Информационная безопасность

Лебедева Т.Ф.

Политика безопасности компьютерных систем и ее реализация 1

Государственные документы об информационной безопасности

Первоначально информационная безопасность была прерогативой государственных организаций, имеющих дело с секретной информацией или отвечающих за обеспечение режима секретности.

В 1983 году Министерство обороны США выпустило книгу в оранжевой обложке с названием ***"Критерии оценки надежных компьютерных систем" (Trusted Computer System Evaluation Criteria, TCSEEC),*** положив тем самым начало систематическому распространению знаний об информационной безопасности за пределами правительственных ведомств, Во второй половине 1980-х годов аналогичные по назначению документы были изданы в ряде Европейских стран.

В 1992 году в России Гостехкомиссия при Президенте РФ издала серию брошюр, посвященных проблеме защиты от несанкционированного доступа. Эта серия не получила широкого распространения.

"Оранжевая книга" и издания, следующие в ее фарватере, не дают ответов на вопросы:

- Как строить безопасные, надежные системы?
- Как поддерживать режим безопасности?
- Какие технические средства имеются на рынке для обеспечения информационной безопасности в офисе?

поскольку ориентированы в первую очередь на разработчиков информационных систем, а не менеджеров. Да и оценки важности различных аспектов безопасности в государственных и коммерческих структурах различны

Политика безопасности компьютерных систем и ее реализация 2

Государственные документы об информационной безопасности

Для режимных государственных организаций на первом месте стоит конфиденциальность, а целостность понимается исключительно как неизменность информации.

Для *коммерческих структур*, вероятно, важнее всего *целостность* (актуальность) и *доступность* данных и услуг по их обработке. По сравнению с государственными, коммерческие организации более открыты и динамичны, поэтому вероятные угрозы для них отличаются и количественно, и качественно.

В "Оранжевой книге" надежная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Идейной основой набора Руководящих документов по защите информации от НСД является "Концепция защиты СВТ и" АС от НСД к информации". Концепция "излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД), являющейся частью общей проблемы безопасности информации".

Политика безопасности компьютерных систем и ее реализация 3

Государственные документы об информационной безопасности

В Концепции различаются понятия средств вычислительной техники (СВТ) и автоматизированной системы (АС).

СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации. ...

Существуют различные способы покушения на информационную безопасность — радиотехнические, акустические, программные и т.п. Среди них несанкционированный доступ к информации (НСД) выделяется как *"доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.*

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС."

Политика безопасности компьютерных систем и ее реализация 4

Государственные документы об информационной безопасности

В Концепции формулируются следующие основные принципы защиты от НСД к информации:

"...

3.2, Защита СВТ обеспечивается комплексом программно-технических средств.

3.3. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

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.

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

3.6. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

3.7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами."

Политика безопасности компьютерных систем и ее реализация 5

Государственные документы об информационной безопасности

В качестве модели нарушителя в АС рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС.

"Нарушители классифицируются по уровню возможностей, предоставляемых им этими средствами. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

*4.2. **Первый уровень** определяет самый низкий уровень возможностей ведения диалога в АС — запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.*

***Второй уровень** определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.*

***Третий уровень** определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.*

***Четвертый уровень** определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.*

4.3. В своем уровне нарушитель является специалистом высшей квалификации, знает все о АС и, в частности, о системе и средствах ее защиты."

Политика безопасности компьютерных систем и ее реализация 6

Государственные документы об информационной безопасности

В качестве главного средства защиты от НСД к информации в Концепции рассматривается система разграничения доступа (СРД) субъектов к объектам доступа. Основными функциями СРД являются:

- *"реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;*
- *реализация ПРД субъектов и их процессов к устройствам создания твердых копий;*
- *изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;*
- *управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;*
- *реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам."*

Политика безопасности компьютерных систем и ее реализация 7

Государственные документы об информационной безопасности

"Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс — седьмой, самый высокий — первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- *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".*

