А.В. Гортинский

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Учебное пособие

Саратов – 2012

Содержание

ВВЕДЕНИЕ

Охрана персональных данных – одно из направлений защиты информационных правоотношений.

Поданным Академии IT более 50% информации утекает из-за случайных причин и около 40% похищается умышленно. Больше всего (около 90%) происходит утечек персональных данных, а утечки коммерческой информации составляют только 2% от общего числа потерь.

С учетом особой роли информации в информационном обществе особое внимание уделяется защите информации от умышленных и неумышленных воздействий, уменьшающих прагматические и иные свойства информации.

Информационная безопасность - механизм защиты, обеспечивающий актуальность следующих прагматических свойств информации:

конфиденциальность: доступ к информации только авторизованных пользователей;

целостность: достоверность и полноту информации и методов ее обработки;

доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости

Исторически сложились следующие направления защиты информации:

– организационная защита – комплекс мер по регламентации деятельности организации и ее работников, которая осуществляется посредством принятия нормативно-правовых актов, уменьшающих риск негативного воздействия на информацию, используемую в деятельности организации;

– техническая защита – использование специальных аппаратных, программных средств в этих же целях;

– правовая защита – принятие совокупности законодательных актов, нормативных документов, устанавливающих особый правовой статус определенной информации, правила ее создания, изменения, использования и удаления.

Подчеркнем, что только комплексные меры по защите информации могут стать предпосылкой успешного решения задачи защиты информации.

Правовая защита информации всегда базируется на понятии права как общественного договора, поэтому на государство возложен мониторинг проблем в сфере оборота информации, в зависимости от общественной значимости этих проблем формулирование общеобязательных правил и норм поведения, фиксация эти правил и норм в законодательных и нормативных актах.

С учетом важности защиты национальных интересов, правовая защита информации реализуется не только на уровне отдельного государства, но и на межгосударственном уровне. На межгосударственном уровне такая правовая защита обеспечена межгосударственными договорами, конвенциями, декларациями и реализуется при помощи патентов, лицензий. На государственном уровне правовая защита информации регулируется государственными и ведомственными актами.

Часть I. ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Различные федеральные законы регулируют те или иные отношения, возникающие при осуществлении деятельности, связанной с использованием информационных технологий.

Так, если организациями и физическими лицами с использованием средств автоматизации или без использования таковых выполняется обработка персональных данных, возникающие в связи с этим отношения регулируются Федеральным законом «О персональных данных».

Отношения, возникающие в связи с приданием юридической силы электронным документам посредством электронной подписи, регулируются Федеральным законом «Об электронной цифровой подписи».

Отношения, возникающие в связи с правовой охраной и использованием программ для ЭВМ и баз данных, регулируются 4-й частью Гражданского кодекса РФ.

Отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства, фонограмм исполнений, постановок, передач организаций эфирного или кабельного вещания, до 01.01.2008 г. регулировались Федеральным законом «Об авторском праве и смежных правах», после 01.01.2008 г. – 4-й частью Гражданского кодекса РФ.

Отношения, связанные с созданием и эксплуатацией всех сетей связи и сооружений связи, использованием радиочастотного спектра, оказанием услуг электросвязи и почтовой связи на территории РФ и на находящихся под юрисдикцией Российской Федерации территориях, регулируются Федеральным законом «О связи».

Отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации, регулируются законом РФ «О Государственной тайне».

Отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, регулируются Федеральным законом «О коммерческой тайне».

Отношения, возникающие в связи с правовой охраной и использованием изобретений, полезных моделей и промышленных образцов, регулируются 4-й частью Гражданского кодекса РФ.

Вместе с тем, наиболее массовыми являются отношения, возникающие при осуществлении права на производство, передачу, получение, распространение, поиск информации; отношения, возникающие при применении информационных технологий в целом и при обеспечении защиты информации в частности. Такие отношения регулируются Федеральным законом «Об информации, информационных технологиях и о защите информации».

Тема 1. *БАЗОВЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ*

Международные нормы

В современном мире, в котором велики тенденции к интеграции между странами, международные нормы в значительной степени влияют на национальное законодательство. Законодательные органы большинства цивилизованных стан стремятся согласовывать свои законы с международными нормами. Поэтому в начале рассмотрим международные нормы, направленные на защиту персональных данных.

В 1979 г. была принята Резолюция Европарламента «О защите прав личности в связи с прогрессом информатизации». Резолюция предложила Совету и Комиссии Европейских сообществ разработать и принять правовые акты по защите данных о личности в связи с техническим прогрессом в области информатики.

В 1980 году принята Конвенция Европейского Союза "О защите лиц при автоматизированной обработке данных персонального характера"

Согласно этому документу, персональные данные, подвергающиеся автоматизированной обработке:

a) собираются и обрабатываются на справедливой и законной основе;

b) хранятся для определенных и законных целей и не используются иным образом, несовместимым с этими целями;

c) являются адекватными, относящимися к делу и не чрезмерными для целей их хранения;

d) являются точными и, когда это необходимо, обновляются;

e) сохраняются в форме, позволяющей идентифицировать субъекты данных, не дольше, чем это требуется для целей хранения этих данных.

В 1980 были приняты Рекомендации Организации по сотрудничеству стран-членов Европейского Союза "О руководящих направлениях по защите частной жизни при межгосударственном обмене данными персонального характера"

В 1981 году государства-участники Европейского Союза подписали в Страсбурге Конвенцию «О защите физических лиц в отношении автоматической обработки персональных данных».

В Конвенции декларированы гарантии частным лицам соблюдения права на личную жизнь в аспекте автоматизированной обработки данных личного характера, в том числе при передаче таких данных через государственные границы, независимо от способа передачи.

В настоящее время вопросы защиты персональных данных детально регламентируются директивами Европарламента и Совета Европейского Союза. Это ***Директивы № 95/46/ЕС и № 2002/58/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных», Директива № 97/66/ЕС Европейского парламента и Совета Европейского Союза от 15 декабря 1997 года***, касающаяся использо-

вания персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций.

Конституция РФ

Основным законом Российской Федерации является ***Конституция, принятая 12 декабря 1993 года***.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

Доктрина информационной безопасности Российской Федерации (09.09.2000) Пр-1895

Определяющим документом в сфере законодательство по защите информации является российская доктрина информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

1. соблюдение конституционных прав и свобод человека и гражданина

2. информационное обеспечение государственной политики Российской Федерации

3. развитие современных информационных технологий

4. защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем

Угрозы соответствуют составляющим национальных интересов. При этом с точки зрения информационно-технической четвертая группа угроз является наиболее интересной, связанной с деятельностью всех организаций и частных лиц, занимающихся хранением, обработкой, распространением и защитой информации.

В Доктрине перечислены эти угрозы:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно- телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации

Согласно Доктрины информационной безопасности России гл. II. Методы обеспечения информационной безопасности российской федерации параграф 5. Общие методы обеспечения информационной безопасности Российской Федерации общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К ***правовым методам*** обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

В сферу ***организационно-технических методов*** обеспечения информационной безопасности Российской Федерации попадают следующие аспекты деятельности по защите информации: разработка организационно-распорядительной документации, разработка, использование и совершенство-

вание средств защиты информации и методов контроля эффективности этих средств, проведение работ по выявлению технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, применение криптографических средств защиты информации, сертификация средств защиты информации, лицензирование деятельности в области защиты информации, совершенствование системы контроля за действиями персонала в защищенных информационных системах.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования, совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Тема 2. ФЕДЕРАЛЬНЫЕ НОРМАТИВНЫЕ АКТЫ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральный Закон 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Этот правовой акт является следующим по значимости в сфере регулирования правоотношений в сфере компьютерной информации.

Настоящий Федеральный закон регулирует отношения, возникающие при:

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

Однако! *Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации*

Этот закон устанавливает, что информация может являться объектом правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Классификация информации согласно категории доступа: общедоступная информация и информация ограниченного доступа. В этом смысле персональные данные граждан, если не оговорено иное в других законодательных актах, являются информацией ограниченного доступа.

Классификация информации согласно порядка ее предоставления и распространения:

1) информация, свободно распространяемая;

2) информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях;

3) информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информация, распространение которой в Российской Федерации ограничивается или запрещается.

Очевидно, что по этой классификации персональные данные относятся ко 2-му классу.

Закон вводит понятие обладателя информации.

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

В этом смысле лица или организации (в дальнейшем – операторы), которые хранят и обрабатывают персональные данные являются обладателями ин-

формации, поскольку именно они создали и структурировали данную информацию в электронном виде.

Закон устанавливает его права и обязанности обладателя информации.

Права обладателя информации:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обязанности обладателя информации:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Именно в связи с этими обязанностями и требуется осуществлять систему мероприятий по защите персональных данных, которые у него хранятся и обрабатываются, а именно обеспечить конфиденциальность и в тоже время доступность этих данных, а в случае, если на основании этой информации системой автоматически принимается решения, влекущие юридические последствия, то и целостность информации.

В связи с этим, согласно данному закону, обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

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

2) своевременное обнаружение фактов несанкционированного доступа к информации;

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

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

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

6) постоянный контроль за обеспечением уровня защищенности информации

Федеральный Закон 27 июля 2006 года N 152-ФЗ «О персональных данных» (с изменениями на 25 июля 2011 года)

Является основным законом, рассматриваемым в нашем курсе. Поэтому его положения будут рассмотрены наиболее подробно.

Утверждение в обществе уважения к личности, ее достоинству на основе создания и соблюдения правовых норм, направленных на защиту прав и интересов человека и гражданина, в частности права на неприкосновенность частной жизни, требует выделение следующих основных приоритетов, обозначенную законодателем в настоящей статье 2 этого закона:

а) защита персональных данных (ПДн) лиц от несанкционированного доступа к ним со стороны криминальных структур, других граждан, представителей государственных органов и служб, не имеющих на то соответствующих полномочий, путем регулирования порядка доступа субъектов персональных данных к своим данным;

б) обеспечение сохранности, целостности и достоверности данных на основе:

- установления режима конфиденциальности соответствующих персональных данных;

- регламентации обязанностей, прав и ответственности держателей (обладателей) массивов персональных данных по работе с этими данными;

в) обеспечение в условиях развития рыночных отношений в стране возможностей для работы с персональными данными держателей (обладателей) или третьих лиц, которым раскрыты персональные данные, имеющих лицензию на проведение работ с этими данными, в частности на основе прямого маркетинга.

В статье 3 даются основные понятия, используемые в законе, с точки зрения юриспруденции. С наиболее значимыми из них мы уже познакомились, однако есть специфические понятия, которые требуют расшифровки. В частности, что такое персональные данные конкретно.

Под персональными данными понимается следующая информация, неразрывно связанная с личностью ее обладателя: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы физического лица.

