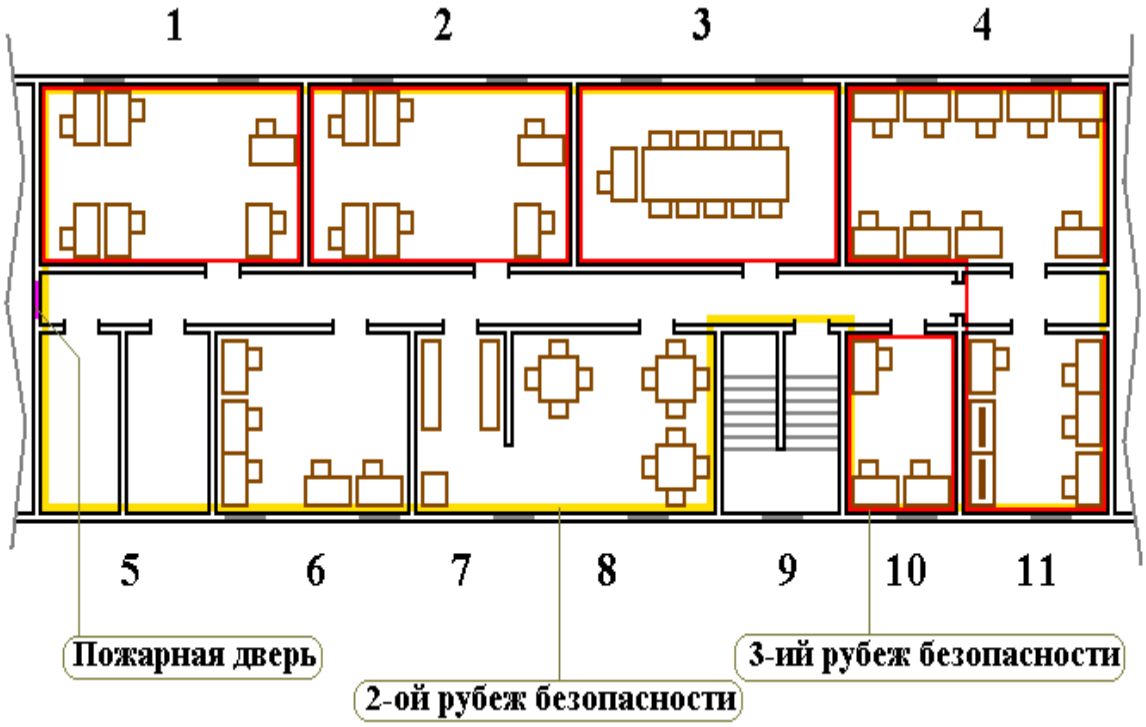
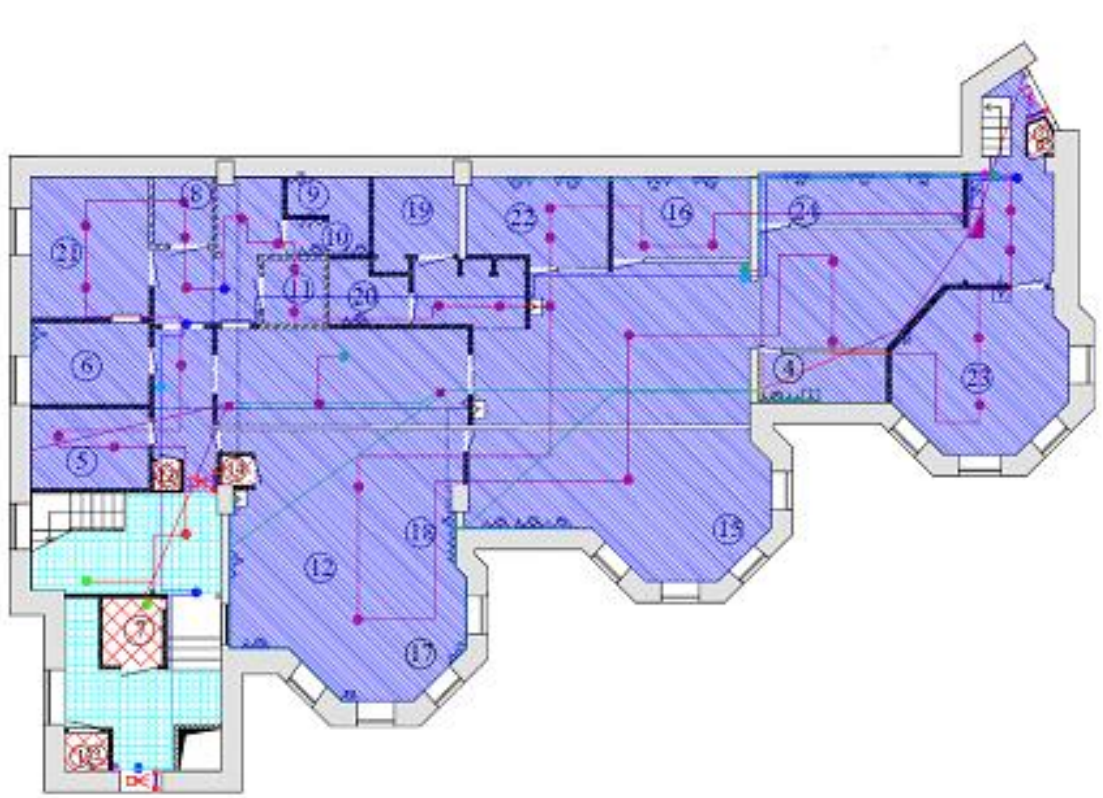



Рисунок 7.2 – Пример формирования зон безопасности офиса, расположенного на арендуемых площадях (2-й этаж)

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 зав. 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 по производству | 12.20 |
| 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 |
| 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 32x16
- 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 8 – Пример формирования зон безопасности в здании офиса

## 8.2 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ И СРЕДСТВА АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИТЫ

Для обеспечения физической защиты зон безопасности на предприятии используются системы инженерно-технических средств охраны и средства антитеррористической защиты (ИТСО и САЗ).

ИТСО и САЗ – понятие, объединяющее средства, системы и специальные конструкции, применяемые для обеспечения безопасности охраняемых объектов от несанкционированного нарушения их границ, хищения материальных и иных ценностей и от проведения террористических актов.

