Тема 1.1 Понятие «информационная безопасность»

1 Проблема информационной безопасности общества

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества.

С понятием «информационная безопасность» в различных контекстах связаны различные определения. Так, в Законе РФ «Об участии в международном информационном обмене» информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Подобное же определение дается и в Доктрине информационной безопасности Российской Федерации, где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Оба эти определения рассматривают информационная безопасность в национальных масштабах и поэтому имеют очень широкое понятие.

Наряду с этим характерно, что применительно к различным сферам деятельности так или иначе связанным с информацией понятие «информационная безопасность» принимает более конкретные очертания. Так, например, в «Концепции информационной безопасности сетей связи общего пользования Российской Федерации» даны два определения этого понятия.

1) Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

2) Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или внешняя среда, например, высокая температура, может привести к сбоям в работе технических средств хранения информации и пр.

2 Понятие «информационная безопасность»

Сформулируем следующее определение «информационной безопасности».

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Рассматривая информацию как товар можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть и автор, потеряют часть рынка и пр.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и пр.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др.

Именно поэтому при определении понятия «информационная безопасность» на первое место ставится защита информации от различных воздействий.

Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно ГОСТу 350922-96 защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи, решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

Исходя из этого, отметим следующие важные выводы:

– задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;

– информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

В ряде случаев понятие «информационная безопасность» подменяется термином «компьютерная безопасность». В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информа-

ционных систем. Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передается с помощью компьютеров.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

3 Выводы по теме 1.1

1) Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества. Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

2) Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

3) Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

4) Задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться.

5) Под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

6) Защита информации (ГОСТ 350922-96) – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Тема 1.2. Составляющие информационной безопасности

1 Доступность информации

Как уже отмечено в предыдущей теме, информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

1) Обеспечением доступности информации.
2) Обеспечением целостности информации.
3) Обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления – производством, транспортом и т. п. Менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет и т. п.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так

же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило. В этом контексте весьма уместной является поговорка: «Дорога ложка к обеду».

2 Целостность информации

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например – техническими, социальными и пр.

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

3 Конфиденциальность информации

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями.

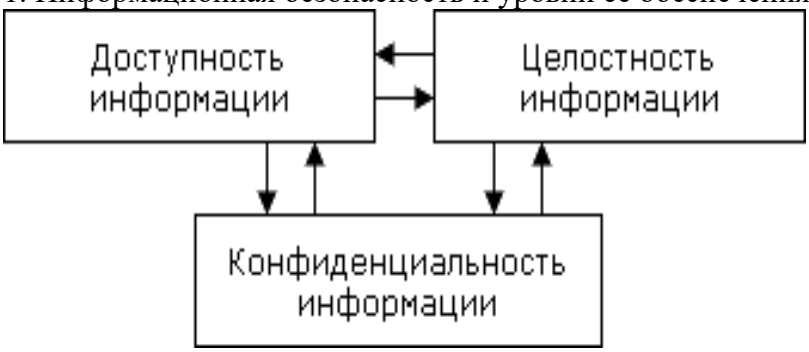

Рисунок 1.2.1 – Составляющие информационной безопасности

Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Как уже отмечалось, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме этого, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

3 Выводы по теме 1.2

1) Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

– обеспечением доступности информации;

– обеспечением целостности информации;

– обеспечением конфиденциальности информации.

2) Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

3) Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

4) Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для которого она предназначена.

Тема 1.3. Система формирования режима информационной безопасности

1 Задачи информационной безопасности общества

Анализ основ информационной безопасности показал, что обеспечение безопасности является задачей комплексной. С одной стороны режима информационной, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих - доступность, целостность и конфиденциальность данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле «пронизаны» все сферы общественной деятельности и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.

В этой связи вполне закономерным является рассмотрение проблемы обеспечения информационной безопасности на нескольких уровнях, которые в совокупности обеспечивали бы защиту информации и информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

Рассматривая проблему информационной безопасности в широком смысле, можно отметить, что в этом случае речь идет об информационной безопасности всего общества и его жизнедеятельности, при этом на информационную безопасность возлагается задача по минимизации всех отрицательных последствий от всеобщей информатизации и содействия развитию всего общества при использовании информации как ресурса его развития.

