1 ПОНЯТИЕ ТАЙНЫ. ВИДЫ ТАЙН

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

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

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

Существует большое число охраняемых законом тайн:

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

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

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

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

Тайна личной жизни

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

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

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

Банковская тайна

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

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

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

Врачебная тайна

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

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

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

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

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

Тайна усыновления

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

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

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

Тайна связи

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

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

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

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

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

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

Налоговая тайна

Налоговая тайна – право налогоплательщика на неразглашение информации, предоставленной налоговым органам, гарантированное ст. 102 Налогового Кодекса. Налоговую тайну составляют любые полученные налоговым органом, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений: разглашенных налогоплательщиком самостоятельно или с его согласия; об идентификационном номере налогоплательщика; о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения; предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенны-

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

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

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

Нотариальная тайна

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

Адвокатская тайна

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

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

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

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

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

Правила сохранения профессиональной тайны распространяются на:

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

Тайна страхования

Тайна страхования – разновидность служебной, а также коммерческой тайны. Согласно ст. 946 ГК РФ страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик отвечает по правилам, предусмотренным положением ГК РФ о служебной и коммерческой тайне. Лица, незаконными методами получившие информацию, которая составляет тайну страхования, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших тайну страхования вопреки трудовому договору, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Служебная тайна

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

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

Персональные данные

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

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

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

Тайна голосования

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

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

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

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

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

Тайна исповеди

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

2 ОБЩЕСИСТЕМНАЯ КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

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

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

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

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

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

3 ФОРМИРОВАНИЕ И СТАНДАРТИЗАЦИЯ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Законодательная и нормативная база по информационной безопасности в Российской Федерации

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

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

Формирование требований к обеспечению ИБ осуществляется с учетом:

