ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.09 Информационная безопасность

Специальность: 38.05.01 Экономическая безопасность
Специализация: Экономико-правовое обеспечение экономической безопасности
Форма обучения: заочная

1. КОНСПЕКТ ЛЕКЦИЙ

1.1 ЛЕКЦИЯ №1 (1 час)

Тема: «**Понятие «Информационная безопасность». Составляющие информационной безопасности»**

1.1.1 Вопросы лекции:

1. Проблема информационной безопасности общества
2. Определение понятия «информационная безопасность»
3. Доступность информации
4. Целостность информации
5. Конфиденциальность информации
6. Задачи информационной безопасности общества
7. Уровни формирования режима информационной безопасности

1.1.2 Краткое содержание вопросов

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 Взаимоувязанной сети связи 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 т. д.

2 Определение понятия «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 т. д.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т. д.), 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 информационных 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 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".

4 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 т. д.

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.

5 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. 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.

6 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.

7 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 т. д.).

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 т. д. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т. д. 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.

1.2 Лекция № 2 (1 час)

Тема: «Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»

1.2.1 Вопросы лекции:

1. Правовые основы информационной безопасности общества
2. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации
3. Ответственность за нарушения в сфере информационной безопасности

1.2.2. Краткое содержание вопросов

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 информа-

ционных 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 Стратегия 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.

- Стратегия национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента РФ от 12 мая 2009 г. N 537) ., 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.

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 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, информационных технологиях и о защите информации" от 27 июля 2006 года №149-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, информационных технологиях и о 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).

Закон "Об информации, информатизации и защите информации" определяет права и обязанности субъектов в области защиты информации. В частности, обязывает 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.

b. 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.

a. 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.

b. 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.

a. 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.

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

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.

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 России.

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.

1.3Лекция № 3 (1 час)

Тема: «Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях»

1.3.1Вопросы лекции

1 Особенности информационной безопасности в компьютерных сетях
2 Специфика средств защиты в компьютерных сетях
3 Понятие протокола передачи данных
4 Принципы организации обмена данными в вычислительных сетях
5 Транспортный протокол TCP и модель TCP/IP
6 Классы удаленных угроз и их характеристика

1.3.2 Краткое содержание вопросов

1. Особенности информационной безопасности в компьютерных сетях

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычислительных сетях наиболее частыми являются угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи. Это определение охватывает обе особенности сетевых систем – распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов информационной безопасности вычислительных сетей рассматриваются два подвида удаленных угроз – это удаленные угрозы на инфраструктуру и протоколы сети и удаленные угрозы на телекоммуникационные службы. Первые используют уязвимости в сетевых протоколах и инфраструктуре сети, а вторые – уязвимости в телекоммуникационных службах.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих "информационной безопасности":

- целостности данных;
- конфиденциальности данных;

- доступности данных.

Целостность данных – одна из основных целей информационной безопасности сетей – предполагает, что данные не были изменены, подменены или уничтожены в процессе их передачи по линиям связи, между узлами вычислительной сети. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных – вторая главная цель сетевой безопасности. При информационном обмене в вычислительных сетях большое количество информации относится к конфиденциальной, например, личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах и др.

Доступность данных – третья цель безопасности данных в вычислительных сетях. Функциями вычислительных сетей являются совместный доступ к аппаратным и программным средствам сети и совместный доступ к данным. Нарушение информационной безопасности как раз и связана с невозможностью реализации этих функций.

В локальной сети должны быть доступны: принтеры, серверы, рабочие станции, данные пользователей и др.

В глобальных вычислительных сетях должны быть доступны информационные ресурсы и различные сервисы, например, почтовый сервер, сервер доменных имен, web-сервер и др.

При рассмотрении вопросов, связанных с информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:

- глобальную связанность;
- разнородность корпоративных информационных систем;
- распространение технологии "клиент/сервер".

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными на протоколах TCP/IP, и предоставляющих аналогичные сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признанным на международном уровне. Национальные границы, законы, стандарты не должны препятствовать защите потоков данных между клиентами и серверами.

Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например, межсетевых экранов.

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры. Если, например, продукт, предназначенный для криптографической защиты, способен функционировать исключительно на платформе Wintel (Windows+Intel), то его практическая применимость вызывает серьезные сомнения.

Корпоративные информационные системы оказываются разнородными еще в одном важном отношении – в разных частях этих систем хранятся и обрабатываются данные разной степени важности и секретности.

Использования технологии "клиент/сервер" с точки зрения информационной безопасности имеет следующие особенности:

- каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности);
- каждый сервис имеет свою трактовку понятий субъекта и объекта;
- каждый сервис имеет специфические угрозы;
- каждый сервис нужно по-своему администрировать;
- средства безопасности в каждый сервис нужно встраивать по-особому.

2 Специфика средств защиты в компьютерных сетях

Особенности вычислительных сетей и, в первую очередь, глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

- защита подключений к внешним сетям;
- защита корпоративных потоков данных, передаваемых по открытым сетям;
- защита потоков данных между клиентами и серверами;
- обеспечение безопасности распределенной программной среды;
- защита важнейших сервисов (в первую очередь – Web-сервиса);
- аутентификация в открытых сетях.