В этой связи основными задачами информационной безопасности в широком смысле являются:

- защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;

- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в узком смысле, отметим, что в этом случае речь идет о совокупности методов и средств защиты информации и ее материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.

Исходя из этого, выделим следующие задачи информационной безопасности:

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

Заметим, что понятие «компьютерная безопасность», которому посвящена большая часть данного курса, как раз подходит под определение информационной безопасности в узком смысле, но не является полным ее содержанием, поскольку информационные системы и материальные носители информации связаны не только с компьютерами.

2 Уровни формирования режима информационной безопасности

С учетом изложенного выделим три уровня формирования режима информационной безопасности:

- законодательно-правовой;
- административный (организационный);
- программно-технический.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на

их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний. Наиболее характерным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США. Тем не менее, эти нормы большей частью не являются обязательными, как законодательные меры.

Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный. Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и пр.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по

ключу и пр. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например, антивирусный пакет и пр. Программы защиты могут быть как отдельные, так и встроенные. Так, шифрование данных можно выполнить встроенной в операционную систему файловой шифрующей системой EFS (Windows 2000, XP) или специальной программой шифрования.

Подчеркнем, что формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах отличается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения.

3 Выводы по теме 1.3

1) Основные задачи информационной безопасности:

- защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информации;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну;
- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

2) Режим информационной безопасности включает три уровня:

- законодательно-правовой;
- административный (организационный);
- программно-технический.

3) Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус.

4) Административный уровень включает комплекс взаимо-координируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации.

5) Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный.

Тема 1.4 Нормативно-правовые основы информационной безопасности в РФ

1 Правовые основы информационной безопасности общества

Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля за исполнением указанных документов. Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

Законодательная база в сфере информационной безопасности включает пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности.

В Конституции РФ гарантируется «тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (ст. 23, ч.2), а также «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ст. 29, ч.4). Кроме этого, Конституцией РФ «гарантируется свобода массовой информации» (ст. 29, ч.5), т. е. массовая информация должна быть доступна гражданам.

Концепция национальной безопасности РФ, введенная указом Президента РФ №24 в январе 2000 г., определяет важнейшие задачи обеспечения информационной безопасности Российской Федерации:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

Для обеспечения прав граждан в сфере информационных технологий и решения задач информационной безопасности, сформулированных в Концепции национальной безопасности РФ, разработаны и продолжают разрабатываться и совершенствоваться нормативные документы в сфере информационных технологий.

2 Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

1) Закон Российской Федерации от 21 июля 1993 года №5485-1 «О государственной тайне» с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В Законе определены следующие основные понятия:

- государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

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

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

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

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

Законом определено, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральную службу безопасности Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации.

2) Закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 года №24-ФЗ – является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям

документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Основными задачами системы защиты информации, нашедшими отражение в Законе «Об информации, информатизации и защите информации», являются:

- предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п., вмешательства в информацию и информационные системы;
- сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;
- сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;
- обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;
- сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;
- соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

В соответствии с законом:

- информационные ресурсы делятся на государственные и негосударственные (ст. 6, ч. 1);
- государственные информационные ресурсы являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа (ст. 10, ч. 1);

– документированная информация с ограниченного доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную (ст. 10, ч. 2).

Закон определяет пять категорий государственных информационных ресурсов:

– открытая общедоступная информация во всех областях знаний и деятельности;

– информация с ограниченным доступом;

– информация, отнесенная к государственной тайне;

– конфиденциальная информация;

– персональные данные о гражданах (относятся к категории конфиденциальной информации, но регламентируются отдельным законом).

Статья 22 Закона «Об информации, информатизации и защите информации» определяет права и обязанности субъектов в области защиты информации. В частности, пункты 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактах нарушения режима защиты информации.

Следует отметить, что процесс законотворчества идет достаточно сложно. Если в вопросах защиты государственной тайны создана более или менее надежная законодательная система, то в вопросах защиты служебной, коммерческой и частной информации существует достаточно много противоречий и «нестыковок».