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

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

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

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

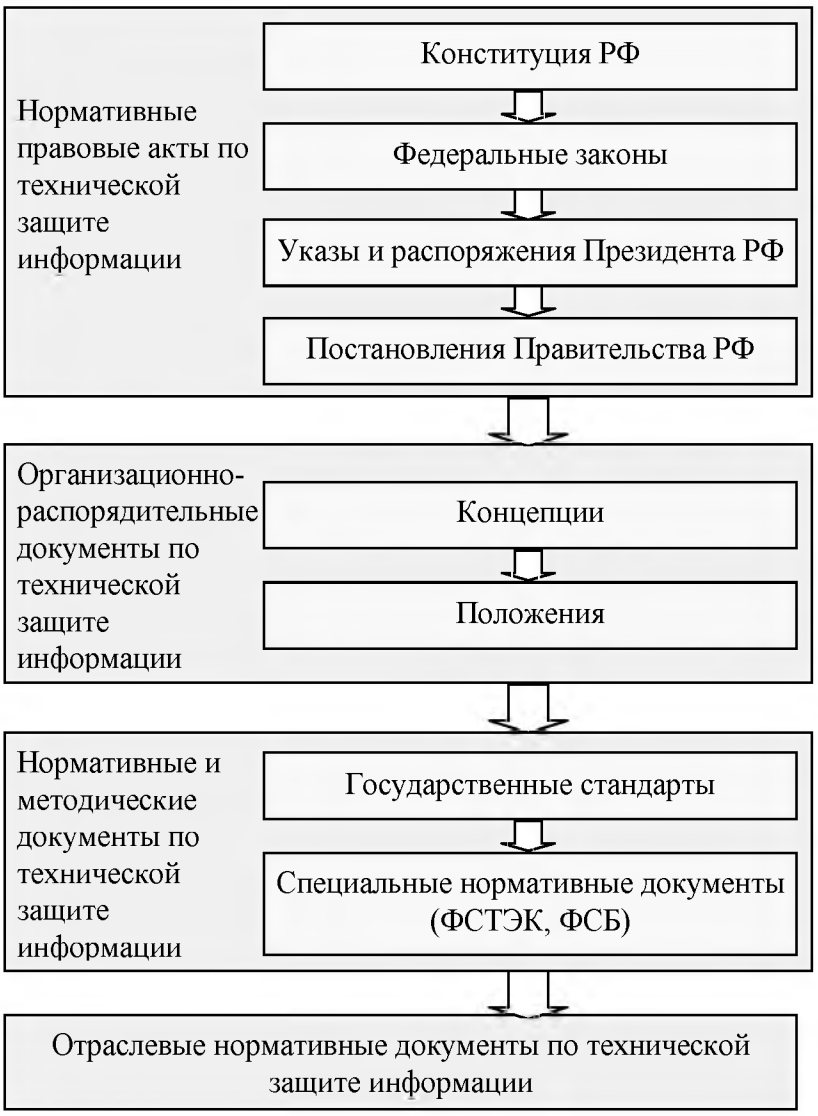

Рисунок 1 – Законодательная и нормативная база в области обеспечения ИБ РФ

Нормативные правовые документы по технической защите информации

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

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

1. Конституция РФ.
2. Кодексы РФ

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

Конституция Российской Федерации

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

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

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

Уголовный кодекс Российской Федерации

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

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

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

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

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

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

Кодекс РФ об административных правонарушениях

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

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

Статья 13.2 налагает административную ответственность за:

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

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

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

Статья 13.14 налагает административную ответственность за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Федеральные законы по технической защите информации

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

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

Указы и распоряжения Президента РФ по технической защите информации

Президентом РФ подписаны следующие указы в области обеспечения ИБ:

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

зовании информационно-телекоммуникационных сетей международного информационного обмена».

5. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Положение о Федеральной службе по техническому и экспортному контролю».

Постановления Правительства РФ по технической защите информации

К постановлениям Правительства РФ по технической защите информации относятся:

1. Постановление Совета министров-правительства РФ от 15.09.1993 года № 912-51 «Положение о государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам».
2. Постановление Правительства РФ от 03.101994 года № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
3. Постановление Правительства РФ от 15.04.1995 года № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».
4. Постановление Правительства РФ от 26.06.1995 № 608 "О сертификации средств защиты информации».
5. Постановление Правительства РФ от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности».
6. Постановление Правительства РФ от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».
7. Постановление Правительства РФ от 03.02.2012 № 79 «Лицензировании деятельности по технической защите конфиденциальной информации».
8. Постановление Правительства РФ от 16.04.2012 №313 «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных

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

Приказы ФСТЭК

В рамках обеспечения технической защиты информации ФСТЭК выпустил следующие приказы.

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

Организационно-распорядительные документы по технической защите информации

К организационно-распорядительным документам по технической защите информации относятся:

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

Нормативные и методические документы по технической защите информации

Государственные стандарты

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

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

В Российской Федерации федеральным законом о техническом регулировании № 184-ФЗ от 27.12.2002 г разделены понятия «технический регламент» и «стандарты» , в связи с чем, все стандарты должны утратить обязательный характер и применяться добровольно. До 1 сентября 2011 года в период до принятия соответствующих технических регламентов закон предусматривал обязательное исполнение требований стандартов в части, соответствующей целям защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества; охраны окружающей среды, жизни или здоровья животных и растений; предупреждения действий, вводящих в заблуждение приобретателей. С 1 сентября 2011 года все нормативные правовые акты и нормативные документы в области технического регулирования, не включенные в перечень обязательных, имеют добровольное применение.

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

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

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

Российские государственные стандарты серии «Информационная технология»

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

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

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

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

Специальные нормативные документы

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

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

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

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

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

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

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

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

– определено 5 классов защищенности межсетевых экранов.

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

– определено 4 уровня контроля отсутствия недекларированных возможностей.

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

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

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

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

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

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

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

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

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

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

Отраслевые нормативные документы по технической защите информации

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

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

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

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

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

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

Требования международных и отечественных стандартов к ИБ

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

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

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

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

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

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

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

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

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

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

Требования к информационной безопасности стандартов ИСО/МЭК 13335

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Требования к информационной безопасности стандарта COBIT

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

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

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

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

Таблица 5 – Перечень ключевых процессов управления ИТ

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

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

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

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

Требования стандарта распространяются на следующие области ИБ:

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

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

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

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

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

Выводы по разделу

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

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

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

4 ОСНОВНЫЕ ПОНЯТИЯ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Государственная тайна - все защищаемые государством сведения.

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

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

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

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

Субъектами правоотношений закона являются:

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

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

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

Основные понятия

Носители сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

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

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.

Доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

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

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

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

Перечень сведений, составляющих государственную тайну – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

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

Особенности режима секретности

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

Режим секретности включает в себя

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