Вопросы реализации таких методов защиты будут рассмотрены далее.

И в заключение рассмотрим еще одну особенность информационной безопасности, связанную с вычислительными сетями. В последнее время все четче просматривается незащищенность вычислительных сетей от глобальных атак.

Исторически первой глобальной атакой на компьютерные сети считается распространение вируса Морриса (4 ноября 1988) в сети "Arpanet", когда примерно из 60 000 компьютеров в сети было заражено около 10% (примерно 6 000). Неконтролируемый процесс распространения вируса привел к блокировке сети.

За последние два года как минимум успешными были три глобальные атаки:

1. 21 октября 2002. Сеть "Internet". Запланированная DoS-атака на Интернет. В момент атаки нагрузка на Европейский сегмент Интернета возросла на 6%.

2. 25 января 2003. Сеть "Internet". Флеш-червь "SQL. Slammer". Неконтролируемый процесс распространения вируса привел к перегрузке каналов передачи данных в Ю. Корее. Нагрузка на Европейский сегмент Интернета возросла примерно на 25%.

3. 12 августа 2003. Сеть "Internet". Сетевой червь "Lovesan".

Успешные глобальные сетевые атаки, безусловно, являются самым разрушительным явлением, которое может произойти в современных сетях.

3 Понятие протокола передачи данных

Обмен информацией между ЭВМ на больших расстояниях всегда казался более важной задачей, чем локальный обмен. Поэтому ему уделялось больше внимания и, соответственно, велось большее финансирование во многих странах. Один из немногих открытых проектов по исследованию вычислительных сетей, финансировавшийся военным ведомством США, известен под названием сеть **ARPA – Advanced Research Projects Agency**. С самого начала в рамках этого проекта велись работы по объединению ресурсов многих вычислительных машин различного типа. В 1960-1970-е годы многие результаты, полученные при эксплуатации сети ARPA, были опубликованы в открытой печати. Это обстоятельство, а также тот факт, что почти все страны занялись практически слепым копированием не только аппаратной архитектуры американских машин, но и базового программного обеспечения, обусловили сильное влияние сети ARPA на многие другие сети, именно поэтому принято считать, что сеть ARPA является предшественницей знаменитой всемирной компьютерной сети Интернет.

Основной задачей сетевой общественности явилась разработка протоколов обмена информацией. Эта задача совершенно справедливо представлялась важнейшей, поскольку настоятельно требовалось заставить понимать друг друга компьютеры, обладавшие различной архитектурой и программным обеспечением. Первоначально разработчики многочисленных корпоративных сетей договаривались о внутренних протоколах информационного обмена в своих сетях. Никакой стандартизации не было. Но уже в 70-е годы специалистам стало совершенно ясно, что стандартизация необходима и неизбежна. В эти годы шел бурный процесс создания многочисленных национальных и международных комитетов и комиссий по стандартизации программных и аппаратных средств в области вычислительной техники и информационного обмена.

В общем случае **протокол сетевого обмена информацией** можно определить как перечень форматов передаваемых блоков данных, а также правил их обработки и соответствующих действий. Другими словами, протокол обмена данными – это подробная инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные, а также набор правил обработки этих данных.

Человек – оператор компьютера, включенного в сеть, тем или иным способом, например, с помощью программ-приложений, формирует и передает по сети сообщения, предназначенные для других людей или компьютеров. В ответ он также ожидает поступления сообщения. В этом смысле сообщение представляет собой логически законченную порцию информации, предназначен-

ную для потребления конечными пользователями – человеком или прикладной программой. Например, это может быть набор алфавитно-цифровой и графической информации на экране или файл целиком. Сейчас сообщения неразрывно связывают с прикладным уровнем или, как его еще называют, уровнем приложений сетевых протоколов.

Сообщения могут проходить довольно сложный путь по сетям, стоять в очередях на передачу или обработку, в том числе, не доходить до адресата, о чем отправитель также должен быть уведомлен специальным сообщением.

Первоначально вычислительные сети были сетями коммутации сообщений. Это было оправдано, пока сообщения были сравнительно короткими. Но параллельно с этим всегда существовали задачи передачи на расстояние больших массивов информации. Решение этой задачи в сетях с коммутацией сообщений является неэффективным, поскольку длины сообщений имеют большой разброс – от очень коротких до очень длинных, что характерно для компьютерных сетей.

В связи с этим было предложено разбивать длинные сообщения на части – пакеты и передавать сообщения не целиком, а пакетами, вставляя в промежутках пакеты других сообщений. На месте назначения сообщения собираются из пакетов. Короткие сообщения при этом были вырожденным случаем пакета, равного сообщению.

В настоящее время почти все сети в мире являются сетями коммутации пакетов. Но способов обмена пакетами тоже может быть множество. Это связано со стратегией подтверждения правильности передачи.

4 Принципы организации обмена данными в вычислительных сетях

Существуют два принципа организации обмена данными:

1. Установление виртуального соединения с подтверждением приема каждого пакета.
2. Передача датаграмм.