При разработке и использовании законодательных и других правовых и нормативных документов, а также при организации защиты информации важно правильно ориентироваться во всем блоке действующей законодательной базы в этой области.

Проблемы, связанные с правильной трактовкой и применением законодательства Российской Федерации, периодически возникают в практической работе по организации защиты информации от ее утечки по техническим каналам, от несанкционированного доступа к информации и от воздействий на нее при обработке в технических средствах информатизации, а также в ходе контроля эффективности принимаемых мер защиты.

3 Ответственность за нарушения в сфере информационной безопасности

Немаловажная роль в системе правового регулирования информационных отношений отводится ответственности субъектов за нарушения в сфере информационной безопасности.

Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации.
- Кодекс Российской Федерации об административных правонарушениях.

В принятом в 1996 году Уголовном кодексе Российской Федерации, как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

1) Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

2) Статья 140. Отказ в предоставлении гражданину информации.

3) Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

4) Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.

5) Статья 283. Разглашение государственной тайны.

6) Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной 28 главе кодекса «Преступления в сфере компьютерной информации». Глава 28 включает следующие статьи:

1) Статья 272. Неправомерный доступ к компьютерной информации.

а) Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы

ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

б) То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

2) Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

а) Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, – наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

б) Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

3) Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

а) Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние

причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

б) То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

4 Выводы по теме 1.4

1) Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности.

2) Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

3) Закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 года № 24-ФЗ является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

4) Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

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

6) Немаловажная роль в системе правового регулирования информационных отношении отводится ответственности субъектов за нарушения в сфере информационной безопасности. Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации;
- Кодекс Российской Федерации об административных правонарушениях.

Тема 1.5 Стандарты информационной безопасности: «Общие критерии»

1 Требования безопасности к информационным системам

Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» (издан 1 декабря 1999 года) относится к оценочным стандартам. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Именно поэтому этот стандарт очень часто называют «Общими критериями».

«Общие критерии» являются метастандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.

Как и «Оранжевая книга», «Общие критерии» содержат два основных вида требований безопасности:

- функциональные – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

В отличие от «Оранжевой книги», «Общие критерии» не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

Очень важно, что безопасность в «Общих критериях» рассматривается не статично, а в привязке к жизненному циклу объекта оценки.

Угрозы безопасности в стандарте характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

2 Принцип иерархии: класс – семейство – компонент – элемент

Для структуризации пространства требований, в «Общих критериях» введена иерархия класс – семейство – компонент – элемент.

Классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим тонкостям требований.

Компонент – минимальный набор требований, фигурирующий как целое.

Элемент – неделимое требование.

Между компонентами могут существовать зависимости, которые возникают, когда компонент сам по себе недостаточен для достижения цели безопасности.

Подобный принцип организации защиты напоминает принцип программирования с использованием библиотек, в которых содержатся стандартные (часто используемые) функции, из комбинаций которых формируется алгоритм решения.

«Общие критерии» позволяют с помощью подобных библиотек (компонент) формировать два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Функциональный пакет – это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

3 Функциональные требования

Все функциональные требования объединены в группы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в «Общих критериях» представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это гораздо больше, чем число аналогичных понятий в «Оранжевой книге».

«Общие критерии» включают следующие классы функциональных требований:

1) Идентификация и аутентификация.

2) Защита данных пользователя.

3) Защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов).

4) Управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности).

5) Аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности).

6) Доступ к объекту оценки.

7) Приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных).

8) Использование ресурсов (требования к доступности информации).

9) Криптографическая поддержка (управление ключами).

10) Связь (аутентификация сторон, участвующих в обмене данными).

11) Доверенный маршрут/канал (для связи с сервисами безопасности).

Рассмотрим содержание одного из классов.

Класс функциональных требований «Использование ресурсов» включает три семейства.

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В стандарте различаются активная и пассивная отказоустойчивость. Активный механизм содержит

специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Аналогично и другие классы включают наборы семейств требований, которые используются для формулировки требований к системе безопасности.