В состав персональных данных подлежат включению также сведения, связанные с поступлением на работу (службу), ее прохождением и увольнением; данные о супруге, детях и иных членах семьи обладателя, данные, позволяющие определить место жительства, почтовый адрес, телефон и иные индивидуальные средства коммуникации гражданского служащего, а также его супруги (ее супруга), детей и иных членов его семьи, данные, позволяющие определить местонахождение объектов недвижимости, принадлежащих гражданскому служащему на праве собственности или находящихся в его пользовании, сведения о доходах, имуществе и обязательствах имущественного характера, сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, владение языками (родной

язык, русский язык, другой язык или другие языки), образование общее (начальное общее, основное общее, среднее (полное) общее) и профессиональное (начальное профессиональное, среднее профессиональное, высшее профессиональное, послевузовское профессиональное), жилищные условия (тип жилого помещения, время постройки дома, размер общей и жилой площади, количество жилых комнат, виды благоустройства жилого помещения), источники средств к существованию (доход от трудовой деятельности или иного занятия, пенсия, в том числе пенсия по инвалидности, стипендия, пособие, другой вид государственного обеспечения, иной источник средств к существованию).

В основу категории "оператор" в процессе ее формирования законодателем в большей степени было положено не столько организационно-правовая форма субъекта, сколько выполняемые ими функции. Законодатель требует четкой определенности целей сбора и обработки персональных данных. Таким образом, цель результатов обработки персональных данных приобретает решающее значение. Последние во многом поставлены в прямую зависимость от непосредственного допуска к персональным данным в процессе их обработки. В этой связи принято различать организационную деятельность, деятельность по обоснованию целей и содержания обработки персональных данных и непосредственно саму обработку.

Обработка персональных данных в информационных системах, в том числе в ходе их обнародования в средствах массовой информации, размещения в информационно-телекоммуникационных сетях осуществляется в соответствии с действующими требованиями к обеспечению безопасности конфиденциальной информации. Кроме получения согласия субъекта персональных данных на их обработку, до момента распространения, использования, блокирования, уничтожения, обезличивания информации, оператор обязан поставить в известность уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

Письменное согласие на обработку персональных данных должно быть получено в случаях:

- обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;
- обработки сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные);
- трансграничной передачи персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных.

В случаях нахождения в информационных системах неполных, устаревших, недостоверных или незаконно полученных персональных данных, право инициировать их блокирование или уничтожение, по смыслу настоящего Закона, наряду с оператором предоставляется субъекту персональных данных, который тем самым реализует возможности своего доступа к ним.

Требование конфиденциальности персональных данных не распространяется на случаи их обработки в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Кроме того, обеспечение конфиденциальности персональных данных не требуется: 1) в случае обезличивания персональных данных; 2) в отношении общедоступных персональных данных. Последнее справедливо для лиц, занимающихся публичной деятельностью, в частности депутатов законодательных собраний.

Так же осуществление трансграничной передачи персональных данных допустимо при условии, что на территории государства - получателя будет обеспечена их адекватная защита, гарантирующая право на неприкосновенность частной жизни.

Контроль и надзор за обработкой персональных данных возложен на федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, который наделяется соответствующими правами и обязанностями. Таковыми являются: Фе-

деральная служба безопасности (ФСБ), Федеральная служба по техническому и экспортному контролю (ФСТЭК), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Законом вводится пять основных принципов обработки персональных данных:

1) законность целей и способов обработки персональных данных и добросовестности;

2) соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Декларируя необходимость получения достоверных сведений для целей их обработки, законодатель допускает возможность проверки полученных персональных данных на предмет соответствия их содержания объективной действительности. Таким образом, получение в указанном случае данных от третьих лиц не требует согласия на их обработку со стороны обладателя.

Законодатель возлагает бремя доказывания получения согласия субъекта персональных данных на их обработку на оператора (ст.9 ч.3).

В следующих случаях обязательно предоставление персональных данных к обработке:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных

данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности;

8) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну;

9) обработка персональных данных необходима в связи с осуществлением правосудия;

10) обработка персональных данных осуществляется в соответствии с законодательством РФ о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ;

11) обработка персональных данных при осуществлении первичного воинского учета.

По запросу субъекта ПДн ему должны быть представлены его персональные данные, хранящиеся и обрабатывающиеся в ИС, кроме случаев предусмотренных иными законодательными актами. Кроме того, субъекту персональных данных могут быть предоставлены и дополнительные сведения, касающиеся обработки его персональных данных, независимо от того, были ли они обозначены в запросе или нет. В состав такого рода сведений включены:

1) подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

2) способы обработки персональных данных, применяемые оператором;

3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых персональных данных и источник их получения;

5) сроки обработки персональных данных, в том числе сроки их хранения;

6) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Кстати: *Закон относит биометрические данные к персональным.*

Согласно ст. 15 оператор может не получать соглашение субъекта на обработку его ПДн, если у этого оператора нет прямых контактов с потенциальными потребителями с помощью средств связи.

При обработке персональных данных оператор обязан:

1. уведомить субъекта о

a. цели обработки персональных данных и ее правовое основание;

b. предполагаемых пользователях персональных данных;

2. принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. ст. 17 ФЗ "О лицензировании отдельных видов деятельности" деятельность по технической защите конфиденциальной информации подлежит обязательному лицензированию в порядке и на условиях, определяемых Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным Постановлением Правительства РФ от 30 апреля 2002 г. N 290. Контроль за этим осуществляет ФСТЭК;

3. по запросу субъекта безвозмездно предоставить имеющие ПДн о нем, и в случае их несоответствия действительности или не соответствия заявленной цели накопления, а так же в случае неправомерного их получения изменить их, блокировать или уничтожить.

Контролирующие органы ведут реестр операторов ПДн, проверяют соответствие защиты систем хранения и обработки ПДн классу хранимых данных. Плановые мероприятия по контролю в отношении каждого оператора проводятся не чаще 1-го раза в 2-а года.

Ниже в организационных основах защиты ПДн, мы будем рассматривать более подробно вопросы издания организационно-распорядительной документации и организации защиты информации. Сейчас упомянем только, что в связи с указанными требованиями требуется осуществить следующую схему действий.

- Уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных (как правило, это федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций).

- Разработать документы, регламентирующие обработку персональных данных в организации (положение по обработке персональных данных, регламенты, положения по защите персональных данных).
- Создать систему защиты персональных данных, в т.ч. выполненить требования по инженерно-технической защите помещений.
- Аттестовать или декларировать соответствие информационной системы персональных данных требованиям безопасности информации.
- Систематически повышать квалификацию сотрудников в области защиты персональных данных.

Информационные системы персональных данных (ИСПДн) представляют собой подкласс автоматизированных информационных систем (АИС). Поэтому основные определяющие суть исследования положения будем брать не только из нормативных актов, специально предназначенных для регулирования отношений в области оборота ПДн, и для АИС или АС (автоматизированных систем).

Федеральный закон от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

Принят с целью регулирования правоотношений, возникающих при разработке, принятии и эксплуатации технических средств, применение которых связано с безопасностью.

Вводит такие понятия как:

аккредитация - официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия;

безопасность - состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений;

декларирование соответствия - форма подтверждения соответствия продукции требованиям технических регламентов;

сертификация - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров;

Устанавливает требования по которым, технические средства и процессы, использование которых связано с вопросами безопасности, могут быть произведены, воспроизведены или применены.

В статье 7. Содержание и применение технических регламентов, п.3. указывает, что оценка соответствия (средства или процесса) проводится в формах государственного контроля (надзора), аккредитации, испытания, регистрации, подтверждения соответствия, приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме. Это означает, что компьютерные средства, которые хранят и обрабатывают персональные данные, а так же средства и процедуры обеспечения безопасности, должны пройти в той или иной форме, установленной законодательно, испытания и быть зарегистрировано.

Здесь фактически идет речь о сертификации продукции и в ст. 26. указывается порядок сертификации.

В совокупности с этим Законом следующий Закон о лицензировании отдельных видов деятельности позволяют создать правовую основу системы гарантирующей, что системы и услуги хранения, обработки, передачи и защиты персональных данных находятся на должном уровне и обеспечивают соблюдение интересов, как субъектов, так и потребителей персональных данных.

Федеральный Закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности»

Служит для стандартизации в области соответствия требованиям безопасности продуктов и услуг в том числе и информационных.

Определяет основные понятия:

"… 1) ***лицензирование*** - деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению,

возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования;

2) ***лицензия*** - специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа;

3) ***лицензируемый вид деятельности*** - вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом, в соответствии с федеральными законами, указанными в части 3 статьи 1 настоящего Федерального закона и регулирующими отношения в соответствующих сферах деятельности;

4) ***лицензирующие органы*** - уполномоченные федеральные органы исполнительной власти или их территориальные органы и в случае передачи осуществления полномочий Российской Федерации в области лицензирования органам государственной власти субъектов Российской Федерации органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование;

…

6) ***лицензиат*** - юридическое лицо или индивидуальный предприниматель, имеющие лицензию;"

Статья 12. Закона устанавливает ***перечень*** видов деятельности, на осуществление которых требуются лицензии. В контексте нашей тематики нас интересуют следующие виды:

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (крипто графических) 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);

2) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

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

4) разработка и производство средств защиты конфиденциальной информации;

5) деятельность по технической защите конфиденциальной информации;

36) оказание услуг связи;

38) деятельность по изготовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин, баз данных и фонограмм на любых видах носителей (за исключением случаев, если указанная деятельность самостоятельно осуществляется лицами, обладающими правами на использование данных объектов авторских и смежных прав в силу федерального закона или договора);

Основными лицензирующими органами в области защиты информации являются Федеральная служба по техническому и экспортному контролю (ФСТЭК) и ФСБ. ФСБ ведает всем, что связано с криптографией, ФСТЭК лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств соответствующей направленности.

Таким образом, технические и программные средства, используемые для защиты конфиденциальной информации, в том числе и персональных данных, должны разрабатываться и внедряться организациями, имеющими на это лицензию ФСТЭК, а если эти средства для защиты информации используют криптографические преобразования, - то лицензию ФСБ. Сами средства должны иметь сертификат соответствия той степени защиты для какой категории конфиденциальности информации они используются. Проверку соответствия производят соответствующие аккредитованные предприятия и организации.

При аттестации объекта информатизации аттестуемая и аттестующая организации руководствуются следующим документом:

Тема 3. *НОРМАТИВНЫЕ АКТЫ, СЛУЖАЩИЕ ОСНОВАНИЕМ ДЛЯ НОРМАТИВНО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ*

Положение по аттестации объектов информатизации по требованиям безопасности информации (Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.)

Аттестация проводится органом по аттестации в установленном настоящим Положением порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;

- предварительное ознакомление с аттестуемым объектом информатизации;

- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Только после получения аттестата соответствия организация может начать обработку конфиденциальной информации, к которым относятся и персональные данные.

Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

Данная Концепция является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

- выработка требований по защите средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа (НСД) к информации;

- создание защищенных от НСД к информации СВТ и АС;

- сертификация защищенных СВТ и АС (п.1.3.)

В этом документе дается определение НСД:

В п. 2.2. НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Непосредственно о защите в данном документе указывается несколько основополагающих моментов:

- защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер;

- ст. 3.4. защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ;

- ст. 3.5. программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС);

- в ст. 3.6. указывается о необходимости оценки эффективности средств защиты;

- в ст. 3.7. указывается, что необходим постоянный контроль эффективности средств защиты от НСД.

В параграфе 4. Дается вводится модели нарушителя. В последующих документов данное понятие будет играть важную роль. На ее основе будет строиться модель угроз в свою очередь являющаяся основой для построения системы защиты.

В параграфе 6. Указываются основные направления защиты, которые в дальнейшем буду детализированы в документах «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» и «Показатели защищенности от несанкционированного доступа к информации».