Установление виртуального соединения или создание виртуального канала является более надежным способом обмена информацией. Поэтому он более предпочтителен при передаче данных на большие расстояния и (или) по физическим каналам, в которых возможны помехи. При виртуальном соединении пункт приема информации уведомляет отправителя о правильном или неправильном приеме каждого пакета. Если какой-то пакет принят неправильно, отправитель повторяет его передачу. Так длится до тех пор, пока все сообщение не будет успешно передано. На время передачи информации между двумя пунктами коммутируется канал, подобный каналу при телефонном разговоре. Виртуальным его называют потому, что в отличие от телефонного коммутированного канала обмен информацией может идти по различным физическим путям даже в процессе передачи одного сообщения.

Термин **датаграмма** образован по аналогии с термином телеграмма. Аналогия заключается том, что короткие пакеты – собственно датаграммы – пересылаются адресату без подтверждения получения каждой из них. О получении всего сообщения целиком должна уведомить целевая программа.

5 Транспортный протокол TCP и модель TCP/IP

За время развития вычислительных сетей было предложено и реализовано много протоколов обмена данными, самыми удачными из которых явились семейство протоколов TCP/IP (Transmission Control Protocol/Internet Protocol – протокол управления передачей/межсетевой протокол).

TCP/IP – это набор протоколов, состоящий из следующих компонентов:

- межсетевой протокол (Internet Protocol), обеспечивающий адресацию в сетях (IP-адресацию);
- межсетевой протокол управления сообщениями (Internet Control Message Protocol – ICMP), который обеспечивает низкоуровневую поддержку протокола IP, включая такие функции, как сообщения об ошибках, квитанции, содействие в маршрутизации и т. п.;
- протокол разрешения адресов (Address Resolution Protocol – ARP), выполняющий преобразование логических сетевых адресов в аппаратные, а также обратный ему RARP (Reverse ARP);
- протокол пользовательских датаграмм (User Datagramm Protocol – UDP);
- протокол управления передачей (Transmission Control Protocol – TCP).

Протокол UDP обеспечивает передачу пакетов без проверки доставки, в то время как протокол TCP требует установления виртуального канала и соответственно подтверждения доставки пакета с повтором в случае ошибки.

Этот набор протоколов образует самую распространенную модель сетевого обмена данными, получившую название – TCP/IP. Модель TCP/IP иерархическая и включает четыре уровня.

Таблица 4 – Уровни модели

Уровень	**Название**	**Функция**
4	Прикладной	Приложения пользователей, создание сообщений
3	Транспортный	Доставка данных между программами в сети
2	Сетевой	Адресация и маршрутизация
1	Канальный	Сетевые аппаратные средства и их драйверы

Прикладной уровень определяет способ общения пользовательских приложений. В системах "клиент-сервер" приложение-клиент должно знать, как посылать запрос, а приложение-сервер должно знать, как ответить на запрос. Этот уровень обеспечивает такие протоколы, как HTTP, FTP, Telnet.

Транспортный уровень позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами.

На сетевом уровне определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними.

На канальном уровне определяется адресация физических интерфейсов сетевых устройств, например, сетевых плат. К этому уровню относятся программы управления физическими сетевыми устройствами, так называемые, драйверы.

Как уже отмечалось ранее, в сетях с коммутацией пакетов, а модель TCP/IP относится к таким, для передачи по сети сообщение (сформированное на прикладном уровне) разбивается на пакеты или датаграммы. **Пакет или датаграмма** – это часть сообщения с добавленным заголовком пакета или датаграммы.

На транспортном уровне к полезной информации добавляется заголовок – служебная информация. Для сетевого уровня полезной информацией является уже пакет или датаграмма транспортного уровня. К ним добавляется заголовок сетевого уровня.

Полученный блок данных называется IP-пакетом. Полезной нагрузкой для канального уровня является уже IP-пакет. Здесь перед передачей по каналу к нему добавляются собственный заголовок и еще завершитель. Получившийся блок называется кадром. Он и передается по сети.

Переданный по сети кадр в пункте назначения преобразуется в обратном порядке, проходя по уровням модели снизу вверх.

6 Классы удаленных угроз и их характеристика

При изложении данного материала в некоторых случаях корректнее говорить об удаленных атаках нежели, об удаленных угрозах объектам вычислительных сетей, тем не менее, все возможные удаленные атаки являются в принципе удаленными угрозами информационной безопасности.

Удаленные угрозы можно классифицировать по следующим признакам.

1. **По характеру воздействия:**

- пассивные (класс 1.1);
- активные (класс 1.2).

Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу сети приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в вычислительных сетях является прослушивание канала связи в сети.

Под активным воздействием на вычислительную сеть понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации, нарушение работоспо-

собности и т. д.) и нарушающее принятую в ней политику безопасности. Практически все типы удаленных угроз являются активными воздействиями. Это связано с тем, что в самой природе разрушающего воздействия содержится активное начало. Очевидной особенностью активного воздействия по сравнению с пассивным является принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят определенные изменения. В отличие от активного, при пассивном воздействии не остается никаких следов (просмотр чужого сообщения ничего не меняет).