«Общие критерии» – достаточно продуманный и полный документ с точки зрения функциональных требований и именно на этот стандарт безопасности ориентируются соответствующие организации в нашей стране и в первую очередь ФСТЭК РФ.

4 Требования доверия

Вторая форма требований безопасности в «Общих критериях» – требования доверия безопасности.

Установление доверия безопасности основывается на активном исследовании объекта оценки.

Форма представления требований доверия, та же, что и для функциональных требований (класс – семейство – компонент).

Всего в «Общих критериях» 10 классов, 44 семейства, 93 компонента требований доверия безопасности.

Классы требований доверия безопасности:

1) Разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации).

2) Поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки).

3) Тестирование.

4) Оценка уязвимостей (включая оценку стойкости функций безопасности).

5) Поставка и эксплуатация.

6) Управление конфигурацией.

7) Руководства (требования к эксплуатационной документации).

8) Поддержка доверия (для поддержки этапов жизненного цикла после сертификации).

9) Оценка профиля защиты.

10) Оценка задания по безопасности.

Применительно к требованиям доверия (для функциональных требований не предусмотрены) в «Общих критериях» введены оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Степень доверия возрастает от первого к седьмому уровню. Так, оценочный уровень доверия 1 (начальный) применяется, когда угрозы не рассматриваются как серьезные, а оценочный уровень 7 применяется к ситуациям чрезвычайно высокого риска.

5 Выводы по теме 1.5

1) Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» (издан 1 декабря 1999 года) относится к оценочным стандартам.

2) «Общие критерии» являются стандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.

3) «Общие критерии» содержат два основных вида требований безопасности:

- функциональные – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

4) Угрозы безопасности в стандарте характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

5) Для структуризации пространства требований в «Общих критериях» введена иерархия класс – семейство – компонент – элемент.

6) Классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности).

7) Семейства в пределах класса различаются по строгости и другим тонкостям требований.

8) Компонент – минимальный набор требований, фигурирующий как целое.

9) Элемент – неделимое требование.

Тема 1.6. Стандарты информационной безопасности распределенных систем

1 Сервисы безопасности в вычислительных сетях

В последнее время с развитием вычислительных сетей и в особенности глобальной сети Интернет вопросы безопасности распределенных систем приобрели особую значимость. Важность этого вопроса косвенно подчеркивается появлением чуть позже «Оранжевой книги» стандарта, получившего название «Рекомендации X.800», который достаточно полно трактовал вопросы информационной безопасности распределенных систем, т. е. вычислительных сетей.

Рекомендации X.800 выделяют следующие сервисы (функции) безопасности и исполняемые ими роли:

1) Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

2) Управление доступом обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

3) Конфиденциальность данных обеспечивает защиту от несанкционированного получения информации. Отдельно выделяется конфиденциальность трафика – это защита информации, которую можно получить, анализируя сетевые потоки данных.

4) Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

5) Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки.

2 Механизмы безопасности

В X.800 определены следующие сетевые механизмы безопасности:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

Следующая таблица иллюстрирует, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

«+» механизм используется для реализации данной функцию безопасности;

«-» механизм не используется для реализации данной функции безопасности.

Таблица 1.6.1. Взаимосвязь функций и механизмов безопасности

Функции	**Механизмы**							
	Шифрование	**Электронная подпись**	**Управление доступом**	**Целостность**	**Аутентификация**	**Дополнение трафика**	**Управление маршрутизацией**	**Нотаризация**
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	+	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

Так, например, «Конфиденциальность трафика» обеспечивается «Шифрованием», «Дополнением трафика» и «Управлением маршрутизацией».

3 Администрирование средств безопасности

В рекомендациях X.800 рассматривается понятие администрирование средств безопасности, которое включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Администрирование информационной системы в целом включает обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Администрирование механизмов безопасности включает:

- управление криптографическими ключами (генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров);
- администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т. п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т. п.);

- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т. п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

В 1987 г. Национальным центром компьютерной безопасности США была опубликована интерпретация «Оранжевой книги» для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Интерпретация отличается от самой «Оранжевой книги» учетом динамичности сетевых конфигураций. В интерпретациях предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети.