Политика безопасности компьютерных систем и ее реализация 8

Государственные документы об информационной безопасности

"Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

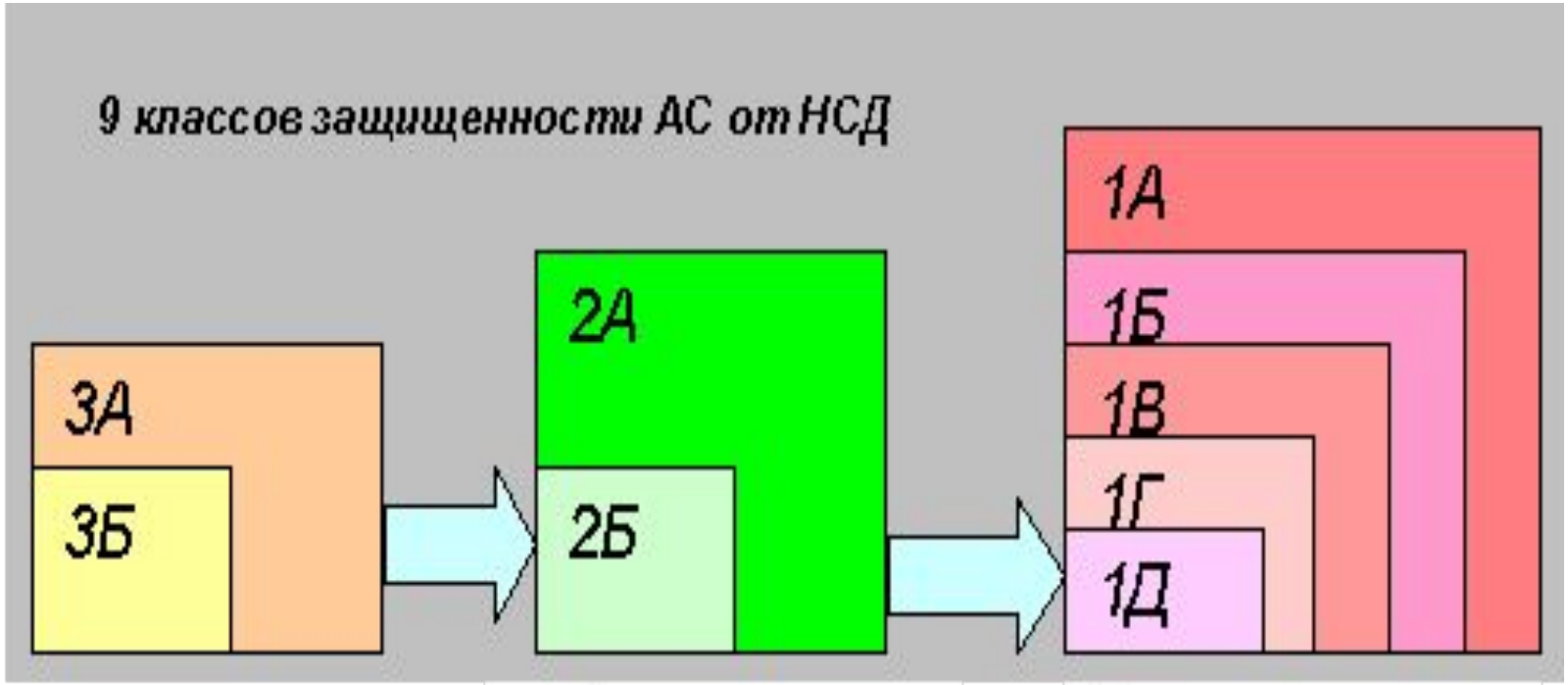
Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

***Третья группа** классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса — 3Б и 3А.*

***Вторая группа** классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса — 2Б и 2А.*

***Первая группа** классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А."*

Классификация АС по степени защищенности от НСД



Один пользователь, допущенный ко все информации

Пользователи имеют одинаковые права доступа

Многопользовательские АС
Не все пользователи имеют права доступа ко все информации