2. **По цели воздействия:**

- нарушение конфиденциальности информации (класс 2.1);
- нарушение целостности информации (класс 2.2);
- нарушение доступности информации (работоспособности системы) (класс 2.3).

Этот классификационный признак является прямой проекцией трех основных типов угроз – раскрытия, целостности и отказа в обслуживании.

Одна из основных целей злоумышленников – получение несанкционированного доступа к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Примером перехвата информации может служить прослушивание канала в сети. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной угрозы, цель которой нарушение целостности информации, может служить типовая удаленная атака "ложный объект распределенной вычислительной сети".

Принципиально другая цель преследуется злоумышленником при реализации угрозы для нарушения работоспособности сети. В этом случае не предполагается получение несанкционированного доступа к информации. Его основная цель – добиться, чтобы узел сети или какой то из сервисов поддерживаемый им вышел из строя и для всех остальных объектов сети доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая удаленная атака "отказ в обслуживании".

3. **По условию начала осуществления воздействия**

Удаленное воздействие, также как и любое другое, может начать осуществляться только при определенных условиях. В вычислительных сетях можно выделить три вида условий начала осуществления удаленной атаки:

- атака по запросу от атакуемого объекта (класс 3.1);
- атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2);
- безусловная атака (класс 3.3).

В первом случае, злоумышленик ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Internet служат DNS-запросы. Отметим, что данный тип удаленных атак наиболее характерен для распределенных вычислительных сетей.

Во втором случае, злоумышленник осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект.

Реализация третьего вида атаки не связана ни с какими событиями и реализуется безусловно по отношению к цели атаки, то есть атака осуществляется немедленно.

4. **По наличию обратной связи с атакуемым объектом:**

- с обратной связью (класс 4.1);
- без обратной связи (однонаправленная атака) (класс 4.2).

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте.

В отличие от атак с обратной связью удаленным атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную удаленную атаку можно называть однонаправленной удаленной атакой. Примером однонаправленных атак является типовая удаленная атака "отказ в обслуживании".

5. **По расположению субъекта атаки относительно атакуемого объекта:**

- внутрисегментное (класс 5.1);
- межсегментное (класс 5.2).

Рассмотрим ряд определений:

Субъект атаки (или источник атаки) – это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

Маршрутизатор (router) – устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

Подсеть (subnetwork) (в терминологии Internet) – совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

Сегмент сети – физическое объединение хостов. Например, сегмент сети образуют совокупность хостов, подключенных к серверу по схеме "общая шина". При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, то есть в одном или в разных сегментах они находятся. В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах.

Данный классификационный признак позволяет судить о так называемой "степени удаленности" атаки.

Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект её и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по локализации субъекта атаки.

6. **По уровню модели ISO/OSI, на котором осуществляется воздействие:**

- физический (класс 6.1);
- канальный (класс 6.2);
- сетевой (класс 6.3);
- транспортный (класс 6.4);
- сеансовый (класс 6.5);
- представительный (класс 6.6);
- прикладной (класс 6.7).

1.4. Лекция № 4 (1 час)

Тема: « Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей»

1.4.1Вопросы лекции:

1 Удаленная атака "анализ сетевого трафика"
2 Удаленная атака "подмена доверенного объекта"
3 Удаленная атака "ложный объект"
4 Удаленная атака "отказ в обслуживании"
5 Причины успешной реализации удаленных угроз в вычислительных сетях

1.4.2 Краткое содержание вопросов:

1. Удаленная атака "анализ сетевого трафика"

Основной особенностью распределенной вычислительной сети является распределенность ее объектов в пространстве и связь между ними по физическим линиям связи. При этом все управляющие сообщения и данные, пересылаемые между объектами вычислительной сети, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность привела к появлению специфичного для распределенных вычислительных сетей типового удаленного воздействия, заключающегося в прослушивании канала связи, называемого **анализом сетевого трафика**.

Анализ сетевого трафика позволяет:

- изучить логику работы распределенной вычислительной сети, это достигается путем перехвата и анализа пакетов обмена на канальном уровне (знание логики работы сети позволяет на практике моделировать и осуществлять другие типовые удаленные атаки);
- перехватить поток данных, которыми обмениваются объекты сети, т. е. удаленная атака данного типа заключается в получении несанкционированного доступа к информации, которой обмениваются пользователи (примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети).

По характеру воздействия анализ сетевого трафика является пассивным воздействием (класс 1.1). Осуществление данной атаки без обратной связи (класс 4.2) ведет к нарушению конфиденциальности информации (класс 2.1) внутри одного сегмента сети (класс 5.1) на канальном уровне OSI (класс 6.2). При этом начало осуществления атаки безусловно по отношению к цели атаки (класс 3.3).

2. Удаленная атака "подмена доверенного объекта"

Одной из проблем безопасности распределенной ВС является недостаточная идентификация и аутентификация (определение подлинности) удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в вычислительных сетях эта проблема решается использованием виртуального канала, по которому объекты обмениваются определенной информацией, уникально идентифицирующей данный канал. Для адресации сообщений в распределенных вычислительных сетях используется сетевой адрес, который уникален для каждого объекта системы (на канальном уровне модели OSI – это аппаратный адрес сетевого адаптера, на сетевом уровне – адрес определяется протоколом сетевого уровня (например, IP-адрес). Сетевой адрес также может использоваться для идентификации объектов сети. Однако сетевой адрес достаточно просто подделывается и поэтому использовать его в качестве единственного средства идентификации объектов недопустимо. В том случае, когда в вычислительной сети использует нестойкие алгоритмы идентификации удаленных объектов, то оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта сети (т. е. подмена объекта или субъекта сети).