Среди защитных механизмов в сетевых конфигурациях на первое место выдвигается криптография, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

В интерпретациях «Оранжевой книги» впервые систематически рассматривается вопрос обеспечения доступности информации.

Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т. п.);
- наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого управления, отсутствие единой точки отказа;
- наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение подсетей и изоляция групп пользователей друг от друга.

4 Выводы по теме 1.6

1) Стандарты информационной безопасности предусматривают следующие сервисы безопасности:

- аутентификация;
- аутентификация источника;
- управление доступом;
- конфиденциальность;
- конфиденциальность трафика;
- целостность соединения;
- целостность вне соединения;
- неотказуемость.

2) Механизмы безопасности:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

3) Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей.

4) Администратор средств безопасности решает следующие задачи:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Тема 1.7 Стандарты информационной безопасности в РФ

1 ФСТЭК и ее роль в обеспечении информационной безопасности в РФ

Таблица 1.7.1. Руководящие документы ФСТЭК

п/п	Наименование
1.	Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
2.	Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
3.	Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
4.	Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
5.	Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992
6.	Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 27.10.1995 N 199
7.	Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 04.06.1999 N 114
8.	Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 02.03.2001 N 282.ДСП
9.	Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.ДСП
10.	Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.ДСП
11.	Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.ДСП
12.	Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электро-акустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.ДСП
13.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008.ДСП
14.	Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 N 638.ДСП
15.	Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 N 27.ДСП

16.	Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 N 28.ДСП
17.	Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 N 17
18.	Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18.02.2013 N 21
19.	Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 N 119.ДСП
20.	Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11.02.2014
21.	Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены приказом ФСТЭК России от 14.03.2014 N 31
22.	Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 N 87.ДСП
23.	Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 N 9.ДСП
24.	Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 г. N 119.ДСП
25.	ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. ДСП
26.	ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. ДСП

В Российской Федерации информационная безопасность обеспечивается соблюдение указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов ФСТЭК России и других нормативных документов.

Наиболее общие документы были рассмотрены ранее при изучении правовых основ информационной безопасности. В РФ с точки зрения стандартизации положений в сфере информационной безопасности первостепенное значение имеют руководящие документы (РД) ФСТЭК России, одной из задач которой является «проведение единой государственной политики в области технической защиты информации».

ФСТЭК России ведет весьма активную нормотворческую деятельность, выпуская руководящие документы, играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления ФСТЭК России выбрала ориентацию на «Общие критерии».

ФСТЭК разработала и довела до уровня национальных стандартов десятки документов, представленных в таблице 1.7.1.

2 Документы по оценке защищенности автоматизированных систем в РФ

Рассмотрим наиболее значимые из этих документов, определяющие критерии для оценки защищенности автоматизированных систем.

Руководящий документ «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Основой для разработки этого документа явилась «Оранжевая книга». Этот оценочный стандарт устанавливается семь классов защищенности СВТ от НСД к информации.

Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

- первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;
- 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 включает только первый класс.

Руководящий документ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

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.

В документе определены 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 и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

В таблице 1.7.2 приведены классы защищенности АС и требования для их обеспечения.

В таблице 1.7.2 систематизированы минимальные требования, которым необходимо следовать, чтобы обеспечить конфиденциальность информации.

Требования по обеспечению целостности представлены отдельной подсистемой (номер 4).

Руководящий документ «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» является основным документом для анализа системы защиты внешнего периметра корпоративной сети. Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ.