Политика безопасности компьютерных систем и ее реализация 10

Государственные документы об информационной безопасности

Требования к классу защищенности 1В:

Подсистема управления доступом:

- *должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;*
- *должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и/или адресам;*
- *должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;*
- *должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;*
- *должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.*

Политика безопасности компьютерных систем и ее реализация 11

Государственные документы об информационной безопасности

Подсистема регистрации и учета:

- *должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова;*
- *должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию;*
- *должна осуществляться регистрация запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;*
- *должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;*
- *должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа;*
- *должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;*
- *должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал; учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);*

Государственные документы об информационной безопасности

- *должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двухкратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;*
- *должна осуществляться сигнализация попыток нарушения защиты.*

Подсистема обеспечения целостности:

- *должна быть обеспечена целостность программных средств ситемы защиты информации (СЗИ) НСД, а также неизменность программной среды, при этом: целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ, целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;*
- *должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;*

Политика безопасности компьютерных систем и ее реализация 13

Государственные документы об информационной безопасности

- *должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение,нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;*
- *должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;*
- *должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности; должны использоваться сертифицированные средства защиты."*

По существу перед нами минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации

Политика безопасности компьютерных систем и ее реализация 14

Требования законодательства к средствам защиты ПД

В соответствии с Законом **персональные данные** - любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПД). К персональным данным в связи с этим могут относиться

- фамилия, имя, отчество,
- год, месяц, дата и место рождения,
- адрес, семейное, социальное, имущественное положение,
- образование, профессия, доходы,
- другая информация, принадлежащая субъекту ПД.

Операторами персональных данных являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Политика безопасности компьютерных систем и ее реализация 15

Требования законодательства к средствам защиты ПД

Информационная система персональных данных (далее ИСПД) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств (**Федеральный закон от 27.07.2006 №152 “О персональных данных”**).

Регуляторами называются органы государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований федерального закона.

В ФЗ "О персональных данных" установлены три регулятора:

- Роскомнадзор (защита прав субъектов персональных данных)
- ФСБ (требования в области криптографии)
- ФСТЭК России (требования по защите информации от несанкционированного доступа и утечки по техническим каналам).

Политика безопасности компьютерных систем и ее реализация 16

Требования законодательства к средствам защиты ПД

Пункт 5 "Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденного *Постановлением Правительства Российской Федерации от 17.11.2007 № 781*, которое гласит,

что средства защиты информации, используемые в ИСПД, должны в установленном порядке проходить процедуру соответствия (сертификацию). Порядок сертификации устанавливается уполномоченными органами, которыми в случае защиты ПД являются ФСТЭК и ФСБ России. Сертификации подлежат системы, продукты и услуги защиты информации от ПД.

В рамках систем обязательной сертификации организации должны сертифицировать средства и продукты. Например, в руководящих документах Гостехкомиссии России продуктом может выступать средство вычислительной техники (СВТ), средство защиты информации (СЗИ), межсетевой экран (МЭ), программное обеспечение (ПО) и др.

Система – это объект информатизации, где обрабатывается реальная информация. По этой причине к системам предъявляются дополнительные требования, касающиеся в том числе организационных мер и физической защиты.

Политика безопасности компьютерных систем и ее реализация 17

Требования законодательства к средствам защиты ПД

Программное обеспечение СЗПД для защиты от угроз конфиденциальности, целостности и доступности, применяемое в ИСПД 1 класса, подлежит сертификации на отсутствие недекларированных возможностей согласно п.2.12 Приказа ФСТЭК России №58. В соответствии с Руководящим документом Гостехкомиссии России "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей", утвержденным приказом Председателя Гостехкомиссии от 04.06.1999 № 114,

недекларированные возможности - функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Политика безопасности компьютерных систем и ее реализация 18

Требования законодательства к средствам защиты ПД

Порядок классификации по уровню контроля отсутствия недекларированных возможностей определен указанным выше руководящим документом Гостехкомисии. Данное требование обусловлено тем, что большинство современных атак использует уязвимости в программном обеспечении системы. Основной метод нахождения уязвимостей в программе – детальное изучение программного кода. *Данное требование может привести к выводу из эксплуатации в ИСПД зарубежных средств защиты информации, так как для сертификации необходимо предоставить код в открытом виде.*

При просмотре сертификата к средству защиты информации необходимо обратить внимание, на соответствие каким документам проводились сертификационные испытания.