Подмена доверенного объекта распределенной вычислительной сети является активным воздействием (класс 1.2), совершаемым с целью нарушения конфиденциальности (класс 2.1) и целостности (класс 2.2) информации, по наступлению на атакуемом объекте определенного события (класс 3.2). Данная удаленная атака может являться как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи (класс 4.2) с атакуемым объектом и осуществляется на сетевом (класс 6.3) и транспортном (класс 6.4) уровнях модели OSI.

3. Удаленная атака "ложный объект"

Принципиальная возможность реализации данного вида удаленной атаки в вычислительных сетях также обусловлена недостаточно надежной идентификацией сетевых управляющих устройств (например, маршрутизаторов). Целью данной атаки является внедрение в сеть ложного объекта путем изменения маршрутизации пакетов, передаваемых в сети. Внедрение ложного объекта в распределенную сеть может быть реализовано навязыванием ложного маршрута, проходя-

щего через ложный объект.

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через сетевые узлы. При этом маршрутом называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждого адресата указывается оптимальный маршрут. Таблицы маршрутизации существуют не только у маршрутизаторов, но и у любых хостов (узлов) в глобальной сети. Для обеспечения эффективной и оптимальной маршрутизации в распределенных ВС применяются специальные управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом (RIP (Routing Internet Protocol), OSPF (Open Shortest Path First)), уведомлять хосты о новом маршруте – ICMP (Internet Control Message Protocol), удаленно управлять маршрутизаторами (SNMP (Simple Network Management Protocol)). Эти протоколы позволяют удаленно изменять маршрутизацию в сети Интернет, то есть являются протоколами управления сетью.

Реализация данной типовой удаленной атаки заключается в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются объекты сети, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов вычислительной сети.

Навязывание ложного маршрута – активное воздействие (класс 1.2), совершаемое с любой из целей из класса 2, безусловно по отношению к цели атаки (класс 3.3). Данная типовая удаленная атака может осуществляться как внутри одного сегмента (класс 5.1), так и межсегментно (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи с атакуемым объектом (класс 4.2) на транспортном (класс 6.3) и прикладном (класс 6.7) уровне модели OSI.

Получив контроль над проходящим потоком информации между объектами, ложный объект вычислительной сети может применять различные методы воздействия на перехваченную информацию, например:

- селекция потока информации и сохранение ее на ложном объекте (нарушение конфиденциальности);
- модификация информации:
  - модификация данных (нарушение целостности),
  - модификация исполняемого кода и внедрение разрушающих программных средств – программных вирусов (нарушение доступности, целостности);
- подмена информации (нарушение целостности).

4. Удаленная атака "отказ в обслуживании"

Одной из основных задач, возлагаемых на сетевую операционную систему, функционирующую на каждом из объектов распределенной вычислительной сети, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в сети каждый субъект системы должен иметь возможность подключиться к любому объекту сети и получить в соответствии со своими правами удаленный доступ к его ресурсам. Обычно в вычислительных сетях возможность предоставления удаленного доступа реализуется следующим образом: на объекте в сетевой операционной системе запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т. п.), предоставляющих удаленный доступ к ресурсам данного объекта. Данные программы-серверы входят в состав телекоммуникационных служб предоставления удаленного доступа. Задача сервера состоит в том, чтобы постоянно ожидать получения запроса на подключение от удаленного объекта и, получив такой запрос, передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты сети. В этом случае непосредственно операционная система обрабатывает приходящие извне запросы на создание виртуального канала и передает их в соответствии с идентификатором запроса (номер порта) прикладному процессу, которым является соответствующий сервер. В зависимости от различных параметров объектов вычислительной сети, основными из которых являются быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи – количество одновременно устанавливаемых виртуальных подключений ограничено, соответст-

венно, ограничено и число запросов, обрабатываемых в единицу времени. С этой особенностью работы вычислительных сетей связана типовая удаленная атака "отказ в обслуживании". Реализация этой угрозы возможна, если в вычислительной сети не предусмотрено средств аутентификации (проверки подлинности) адреса отправителя. В такой вычислительной сети возможна передача с одного объекта (атакующего) на другой (атакуемый) бесконечного числа анонимных запросов на подключение от имени других объектов.

Результат применения этой удаленной атаки – нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов вычислительной сети – отказ в обслуживании. Одна из разновидностей этой типовой удаленной атаки заключается в передаче с одного адреса такого количества запросов на атакуемый объект, какое позволяет трафик. В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов. И последней, третьей разновидностью атаки "отказ в обслуживании" является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы.