Таковыми являются:

- разграничение доступа в том числе и к устройства реализации твердых копий,

- изоляция процессов, запущенный субъектом доступа,

- установление разрешительной системы доступа,

- идентификация субъекта,

- регистрация действий субъекта,

- очистка памяти после завершения работы программ,

- учет носителей копий,

- использование криптографических методов для защиты информации.

Далее в этом документе указывается, что для разработки требований по защите АС требуется их классификация, основывающаяся на ценности информации и вероятности получения доступа к ней в каждой конкретной системе.

Классификация необходима для более детальной, дифференцированной разработки требований по защите от НСД с учетом специфических особенностей этих систем.

В основу системы классификации АС должны быть положены следующие характеристики объектов и субъектов защиты, а также способов их взаимодействия:

- информационные, определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможные последствия неправильного функционирования АС из-за искажения (потери) информации;

- организационные, определяющие полномочия пользователей;

- технологические, определяющие условия обработки информации, например, способ обработки (автономный, мультипрограммный и т.д.), время циркуляции (транзит, хранение и т.д.), вид АС (автономная, сеть, стационарная, подвижная и т.д.)

Так же в данном документе указываются основы организация работ по защите от НСД.

Для упорядочивания используемой терминологии в ряде руководящих документов был принят специальный документ.

Руководящий документ «Защита от несанкционированного доступа к информации». Термины и определения. (Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.)

Его содержание мы не рассматриваем, поскольку необходимые термины будут пояснены по мере необходимости при рассмотрении других документов.

Планированием, организацией и защитой информации в организации занимаются конкретные люди. Они организованы в структурные и межструктурные подразделения. Главным ответственным лицом в организации является руководитель этой организации. Наиболее важным организующим о контролирующим межструктурным органом является постоянно действующая техническая комиссия (ПДТК). В нее входит один из заместителей руководителя и ряд должностных лиц соответствующих отделов, ответственных за обеспечение безопасности, например: отдела кадров, отдела безопасности, отдела информатизации.

ПДТК отслеживает основные мероприятия по обеспечению информационной безопасности. Ее председатель утверждает ряд организационно-распорядительных и информационных документов.

Понятие данного межструктурного органа вводится, поскольку оно будет использовано в ряде последующих документов.

ПДТК объявляется приказом руководителя, ее деятельность регламентируется положением, а состав соответствующим распоряжением, которые так же утверждает руководитель.

Следующим логическим шагом к построению системы защиты информации стало принятие нижеследующего документа.

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. «Классификация автоматизированных систем и требования по защите информации». (Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации

Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности (документ утверждается руководителем организации);

- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий (документ утверждается);

- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

- режим обработки данных в АС.

Как и было определено в предыдущем документе здесь указывается, что к числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;

- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

- режим обработки данных в АС - коллективный или индивидуальный.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б (конфиденциальная информация) и 3А (государственная тайна).

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б (конфиденциальная информация) и 2А (государственная тайна).

Третья группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, (конфиденциальная информация) 1В, 1Б и 1А (государственная тайна).

Компания Академия АТ, предлагает такую иллюстрацию.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;

- регистрации и учета;

- криптографической;

- обеспечения целостности.

В параграфе 2 данного документа рассматриваются требования к указанным подсистемам, то есть, какие требования безопасности должны выполняться в каждом классе этих систем.

1. управления доступом, 2. регистрации и учета, 3. обеспечения целостности, 4. криптографической защиты, 5. межсетевого взаимодействия,	Требования для АС
6. антивирусной защиты, 7. обнаружения вторжений, 8. анализа защищенности	Требования для ИСПДн

Классы									
Подсистемы и требования	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
Подсистема управления доступом									
Идентификация, аутентификация и контроль доступа субъектов									
в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам	-	-	-	+	-	+	+	+	+
к программам	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям	-	-	-	+	-	+	+	+	+
Управление потоками информации.	-	-	-	+	-	-	+	+	+
Подсистема регистрации и учёта									
входа/выхода субъектов доступа в/из системы	+	+	+	+	+	+	+	+	+
выдачи печатных выходных документов	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
Учет носителей информации	+	+	+	+	+	+	+	+	+
Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+

Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
Подсистема криптографической защиты									
Шифрование конфиденциальной информации	-	-	-	+	-	-	-	+	+
Шифрование информации, принадлежащей различным субъектам доступа на разных ключах	-	-	-	-	-	-	-	-	+
Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	-	-	-	+	+
Подсистема обеспечения целостности									
Обеспечение целостности программных средств и информации	+	+	+	+	+	+	+	+	+
Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
Наличие администратора (службы) защиты информации в АС	-	-	-	+	-	-	+	+	+
Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
Использование сертифицированных средств защиты	-	+	-	+	-	-	+	+	+

В случае объединения АС посредством межсетевого экрана, каждая из объединяющихся АС может сохранять свой класс защищенности.

Выбор класса АС производится в следующей последовательности:

- Разработка и анализ исходных данных.
- Выявление основных признаков АС, необходимых для классификации.
- Сравнение выявленных признаков АС с классифицируемыми.
- Присвоение АС соответствующего класса защиты информации от НСД.

Исходные данные необходимые для проведения классификации конкретной АС:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий

- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС режим обработки данных в АС.

Определяющие признаки при классификации АС:

- наличие в АС информации различного уровня конфиденциальности,
- различия полномочий доступа субъектов АС к защищаемой информации,
- режим обработки данных в АИС (коллективный или индивидуальный).

Указанные классы АС должны защищаться соответствующим образом. Для того, что бы установить необходимый уровень защиты для каждого класса и определить необходимые мероприятия был введен в действие следующий документ.

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. (Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

Это документ устанавливает классы защищенности АС, т.е. требования, при выполнении которых система будет считаться защищенной по требованиям определенного класса, и формулирует показатели для этих классов.

Устанавливается семь классов защищенности средств вычислительной техники от НСД к информации.

Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы:

• первая группа содержит только один седьмой класс;

• вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

• третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

• четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

В контексте данного деления строится система показателей защищенности, которые и излагаются в параграфе 2. данного документа.

Здесь показатели защищенности более детализированы по сравнению с теми направлениями защиты, которые указаны в предыдущем документе – «Концепции защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

В данном документе учитываются следующие показатели защищенности:

- дискреционный принцип контроля доступа (для каждой пары объект-субъект указаны допустимые действия);

- мандатный принцип контроля доступа (каждому объекту и субъекту присваиваются метки, имеющие строгую иерархию. Доступ субъекта к объектам определяется по соотношению меток в иерархии);

- очистка памяти после прекращения работы процесса;

- изоляция модулей (программы разных пользователей не имеют общих областей памяти);

- маркировка документов (при заполнении документа обязательно в его начале и в конце указываются реквизиты);

- защита ввода и вывода на отчуждаемый физический носитель информации (метка передаваемой информации должна соответствовать метке устройства или канала ввода-вывода);

- сопоставление пользователя с устройством (конкретный пользователь может выводить информацию только на конкретное устройство);

- идентификация и аутентификация (на этапе идентификации пользователь запрашивает определенные права доступа, на этапе аутентификации устанавливается, что идентифицированный пользователь действительно тот, за кого себя выдает);

- регистрация (фиксация действий, которые производились в системе не зависимо то того привели они к успеху или нет);

- взаимодействие пользователя с комплексом средств защиты (КСЗ) (интерфейс пользователя и КСЗ должен быть структурирован и точно определен. Он должен быть надежным. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов);

- надежное восстановление (процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ);

- целостность КСЗ (периодический контроль за наличием и полнотой функционирования всех модулей защиты);

- контроль модификации (гибкость системы должна сочетаться с контролем изменений и возможность сверки элементов системы с эталонами);

- контроль дистрибуции (контроль точности копирования в СВТ при изготовлении копий с образца);

- гарантии архитектуры (КСЗ должен обладать механизмом, гарантирующим перехват диспетчером доступа всех обращений субъектов к объектам);

- тестирование (проверка работоспособности всех модулей защиты);

- руководство для пользователя.

Так же должны присутствовать руководство по КСЗ, тестовая документация и конструкторская (проектная) документация.

Рекомендуется:

- АС, обрабатывающие информацию, составляющую служебную тайну, относить по уровню защищенности к классам не ниже 3Б, 2Б,
- АС, обрабатывающие персональные данные, относить по уровню защищенности к классам не ниже 3Б, 2Б и 1Г.

При этом в АС целесообразно применять СВТ:

• не ниже 5 класса - для класса защищенности АС 1Д,

• не ниже 4 класса - для класса защищенности АС 1Г

При передаче конфиденциальной информации в сетях, сопряженных с сетями международного обмена информацией следует руководствоваться следующими документами.

Указ Президента Российской Федерации от 17 марта 2008 г. № 351(в ред. Указа Президента РФ от 21.10.2008 № 1510) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

Данный документ направлен на обеспечение безопасности при передаче данных через международные сети. В нем указывается, что подключение к глобальным международным компьютерам сетям (например, Интернет) компьютеров, содержащих государственную или служебную тайну не допускается. В случае, если такое подключение необходимо, то оно должно производиться с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в ФСБ РФ и (или) получивших подтверждение соответствия в ФСТЭК. По смыслу можно предположить, что для госучреждений, компьютеры, содержащие служебную информацию, в том числе и персональные данные могут подключаться к глобальной международной сети через межсетевой экран, но сертифицированный ФСБ, для коммерческих учреждений – сертифицированный ФСТЭК. Для учреждений, компьютеры которых содержат гостайну – только с использованием криптографических средств и сертифицированных, соответственно, ФСБ. Но в последнем случае лучше не подключать.

Указанный документ, опирается на ранее принятый Гостехкомиссией нижеследующий руководящий документ, в котором конкретизируются меры защиты информации при межсетевом обмене.

Руководящий документ. Средства вычислительной техники. «Межсетевые экраны». Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. (Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.)

В нем дается определение, ***межсетового экрана*** (терминов брандмауэр или файерволл в официальной документации следует избегать):

МЭ представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Документ служит для установления соответствия между классами автоматизированных информационных систем и межсетевых экранов.

В п. 1.5. устанавливается пять классов защищенности МЭ.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

В п.1.6. указывается, что для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Параграф 2 посвящен требованиям, которым должны удовлетворять МЭ соответствующего класса защищенности по таким параметрам как:

Управление доступом (фильтрация данных и трансляция адресов)

Идентификация и аутентификация (пользователей и администратора)

Регистрация (пакетов данных, событий и инцендентов)

Целостность (контроль)

Восстановление (состояния и критических данных после сбоя системы)

Тестирование (реализации правил фильтрации, процесса идентификации и аутентификации администратора, процесса регистрации действий администратора МЭ, процесса контроля за целостностью программной и информационной части МЭ, процедуры восстановления)

Конкретные мероприятия и рекомендации по защите конфиденциальной информации изложены в следующем документе.

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (Решение Коллегии Гостехкомиссии России № 7.2/02.03.2001 г.)

Данный документ содержит набор требований к технической защите информации и алгоритм действий при построении защиты АС.

Во-первых, в этом документе устанавливаются требования и даются рекомендации по защите речевой конфиденциальной информации. Указываются каналы утечки информации (акустические, виброакустические, электрические, на основе побочных излучений, наводимых и радиоизлучений). Даются рекомендации по подготовке помещений и дезавуации устройств, могущих послужить неконтролируемыми передатчиками речевой информации.