Что касается ФСТЭК России, то это может быть:

- руководящие документы Гостехкомиссии России по защите от несанкционированного доступа к информации (для АС, СВТ или МЭ),
- руководящий документ Гостехкомиссии России по контролю отсутствия недекларированных возможностей,
- техническое условие или формуляр,
- задание по безопасности (по требованиям ГОСТ ИСО/МЭК 15408-2002).

Политика безопасности компьютерных систем и ее реализация 19

Требования законодательства к средствам защиты ПД

Необходимо отметить, что нормативные документы ФСТЭК на настоящее время не охватывают требования ко всем средствам технической защиты информации в области ПД.

Рекомендации и требования предусмотрены для межсетевых экранов (МЭ) и систем обнаружения вторжений (IDS).

- для ИСПД 1 класса – МЭ 3 класса, в IDS должны использоваться аномальные и сигнатурные методы обнаружения вторжений;
- для ИСПД 2 класса – МЭ 4 класса, в IDS должны использоваться аномальные и сигнатурные методы обнаружения вторжений;
- для ИСПД 3 класса – МЭ 5 класса, в IDS должен использоваться сигнатурный метод обнаружения вторжений;
- для ИСПД 4 класса – МЭ 5 класса, в IDS должен использоваться сигнатурный метод обнаружения вторжений.

Требования к средствам защиты ИСПД частично совпадают с требованиями к автоматизированным системам, которые были разработаны ранее в руководящих документах Гостехкомиссии России, в целях преемственности и совместимости.

Таблица 1. Корреляция требований к средствам защиты в ИСПД с документами по АС

Класс ИСПД	Класс АС	Класс МЭ	
		Без подключения к СОД	С подключением к СОД
К1, однопользовательскаяя	3А		2
К1, многопользовательская с одинаковыми правами	2А	4	2
К1, многопользовательская с разными правами	1В	4	2
К2, однопользовательская	3В+		3
К2, многопользовательская с одинаковыми правами	2В+	4	2
К2, многопользовательская с разными правами	1Г	4	2
К3, однопользовательская	3Б		4
К3, многопользовательская с одинаковыми правами	2Б	4	2
К3, многопользовательская с разными правами	1Д	4	2
К4	Определяется оператором		

Политика безопасности компьютерных систем и ее реализация 21

Требования законодательства к ИСПД

До февраля 2010 года проведение аттестации ИСПД было обязательным этапом построения системы защиты. После введения Приказа ФСТЭК №58 **Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных (Приказ ФСТЭК России от 5.02.2010 N 58 зарегистрирован в Минюсте России 19.02.2010 № 16456)**

ситуация изменилась, так как документ отменил обязательность аттестации, предоставив операторам самим решать, проводить ее или нет. Тем не менее, это не отменяет необходимости проведения оценки соответствия принятых мер по обеспечению безопасности требованиям законодательства, о чем говорят в частности – постановление Правительства РФ № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке и ИСПДн" и 184-ФЗ "О техническом регулировании".

Аттестация ИСПД предназначена для официального подтверждения эффективности и достаточности мер по обеспечению безопасности ПД в данной ИСПД. Аттестация должна предшествовать началу обработки данных. Порядок проведения аттестации регламентирован "Положением по аттестации объектов информатизации по требованиям безопасности информации" от 25 ноября 1994 г.