Всего выделяется пять показателей защищенности:

- управление доступом;
- идентификация и аутентификация;
- регистрация событий и оповещение;
- контроль целостности;
- восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

Таблица 1.7.2 –Требования к защищенности автоматизированных систем

Подсистемы и требования	**Классы**								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1 Подсистема управления доступом									
1.1 Идентификация, проверка подлинности и контроль доступа субъектов:									
- в систему	+	+	+	+	+	+	+	+	+
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
- к программам	-	-	-	+	-	+	+	+	+
- к томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
1.2 Управление потоками информации	-	-	-	+	-	-	+	+	+
2 Подсистема регистрации и учета									
2.1 Регистрация и учет:									
- входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
- выдачи печатных (графических) выходных документов	-	+	-	+	-	+	+	+	+
- запуска/завершения программ и процессов (заданий, задач)	-	-	-	+	-	+	+	+	+
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
- изменения полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
- создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
2.2 Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3 Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4 Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	+
3 Криптографическая подсистема									
3.1 Шифрование конфиденциальной информации	-	-	-	+	-	-	-	+	+
3.2 Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	-	-	-	-	+
3.3 Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	-	-	-	+	+
4 Подсистема обеспечения целостности									
4.1 Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2 Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3 Наличие администратора (службы защиты) информации в АС	-	-	-	+	-	-	+	+	+
4.4 Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5 Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6 Использование сертифицированных средств защиты	-	+	-	+	-	-	+	+	+
«-» нет требований к данному классу; «+» есть требования к данному классу «СЗИ НСД» – система защиты информации от несанкционированного доступа.									

- простейшие фильтрующие маршрутизаторы – 5 класс;
- пакетные фильтры сетевого уровня – 4 класс;
- простейшие МЭ прикладного уровня – 3 класс;
- МЭ базового уровня – 2 класс;
- продвинутые МЭ – 1 класс.

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию «Особой важности». Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки «совершенно секретной» информации и т. п.

Согласно первому из них, 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, имеющий доступ 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) хранящейся 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.

3 Выводы по теме 1.7

1) В Российской Федерации информационная безопасность обеспечивается соблюдением Указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов ФСТЭК России и других нормативных документов.

2) Стандартами в сфере информационной безопасности в РФ являются руководящие документы ФСТЭК России, одной из задач которой является «проведение единой государственной политики в области технической защиты информации».

3) При разработке национальных стандартов ФСТЭК России ориентируется на «Общие критерии».

4) Руководящий документ «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Этот оценочный стандарт устанавливает семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты.

5) Руководящий документ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации и требования по защите информации в АС различных классов. 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.

6) Руководящий документ «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» является основным документом для анализа системы защиты внешнего периметра корпоративной сети. Данный документ определяет показатели защищенности межсетевых экранов. Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ. Всего выделяется пять показателей защищенности:

- управление доступом;
- идентификация и аутентификация;
- регистрация событий и оповещение;

- контроль целостности;
- восстановление работоспособности.

Тема 1.8. Административный уровень обеспечения информационной безопасности

1 Цели, задачи и содержание административного уровня

Административный уровень является промежуточным между законодательно-правовым и программно-техническим уровнями формирования режима информационной безопасности. Законы и стандарты в области информационной безопасности являются лишь отправным нормативным базисом информационной безопасности. Основой практического построения комплексной системы безопасности является административный уровень, определяющий главные направления работ по защите информационных систем.

Задачей административного уровня является разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

Кроме этого, что немаловажно, именно на административном уровне определяются механизмы защиты, которые составляют третий уровень информационной безопасности – программно-технический.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.

Содержанием административного уровня являются следующие мероприятия:

1) Разработка политики безопасности.
2) Проведение анализа угроз и расчета рисков.

2 Разработка политики информационной безопасности

Разработка политики безопасности ведется для конкретных условий функционирования информационной системы. Как правило, речь идет о политике безопасности организации, предприятия или учебного заведения. С учетом этого рассмотрим следующее определение политики безопасности.

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Основные направления разработки политики безопасности:

- определение объема и требуемого уровня защиты данных;
- определение ролей субъектов информационных отношений.

В «Оранжевой книге» политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Результатом разработки политики безопасности является комплексный документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Этот документ является методологической основой практических мер по обеспечению информационной безопасности и включает следующие группы сведений:

- основные положения информационной безопасности организации;
- область применения политики безопасности;
- цели и задачи обеспечения информационной безопасности организации;
- распределение ролей и ответственности субъектов информационных отношений организации и их общие обязанности.