Во-вторых, указываются основные мероприятия и документы, которые должны быть подготовлены при организации защиты информации, циркулирующей в АС. А именно:

- документальное оформление перечня сведений конфиденциального характера (утверждается руководителем и служит для построения матрицы доступа);

- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам (запрещено все, что явно не разрешено);

- ограничение доступа персонала и посторонних лиц в ЗП и помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации, (т.е. организация физической защиты,

необходимы распоряжения, списки допускаемых в помещение лиц, система ключей и замков);

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (матрица доступа к ресурсам);

- регистрация наиболее значимых для безопасности действий пользователей АС и обслуживающего персонала (придание системным журналам статуса источника информации об инциденте);

- учет и надежное хранение бумажных и машинных носителей конфиденциальной информации (ведение журналов выдачи таких носителей);

- использование сертифицированных по требованиям безопасности информации специальных защитных знаков, создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки (закупка соответствующих компонент);

- резервирование и дублирование устройств обработки, а так же массивов и носителей информации (закупка соответствующего оборудования или программ);

- использование сертифицированных технических средств обработки, передачи и хранения информации (закупка соответствующего оборудования или программ);

- использование сертифицированных средств защиты информации (закупка соответствующего оборудования или программ);

- размещение объектов защиты на максимально возможном расстоянии от границы контролируемой зоны (КЗ). Существуют две зоны, которые должны находиться внутри КЗ. Зона 1 – пространство вокруг основного технического средства и системы (ОТСС), на границе и за пределами которого уровень сигнала наведенного от ОТСС во вспомогательном техническом средстве и системе (ВТСС) не превышает нормированного значения. Зона 2 - пространство вокруг (ОТСС), на границе и за пределами которого уровень сигнала ОТСС не превышает нормированного значения (создание утвержденного плана размещения ОТСС и ВТСС);

- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ (заказ на установку оборудования);

- использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания) (закупка соответствующих компонент)

- развязка цепей электропитания объектов защиты с помощью сетевых помехо-подавляющих фильтров, блокирующих (подавляющих) информативный сигнал (закупка соответствующего оборудования);

- электромагнитная развязка между информационными цепями, по которым циркулирует защищаемая информация, и линиями связи, другими цепями ВТСС, выходящими за пределы КЗ (закупка соответствующего оборудования);

- использование защищенных каналов связи (закупка соответствующего оборудования);

- размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр (создание утвержденного плана размещения ОТСС и ВТСС);

- предотвращение внедрения в АС программ-вирусов, программных закладок (закупка средств антивирусной и антитроянской защиты).

Далее в этом документе указываются что при классификации АС должна учитываться возможность монопольного или многопользовательского доступа к защищаемой информации и это существенно влияет на уровень ее защищенности.

В п. 5.1.10. прямо указано, что «Конкретные требования по защите информации и мероприятия по их выполнению определяются в зависимости от установленного для АС класса защищенности. Требования к классам защищенности определены РД Гостехкомиссии России», т.е. в руководящем документе «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», который мы рассмотрели ранее.

На основании указанных требований в документ дается подробный перечень необходимый документов и действий, которые должны быть выполнены при создании системы защиты конфиденциальной информации.

Однако данный документ носит гриф ДСП и в этой части не может быть рассмотрен. Укажем лишь, что в нем рассматриваются следующие положения:

- основные требования и рекомендации по защите информации (где прямо указывается, что АС, обрабатывающие информацию, содержащую сведения, составляющие служебную тайну, или персональные данные, должны иметь класс защищенности не ниже 3Б, 2Б и 1Г и 3Б, 2Б и 1Д соответственно);

- порядок обеспечения защиты информации при эксплуатации АС;

- защита информации на автоматизированных рабочих местах
на базе автономных ПЭВМ;

- защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ;

- защита информации в локальных вычислительных сетях;

- защита информации при межсетевом взаимодействии;

- защита информации при работе с системами управления базами данных;

- рекомендации по обеспечению защиты конфиденциальной информации,
содержащейся в негосударственных информационных ресурсах, при взаимодействии абонентов с информационными сетями общего пользования;

Для обеспечения безопасности персональных данных был принят ряд отдельных документов, по сути повторяющих рассмотренные выше, однако в них имеются некоторые отличия, требующие проведения конктерных дополнительных мероприятий.

Тема 4. *НОРМАТИВНЫЕ АКТЫ, СЛУЖАЩИЕ ОСНОВАНИЕМ ДЛЯ НОРМАТИВНО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ*

Приказ ФСТЭК, ФСБ, Минсвязи России от 13 февраля 2008 года «Об утверждении порядка проведения классификации информационных систем персональных данных»

Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

Проведение классификации информационных систем включает в себя следующие этапы:

– сбор и анализ исходных данных по информационной системе;

– присвоение информационной системе соответствующего класса и его документальное оформление.

В документе дается наиболее внятное определение классов для типовой ИСПДн, в которой требуется обеспечить только конфиденциальность информации (п. 8).

Однако требования к обеспечению безопасности информации гласят, что должны сохраняться все прагматические свойства информации, а именно: конфиденциальность, целостность, доступность. Поэтому практически не существует типовых ИСПДн.

Специальные ИСПДн это все остальные, которые являются реальными и на сегодняшний день, по все видимости составляют подавляющее большинство.

Для того, что бы определить класс ИСПДн, и, соответственно, требования к ее защите, необходимо учитывать:

- категорию обрабатываемых в информационной системе персональных данных – Хпд;

Это то, что требуется для классификация типовых ИСПДн. Такая классификация является базовой и может быть использована как составная часть при

классификации специальных систем. Установив класс «типовой» части информационной системы к ее характеристикам, требующим защиты следует добавить еще:

- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) – Хнпд;

- структуру ИСПДн (изолированная, локальная, распределенная);

- наличие подключения к сетям международного информационного обмена;

- однопользовательская данная система или она допускает наличие множества пользователей;

- если система многопользовательская, то необходимо учитывать разные или равные права имеют пользователи в системе;

- находится ли система целиком на территории России или хотя бы часть ее компонент размещается за рубежом.

Как видим, подход напоминает классификацию АС.

Класс типовой информационной системы определяется следующим образом.

I - определяется категория обрабатываемых в информационной системе персональных данных (Хпд):

– категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

– категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

– категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;

– категория 4 – обезличенные и (или) общедоступные персональные данные.

II- определяются граничные значения объемов обрабатываемых данных (Хнпд) может принимать следующие значения:

1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 – в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Собственно класс типовой ИСПДн определяется из таблицы

ХПД \ ХНПД	**3**	**2**	**1**
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

При этом считается, что

– класс 1 (К1) – это такие информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

– класс 2 (К2) – это такие информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

– класс 3 (К3) – это такие информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

– класс 4 (К4) – это такие информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Для определения требуемой степени защиты специальной информационной системы вначале требуется построить модель угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", который мы ниже и рассмотрим.

Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Это Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

В п.2. Положения указывается, что «Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.»

В этом документе упоминается о том, что защита персональных данных не заканчивается автоматизированными системами. Защите подлежат так же и акустические и электромагнитные каналы. Эти требования мы указывали при рассмотрении Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К).

В п.6. указывается, что для установления достаточной защиты системы должны быть классифицированы. Однако, как мы уже видели ранее, при изучении Приказа ФСТЭК, ФСБ, Минсвязи России от 13 февраля 2008 года «Об утверждении порядка проведения классификации информационных систем персональных данных», классификация ИСПДн основывается на построении модели угроз ИС.

Модель угроз ИСПДн называется частной моделью, если она построена для конкретной системы. Для облегчения такой работы ФСТЭК разработала базовую модель угроз. Использование базовой модели угроз для построения частной модели регламентируется следующим документом:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.; выписка)

Этот методический документ предназначен для операторов, организующих и (или) осуществляющих обработку ПДн и позволяет решить следующие задачи:

- разработку частных моделей угроз безопасности ПДн в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;

- анализировать защищенность ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

- разработать системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

- провести мероприятия, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

- не допустить воздействие на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

- контролировать уровнь защищенности персональных данных.

Как указывает документ в начале необходимо произвести классификацию угроз безопасности ПДн.

Как известно, на безопасность ПДн в ИСПДн влияют характеристики самой ИСПДн и окружающая среда, которая так же может являться поставщиком каналов утечки информации.

Возможности источников угроз безопасности данных (УБПДн) обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, приводящего к негативным последствиям и нарушениям прагматических качеств информации.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн.

Угрозы классифицируются в соответствии со следующими признаками:

- по виду защищаемой от УБПДн информации, содержащей ПДн;

- по видам возможных источников УБПДн;

- по типу ИСПДн, на которые направлена реализация УБПДн;

- по способу реализации УБПДн;

- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

- по используемой уязвимости;

- по объекту воздействия.

Далее в документе рассматриваются источники угроз, соответствующие каналам утечки или воздействия на информацию:

- угрозы, связанные с техническими каналами,

- угрозы, связанные с акустическими каналами,

- угрозы, связанные с видовыми каналами,

- угрозы, связанные с побочными электромагнитными излучениями и наводками,

- угрозы, связанные с несанкционированным доступом к информации в информационной системе персональных данных.

Далее в документе анализируются источники угроз, каковыми являются: нарушитель; носитель вредоносной программы; аппаратная закладка. Рассмотрены внешние и внутренние нарушители и их возможности. Всего имеется 5-ть категорий внешних нарушителей и 8-мь категорий внутренних.

Согласно положений рассматриваемого документа, причинами возникновения уязвимостей являются как умышленные, так и не умышленные действия, а также причины как объективного так и субъективного плана (п. 5.2.):

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;

- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;

- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;

- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;

- сбои в работе аппаратного и программного обеспечения.

Уязвимости программного обеспечения подразделяются на уязвимости прикладного и системного характера, подробно анализируются в частности уязвимости отдельных протоколов стека протоколов TCP/IP.

Далее рассматриваются: угрозы непосредственного доступа в операционную среду информационной системы персональных данных, угрозы, реализуемые с использованием протоколов межсетевого взаимодействия (очень подробно, рассматриваются технические основы нескольких видов сетевых атак), угрозы программно-математических воздействий, угрозы, реализуемые методами сокрытой передачи информации.

В п.6. рассматриваются типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

Рассмотрение различных классов этих угроз позволяет выбрать те, которые могут реализовываться в конкретной ИСПДн и на этой основе построить частную модель угроз, то есть именно ту, которая присуща конкретной системе.

При составлении частной модели угроз безопасности персональных данных, необходимо учитывать актуальность этих угроз. Такую возможность предоставляет следующий документ.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.)

Этот документ предлагает определять перечень актуальных угроз безопасности ПДн на основе перечня источников угроз ПДн (формируется методом опроса), перечня уязвимых звеньев ИСПДн (формируется методом опроса и сетевого сканирования), перечня технических каналов утечки информации (по данным обследования ИСПДн).

Вводятся три уровня защищенности ИСПДн: высокий, средний, низкий.

Исходя из этой градации оцениваются риски защищенности ИСПДн по:

- территориальному размещению,
- наличию соединения с сетями общего пользования,
- встроенным (легальным) операциям с записями баз персональных данных,
- разграничению доступа к персональным данным,
- наличию соединений с другими базами ПДн иных ИСПДн,
- уровню обобщения (обезличивания) ПДн,
- объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки.