Типовая удаленная атака "отказ в обслуживании" является активным (класс 1.2) однонаправленным воздействием (класс 4.2), осуществляемым с целью нарушения работоспособности системы (класс 2.3) на транспортном (класс 6.4) и прикладном (класс 6.7) уровнях модели OSI.

5. Причины успешной реализации удаленных угроз в вычислительных сетях

Применительно к вычислительным сетям, чтобы ликвидировать угрозы (удаленные атаки), осуществляемые по каналам связи, необходимо ликвидировать причины, их порождающие. Анализ механизмов реализации типовых удаленных атак позволяет сформулировать причины, по которым данные удаленные атаки оказались возможными.

Отсутствие выделенного канала связи между объектами вычислительной сети. Данная причина обуславливает типовую удаленную атаку "анализ сетевого трафика". Такая атака программно возможна только в случае, если атакующий находится в сети с физически широковещательной средой передачи данных как, например, всем известная и получившая широкое распространение среда Ethernet (общая "шина"). Такая атака невозможна в сетях с топологией "звезда" (Token Ring), которая не является широковещательной, но и не имеет достаточного распространения. Анализ сетевого трафика программными средствами практически невозможен, если у каждого объекта системы существует для связи с любым другим объектом выделенный канал. Следовательно, причина успеха типовой удаленной атаки заключается в широковещательной среде передачи данных или отсутствие выделенного канала связи между объектами сети.

Недостаточная идентификация объектов и субъектов сети неоднократно упоминались при рассмотрении удаленных угроз информационной безопасности. Эта причина предопределяет такие типовые удаленные атаки как "ложный объект" и "подмена доверенного объекта", а в некоторых случаях и "отказ в обслуживании".

Взаимодействие объектов без установления виртуального канала – еще одна причина возможных угроз информационной безопасности. Объекты распределенных вычислительных сетей могут взаимодействовать двумя способами:

- с использованием виртуального канала;
- без использования виртуального канала.

При создании виртуального канала объекты вычислительной сети обмениваются динамически вырабатываемой ключевой информацией, позволяющей уникально идентифицировать канал, тем самым подтверждается подлинность объектов информационного обмена друг перед другом.

Однако ошибочно считать распределенную вычислительную сеть безопасной, даже если все взаимодействие объектов происходит с созданием виртуального канала. Виртуальный канал является необходимым, но не достаточным условием безопасного взаимодействия. Чрезвычайно важным в данном случае становится выбор алгоритма идентификации при создании виртуального

канала. Так, например, **отсутствие контроля за виртуальными каналами связи между объектами** сети может привести к нарушению работоспособности системы путем формирования множества запросов на создание соединения (виртуального канала), в результате чего либо переполняется число возможных соединений, либо система, занятая обработкой ответов на запросы, вообще перестает функционировать (типовая удаленная атака "отказ в обслуживании"). В данном случае успех удаленной атаки возможен из-за отсутствия контроля при создании соединения, т. е. один узел анонимно или от имени другого узла сети формирует множество запросов, а система не имеет возможности фильтровать подобные запросы.

Отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений – еще одна из возможных причин успешной реализации удаленных угроз информационной безопасности.

Если в вычислительных сетях не предусмотрены возможности контроля за маршрутом сообщения, то адрес отправителя сообщения оказывается ничем не подтвержден. Таким образом, в системе будет существовать возможность отправки сообщения от имени любого объекта системы, а именно, путем указания в заголовке сообщения чужого адреса отправителя. Также в таких сетях будет невозможно определить, откуда на самом деле пришло сообщение, а следовательно, вычислить координаты атакующего. Отсутствие в вычислительной сети контроля за маршрутом сообщений порождает как невозможность контроля за созданием соединений, так и возможность анонимной отправки сообщения, следовательно, является причиной успеха таких удаленных угроз, как "подмена доверенного объекта" и "ложный объект сети".

Отсутствие в распределенных вычислительных сетях полной информации о ее объектах также является потенциальной причиной успеха удаленных угроз, поскольку в распределенной системе с разветвленной структурой, состоящей из большого числа объектов, может возникнуть ситуация, когда для доступа к определенному объекту системы у субъекта взаимодействия может не оказаться необходимой информации об интересующем объекте. Обычно такой недостающей информацией об объекте является его адрес. В этом случае осуществляется широковещательный запрос в сеть, на который реагирует искомый узел. Такая ситуация характерна особенно для сети Интернет, при работе в которой пользователь знает доменное имя узла, но для соединения с ним необходим IP-адрес, поэтому при вводе доменного имени операционная система формирует запрос к серверу доменных имен. В ответ DNS сервер сообщает IP-адрес запрашиваемого узла. В такой схеме существует возможность выдачи ложного ответа на запрос пользователя, например, путем перехвата DNS-запроса пользователя и выдачей ложного DNS-ответа.

В системе с заложенной в нее неопределенностью существуют потенциальные возможности внесения в систему ложного объекта и получение ложного ответа, в котором вместо информации о запрашиваемом объекте будет информация о ложном объекте.

Примером распределенной вычислительной сети с заложенной неопределенностью является сеть Интернет. Во-первых, у узлов, находящихся в одном сегменте, может не быть информации об аппаратных адресах друг друга. Во-вторых, применяются непригодные для непосредственной адресации доменные имена узлов, используемые для удобства пользователей при обращении к удаленным системам.