Функционально ИТСО и САЗ делятся на:

- инженерные средства охраны;
- технические средства охраны;
- средства антитеррористической защиты.

**Инженерные средства охраны** – защитные и преграждающие средства и конструкции, обеспечивающие задержку или блокирование несанкционированных действий или проникновения на охраняемый объект или в зону.

**Технические средства охраны** – технические средства и системы обнаружения факта несанкционированного нарушения или попытки нарушения границ охраняемой зоны либо режима охраняемого объекта, формирования извещений об этом факте для принятия соответствующих решений, обработки, приема-передачи и регистрации информации о тревожных сообщениях.

**Средства антитеррористической защиты** – конструкции, средства и системы обнаружения признаков подготовки и осуществления террористических актов, а также противодействия и уменьшения возможных последствий их осуществления.

Выбор ИТСО и САЗ для различных объектов определяется их категорией, вероятными угрозами, концепцией обеспечения безопасности, способом охраны, условиями эксплуатации и обслуживания, помехами, присутствующими на объекте, архитектурно-планировочными решениями, а также рядом других факторов, которые необходимо учитывать при проектировании системы безопасности объекта.

Комплекс ИТСО предназначен для выполнения следующих задач:

- обнаружение несанкционированного проникновения;
- обнаружение несанкционированных действий;
- осуществление контроля и управления доступом;
- контроль и обнаружение проноса запрещенных предметов.

В состав комплекса ИТСО входят системы, комплексы и технические средства, предназначенные для выполнения соответствующих функций по обеспечению охраны объекта:

- системы охранной сигнализации;
- системы контроля и управления доступом
- системы охранные телевизионные;
- системы постовой связи;
- системы охранного освещения;
- системы сбора, обработки и отображения информации;
- системы электропитания, заземления и молниезащиты технических средств охраны и антитеррористической защиты;
- САЗ.

# 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 работников, посетителей, транспорта;
- контроль перемещения через границу предприятия материальных и финансовых ценностей;
- поддержание соответствующего режима и состояния территории внутри предприятия.

## 9.1 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

В перечень объектов охраны предприятия входят:

- территория предприятия;
- расположенные на территории предприятия объекты (здания, сооружения);
- носители конфиденциальной информации (документы, технические средства);
- материальные ценности (грузы, технические средства обработки информации, средства производства и т.п.);

– руководство предприятия персонал, допущенный к конфиденциальной информации.

Организация охраны руководства и работников предприятия регулируются отдельным положением (инструкцией), которое утверждается руководителем 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

## Цели охраны предприятия

Целями охраны предприятия являются:

– 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.

## Задачи охраны предприятия

Основными задачами охраны предприятия являются

– 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 ввоза/вывоза 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.

### Руководство организацией охраны предприятия

Возлагается на заместителя руководителя предприятия по безопасности, или начальника службы безопасности. 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 работник, либо по графику дежурство возлагается на заместителей руководителя предприятия или руководителей крупных структурных подразделений.

## 9.2 СИСТЕМА ОХРАНЫ ПРЕДПРИЯТИЯ

**Система охраны предприятия** – совокупность используемых для охраны предприятия сил и средств, а также способов и методов охраны предприятия и его объектов. Система охраны предприятия 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) работников 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).

В своей деятельности по выполнению задач охраны предприятия работники 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 работников 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.

**Работники 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 РФ, применять физическую силу, специальные средства и огнестрельное оружие.

Права и обязанности работников 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 ФЗ «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 законодательством осуществлять этот вид деятельности. Порядок оказания услуг такими предприятиями, права и обязанности их работников при выполнении задач охраны объектов определены Законом РФ № 2487-1 «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 работниками 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 РФ.

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 работниками 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 работники 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 упоминавшийся 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 работники предприятия, способные в любых условиях обеспечить сохранность перевозимого имущества. Работники 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 работников 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 работники охраны обязаны путем применения всех имеющихся средств и способов охраны обеспечить защиту указанных лиц, исключить хищение имущества или завладение им посторонними лицами (злоумышленниками).

## 9.3 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 работников 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 работников охраны, либо через автоматизированные посты, оборудованные соответствующими техническими средствами.

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

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

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 работника пропуск должен сдаваться в службу безопасности.

Существуют 3 вида пропусков:

- постоянный;
- временный;
- разовый.

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

При выдаче пропуска работник должен обязательно знакомиться под расписку с правилами внутреннего распорядка.

При утере пропуска проводится служебное расследование. На период проведения служебного расследования работнику 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 работника (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 работника 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.

Работники, 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.

Работники МЧС, скорой помощи проезжают на собственной машине в сопровождении работников 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 работники 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 документов 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 составляться 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 работниками других предприятий рекомендуется оборудовать специальные изолированные комнаты переговоров, расположенные на нережимной территории предприятия.

## 9.4 ОРГАНИЗАЦИЯ ВНУТРИОБЪЕКТОВОГО РЕЖИМА

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

Учет посещений 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.

Работники 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 работников в выходные и праздничные дни. Такое нахождение допускается в исключительных случаях по производственной необходимости и строго индивидуально по предварительному согласованию.

Отдельно должен быть оговорен пронос на территорию предприятия (без соответствующего разрешения) личной кино- и фотосъемочной аппаратуры, звуко- и видеозаписывающей аппаратуры, множительной, 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 работника, 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 работника, 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 работников, вскрытие помещений, спасение документов и изделий.

# 10 ОРГАНИЗАЦИЯ ЗАЩИТЫ 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;
- защита диссертаций, дипломных проектов, если они содержат государственную тайну;
- лекции по закрытой тематике.

Совещания могут проводиться как среди работников предприятия (внутренние совещания), так и с привлечением работников сторонних предприятий или даже работников 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 работников предприятия, проводящего совещание, так и сторонних предприятий. 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 работников 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 работников 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.

Выше перечисленные обстоятельства усложняют задачи и ужесточают требования по защите информации, прежде всего требования по защите помещений перед проведением совещания, а также требования по 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 работники, не имеющие на него допуск, могли покинуть помещение.

За соблюдением режима конфиденциальности при проведении совещания отвечает специально назначенный работник из работников службы безопасности или участников совещания.

# 11 ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРЕДСТАВЛЕНИИ ЕЁ В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

Деятельность средств массовой информации (СМИ) регламентируется Федеральным законом № 2124-I от 27.12.1997 «О средствах массовой информации» (последняя редакция от 30.12.2015). Вопросы защиты государственной и иной защищаемой законом тайны прописаны в законе декларативно.