Каждая из семи характеристик состоит из составляющих и оценивается по их совокупности.

Исходная степень защищенности определяется следующим образом:

- ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому

уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

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

- ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

Таким образом будет получено суммарное значение.

За тем каждой характеристике на основе выше полученного суммарного значения должен быть сопоставлен коэффициент (Y1):

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Другой коэффициент определяется исходя из вероятности возникновения и реализации угрозы для каждой характеристики (Y2):

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

На основании этих коэффициентов по формуле Y=(Y1+Y2)/20 вычисляется коэффициент реализуемости угрозы. По нему формируется вербальная интерпретация реализуемости угрозы следующим образом:

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

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

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

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

Указанное вербальное значение и будет одним из окончательных коэффициентов.

Другим определяемым окончательным коэффициентом является опасность угрозы каждой характеристики. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем формируется список актуальных угроз в соответствии с правилами, приведенными в таблице.

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

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

Определившись с моделью угроз, представляющей собой набор угроз и как следствие каналов утечки информации, можно перейти к формированию системы мероприятий, обеспечивающих безопасность ИСПДн.

Практические рекомендации по защите информации изложены в Приказе ФСТЭК от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

Приказ ФСТЭК от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»

В техническом и организационном плане практическое значение имеет приложение к данному приказу.

В п. 2.1. этого приложения указывается, что методами и способами защиты информации от несанкционированного доступа являются:

-реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

- резервирование технических средств, дублирование массивов и носителей информации;

- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- использование защищенных каналов связи;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

Далее в соответствии с требованиями классификации ИСПДн указываются меры защиты, в случае ее подключения к международным линиям связи – сетевой экран, средства антивирусной защиты, средства контроля эффективности защиты (сетевые сканеры), фильтрация пакетов, централизованное управление безопасностью (на основе технологии доменных политик безопасности).

Для предотвращения утечек речевой информации по электромагнитным каналам предусматривается:

- использование технических средств в защищенном исполнении;

-использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- размещение объектов защиты в соответствии с предписанием на эксплуатацию;

- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;

- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

Далее в приложении к приложению рассматриваются методы и способы защиты информации от несанкционированного доступа в зависимости от класса информационной системы. Здесь-то нам и пригодится классификация типовых ИСПДн. В данном документе по очереди рассматриваются типовые ИСПДн 4-1 классов, с учетом ранее определенных дополнительных классификационных признаков, влияющих на систему мер защиты, а именно: режим обработки информации, наличие межсетевого взаимодействия, подключения к международным сетям.

Информационные системы 4-го класса не имеют строгих предписаний к защите и предполагается, что степень их защиты определяется самим оператором.

Рассматриваются методы защиты по видам мероприятий:

- управление доступом,
- регистрация и учет,
- обеспечение целостности

для каждого из случаев:

- однопользовательский режим,
- многопользовательский режим обработки персональных данных и равных правах доступа,
- многопользовательский режим обработки персональных данных и разных правах доступа,
- межсетевое взаимодействие при подключении к сетям международного информационного обмена,

и для каждого из классов: 3,2,1.

Методы защиты реализуется посредством системы мероприятий, которые изложены в следующем документе.

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных (Утверждены Заместителем директора ФСТЭК России 15 февраля 2008 г.)

В п. 3.1. указывается, что под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

Кроме того в в 3.2. уточняется, что обязанности по реализации этих мероприятий возлагаются на оператора, а для разработки и осуществления этих мероприятий оператором (или уполномоченным им лицом) создается структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности ПДн.

Далее в документе рассматриваются стадии создания средств защиты ПДн (СЗПДн), содержание технического задания на разработку СЗПДн.

Отдельно указывается, что оценка соответствия ИСПДн требованиям безопасности ПДн проводится в виде:

для ИСПДн 1 и 2 классов – обязательной сертификации (аттестации) по требованиям безопасности информации;

для ИСПДн 3 класса – декларирования соответствия требованиям безопасности информации.

Для ИСПДн 4 класса оценка соответствия проводится по решению оператора.

В п. 4.2. данного документа указывается, что

В состав мероприятий по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий входят следующие мероприятия:

защита от НСД при однопользовательском режиме обработки ПДн;

защита от НСД при многопользовательском режиме обработки ПДн и равных правах доступа к ним субъектов доступа;

защита от НСД при многопользовательском режиме обработки ПДн и разных правах доступа;

защита информации при межсетевом взаимодействии ИСПДн;

антивирусная защита;

обнаружение вторжений.

Мероприятия по защите ПДн реализуются в рамках подсистем: управления доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты, обнаружения вторжений.

Мероприятия по обнаружению вторжений в ИСПДн проводятся в соответствии с требованиями нормативных документов Федеральной службы безопасности Российской Федерации.

Кроме этого, в ИСПДн должен проводиться контроль на наличие недекларированных возможностей в программном и программно-аппаратном обеспечении и анализ защищенности системного и прикладного программного обеспечения.

Далее подробно рассматриваются перечни мероприятий для ИСПДн 3,2 и 1 классов при условии различных режимов обработки данных, а так же с учетом подключения к локальной или глобальной сети по всем подсистемам (управления доступом, обеспечения целостности, антивирусной защиты).

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждены Заместителем директора ФСТЭК России 15 февраля 2008 г.)

Данные документ носит некий обобщающий характер, ранее принятых документов с внесением некоторых уточнений.

В главе 3 рассматривается классификация информационных систем персональных данных в том смысле, в котором мы уже проследили ее в нашем курсе.

В главе 4 рассматривается порядок организации обеспечения безопасности ПДн в ИСПДн, который по мнению авторов должен предусматривать:

оценку обстановки;

обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;

разработку замысла обеспечения безопасности ПДн;

выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;

решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;

обеспечение реализации принятого замысла защиты;

планирование мероприятий по защите ПДн;

организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, а также решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;

разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;

развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;

доработку СЗПДн по результатам опытной эксплуатации.

Далее в 5 главе обзорно рассматриваются мероприятия по:

выявлению и закрытию технических каналов утечки ПДн в ИСПДн;

защите ПДн от несанкционированного доступа и неправомерных действий;

установке, настройке и применению средств защиты.

В ней обобщенно рассмативаются мероприятия по защите данных, основанные на методах, детально показанных в документе Приказ ФСТЭК от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

Упоминается рассмотренная ранее классификация сетевых экранов применительно к ИСПДн (ранее рассматривалось для АС в руководящем докумен-

те «Средства вычислительной техники. «Межсетевые экраны». Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»). Указывается, что

Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 3 и 4 классов рекомендуется использовать МЭ не ниже пятого уровня защищенности.

Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 2 класса рекомендуется использовать МЭ не ниже четвертого уровня защищенности.

Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 1 класса рекомендуется использовать МЭ не ниже третьего уровня защищенности.

Даются некоторые рекомендации по анализу защищенности и обнаружению вторжений, рассматриваются вопросы защиты речевой информации. Детально рассматриваются вопросы защиты по электромагнитным каналам в зонах первичного и наведенного излучения (зона 1 и 2).

Для упорядочивания надзора за соблюдением закона «О персональных данных» был введен следующий документ.

Приказ Минкомсвязи РФ № 18 от 30.01.2010 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных»»

Им устанавливается административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции "Ведение реестра операторов, осуществляющих обработку персональных данных". В котором устанавливаются сроки и последовательность административных процедур и административных действий Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальных органов, а также

порядок взаимодействия Минкомсвязи и его территориальных органов с операторами, осуществляющими обработку персональных данных, при осуществлении полномочий по ведению реестра операторов, осуществляющих обработку персональных данных.

Главным образом в этом документе говорится о правилах ведения реестра операторов.

Глава III. п.24 устанавливает, что уведомление о обработке персональных данных, предусмотренное законом о персональных данных, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. В документе перечисляются сведения, которые должны содержаться в уведомлении, при этом производится отсылка к Закону о персональных данных и дается собственный перечень. Однако в Законе о персональных данных это перечень более полный, приведем его. И так в уведомлении должно содержаться:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных статьями 18_1 и 19 настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств (пункт в редакции, введенной в действие с 27 июля 2011 года Федеральным законом от 25 июля 2011 года N 261-ФЗ, распространяется на правоотношения, возникшие с 1 июля 2011 года, - см. предыдущую редакцию);

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной

почты (пункт дополнительно включен с 27 июля 2011 года Федеральным законом от 25 июля 2011 года N 261-ФЗ, распространяется на правоотношения, возникшие с 1 июля 2011 года);

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки (пункт дополнительно включен с 27 июля 2011 года Федеральным законом от 25 июля 2011 года N 261-ФЗ, распространяется на правоотношения, возникшие с 1 июля 2011 года);

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации (пункт дополнительно включен с 27 июля 2011 года Федеральным законом от 25 июля 2011 года N 261-ФЗ, распространяется на правоотношения, возникшие с 1 июля 2011 года).

В рассмотренных нами ранее нормативных актах неоднократно упоминалось, что при защите ПДн возможно использование средств криптографии. В большинстве случаев этого не требуется (см. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. «Классификация автоматизированных систем и требования по защите информации».), поскольку ИСПДн чаще всего относятся к классу 1Г. Однако, если ИСПДн подключена к сетям международного обмена, коей является Интернет, то согласно Указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению ин-формационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» требуется использование средств шифрования, а также согласно документу «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» ИСПДн 1 класса при многопользовательском режиме обработки ПДн должны использовать методы шифрования.

Поэтому рассмотрим еще два документа, которые позволят определить меры и мероприятия при криптографической защите информации не содержащей государственную тайну.

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/5-144)

Данные рекомендации позволяют сформировать модель угроз в случае, когда оператор установил необходимость обеспечения безопасности персональных данных с использованием криптосредств.

В этом документе особо подчеркивается, для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства. В противном случае, результат не достигается.

Различают модель угроз верхнего уровня и детализированную модель угроз.

Модель угроз верхнего уровня предназначена для определения характеристик безопасности защищаемых персональных данных и других объектов защиты. Эта модель также определяет исходные данные для детализированной модели угроз.

Детализированная модель угроз предназначена для определения требуемого уровня криптографической защиты.

П. 3.2. формулирует методологию формирования модели угроз верхнего уровня. При формировании этой модели учитываются:

- условия создания и использования персональных данных (кто и для кого создает ПДн, правила обработки информации в ИСПДн и обеъкты, могущие нести уязвимости);

- формы представления персональных данных (т.е. какими программные средствами и в каких участках памяти они формируются);

- информация, сопутствующая процессам создания и использования персональных данных (ключевая, аутендификационная, конфигурационная, регистрационная, резервная остаточная);

- характеристики безопасности (конфиденциальность, целостность и доступность).

Для формирования детализированной модели угроз требуется различать атаки и угрозы не являющиеся атаками.

Угрозы не являющиеся атаками: природные явления, социально–политические, ошибочные действия (от непредумышленного искажения данных до нарушения правил хранения информации).

Атаки могут осуществляться ка на этапе проектирования ИСПДн и системы защиты так и на этапе эксплуатации.

На этапах разработки, производства и транспортировки технических и программных средств криптосредства атаки могут проводиться только вне зоны ответственности оператора.