Отсутствие в распределенных вычислительных сетях криптозащиты сообщений – последняя из рассматриваемых в данной теме причин успеха удаленных угроз информационной безопасности.

Поскольку в вычислительных сетях связь между объектами осуществляется по каналам связи, то всегда существует принципиальная возможность для злоумышленника прослушать канал и получить несанкционированный доступ к информации, которой обмениваются по сети ее абоненты. В том случае, если проходящая по каналу информация не зашифрована и атакующий каким-либо образом получает доступ к каналу, то удаленная атака "анализ сетевого трафика" является наиболее эффективным способом получения информации. Очевидна и причина, делающая эту атаку столь эффективной. Эта причина – **передача по сети незашифрованной информации**.

6 Принципы построения защищенных вычислительных сетей

В предыдущих темах были рассмотрены основные угрозы информационной безопасности в распределенных вычислительных сетях и причины, следствием которых они являются.

В данной теме рассмотрим принципы построения защищенных вычислительных сетей.

Принципы построения защищенных вычислительных сетей по своей сути являются правилами построения защищенных систем, учитывающие, в том числе, действия субъектов вычислительной сети, направленные на обеспечение информационной безопасности.

Напомним, что одним из базовых принципов обеспечения информационной безопасности для любых объектов информационных отношений является борьба не с угрозами, являющимися следствием недостатков системы, а с причинами возможного успеха нарушений информационной безопасности.

Перечислим установленные ранее причины успеха удаленных угроз информационной безопасности:

1. Отсутствие выделенного канала связи между объектами вычислительной сети.
2. Недостаточная идентификация объектов и субъектов сети.
3. Взаимодействие объектов без установления виртуального канала.
4. Отсутствие контроля за виртуальными каналами связи между объектами сети.
5. Отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений.
6. Отсутствие в распределенных вычислительных сетях полной информации о ее объектах.
7. Отсутствие в распределенных вычислительных сетях криптозащиты сообщений.

Для устранения первой причины ("отсутствие выделенного канала...") идеальным случаем было бы установление выделенных каналов связи между всеми объектами сети. Однако это практически невозможно и нерационально, в первую очередь, из-за высокой стоимости такой топологии вычислительной сети.

Существуют два возможных способа организации топологии распределенной вычислительной сети с выделенными каналами. В первом случае каждый объект связывается физическими линиями связи со всеми объектами системы. Во втором случае в системе может использоваться сетевой концентратор, через который осуществляется связь между объектами (топология "звезда").

Преимущества сети с выделенным каналом связи между объектами заключаются:

- в передаче сообщений напрямую между источником и приемником, минуя остальные объекты системы;
- в возможности идентифицировать объекты распределенной системы на канальном уровне по их адресам без использования специальных криптоалгоритмов шифрования трафика;
- в отсутствии неопределенности информации о ее объектах, поскольку каждый объект в такой системе изначально однозначно идентифицируется и обладает полной информацией о других объектах системы.

Недостатки сети с выделенными каналами:

- сложность реализации и высокие затраты на создание;
- ограниченное число объектов системы (зависит от числа входов у концентратора).

Альтернативой сетям с выделенным каналом являются сети с широковещательной передачей данных, надежная идентификация объектов в которых может обеспечиваться использованием специальных криптокарт, осуществляющих шифрование на канальном уровне.

Отметим, что создание распределенных систем только с использованием широковещательной среды передачи или только с выделенными каналами неэффективно, поэтому представляется правильным при построении распределенных вычислительных сетей с разветвленной топологией и большим числом объектов использовать комбинированные варианты соединений объектов. Для обеспечения связи между объектами большой степени значимости можно использовать выделенный канал. Связь менее значимых объектов системы может осуществляться с использованием комбинации "общая шина" – выделенный канал.

Безопасная физическая топология сети (выделенный канал) является необходимым, но не достаточным условием устранения причин угроз информационной безопасности, поэтому необходимы дополнительные меры по повышению защищенности объектов вычислительных сетей. Дальнейшее повышение защищенности вычислительных сетей связано с использованием виртуальных каналов, обеспечивающих дополнительную идентификацию и аутентификацию объектов вычислительной сети.

Для повышения защищенности вычислительных сетей при установлении виртуального соединения необходимо использовать криптоалгоритмы с открытым ключом (рассмотрим далее).

Одной из разновидностей шифрования с открытым ключом является цифровая подпись сообщений, надежно идентифицирующая объект распределенной вычислительной сети и виртуальный канал.

Отсутствие контроля за маршрутом сообщения в сети является одной из причин успеха удаленных угроз. Рассмотрим один из вариантов устранения этой причины.

Все сообщения, передаваемые в распределенных сетях, проходят по цепочке маршрутизаторов, задачей которых является анализ адреса назначения, выбор оптимального маршрута и передача по этому маршруту пакета или на другой маршрутизатор или непосредственно абоненту, если он напрямую подключен к данному узлу. Информация о маршруте передачи сообщения может быть использована для идентификации источника этого сообщения с точностью до подсети, т. е. от первого маршрутизатора.