Результатом аттестации является документ, называемый "Аттестат соответствия", который подтверждает, что ИСПД удовлетворяет требованиям стандартов и нормативно-технических документов по безопасности ПД ФСТЭК и Гостехкомиссии России.

Политика безопасности компьютерных систем и ее реализация 22

Требования законодательства к ИСПД

Этапы аттестации включают в себя:

1. подачу и рассмотрение заявки на аттестацию;
2. предварительное ознакомление с аттестуемым объектом;
3. испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
4. разработка программы и методики аттестационных испытаний;
5. заключение договоров на аттестацию;
6. проведение аттестационных испытаний объекта информатизации;
7. оформление, регистрация и выдача "Аттестата соответствия";
8. осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
9. рассмотрение апелляций.

Политика безопасности компьютерных систем и ее реализация 23

Требования законодательства к ИСПД

Аттестационные испытания предполагают проведение следующих проверок:

- проверка состояния технологического процесса автоматизированной обработки персональных данных в ИСПД;
- проверка ИСПД на соответствие организационно-техническим требованиям по защите информации;
- испытания ИСПД на соответствие требованиям по защите информации от несанкционированного доступа.

Результатом аттестации являются:

- Протокол аттестационных испытаний;
- Заключение по результатам аттестационных испытаний;
- Аттестат соответствия на ИСПД (выдается в случае положительного Заключения);
- Акт о переводе СЗПД в промышленную эксплуатацию (в случае наличия положительного заключения по результатам аттестационных испытаний ИСПД).

Следует указать, что если заявитель пожелает только аттестовать ИСПД как объект информатизации, то пока действуют традиционные нормативные требования по аттестации объектов информатизации (СТР-К), в которых обрабатывается конфиденциальная информация.

Таблица 2. Перечень подсистем СЗПД в зависимости от класса и типа ИСПД 24

Класс и тип ИСПД	Антивирусная защита	Подсистема управления доступом, регистрации и учета	Подсистема обеспечения целостности	Анализ защищенности	Подсистема обнаружения вторжений	Подсистема безопасности межсетевого взаимодействия	Подсистема криптографической защиты информации
ИСПД 1кл.	распред.	+	+	+	+	+	+
ИСПД 1 кл.	локальная	+	+	+	-	-	+
ИСПД 2 кл.	распред.	+	+	+	+	+	-
ИСПД 2 кл.	локальная	+	+	+	-	-	-
ИСПД 3 кл.	распред.	+	+	+	+	+	-
ИСПД 3 кл.	локальная	+	+	+	-	-	-

Политика безопасности компьютерных систем и ее реализация 25

Требования законодательства к ИСПД

В таблице 2 приведена информация о подсистемах, которые должны быть внедрены в зависимости от класса ИСПД в соответствии с руководящими документами ФСТЭК. Рассмотрим функции, которые должна выполнять каждая из перечисленных в таблице подсистем:

1.подсистема управления доступом, регистрации и учета предназначена для защиты от несанкционированного доступа и реализуется с помощью средств блокирования НСД, регистрации попыток доступа и сигнализации. Средства данной группы могут быть программными или программно-аппаратными. Функция регистрации реализуется журналированием действий и операций в ИСПД, сигнализации - извещение в случае выявления нарушения нормального режима функционирования ИСПД или попыток НСД к ИСПД.

2.подсистема обеспечения целостности может быть реализована с помощью средств операционной системы, СУБД или с помощью специальных программных средств. Функция контроля целостности основывается, как правило, на вычислении контрольных сумм, хэш-функциях или ЭЦП.

Политика безопасности компьютерных систем и ее реализация 26

Требования законодательства к ИСПД

3.подсистема анализа защищенности предназначена для контроля настроек операционных систем на рабочих станциях и серверах, средств защиты и сетевого оборудования. Функционал данной подсистемы реализуется с помощью специальных программ – сканеров. Сканеры обследуют сеть и ведут поиск "слабых" мест, таких как:

- слабые пароли и механизмы аутентификации в целом;
- "люки" в программах;
- неправильная настройка межсетевых экранов, операционных систем, баз данных и пр.;
- использование сетевых протоколов, имеющих уязвимости.
- открытые порты.