На этапе хранения технических и программных средств криптосредства атаки могут проводиться как в зоне, так и вне зоны ответственности оператора;

И на этапе ввода в эксплуатацию технических и программных средств криптосредства атаки могут проводиться в зоне ответственности оператора.

На этапе эксплуатации атаки характеризуются объектом, типом нарушителя, целями, имеющейся у нарушителя информацией об объекте атаки, имеющимся у нарушителя средствами атаки и каналами атаки.

Объекты атаки:

- документация на криптосредство и на технические и программные компоненты СФК;

- защищаемые персональные данные;

- ключевая, аутентифицирующая и парольная информация;

- криптографически опасная информация (КОИ);

- криптосредство (программные и аппаратные компоненты криптосредства);

- технические и программные компоненты СФК;

- данные, передаваемые по каналам связи;

- помещения, в которых находятся защищаемые ресурсы информационной системы.

Атаки тесно связаны с личностью нарушителя, его возможностями и способностями. Поэтому в данном документе дается правило построения модели нарушителя.

Различают шесть основных типов нарушителей: H_1, H_2, ... , H_6

Возможности нарушителя типа H_{i+1} включают в себя возможности нарушителя типа H_i ($1 \leq i \leq 5$).

В документе указывается какой тип нарушителя (H_1, ... , H_6) какой информацией об объекте обладает атаки и какими средствами нападения располагает.

Далее описываются каналы атаки:

- каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами;
- штатные средства.
- Возможными каналами атак, в частности, могут быть:
- каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);
- машинные носители информации;
- носители информации, выведенные из употребления;
- технические каналы утечки;
- сигнальные цепи;
- цепи электропитания;
- цепи заземления;
- канал утечки за счет электронных устройств негласного получения информации;
- информационные и управляющие интерфейсы СВТ.

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 (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622)

Данный документ определяет порядок организации и обеспечения функционирования криптографических средств, в случае их использования для обеспечения безопасности ПДн при их обработке в ИСПДн.

В п. 2.3. документа указывается порядок мероприятий, которые проводит оператор, обязательных для осуществления эффективной защиты ИСПДн криптосредствами. Вот краткий список этих мероприятий:

- разработка для каждой ИСПДн модели угроз безопасности ПДн при их обработке;

- разработка на основе модели угроз системы безопасности ПДн, обеспечивающей нейтрализацию всех перечисленных в модели угроз;

- определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств (защита от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, распространения);

- установка и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;

- проверка готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;

- обучение лиц, использующих криптосредства, работе с ними;

- поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе;

- контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

- разбирательство и составление заключений по фактам нарушения условий хранения носителей ПДн, использования криптосредств, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание организационных и технических мер, необходимых при обеспечении безопасности ПДн с использованием криптосредств, с указанием в частности:

а) индекса, условного наименования и регистрационных номеров используемых криптосредств;

б) соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;

в) соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;

г) выполнения Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Как было ранее сказано, описание принятых мер должно быть включено в уведомление об обработке ПДн.

Далее указываются обязанности пользователей криптосредств, важнейшим из которых является индивидуальная ответственность пользователя за вверенное ему криптосресдтво.

Параграф 3 посвящен порядку обращения с криптосредствами. В нем указываются такие моменты как:

- обязанности пользователей,

- правила передачи криптоключей,

- правила учета криптосредств,

- правила передачи криптосредств и документации к ним,

- правила контроля за целостностью криптосредств и их уничтожением.

Параграф 4. посвящен оборудованию помещений, с которых размещены криптосредства.

В контексте рассматриваемого вопроса об обеспечении безопасности персональных данных следует упомянуть еще несколько документов:

Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных (Утверждены Постановлением Правительства Российской Федерации от 6 июля 2008 г. N 512)

Нормативный акт требует защиту от несанкционированного доступа к биометрическим данным, хранящимся на носителе, возможность идентификации системы и оператора, осуществившего запись, проверку наличия письменного согласия субъекта на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством РФ.

Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

В ст.1 указывается, что обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации

(неавтоматизированной), если такие действия с персональными данными, как ***использование***, ***уточнение***, ***распространение***, ***уничтожение*** персональных данных в отношении каждого из субъектов персональных данных, ***осуществляются при непосредственном участии человека***.

ст.2 указывает, что обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Эти два положения указывают на то, что обработка персональных данных только тогда считается автоматизированной, когда изменение в содержании, состоянии или размещении данных в системе может происходить без непосредственного участия лица, осуществляющего обработку или ответственного за хранение и передачу персональных данных.

Поэтому, если персональные данные хранятся в системе в виде файлов, обрабатываемых текстовым процессором или электронными таблицами или в формате базы данных и используются, без применения процедур (макропрограмм) автоматизации обработки, то такую обработку можно считать неавтоматизированной.

Федеральный закон об электронной цифровой подписи

Средства цифровой подписи относятся к удостоверительным средствам, однако, поскольку в них используются алгоритмы криптографического преобразования, к средствам реализующим эту процедуру применяются те же требования, что и к обычным криптографическим средствам.

1. Организационные основы

Существует четыре группы документов, которые должны разрабатываться и вестись при проведении мероприятий по обеспечению ИБ:

1- Документы, содержащие положения корпоративной политики ИБ (определяют высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенные для организации в целом),

2- Документы, содержащие положения частных политик ИБ (детализируют положения корпоративной политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации)

3- Документы, содержащие требования информационной безопасности к процедурам (содержат: правила и параметры, устанавливающие способ осуществления и выполнения конкретных действий, связанных с ИБ; ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых технологических процессах),

4- Документы, содержащие свидетельства выполненной деятельности по обеспечению информационной безопасности (Отражают достигнутые результаты по обеспечению ИБ организации).

Тема 5. *ДОКУМЕНТАРНОЕ ОБЕСПЕЧЕНИЕ МЕРОПРИЯТИЙ*

Документы, которые подтверждают принятие мер по обеспечению информационной безопасности:

1. Приказ о назначении структурного подразделения или должностного лица (работника), ответственного за обеспечение безопасности персональных данных;
2. Приказ или распоряжение об утверждении списка лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей;
3. Учтенный установленным порядком в делопроизводстве журнал учета допуска к работе в ИСПДн, обеспечивающий учет логических имен пользователей;
4. Учтенный установленным порядком в делопроизводстве журнал учета средств защиты информации, эксплуатационной и технической документации к ним;

5. Учтенный установленным порядком в делопроизводстве журнал учета машинных носителей персональных данных;
6. Перечень персональных данных, подлежащих защите;
7. Акт классификации ИСПДн;
8. Частная модель угроз с протоколами экспертной оценки актуальности угроз. До разработки модели должны быть приняты следующие документы:

   • решение об актуальности угроз безопасности персональных данных принимается исключительно на основании экспертной оценки,

   • протоколы экспертной оценки должны разрабатываться и оформляться экспертами (специалистами в области защиты информации).

   При этом низкая опасность исключенных угроз безопасности информации может быть подтверждена:

   • многократным превышением стоимости реализации угрозы над стоимостью ущерба, наносимого субъекту персональных данных, в случае ее реализации,

   • низким значением вероятности реализации угрозы, определенной по результатам статистически значимого количества инструментальных обследований однотипных объектов
9. Требования по обеспечению безопасности персональных данных при их обработке в ИСПДн, в том числе:

   • порядок охраны и допуска лиц (в том числе посторонних) в помещения, в которых установлены технические средства ИСПДн;

   • условия расположения относительно границы контролируемой зоны).
10. Инструкция по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения ИСПДн, информационных массивов персональных данных и технических средств защиты;

11. Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн. Данный документ включает в себя:

- общий порядок организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- обязанности должностных лиц, эксплуатирующих ИСПДн, в части обеспечения безопасности персональных данных при их обработке в ИСПДн;
- порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и нарушения порядка предоставления персональных данных, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления;
- порядок обучения администраторов средств (систем) защиты информации, в том числе средств антивирусной защиты, и первичного инструктажа пользователей;
- порядок проверки электронного журнала обращений к ИСПДн;
- правила парольной защиты;
- правила антивирусной защиты;
- правила обновления общесистемного и прикладного программного обеспечения;
- порядок контроля за соблюдением условий использования средств защиты информации.

12. Описание конфигурации и топологии ИСПДн, физических, функциональных и технологических связей, а также режимов обработки персональных данных;
13. Описание степени участия персонала в обработке персональных данных;
14. Матрица доступа для ИСПДн;
15. Перечни технических средств ИСПДн, общесистемного и прикладного программного обеспечения, используемого в ней;
16. Приказ о назначении подразделения (лица), ответственного за эксплуатацию средств защиты информации;
17. Эксплуатационная документация на ИСПДн и средства защиты информации для пользователей и администратора, в том числе антивирусной защиты (для каждого средства защиты должны быть представлены инструкции по их установке и настройке, инструкции администратору и пользователю);

18. Акт установки и настройки средств защиты информации, который подтверждает, что внедренные технические мероприятия обеспечивают выполнение требований по обеспечению безопасности персональных данных при их обработке в данной ИСПДн или что установка и настройка средств защиты информации проведена в соответствии с техническим заданием на ИСПДн (частным техническим заданием на систему защиты персональных данных).

Перечень документов заявителя для аттестации автоматизированной системы.

1. Приказ «О назначении комиссии по сопровождению аттестации автоматизированной системы»
2. Перечень защищаемых помещений, в которых проводятся конфиденциальные мероприятия, и объектов информатизации, используемых для обработки конфиденциальной информации
3. Перечень сведений конфиденциального характера
4. Карта с границами контролируемой зоны

5. Перечень лиц, имеющих право самостоятельного доступа в помещение №____ с АС «____» _____

6. Приказ «О назначении администратора информационной безопасности (уполномоченного по защите информации)»

7. Данные по уровню подготовки кадров, обеспечивающих защиту информации

8. Акт классификации автоматизированной системы «____» _____

9. Перечень защищаемых ресурсов АС «____» _____ и уровень их конфиденциальности

10. Перечень лиц, обслуживающих автоматизированную систему «____» _____

11. Перечень лиц, имеющих право самостоятельного доступа к штатным средствам автоматизированной системы «____» _____

Перечень документов, которые получает аттестуемый и которые он разрабатывает после проведения аттестации:

12. Аттестата соответствия

13. Инструкция по обеспечению защиты конфиденциальной информации, обрабатываемой в АС «____» _____

14. Состав программного обеспечения автоматизированной системы «____» _____

15. Описание технологического процесса обработки информации в АС «____» _____

16. Схема информационных потоков автоматизированной системы «____» (Приложение №1 к Описанию технологического процесса…,)

17. Технический паспорт автоматизированной системы «____» _____

18. Матрица доступа субъектов автоматизированной системы «____» _____ к ее защищаемым информационным ресурсам

19. Акт установки системы защиты информации от несанкционированного доступа «_____» в автоматизированную систему «____»

20. Описание системы разграничения доступа и настроек СЗИ НСД «Secret Net» в АС ОИ «____» _____

21. Распоряжение о допуске сотрудников

22. Распоряжение о вводе в эксплуатацию

Некоторые рекомендации по проведению мероприятий по защите информации и выбору параметров защиты.

В ПДТК должны входить как лица, отвечающие за защиту информации, так и лица руководящего состава. Для назначения ПДТК издается руководителя организации.