Задачу проверки подлинности адреса сообщения можно частично решить на уровне маршрутизатора. Сравнивая адреса отправителя, указанные в сообщении с адресом подсети, из которой получено сообщение, маршрутизатор выявляет те сообщения, у которых эти параметры не совпадают, и соответственно, отфильтровывает такие сообщения.

Контроль за виртуальным соединением можно рассматривать как принцип построения защищенных систем, поскольку в этом случае определяются те правила, исходя из которых система могла бы либо поставить запрос в очередь, либо нет. Для предотвращения такой атаки как "отказ в обслуживании", вызванной "лавиной" направленных запросов на атакуемый узел целесообразно ввести ограничения на постановку в очередь запросов от одного объекта. Очевидно, что данная мера имеет смысл в тех случаях, когда надежно решена проблема идентификации объекта – отправителя запроса. В противном случае злоумышленник может отправлять запросы от чужого имени.

Для повышения защищенности распределенных вычислительных сетей **целесообразно проектировать их с полностью определенной информацией о ее объектах,** что позволит устранить шестую из указанных причин успешной реализации удаленных угроз.

Однако в вычислительных сетях с неопределенным и достаточно большим числом объектов (например, Интернет) спроектировать систему с отсутствием неопределенности практически невозможно, а отказаться от алгоритмов удаленного поиска не представляется возможным.

Из существующих двух типов алгоритмов удаленного поиска (с использованием информационно-поискового сервера и с использованием широковещательных запросов) более безопасным является алгоритм удаленного поиска с использованием информационно-поискового сервера. Однако для большей безопасности связь объекта, формирующего запрос с сервером, необходимо осуществлять с подключением по виртуальному каналу. Кроме этого, объекты, подключенные к данному серверу, и сам сервер должны содержать заранее определенную статическую ключевую информацию, используемую при создании виртуального канала (например, закрытый криптографический ключ).

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

2.1 Лабораторная работа №1 (2 часа).

Тема: «Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»»

2.1.1 Цель работы: Изучение нормативно-правовых основ информационной безопасности в РФ и стандартов информационной безопасности: «Общие критерии»

2.1.2 Задачи работы:

1. Изучить законодательные меры в сфере информационной безопасности

2. Изучить Стратегию национальной безопасности Российской Федерации до 2020 года

2.1.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютеры Pentium Core2 1,6GHz,

2. Мониторы LCD 17" Acer.

2.1.4 Описание (ход) работы:

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 Стратегия 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.
- Стратегия национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента РФ от 12 мая 2009 г. N 537) ., 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.

2.2 Лабораторная работа №2 (2 часа).

Тема: «Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях**»**

2.2.1 Цель работы: рассмотреть принципы организации обмена данными в вычислительных сетях

2.2.2 Задачи работы:

1. Специфика средств защиты в компьютерных сетях

2. Понятие протокола передачи данных

2.2.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютеры Pentium Core2 1,6GHz,

2. Мониторы LCD 17" Acer.

2.2.4 Описание (ход) работы:

Особенности вычислительных сетей и, в первую очередь, глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

- защита подключений к внешним сетям;
- защита корпоративных потоков данных, передаваемых по открытым сетям;
- защита потоков данных между клиентами и серверами;
- обеспечение безопасности распределенной программной среды;
- защита важнейших сервисов (в первую очередь – Web-сервиса);
- аутентификация в открытых сетях.

Обмен информацией между ЭВМ на больших расстояниях всегда казался более важной задачей, чем локальный обмен. Поэтому ему уделялось больше внимания и, соответственно, велось большее финансирование во многих странах. Один из немногих открытых проектов по исследованию вычислительных сетей, финансировавшийся военным ведомством США, известен под названием сеть **ARPA – Advanced Research Projects Agency**. С самого начала в рамках этого проекта велись работы по объединению ресурсов многих вычислительных машин различного типа. В 1960-1970-е годы многие результаты, полученные при эксплуатации сети ARPA, были опубликованы в открытой печати. Это обстоятельство, а также тот факт, что почти все страны занялись практически слепым копированием не только аппаратной архитектуры американских машин, но и базового программного обеспечения, обусловили сильное влияние сети ARPA на многие другие сети, именно поэтому принято считать, что сеть ARPA является предшественницей знаменитой всемирной компьютерной сети Интернет.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1Практическое занятие № 1 (2 часа) Тема: « Понятие «Информационная безопасность.

Составляющие информационной безопасности»

3.1.1 Задание для работы:

1 Проблема информационной безопасности общества

2 Определение понятия «информационная безопасность»

3 Доступность информации

4 Целостность информации

5 Конфиденциальность информации

6 Задачи информационной безопасности общества

7 Уровни формирования режима информационной безопасности

3.1.2. Краткое описание проводимого занятия

1. Ознакомление с составляющими информационной безопасности
2. Рассмотреть вопросы, связанные с уровнями формирования режима информационной безопасности
3. С помощью устного опроса и (или) тестирования оценить уровень усвоения студентами изученного материала.

3.1.3.Результаты и выводы

Усвоение студентами знаний по теме практического занятия.

Разработал(а): _____ О.Я. Набокина