СМИ 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 услуги по регистрации средств массовой информации (приказ Министерства связи и массовых коммуникаций РФ от 29.12.2011 г. № 362).

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

В соответствии с ФЗ РФ «О средствах массовой информации» не требуется регистрация:

- СМИ, учреждаемые 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 работников этих предприятий.

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 СМИ 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.

В соответствии ФЗ не допускается использование СМИ 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.

## 11.1 ПРЕДОСТАВЛЕНИЕ РЕЗУЛЬТАТОВ НАУЧНОЙ, ПРОИЗВОДСТВЕННОЙ ИНОЙ ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИИ В СМИ

Одним из направлений утечки конфиденциальной информации может служить ее публикация в СМИ – статьях, рекламе, 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 СМИ и печать традиционно являются самыми ёмкими и наиболее используемыми каналами получения информации. При грамотно организованном поиске в СМИ можно получить информацию широкому кругу вопросов, интересующих разведывательные подразделения конкурирующих фирм.

Исполнение основных правил предоставления результатов научной, производственной иной деятельности информации в СМИ, позволяющих исключить или уменьшить вероятность попадания в СМИ 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 работники службы безопасности.

Экспертное заключение утверждается руководителем предприятия.

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

## 11.2 СБОР ИНФОРМАЦИИ СИЛАМИ ПРЕДПРИЯТИЯ

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.

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 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.

При невозможности выделения отдельной штатной единицы для работы с прессой, эта работа может быть распределена между работниками 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.

## 11.3 СБОР ИНФОРМАЦИИ С ПРИВЛЕЧЕНИЕМ СТОРОННИХ ФИРМ

В ряде случаев информация может приобретаться предприятием на стороне. Эту работу целесообразно поручить специально подготовленным ра-

ботникам, так как сам факт сбора информации является «демаскирующим» признаком.

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

За относительно невысокую плату можно приобрести информацию в редакциях изданий. Сегодня при газетах, службах новостей очень часто имеются подразделения, в которых 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 недорого и достаточно профессионально выполнят мониторинг требуемых изданий, в том числе и иностранных.

Большое значение имеет при сборе информации соблюдение режима конспирации для того, чтобы исполнители не имели представления, для кого и с какой целью они это делают.

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.

# 12 ОРГАНИЗАЦИЯ ЗАЩИТЫ 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 ФЗ «О рекламе» от 13.03.2006 № 38-ФЗ.

В соответствии со ст.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 РФ с иностранными государствами;
- оружия, не указанного в частях 3 - 5 статьи ФЗ.

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

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 РФ о военно-техническом сотрудничестве РФ, 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 ст. 26 прямо указывает на запрет в рекламе сведений, прямо или косвенно раскрывающих **государственную тайну.**

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

– товаров, производство и (или) реализация которых запрещены законодательством РФ;
– 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.

# 13 ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организация обеспечения безопасности информации должна носить комплексный характер и основываться на результатах оценки рисков ИБ.

В начале 1960-х годов на атомных электростанциях Европы и Америки стала использоваться оценка рисков, которая впоследствии развивалась и стала применяться аэрокосмической инженерии, химической промышленности, охране окружающей среды, здравоохранении, спорте, развитии национальной экономики и многих других областях.

Оценка рисков осуществляется с целью прогнозирования возможного ущерба, связанного с реализацией угроз, и соответственно оценки необходимого размера инвестиций на построение систем защиты информации.

Предприятия любого типа и величины:

- собирают, обрабатывают, хранят и передают большое количество информации;
- понимают, что информация и относящиеся к ней процессы, системы, сети и персонал являются важными ресурсами для решения задач, стоящих перед организацией;
- сталкиваются с рядом рисков, которые могут оказывать воздействие на функционирование активов предприятия;
- ослабляют риски, осуществляя управление ИБ.

Предприятие осуществляет защиту активов (информации) с целью:

- достижения целей и задач обработки информации;
- выполнения требований законодательства;
- поддержания репутации.

В процессе оценивания рисков определяются характеристики рисков по отношению к активам предприятия. На основе полученных данных могут быть выбраны необходимые средства защиты. При оценивании рисков учитываются многие факторы: ценность активов, оценка значимости угроз и уязвимостей, эффективность существующих и планируемых средств защиты и многое другое.

Под **риском** понимается сочетание вероятности события и его последствий [ГОСТ Р ИСО/МЭК 27002-2012 «Свод норм и правил менеджмента информационной безопасности»].

Под **риском ИБ** понимается потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для предприятия [ГОСТ Р

ИСО/МЭК 27005-2010 «Менеджмент риска информационной безопасности»].

Процесс оценки рисков ИБ представлен на рисунке 9.