Основные положения определяют важность обеспечения информационной безопасности, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

При описании области применения политики безопасности перечисляются компоненты автоматизированной системы обработки, хранения и передачи информации, подлежащие защите.

В состав автоматизированной информационной системы входят следующие компоненты:

- аппаратные средства – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры), кабели, линии связи и пр.;
- программное обеспечение – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и пр.;
- данные – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и пр.;
- персонал – обслуживающий персонал и пользователи.

Цели, задачи, критерии оценки информационной безопасности определяются функциональным назначением организации. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и пр.

Политика безопасности затрагивает всех субъектов информационных отношений в организации, поэтому на этапе разработки политики безопасности очень важно разграничить их права и обязанности, связанные с их непосредственной деятельностью.

С точки зрения обеспечения информационной безопасности разграничение прав и обязанностей целесообразно провести по следующим группам (ролям):

- специалист по информационной безопасности;
- владелец информации;
- поставщики аппаратного и программного обеспечения;
- менеджер отдела;
- операторы;
- аудиторы.

В зависимости от размеров организации, степени развитости ее информационной системы, некоторые из перечисленных ролей могут отсутствовать вообще, а некоторые могут совмещаться одним и тем же физическим лицом.

Специалист по информационной безопасности (начальник службы безопасности, администратор по безопасности) играет основную роль в разработке и соблюдении политики безопасности предприятия. Он проводит расчет и перерасчет рисков, выявляет уязвимости системы безопасности по всем направлениям (аппаратные средства, программное обеспечение и пр.).

Владелец информации – лицо, непосредственно владеющее информацией и работающее с ней. В большинстве случае именно владелец информации может определить ее ценность и конфиденциальность.

Поставщики аппаратного и программного обеспечения обычно являются сторонними лицами, которые несут ответственность за поддержание должного уровня информационной безопасности в поставляемых им продуктах.

Администратор сети – лицо, занимающееся обеспечением функционирования информационной сети организации, поддержанием сетевых сервисов, разграничением прав доступа к ресурсам сети на основании соответствующей политики безопасности.

Менеджер отдела является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача – своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за их выполнением на рабочих местах. Менеджеры должны доводить до подчиненных все аспекты политики безопасности, которые непосредственно их касаются.

Операторы обрабатывают информацию, поэтому должны знать класс конфиденциальности информации и какой ущерб будет нанесен организации при ее раскрытии.

Аудиторы – внешние специалисты по безопасности, нанимаемые организацией для периодической проверки функционирования всей системы безопасности организации.

3 Выводы по теме 1.8

1) Административный уровень является промежуточным уровнем между законодательно-правовым и программно-техническим уровнями формирования режима информационной безопасности, задачей которого является разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

2) Задачей административного уровня является разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

3) Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.

4) Содержанием административного уровня являются следующие мероприятия:

- разработка политики безопасности;
- проведение анализа угроз и расчета рисков;
- выбор механизмов и средств обеспечения информационной безопасности.

5) Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений. При этом в политике безопасности излагается политика ролей субъектов информационных отношений.

6) Основные направления разработки политики безопасности:

- определение объема и требуемого уровня защиты данных;
- определение ролей субъектов информационных отношений.

Тема 1.9. Классификация угроз «информационной безопасности»

1 Классы угроз информационной безопасности

Анализ и выявление угроз информационной безопасности является второй важной функцией административного уровня обеспечения информационной безопасности. Во многом облик разрабатываемой системы защиты и состав механизмов ее реализации определяется потенциальными угрозами, выявленными на этом этапе. Например, если пользователи вычислительной сети организации имеют доступ в Интернет, то количество угроз информационной безопасности резко возрастает, соответственно, это отражается на методах и средствах защиты и пр.

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например, неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение (к сожалению, даже лицензионное программное обеспечение не лишено уязвимостей).

История развития информационных систем показывает, что новые уязвимые места появляются постоянно. С такой же регулярностью, но с небольшим отставанием, появляются и средства защиты. В большинстве своем средства защиты появляются в ответ на возникающие угрозы, так, например, постоянно появляются исправления к программному обеспечению фирмы Microsoft, устраняющие очередные его уязвимые места и др. Такой подход к обеспечению безопасности малоэффективен, поскольку всегда существует промежуток времени между моментом выявления угрозы и ее устранением. Именно в этот промежуток времени злоумышленник может нанести непоправимый вред информации.