План работы ПДТК составляется более чем на полгода. В конце каждого полугодия подводятся итоги по результатам выполнения плана.

Деятельность комиссии ПДТК оформляется протоколами заседаний.

Перед категорированием информации должна быть создана комиссия по категорированию и классификации объектов информатизации. Деятельность ее регламентируется положением о комиссии по категорированию и классификации объектов информатизации, которое должно утверждаться руководителем организации.

Категорирование информации производится и утверждается данной комиссией о чем составляется акт.

Информационно-логический паспорт объекта информатизации включает в себя:

- сведения о должностных лицах,
- сведения о специалистов по ИБ,
- сведения о ЛВС,
- перечень объектов ВТ,
- физическую схему ЛВС,
- логическую схему ЛВС,
- сведения об опечатывании и блокировании портов ввода-вывода и устройств со сменными носителями,

- схему контролируемой зоны. Границы контролируемой зоны должны соответствовать тому периметру, который реально контролируется и на котором возможно физическое воздействие для пресечения неправомерных действий. Схема составляется поэтажно: вид сверху и вид сбоку. Схема расположения объектов информатизации в пределах контролируемой зоны составляется таким образом, что бы на ней были показаны все возможные каналы утечки информации: проводные телефонные линии, линии электропередач до трансформаторной подстанции или до границ контролируемой зоны, оконные и дверные проемы, линии пожарной сигнализации и пр.,
- перечень используемых программных продуктов,
- информационные ресурсы, обрабатываемые и хранящиеся на бумажных носителях,
- перечень информационных ресурсов по категории критичности,
- объекты и субъекты защиты, модель угроз информационной безопасности,
- перечень объектов информатизации, подлежащих защите,
- модель угроз ИСПДн,
- модель угроз и вероятного нарушителя,

Акт классификации автоматизированной системы (АС) и акт классификации ИСПДн должны составляться согласно требованиям нормативных актов.

Методические рекомендации по организации доступа к информационным ресурсам автоматизированной системы с использованием парольной защиты и методические рекомендации по обеспечению безопасности работе в локальной сети для пользователей должны присутствовать на рабочих местах сотрудников.

Список пользователей ИСПДн с указанием ролей, если ИСПДн обладает собственными средствами разграничения доступа.

Порядок ограничения доступа к информации, хранящейся в электронном виде должен предусматривать рекомендации пользователям по размещению

информации в открытых и закрытых ресурсах, если в системе отсутствует мандатная защита.

Матрица доступа к защищаемым информационным ресурсам должна содержать следующие сведения: наименование сетевых информационных и программных ресурсов, путь доступа, полномочия на сетевые ресурсы (чтение папки, чтение, запись, выполнение, печать файлов).

Рекомендации об учете, порядке работы, хранения, уничтожения документов и машиночитаемых носителей информации должны учитывать разновидности носителей информации по физическому принципу записи информации.

Перечень защищаемых помещений должен содержать список помещений с указанием из расположения относительно других помещений. Информация должна носить гриф - для служебного пользования.

Технические паспорта защищаемых помещений включают перечень оборудования, могущего представлять собой каналы утечки информации, линий электропроводки и проходящих (а не только исходящих) линий связи и электропитания, степень электромагнитной и акустической проницаемости стен и оконных проемов.

Порядок доступа сотрудников в защищаемые помещения определяет прием – сдачу ключей или порядок смены и предоставления сотрудникам кодов доступа.

Должны вестись журналы: учета СКЗИ, выдачи СКЗИ пользователям, доступа с защищаемые помещения, учета записанных носителей с ПДн, учета носителей информации

Группа обеспечения информационной безопасности комплектуется специалистами хорошо владеющими системным администрированием и разбирающимися в физических основах передачи и хранения информации.

Периодически должны проводиться проверки контроля состояния информационной безопасности.

Должен постоянно вестись учет программно-аппаратного обеспечения объектов информатизации. При замене какого-нибудь устройства ВТ, необходимо это факт отражать в ведомости учета СВТ.

Для составления матрицы доступа и определения объектов уязвимостей предварительно производится учет информационных ресурсов.

Мероприятия, которые необходимо произвести в начале создания системы безопасности: опечатывание корпусов, блокирование портов ввода/вывода, установка лицензионного антивирусного обеспечения, разграничение прав доступа (в windows наиболее эффективно это выполняется на основе групповых политик), установка расписания резервирования наиболее критичной информации.

Контроль утечек информации производится либо с использованием специализированных аппаратных средств (с привлечением специалистов, имеющих лицензию на это вид деятельности) и проделывается это как правило при проведении повторных аттестаций, либо визуальным осмотром, при котором необходимо убедиться в том, что все СВТ находятся на своих местах и не появилось никаких дополнительных средств, могущих передавать информацию (в том числе и методом электромагнитных наводок).

Мероприятия по организации защищенного электронного межведомственного документооборота состоят в организации выдачи и поддержания использования средств ЭЦП. Носители ключевой информации должны учитываться в журнале.

Установка средств разграничения доступа в сети как правило заключается во введении в эксплуатацию межсетевого экрана. Межсетевой экран должен быть сертифицирован в РФ.

Примеры оформления некоторых организационно-распорядительных документов

Рекомендуемый перечень
организационно-распорядительных документов для организации защиты информации
в органах исполнительной власти субъекта Российской Федерации

№ п/п	Наименование документа	Каким нормативным правовым актом определен	Каким документом регламентирована разработка	Кем вводится в действие
1.	Положение о порядке организации и проведения работ по защите конфиденциальной информации	СТР-К	СТР-К	Утверждается руководителем
2.	Положение о ПДТК, План работы ПДТК	Положение-93	Совместный приказ Директора ФСБ России и Председателя Гостехкомиссии России от 28.07.01 г. № 309/405	Утверждается руководителем
3.	Перечень сведений конфиденциального характера	СТР-К	Указ Президента РФ от 06.03.97 г. № 188, Федеральные законы, СТР-К	Утверждается руководителем
4.	Перечень информационных ресурсов органа управления	ФЗ 20.02.95 г. № 24-фз	Методические рекомендации Гостехкомиссии России Решение ГТК России от 21.04.98 № 18	Утверждается руководителем
5.	Положение о подразделении по защите информации	Положение-93, Решение Гостехкомиссии России от 14.03.95 г. № 32	Решение Гостехкомиссии России от 14 03 95 г. № 32	Утверждается руководителем
6.	Должностные обязанности специалистов по защите информации (ЗИ)	Положение-93, Решение Гостехкомиссии России от 14.03.95 г. № 32	Решение Гостехкомиссии России от 14 03 95 г. № 32	Утверждаются руководителем
7.	Перспективный план по организации ЗИ	СТР-К	Решение Гостехкомиссии России от 03.10.95 № 42.	Утверждается руководителем
8.	План организации ЗИ на год	СТР-К	Решение Гостехкомиссии России от 03.10.95 № 42.	Утверждается руководителем
9.	План контроля эффективности ЗИ	Положение-93		Утверждается руководителем
10.	Перечень объектов информатизации, подлежащих защите	СТР-К	СТР-К	Утверждается руководителем
11.	Аттестаты соответствия	СТР-К	СТР-К	
12.	Приказ о создании комиссии по категорированию и классификации объектов информатизации, Акт классификации объектов информатизации	СТР-К	СТР-К	Утверждается руководителем
13.	Приказ о назначении лиц, ответственных за эксплуатацию объекта информатизации	СТР-К		Утверждается руководителем
14.	Технический паспорт на АС	СТР-К	СТР-К	Утверждается руководителем
15.	Технический паспорт на защищаемое помещение	СТР-К	СТР-К	Утверждается руководителем

16.	Инструкция пользователя при работе на ПЭВМ, имеющих выход в ЛВС органа управления			Утверждается руководителем
17.	Инструкция пользователя при работе на ПЭВМ, имеющих выход в Интернет			Утверждается руководителем

Пример документального оформления перечня сведений конфиденциального характера

Для служебного пользования

Экз. №

УТВЕРЖДАЮ

Руководитель организации

{подпись, инициалы, фамилия)

«____»_____

(дата)

ПЕРЕЧЕНЬ

сведений конфиденциального характера

№ п/п	Наименование сведений	Примечание
1	Сведения, раскрывающие систему, средства защиты информации ЛВС организации от НСД, а также значения действующих кодов и паролей	
2	Сводный перечень работ организации на перспективу, на год (квартал)	
3	Сведения, содержащиеся в лицевых счетах пайщиков страховых взносов	
4	Сведения, содержащиеся в индивидуальном лицевом счете застрахованного лица	
5	Основные показатели задания на проектирование комплекса (установки). НОУ - ХАУ технологии - различные технические, коммерческие и другие сведения, оформленные в виде технической документации	
6	Методические материалы, типовые технологические и конструктивные решения, разработанные организацией и используемые при проектировании	
7	Требования по обеспечению сохранения служебной тайны при выполнении работ в организации	
8	Порядок передачи служебной информации ограниченного распространения другим организациям	

Форма технического паспорта на автоматизированную систему

УТВЕРЖДАЮ

Руководитель организации

{подпись, инициалы, фамилия)

«____»_____

(дата)

ТЕХНИЧЕСКИЙ ПАСПОРТ

(указывается полное наименование автоматизированной системы)

СОГЛАСОВАНО	РАЗРАБОТАЛ
(должность, подпись, инициалы, фамилия представителя подразделения по защите информации) «____»_____ *(дата)*	*(должность, подпись, инициалы, фамилия ответственного за эксплуатацию АС)* «____»_____ *(дата)*

Год

1. Общие сведения об АС

1.1. Наименование АС____

(полное наименование АС)

1.2. Расположение АС_____

(адрес, здание, строение, этаж, комнаты)

1.3. Класс АС_____

(номер и дата акта классификации АС, класс АС)

2. Состав оборудования АС

2.1. Перечень основных технических средств и систем, входящих в состав АС

№ п/п	Тип ОТСС	Заводской Номер	Сведения по сертификации, специсследованиям и спецпроверкам

2.2. Перечень вспомогательных технических средств, входящих в состав АС (средств вычислительной техники, не участвующих в обработке конфиденциальной информации)

№ п/п	Тип ВТСС	Заводской номер	Примечание

2.3. Структура, топология и размещение ОТСС относительно границ контролируемой зоны объекта:

Структурная (топологическая) схема с указанием информационных связей между устройствами, схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны, схема прокладки линий передачи конфиденциальной информации с привязкой к . границам контролируемой зоны объекта.

2.4. Системы электропитания и заземления:

Схемы электропитания и заземления ОТСС объекта, схемы прокладки кабелей и шины заземления, схемы расположения трансформаторной подстанции и заземляющих устройств с привязкой к границам контролируемой зоны объекта, схемы электропитания розеточной и осветительной сети объекта, сведения о величине сопротивления заземляющего устройства.

2.5. Перечень средств защиты информации, установленных на АС

№ п/п	Наименование и тип технического средства	Заводской номер	Сведения о сертификате	Место и дата установки

2.6. Перечень используемых в АС программных средств

№ п/п	Наименование и тип программного средства	Серийный номер (номер лицензии)	Сведения о сертификате	Дата установки

3. Сведения об аттестации объекта информатизации на соответствие Требованиям по безопасности информации

Инвентарные номера аттестата соответствия, заключения по результатам аттестационных испытаний, протоколов испытаний и даты их регистрации.