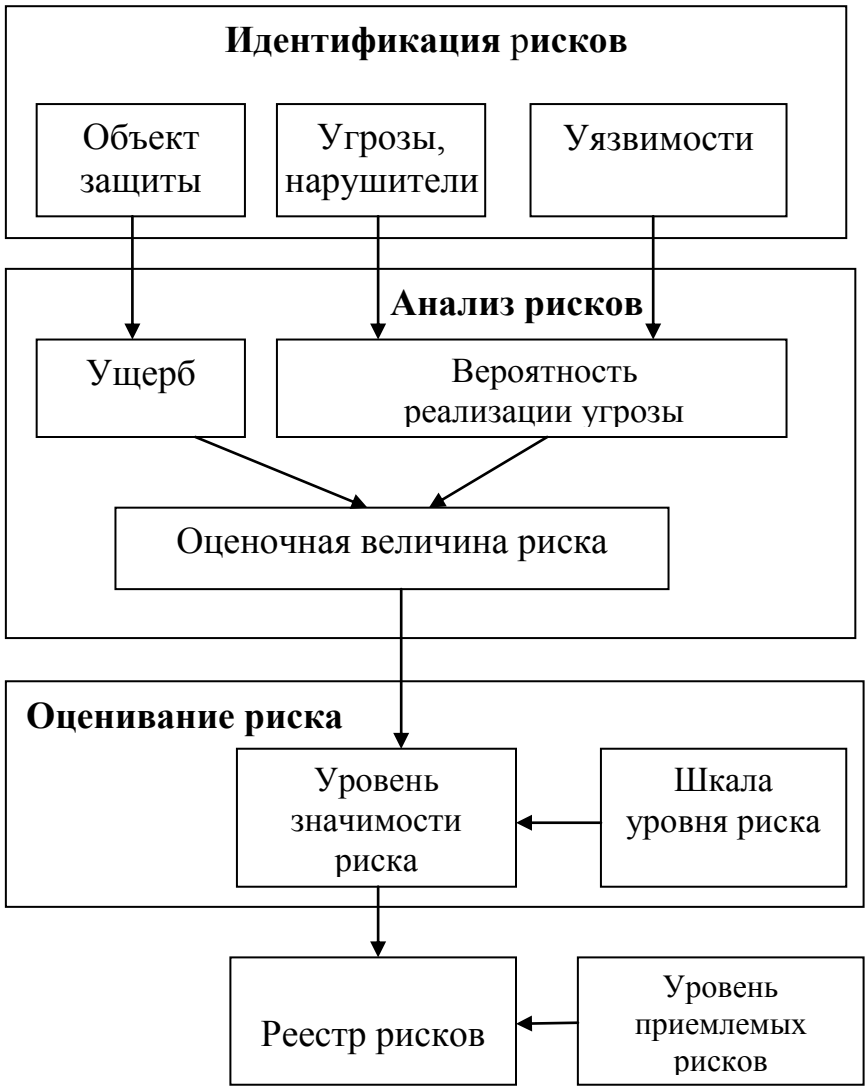



Рисунок 9 – Процесс оценки рисков ИБ

## 13.1 ИДЕНТИФИКАЦИЯ РИСКОВ

Идентификация риска заключается в составлении перечня и описании элементов риска:

- объектов защиты;
- угроз и нарушителей безопасности;
- уязвимостей.

На этапе идентификации рисков так же выполняется идентификация угроз и уязвимостей. В качестве исходных данных для этого используются:

- результаты аудитов;

– данные об инцидентах ИБ;
– экспертные оценки пользователей, специалистов по информационной безопасности, ИТ-специалистов и внешних консультантов.

### *Классификация объектов защиты*

Актив (объект защиты) – что-либо, что имеет ценность для организации [ГОСТ Р ИСО/МЭК 27002-2012 «Свод норм и правил менеджмента информационной безопасности»]:

– информационные активы:
  – файлы;
  – документы;
  – файловые хранилища;
  – сообщения;
  – базы данных;
  – и др.
– ПО:
  – системное ПО;
  – прикладное ПО;
  – вспомогательное ПО;
  – утилиты;
  – средства защиты информации;
  – и др.
– ТС:
  – автоматизированные рабочие места;
  – ноутбуки;
  – серверы;
  – каналы связи;
  – роутеры;
  – коммутаторы;
  – маршрутизаторы;
  – съемные носители информации;
  – мобильные устройства связи;
  – принтеры;
  – и др.
– бизнес-процессы;
– люди и их квалификация, навыки и опыт;
– нематериальные активы, такие как репутация и имидж.

При обеспечении физической защиты предприятия и его объектов в качестве объектов защиты могут рассматриваться: прилегающая территория, помещения, склады, кабинеты, офисы и т.п.

### *Классификация угроз безопасности*

**Угроза** – потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации [ГОСТ Р ИСО/МЭК 27002-2012 «Свод норм и правил менеджмента информационной безопасности»].

**Угроза безопасности информации** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [ГОСТ Р 5646-2015 «Классификация уязвимостей информационных сетей»].

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. Источником таких угроз называют нарушителем;
- преднамеренные или умышленные угрозы (угрозы, при которых человек сознательно искажает, портит, крадет информацию и т.д.). Источника таких угроз называют злоумышленником.

Умышленные угрозы могут проявляться путем:

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

Классификация угроз безопасности с учетом вида воздействия угроз, источника и объекта угрозы представлена на рисунке 10.

Перечень типовых угроз безопасности в себя включает:

1. физические угрозы:

- физический НСД в помещения, серверные, к бумажным носителям, ТС, съемным носителям информации;
- кража или повреждение ТС;
- физический доступ к комплексу средств защиты с целью переконфигурирования или создания обхода средств защиты;
- кража бумажных носителей.

2. нецелевое использование компьютерного оборудования и сети Интернет работниками предприятия:

- злоупотребление средствами аудита, средствами обработки информации;