В этой связи более приемлемым является другой способ - способ упреждающей защиты, заключающийся в разработке механизмов защиты от возможных, предполагаемых и потенциальных угроз.

Отметим, что некоторые угрозы нельзя считать следствием целенаправленных действий вредного характера. Существуют угрозы, вызванные случайными ошибками или техногенными явлениями.

Знание возможных угроз информационной безопасности, а также уязвимых мест системы защиты, необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности.

Угрозы информационной безопасности классифицируются по нескольким признакам:

- по составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- по характеру воздействия (случайные или преднамеренные, действия природного или техногенного характера);
- по расположению источника угроз (внутри или вне рассматриваемой информационной системы).

Отправной точкой при анализе угроз информационной безопасности является определение составляющей информационной безопасности, которая может быть нарушена той или иной угрозой: конфиденциальность, целостность или доступность.

На рисунке 1.9.1 показано, что все виды угроз, классифицируемые по другим признакам, могут воздействовать на все составляющие информационной безопасности.

Рассмотрим угрозы по характеру воздействия.

Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

Причинами случайных воздействий при эксплуатации могут быть:

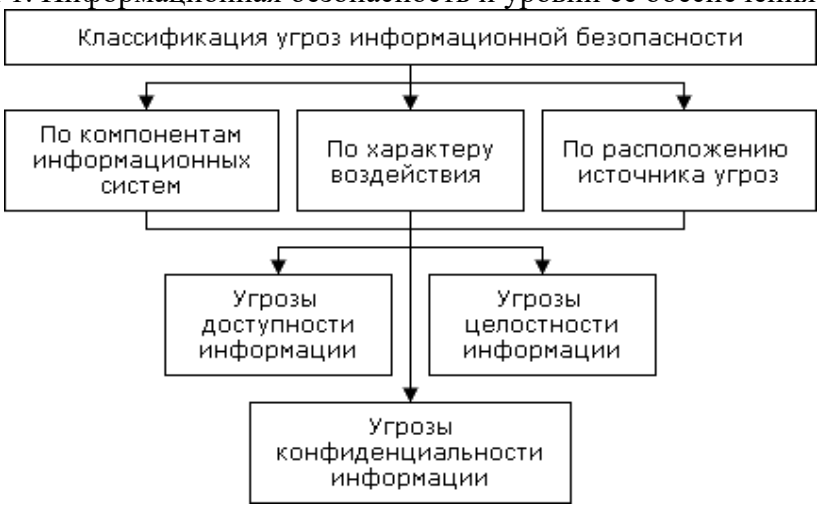

Рисунок 1.9.1 – Классификация угроз информационной безопасности

- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например:

- недовольством служащего служебным положением;
- любопытством;
- конкурентной борьбой;
- уязвленным самолюбием и пр.

Угрозы, классифицируемые по расположению источника угроз, бывают внутренние и внешние.

Внешние угрозы обусловлены применением вычислительных сетей и создание на их основе информационных систем.

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно, т.е. с помощью механизма сообщений.

При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

2 Каналы несанкционированного доступа к информации

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющим нанести ущерб любой из составляющих информационной безопасности является несанкционированный доступ. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

Каналы НСД классифицируются по компонентам автоматизированных информационных систем:

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;
- расшифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и пр.

3 Выводы по теме 1.9

1) Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности.

2) Преднамеренная реализация угрозы называется атакой на информационную систему.

3) Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

4) Угрозы информационной безопасности классифицируются по нескольким признакам:

- по составляющим информационной безопасности;
- по компонентам информационных систем;
- по характеру воздействия;
- по расположению источника угроз.

5) Несанкционированный доступ является одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющим нанести ущерб любой из составляющих информационной безопасности.

6) Каналы НСД классифицируются по компонентам автоматизированных информационных систем: пользователь, программа, аппаратные средства.