4. **Результаты периодического контроля**

Дата проведения	Наименование организации, проводившей проверку	Результаты проверки, номер отчетного документа

Лист регистрации изменений

Форма технического паспорта на защищаемое помещение

УТВЕРЖДАЮ

Руководитель организации

{подпись, инициалы, фамилия)

«____»_____

(дата)

ТЕХНИЧЕСКИЙ ПАСПОРТ

на защищаемое помещение № _____

СОСТАВИЛ

(должность, подпись, инициалы, фамилия специалиста подразделения по защите информации)

«____»_____

(дата)

РАЗРАБОТАЛ

(должность, подпись, инициалы, фамилия ответственного за помещение)

«____»_____

(дата)

Год

1. Памятка

по обеспечению режима безопасности и эксплуатации
оборудования, установленного в защищаемом
помещении №_____

(Примерный текст)

1. Ответственность за режим безопасности в защищаемом помещении (ЗП) и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, или лицо, специально на то уполномоченное.

2. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с подразделением (специалистом) по защите информации предприятия.

3. В нерабочее время помещение должно закрываться на ключ.

4. В рабочее время, в случае ухода руководителя, помещение должно быть закрыто на ключ или оставлено под ответственность лиц, назначенных руководителем подразделения.

5. При проведении конфиденциальных мероприятий бытовая радиоаппаратура, установленная в помещении (телевизоры, радиоприемники и т.п.), должна отключаться от сети электропитания.

6. Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

7. Должны выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении.

8. Запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи. При установке в ЗП, имеющих выход в городскую АТС, телефонных и факсимильных аппаратов с автоответчиком и (или) спикерфоном следует отключать эти аппараты на время проведения конфиденциальных мероприятий.

9. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение, и служба безопасности организации.

10. Периодический контроль эффективности мер защиты помещения осуществляется специалистами по защите информации.

Примечание.

В памятку целесообразно включать и другие сведения, учитывающие особенности установленного в ЗП оборудования, действия персонала в случае срабатывания установленной в помещении пожарной и охранной сигнализации, порядок включения средств защиты, организационные меры защиты и т.п.

2. Перечень оборудования, установленного в помещении

Вид оборудования	Тип	Учетный (зав.) номер	Дата установки	Класс ТС (ОТСС или ВТСС)	Сведения по сертификации, специсследованиям и спецпроверкам

3. Меры защиты информации

(Пример)

1. Телефонный аппарат коммутатора директора (инв. № 7). Выполнены требования предписания на эксплуатацию (Перечень предусмотренных мер защиты согласно предписанию).

2. Телефонный аппарат № 7-17.

На линию установлено защитное устройство «Сигнал-5», зав. № 017.

3. Пульт коммутатора.

Выполнены требования предписания на эксплуатацию.

4. Часы электронные.

Выполнены требования предписания на эксплуатацию.

5. Вход в помещение оборудован тамбуром, двери двойные, обшиты слоем ваты и дерматина. Дверные притворы имеют резиновые уплотнения.

6. Доступ к вентиляционным каналам, выходящим на чердак здания, посторонних лиц исключен (приводятся предусмотренные для этого меры).

4. Отметка о проверке средств защиты

Вид оборудования	Учетный номер	Дата проверки	Результаты проверки и № отчетного документа

5. Результаты аттестационного и периодического контроля помещения

Дата проведения	Результаты аттестации или периодического контроля, № отчетного документа	Подпись проверяющего

Форма аттестата соответствия автоматизированной системы

АТТЕСТАТ СООТВЕТСТВИЯ

требованиям по безопасности информации

_____

(указывается полное наименование автоматизированной системы)

№

Выдан «____»_____

(дата)

----------*Со следующей страницы*----------

1. Настоящим АТТЕСТАТОМ удостоверяется:_____

_____

(полное наименование автоматизированной системы)

класс защищенности _____, соответствует требованиям нормативной документации по безопасности информации.

Состав комплекса технических средств автоматизированной системы (АС) с указанием заводских номеров, модели, изготовителя, номеров сертификатов соответствия, схема размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов соответствия) указаны в техническом паспорте на АС.

2. Организационная структура и уровень подготовки специалистов обеспечивают поддержание уровня защищенности АС в процессе эксплуатации в соответствии с установленными требованиями.

3. Аттестация АС выполнена в соответствии с программой и методиками аттестационных испытаний, утвержденными руководителем организации (указываются номера документов).

4. С учетом результатов аттестационных испытаний в АС разрешается обработка конфиденциальной информации..

5. При эксплуатации АС запрещается:

■ вносить изменения в комплектность АС, которые могут

снизить уровень защищенности информации;

■ проводить обработку защищаемой информации без выполнения всех мероприятий по защите информации;

■ подключать к основным техническим средствам нештатные блоки и устройства;

■ вносить изменения в состав, конструкцию, конфигурацию, размещение средств вычислительной техники;

■ допускать к обработке защищаемой информации лиц, не оформленных в установленном порядке;

■ производить копирование защищаемой информации на неучтенные магнитные носители информации, в том числе для временного хранения информации;

■ работать при отключенном заземлении;

■ обрабатывать на ПЭВМ защищаемую информацию при обнаружении каких-либо неисправностей.

6. Контроль за эффективностью реализованных мер и средств защиты возлагается

_____

(наименование подразделения, должность лица, осуществляющего контроль)

7. Результаты аттестационных испытаний приведены в заключении аттестационной комиссии (№ ___ от ____) и протоколах испытаний.

8. «Аттестат соответствия» выдан на ___ года (лет), в течение которых должна быть обеспечена неизменность условий функционирования АС и технологии обработки защищаемой информации, могущих повлиять на характеристики защищенности АС.

Руководитель аттестационной комиссии

_____

(должность с указанием наименования организации, подпись, инициалы, фамилия)

«_____»_____

(дата)

Отметки органа надзора

Форма аттестата соответствия защищаемого помещения

АТТЕСТАТ СООТВЕТСТВИЯ

требованиям по безопасности информации

_____

(наименование защищаемого помещения)

№

Выдан «____»_____

(дата)

----------*Со следующей страницы*----------

1. Настоящим Аттестатом удостоверяется:

_____

(полное наименование защищаемого помещения)

с установленным в нем оборудованием соответствует требованиям нормативных документов по безопасности информации (Заключение по результатам аттестации №____ от____) и в нем разрешается проведение конфиденциальных мероприятий.

Схема размещения помещения относительно границ контролируемой зоны, перечень установленного в нем оборудования, используемых средств защиты информации указаны в техническом паспорте на защищаемое помещение (ЗП).

2. Установленный порядок пользования ЗП позволяет осуществлять его эксплуатацию, расположенного в нем оборудования и средств защиты в соответствии с требованиями по защите конфиденциальной информации.

3. Повседневный контроль за выполнением установленных правил эксплуатации ЗП осуществляется_____

(наименование подразделения, фамилия должностного лица, осуществляющего контроль)

4. В ЗП запрещается проводить ремонтно-строительные работы, замену (установку новых) элементов интерьера, вносить изменения в состав оборудования и средства защиты информации без согласования с_____

(наименование подразделения, фамилия должностного лица, осуществляющего контроль)

5. Лицо, ответственное за эксплуатацию защищаемого помещения, обязано незамедлительно извещать_____

(наименование подразделения, фамилия должностного лица, осуществляющего контроль)

■ о предполагаемых ремонтно-строительных работах и изменениях в размещении и монтаже установленного оборудования, технических средств и систем, средств защиты информации, в интерьере помещения;

■ о нарушениях в работе средств защиты информации;

■ о фактах несанкционированного доступа в помещение.

Руководитель аттестационной комиссии

_____

(должность с указанием наименования организации, подпись, инициалы, фамилия)

«_____»_____

(дата)

Отметки органа надзора

Форма акта классификации автоматизированной системы, предназначенной для обработки конфиденциальной информации

Для служебного пользования

Экз. №

УТВЕРЖДАЮ

Руководитель организации

{подпись, инициалы, фамилия)

«____»_____

(дата)

АКТ

классификации автоматизированной системы, предназначенной для обработки конфиденциальной информации

_____

(наименование автоматизированной системы)

Комиссия в составе:

Председатель_____

члены комиссии_____

_____;_____

рассмотрев исходные данные на автоматизированную систему (АС)_____,

(наименование автоматизированной системы)

условия ее эксплуатации (многопользовательский, однопользовательский с равными или разными правами доступа к информации), с учетом характера обрабатываемой информации (служебная тайна, коммерческая тайна, персональные данные и т.д.) и в соответствии с руководящими документами Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»,

РЕШИЛА

Установить АС_____

(наименование автоматизированной системы)

Класс защищенности _____

Председатель комиссии _____ _____

личная подпись инициалы, фамилия

Члены комиссии: _____ _____

личная подпись инициалы, фамилия

_____ _____

личная подпись инициалы, фамилия

ТИПОВАЯ ФОРМА

журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

№ п.п.	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

ТИПОВАЯ ФОРМА

технического (аппаратного) журнала

№ п.п.	Дата	Тип и регистрационные номера используемых криптосредств	Записи по обслуживанию криптосредств	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны криптосредств, в которую введены криптоключи	Дата	Подпись пользователя криптосредств	
1	2	3	4	5	6	7	8	9	10

КОНТРОЛЬНЫЕ ВОПРОСЫ

К КУРСУ «ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ»

1. Какая мысль положена в основу законодательства, защищающего персональные данные граждан?
2. Каковы основные направления деятельности по защите персональных данных?
3. Является ли гражданин, чьи персональные данные содержатся в автоматизированной информационной системе обладателем персональных данных?
4. В каких случаях персональные данные гражданина могут быть переданы оператором третьей стороне без испрашивания разрешения?
5. Зачем нужны нормы, устанавливающие отношения в области сертификации и лицензирования, для защиты персональных данных?
6. Каковы основные направления защиты информации в автоматизированных системах?
7. Каковы исходные данные для классификации автоматизированных (информационных) систем?
8. Объясните классификацию автоматизированных систем согласно руководящему документу «Классификация автоматизированных систем и требования по защите информации».
9. Опишите кратко систему мероприятий по защите информации в автоматизированных системах класса 1Г.
10. Какие показатели защищенности автоматизированных систем Вы знаете?
11. Какой класс защищенности следует выбрать для автоматизированных система класса 1Г?
12. Разрешено ли подключать системы, содержащие персональные данные категории 3 и выше к сети Интернет?
13. Как определяется класс типовой информационной системы персональных данных?

14. По каким основаниям определяется класс специальной информационной системы персональных данных?
15. Каким образом и для чего разрабатывается частная модель угроз безопасности персональных данных?
16. Опишите методику определения актуальности угроз персональным данным.
17. Опишите систему методов и способов защиты информации от несанкционированного доступа в системах, хранящих персональные данные? Каким документов вводятся эти меры?
18. Каковы рекомендации ФСБ России по использованию криптосредств для защиты персональных данных?
19. Каковы каналы атаки на информационные системы персональных данных, описываемые в Методических рекомендациях по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации?
20. Кратко охарактеризуйте порядок мероприятий, которые должен проводить оператор, для осуществления эффективной защиты ИСПДн криптосредствами.
21. Перечислите основные организационно-распорядительные документы по информационной безопасности.