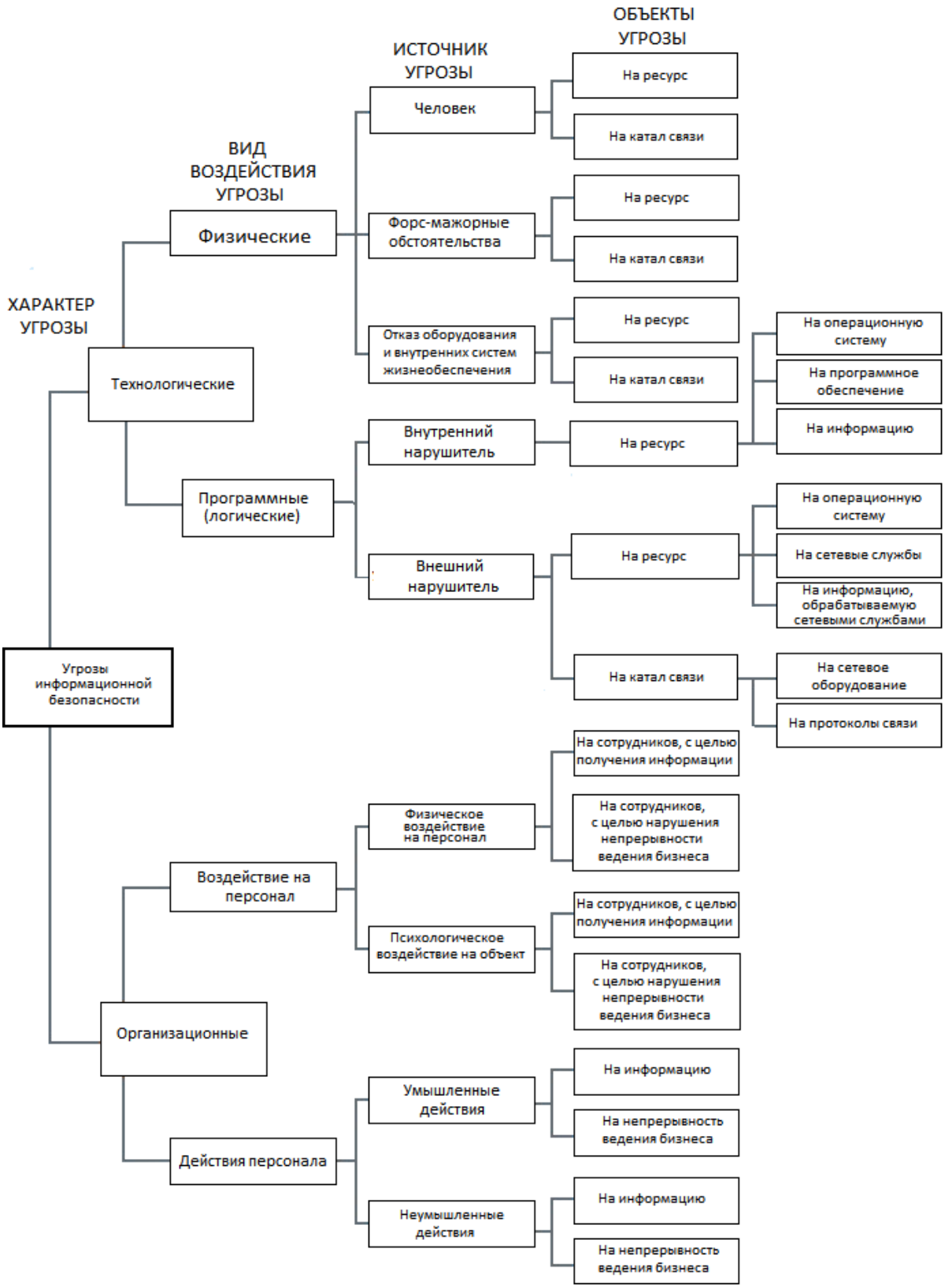



Рисунок 10 – Классификация угроз безопасности с учетом вида воздействия угроз, источника и объекта угрозы

– нецелевое использование Интернет-ресурсов и информационных активов;
– несанкционированное использование ПО
– и др.

3. Угрозы утечки конфиденциальной информации;

– перехват информации, передаваемой по каналам связи;
– нарушение конфиденциальности данных, передаваемых за пределы контролируемой зоны;
– нарушение конфиденциальности данных, передаваемых в пределах контролируемой зоны;
– утечка конфиденциальной информации, хранимой на съемных носителях, ноутбуках и мобильных устройствах;
– и др.

4. Угрозы утечки информации по техническим каналам:

– угроз утечки акустической (речевой) информации;
– угроз утечки видовой информации;
– угроз утечки информации по каналам побочных электромагнитных излучений и наводок.

5. Угрозы НСД:

– угроза доступа (проникновения) в операционную среду компьютера с использованием штатного ПО (средств операционной системы или прикладных программ);
– угроза создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
– угрозы внедрения вредоносных программ (программно-математического воздействия):
– НСД к резервным копиям;
– НСД К беспроводной сети;
– НСД к журналам аудита;
– и др.

6. Угрозы недоступности ИТ-сервисов и разрушения (утраты) информационных активов:

– атаки на отказ в обслуживании;
– повреждение носителей информации;
– сбой сетевого оборудования;
– недоступность ИТ-сервисов в результате тестирования на проникновение;

– умышленная порча ПО и резервных копий;
– сбой системы кондиционирования
– и др.

7. Угрозы нарушения целостности и несанкционированной модификации данных:

– нарушение целостности в результате ошибок пользователей;
– несанкционированная модификация журналов аудита
– фальсификация записей;
– нарушение целостности систем и данных, модификация системной конфигурации, файлов баз данных, отчетов и др. в результате ошибок технического персонала.

8. угрозы антропогенных и природных катастроф:

– военные действия, терроризм;
– забастовки;
– природные катастрофы (затопление, пожар, землетрясение и др.)
– и др.

9. Юридические угрозы:

– нарушение (несоответствие требованиям) законодательства;
– несанкционированное использование информационных материалов, являющихся интеллектуальной собственностью;
– нелегальное использование ПО;
– и др.

Предприятие может самостоятельно выбирать соответствующие подходы к оценке и управлению рисками, учитывающие и идентифицирующие полный диапазон угроз и уязвимостей, имеющих отношение к его бизнес-окружению. Для оценки рисков может использоваться как полный перечень угроз, так и его часть.

### *Классификация источников угроз*

**Источник угрозы** – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации – внутренние источники, так и вне ее – внешние источники.

Деление источников на субъективные и объективные оправдано исходя из определения вины или риска ущерба информации.

Деление источников на внутренние и внешние оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников могу быть разными [1].

Все источники угроз безопасности информации можно разделить на три основные группы:

- обусловленные действиями субъекта (антропогенные источники угроз);
- обусловленные техническими средствами (техногенные источники угроз);
- обусловленные стихийными источниками.

Классификация источников угроз представлена на рисунке 11.

***Антропогенные источники угроз***

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорить о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от заинтересованности руководства в обеспечении ИБ.

Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние субъекты (источники) могут быть случайными или преднамеренными и иметь разный уровень квалификации

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации ПО и ТС, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и ТС сети.

***Техногенные источники угроз***

Группа техногенных источников угроз содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Последствия, вызванные такой деятельностью, могут выйти из-под контроля человека и существовать сами по себе. Такие источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.


Рисунок 11 – Классификация источников угроз

ТС, являющиеся источниками потенциальных угроз безопасности информации, так же могут быть внешними и внутренними.

***Стихийные источники угроз***

В группе стихийные источники угроз объединяются обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности, как правило, являются внешними по отношению к защищаемому объекту и под ними понимаются, прежде всего, природные катаклизмы.

## *Классификация уязвимостей*

**Уязвимость** – слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами [ГОСТ Р ИСО/МЭК 27002-2012 «Свод норм и правил менеджмента информационной безопасности»].

В ГОСТ Р 56546-2015 «Классификация уязвимостей информационных систем» дано следующее определение уязвимости – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Уязвимости могут быть выявлены в следующих областях:

- организация работ;
- процессы и процедуры;
- установившийся порядок управления;
- персонал;
- физическая среда;
- конфигурация ИС;
- аппаратные средства, ПО и аппаратура связи;
- зависимость от внешних сторон

В соответствии с ГОСТ Р 56546-2015 уязвимости ИС по области происхождения подразделяются на следующие классы:

- уязвимости кода;
- уязвимости конфигураций;

– уязвимости архитектуры;
– организационные уязвимости;
– многофакторные уязвимости.