Сканеры находят только известные уязвимости, детальным образом описанные в их базе данных. Функционировать они могут на сетевом уровне, уровне операционной системы и уровне приложения. Поимо выявления уязвимостей средства анализа защищенности могут помочь построить топологию сети: выявить узлы корпоративной сети, протоколы и сервисы, приложения и пр. Как правило, эти средства также дают рекомендации и пошаговые инструкции для устранения выявленных уязвимостей.

Требования законодательства к ИСПД

4. подсистема криптографической защиты информации. Как правило, предназначена для защиты ПД при передаче по открытым каналам связи или в несегментированной сети. Криптографические средства также могут применяться при хранении, обработке ПД, при аутентификации пользователей. Данное требование выдвигается только к ИСПД 1 класса.

В ряде случаев необходима также **подсистема защиты от утечки по техническим каналам**. Данная подсистема предназначена для защиты акустической, видовой информации, а также от утечек информации через ПЭМИН. При этом выделяются **пассивные** и **активные меры защиты**.

5.подсистема обеспечения безопасности межсетевого взаимодействия ИСПД предназначена для разграничения доступа к компонентам ИСПД и обрабатываемым ПД при межсетевом взаимодействии. Функционал подсистемы реализуется с помощью программных и программно-аппаратных межсетевых экранов (МЭ).

Политика безопасности компьютерных систем и ее реализация 28

Требования законодательства к ИСПД

6. подсистема антивирусной защиты предназначена для защиты информационной системы от вирусов (вредоносных программ) и реализуется с помощью антивирусных программ. Для обнаружения вирусов антивирус использует 2 метода: сигнатурный, эвристический.

7. подсистема обнаружения вторжений предназначена для обнаружения несанкционированных попыток доступа к системе. Системы обнаружения вторжений (IDS) работают наподобие сигнализации здания Существует два типа IDS- узловые (HIDS) и сетевые (NIDS). HIDS располагается на отдельном узле и отслеживает признаки атак на этот узел. Узловые IDS представляют собой систему датчиков, которые отслеживают различные события в системе на предмет аномальной активности. NIDS располагается на отдельной системе и анализирует весь трафик сети на признаки атак. В данные систем встроена база данных признаков атак, на которые система анализирует сетевой трафик.. В случае обнаружения атаки IDS может принимать пассивные или активные действия. Пассивные действия заключаются в уведомлении соответствующего должностного лица, например, администратора безопасности, о факте атаки. Активная обработка событий заключается в попытке остановить атаку – завершить подозрительный процесс, прервать соединение или сеанс.

Политика безопасности компьютерных систем и ее реализация 29

Требования законодательства к ИСПД

Общая схема взаимодействия регуляторов и операторов персональных данных представлена на рисунке. В соответствии с ФЗ "О персональных данных" выделяют три *регулятора* в области защиты персональных данных:

- **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее Роскомнадзор)** в части, касающейся соблюдения норм и требований по обработке персональных данных и защиты прав субъектов персональных данных;
- **Федеральная служба безопасности РФ (далее ФСБ)** в части, касающейся соблюдения требований по организации и обеспечению функционирования шифровальных (криптографических) средств в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПД;
- **Федеральная служба по техническому и экспортному контролю (далее ФСТЭК)** в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПД (не криптографическими методами) при их обработке в ИСПД.

Операторы: государственный орган, муниципальный орган, юридическое лицо, физическое лицо.


РОСКОМНАДЗОР
Защита прав
Субъект персональных данных
Регистрация, контроль и надзор
Персональные данные:
Основные ПД
Специальные ПД
Биометрические ПД
ОПЕРАТОР
-государственный орган;
-муниципальный орган;
-юридическое лицо;
-физическое лицо
Обработка персональных данных
Контроль и надзор
ФСБ
ФСТЭК