Уязвимости по типам недостатков ИС подразделяют на недостатки связанные с:

– неправильной настройкой параметров ПО;
– возможностью прослеживания пути доступа к каталогам;
– возможностью внедрения команд операционной системы;
– переполнением буфера памяти;
– внедрением произвольного кода;
– приводящие к утечке/раскрытию информации ограниченного доступа;
– управлением полномочиями (учетными данными);
– управлением разрешениями, полномочиями (учетными данными);
– управлением ресурсами;
– и др.

Уязвимости ИС по месту возникновения (проявления) подразделяются на следующие уязвимости в:

– прикладном ПО;
– общесистемном ПО;
– специальном ПО;
– ТС;
– портативных ТС;
– сетевом (коммуникационном, телекоммуникационном) оборудовании;
– средствах защиты.

Примеры уязвимостей и угроз, использующих эти уязвимости, приведены в таблице 7. В таблице 7 рассмотрены уязвимости и угрозы по направлениям безопасности, определенных в ГОСТ Р ИСО/МЭК 27002-2012.

Таблица 7 – Примеры уязвимостей и угроз, использующих эти уязвимости

| **Уязвимость** | **Угроза, использующая уязвимость** |
|---|---|
| **Безопасность, связанная с персоналом** | |
| Недостаточное обучение в вопросах безопасности | Ошибка персонала технической поддержки |
| Низкая осведомлённость в области ИБ | Ошибки пользователей |
| Отсутствие механизмов мониторинга | Несанкционированное (нецелевое) использование ПО |
| Отсутствие правил использования средств телекоммуникаций и передачи сообщений | Несанкционированное использование сетевого оборудования.<br>Заражение вредоносным ПО |

| Уязвимость | Угроза, использующая уязвимость |
|---|---|
| Отсутствие процедур возврата активов при увольнении | Кража активов |
| Отсутствие процедуры учета и контроля персонала, работающего в неурочное время | Кража активов.<br>НСД к активам |
| Отсутствие процедуры блокирования правд доступа при увольнении | НСД к активам |
| **Физическая безопасность и защиты от воздействий окружающей среды** | |
| Пренебрежение правилами использования механизмов физического контроля доступа в здания, помещения и офисы | Умышленное уничтожение активов.<br>НСД к активам.<br>Кража активов |
| Отсутствие физической защиты зданий, дверей, окон | Кража активов.<br>Уничтожение активов |
| Размещение активов в зоне подверженной затоплению | Уничтожение активов.<br>Остановка бизнес-процессов |
| Незащищенное хранение активов | Кража активов.<br>НСД к активам |
| Отсутствие схемы периодической замены оборудования | Выход из строя средств хранения и обработки информации.<br>Уничтожение (потеря) информации |
| Подверженность оборудования влажности, пыли, загрязнению | Сбой оборудования |
| Подверженность ТС перепадам температур | Нарушение температурного режима.<br>Сбой работы ТС |
| Нестабильное электропитание | Сбой электропитания.<br>Остановка работы бизнес-процессов |
| **Управление коммуникациями и операциями** | |
| Сложный пользовательский интерфейс | Ошибки персонала при работе с ПО и информацией |
| Передача или повторное использование средств хранения информации без надлежащей очистки памяти | НСД к информации |
| Неадекватное управление сетью | Перегрузка сети |
| Отсутствие процедур резервного | Потеря информации |

| Уязвимость | Угроза, использующая уязвимость |
|---|---|
| копирования | |
| Отсутствие доказательств отправки и получения электронных сообщений | Уход от ответственности<br>Утечка информации |
| Отсутствие обновления средств защиты от вредоносного ПО | Проникновение вредоносного ПО |
| Отсутствие разделения тестовых и рабочих ТС | Несанкционированная модификация действующих систем |
| Неконтролируемое копирование информации | Утечка информации |
| **Контроль доступа** | |
| Неправильное разграничение прав доступа в сетях | НСД к ресурсам сети, активам |
| Отсутствие политик «чистого стола» и «чистого экрана» | НСД к информации |
| Отсутствие механизмов аутентификации и идентификации | НСД к информации, системам и ПО |
| Отсутствие парольной политики или ненадлежащее её использование (легко угадываемые пароли, недостаточно частая смена пароля, хранение пароля) | Присвоение чужого пароля |
| Неконтролируемое использование системных утилит | Обход механизмов контроля системы или приложения |
| **Приобретение, разработка и сопровождение ИС** | |
| Недостаточная защита криптографических ключей | НСД к информации |
| Несовершенная политика в области криптографической защиты | Нарушение требований законодательной и нормативной базы |
| Неконтролируемая загрузка и использование ПО | Проникновение вредоносного ПО |
| Некорректный выбор тестовых данных | НСД к информации |
| Невыполнение или выполнение в недостаточном объеме тестирования ПО | Использование ПО неавторизированными пользователями |

Список уязвимостей и угроз, представленных в таблице 7, может быть дополнен.

Наличие уязвимости само по себе не наносит ущерба, поскольку необходимо наличие угрозы, которая сможет воспользоваться ею. Для уязвимости, которой не соответствует определенная угроза, может не потребоваться внедрение средства контроля и управления, но она должна осознаваться и подвергаться мониторингу на предмет изменений. Следует отметить, что неверно реализованное, неправильно функционирующее или неправильно используемое средство контроля и управления само может стать уязвимостью. Меры и средства контроля и управления могут быть эффективными или неэффективными в зависимости от среды, в которой они функционируют. С другой стороны, угроза, которой не соответствует определенная уязвимость, может не приводить к риску.

Уязвимости могут быть связаны со свойствами актива. Способ и цели использования актива могут отличаться от планируемых при приобретении или создании актива. Необходимо учитывать уязвимости, возникающие из разных источников, например те, которые являются внешними или внутренними по отношению к активу.

## 13.2 АНАЛИЗ РИСКОВ

Информация, полученная на этапе идентификации рисков, используется в процессе анализа рисков для определения:

- возможного ущерба, наносимого организации в результате нарушений безопасности активов;
- вероятности реализации угроз;
- величины риска.

### Ущерб

Под термином «ущерб» понимаются убытки, непредвиденные расходы, утрата имущества и денег, недополученная выгода.

Проявления возможного ущерба могут быть различны [1]:

- моральный и материальный ущерб деловой репутации предприятия;
- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

– материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
– моральный и материальный ущерб от дезорганизации деятельности предприятия;
– материальный и моральный ущерб от нарушения международных отношений.

Величина возможного ущерба формируется с учетом стоимости активов и тяжести последствий нарушения их безопасности.

Необходимо определить степень тяжести последствий от нарушения конфиденциальности, целостности, доступности и других важных свойств актива, а затем произвести общую оценку.

### Вероятность реализации угроз

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данного актива в складывающихся условиях обстановки.

Для вербальной градации вероятности реализации угроз могут использоваться четыре 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 недостаточны;

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности информации не приняты.

### Величина риска

После того, как была определены величина возможного ущерба и вероятность реализации угроз, определяется величина риска.

Вычисление рисков производится путем комбинирования возможного ущерба, выражающего вероятные последствия нарушения безопасности активов, и вероятности реализации угроз. Такое комбинирование часто

осуществляется при помощи матрицы, где в строках размещаются возможные значения ущерба, а в столбцах – вероятности реализации угрозы, на пересечение – величина риска.

Далее производится сравнение вычисленных уровней риска со шкалой уровня риска. Это необходимо для того, чтобы реалистично оценивать влияние, которое вычисленные риски оказывают на бизнес организации, и доносить смысл уровней риска до руководства [3].

## 13.3 ОЦЕНКА РИСКА

Результатом процесса оценки рисков является выявление (понимание наличия) риска.

По результатам оценки рисков формируется перечень рисков с назначенными приоритетами в соответствии с критериями оценки рисков.

### Методики оценки рисков

Существует множество методик анализа рисков. Некоторые из них основаны на достаточно простых табличных методах и не предполагают применения специализированного программного инструментария, другие наоборот, активно его используют.

Для решения задачи оценки рисков информационной безопасности в настоящее время наиболее часто используются следующие программные комплексы: CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), ГРИФ, CORAS и ряд других. Все известные методики можно разделить на:

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»), к таким методикам, в частности, относится FRAP;
- количественные методики (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь), к этому классу относится методика RiskWatch;
- методики, использующие смешанные оценки (такой подход используется в CRAMM, методике MSAT).

До принятия решения о внедрении той или иной методики управления рисками информационной безопасности следует убедиться, что она достаточно полно учитывает бизнес-потребности предприятия, его масштабы, а также соответствует лучшим мировым практикам и имеет достаточно подробное описание процессов и требуемых действий [3].

### Обработка рисков

На рисунке 12 представлен процесс обработки рисков. Процесс обработки включает в себя четыре варианта обработки рисков:

- снижение риска – уровень риска снижается путем выбора меры и средств контроля и управления, так что бы остаточный риск мог быть повторно оценен как допустимый;
- сохранение риска – принятие риска, при условии, что он отвечает политика и критериям предприятия, касающимся принятия риска;
- предотвращение – отказ от деятельности или условия, вызывающего конкретный риск;
- перенос риска – риск перенесен на стороны, которая может эффективно осуществлять управление конкретным риском, (например страхование риска).

Варианты обработки рисков не являются взаимоисключающими, и могут объединяться.

Варианты обработки рисков выбираются с учетом результатов оценки рисков, предполагаемой стоимости реализации мер защиты и их ожидаемой эффективности.

## 13.4 ПРИНЯТИЕ РИСКА

Основными факторами, влияющими на принятие рисков, являются:

- возможные последствия осуществления риска, т.е. расходы предприятия в каждом случае, когда это происходит;
- ожидаемая частота подобных событий.

Предприятие устанавливает критерии принятия рисков, определяющие максимально допустимый уровень остаточного риска, а также возможные исключения для определенных рисков при определенных обстоятельствах.

Риски, превышающие установленный руководством предприятия допустимый уровень, – это те риски, которые являются неприемлемыми для бизнеса, а связанная с ним деятельность – слишком рискованной. Все остальные риски, ниже этого уровня, являются допустимыми и могут быть приняты без дальнейшей обработки.

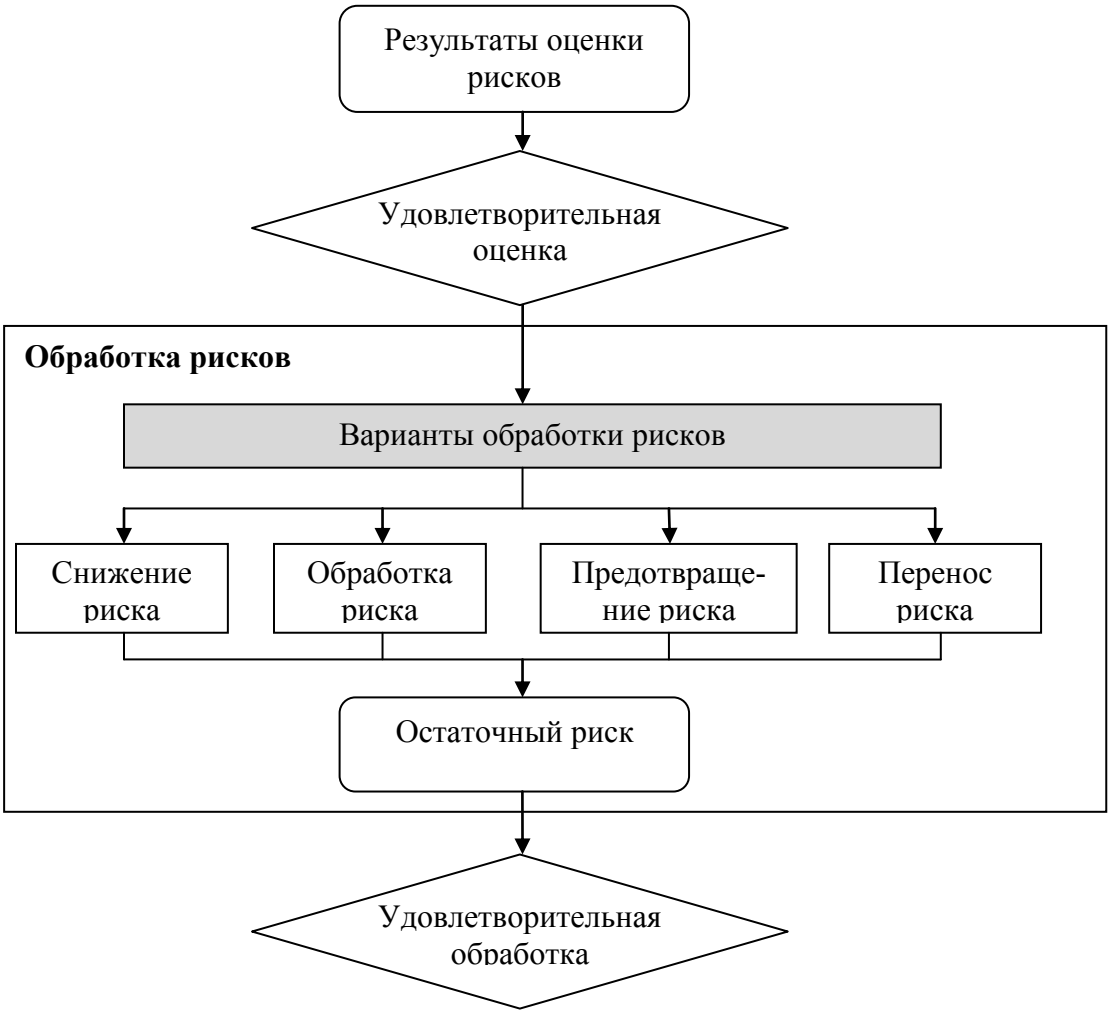



Рисунок 12 – Процесс обработки рисков

## ВЫВОДЫ

Для обеспечения эффективной защиты информации предприятия должны выполняться следующие шаги по внедрению, контролю и поддержке системы управления ИБ:

- проведение классификации объектов защиты и определение их критичности;
- оценка рисков ИБ;
- выбор и реализация соответствующих требований обеспечения ИБ, снижающих уровень рисков;
- осуществление контроля, поддержки и повышения эффективности средств управления безопасностью, связанных с активами организации.

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

| | | |
|---|---|---|
| ISO/IEC | – | International Organization for Standardization / International Electrotechnical Commission |
| ГОСТ | – | Государственный стандарт |
| ИБ | – | Информационная безопасность |
| ИС | – | Информационная система |
| ИСО/МЭК | – | Международная организация по стандартизации / Международная электротехническая комиссия |
| ИСПДн | – | Информационные системы персональных данных |
| ИТ | – | Информационные технологии |
| ИТСО | – | Инженерно-технические средства охраны |
| КТ | – | Коммерческая тайна |
| НИР | – | Научно-исследовательская работа |
| НСД | – | Несанкционированный доступ |
| ОКР | – | Опытно-конструкторская работа |
| ПДн | – | Персональные данные |
| ПО | – | Программное обеспечение |
| РД | – | Руководящий документ |
| РФ | – | Российская Федерация |
| САЗ | – | Средства антитеррористической защиты |
| СМИ | – | Средства массовой информации |
| СТО | – | Стандарт организации |
| ТС | – | Технические средства |
| ФБО | – | Функции безопасности объекта оценки |
| ФЗ | – | Федеральный закон |
| ФСБ | – | Федеральная служба безопасности |
| ФСТЭК | – | Федеральная служба по техническому и экспортному контролю |

## ЛИТЕРАТУРА


1. Вихорев С.С. Классификация угроз безопасности. Cnews.ru годовой обзор «Сетевые атаки и системы информационной безопасности 2001», 2001.
2. Козлова Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации // Молодой ученый. — 2013. — №5. — С. 154-161.
3. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности, М: Образовательные ресурсы и технологии, 2015 (1) –С. 73-79.
4. 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.
5. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа, М: РадиоСофт, 2010. – 232 с.
6. И. А. Баймакова, А. В. Новиков, А. И. Рогачев, А. Х. Хыдыров, М: 1С-Паблишинг, 2010 – 270 с.


## НОРМАТИВНЫЕ ДОКУМЕНТЫ


1. Конституция ФЗ РФ от 25.12.1993.
2. Кодекс ФЗ РФ об административных правонарушениях от 30.12.2001 №195-ФЗ.
3. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»
4. Уголовный кодекс РФ от 13.06.1996 N 63-ФЗ
5. ФЗ РФ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. ФЗ РФ от 27.12.2002 №184-фз «О техническом регулировании».
7. ФЗ РФ от 27.07.2006 №152-ФЗ «О персональных данных».
8. ФЗ РФ от 29.07.2004 №98-ФЗ «О коммерческой тайне».
9. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»
10. ГОСТ Р 1.4-2004. Стандартизация в Российской Федерации. Стандарты организаций. Общие положения. – Введ. 01.06.2005. – М: Стандартинформ. – 6 с.

11. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 27.12.2006. – М: Стандартинформ. – 12 с.
12. ГОСТ Р 27002-2012. Информационная технология. Практические правила управления информационной безопасностью. – Введ. 29.12.2005.– М: Стандартинформ. – 55 с.
13. ГОСТ Р ИСО/МЭК 27005-2010 Менеджмент риска информационной безопасности. – Введ. 01.12.2011.– М: Стандартинформ. – 58 с.
14. ГОСТ Р 56546-2015 Классификация уязвимостей информационных систем. – Введ. 19.08.2015.– М: Стандартинформ. – 17 с
15. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» утвержденный приказом Гостехкомиссии России от 30.08.2002 г. № 282.
16. Приказ Министерства юстиции Российской Федерации от 4 мая 2007 г. № 88 г. Москва «Об утверждении разъяснений о применении правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации».
17. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.
18. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.
19. СТО Газпром 1.0-2009 «Система стандартизации ОАО «Газпром». Основные положения».

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».

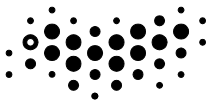
Николай Сергеевич КАРМАНОВСКИЙ
Ольга Викторовна МИХАЙЛИЧЕНКО
Николай Николаевич ПРОХОЖЕВ

# Организационно-правовое и методическое обеспечение информационной безопасности

**Учебное пособие**

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати 17 марта 2016 г.
Заказ № 3659
Тираж 100 экз.
Отпечатано на ризографе

**Редакционно-издательский отдел**
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49



УНИВЕРСИТЕТ ИТМО