

**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: очная

# 1. КОНСПЕКТ ЛЕКЦИЙ

## 1.1 ЛЕКЦИЯ №1 (2 часа)

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 скоординированных 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 (2 часа)**

**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 международного 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 огра-



ниченного 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 сильном действующем 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. Соккрытие 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 копиро-

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

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

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

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

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

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

а. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

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

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.

### **1.3 Лекция № 3 (2 часа)**

**Тема: «Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ»**

#### **1.3.1 Вопросы лекции:**

- 1 Сервисы безопасности в вычислительных сетях
- 2 Механизмы безопасности
- 3 Администрирование средств безопасности
- 4 Документы по оценке защищенности автоматизированных систем в РФ

#### **1.3.2 Краткое содержание вопросов**

##### **1 Сервисы безопасности в вычислительных сетях**

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

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

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

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

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

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

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

ФСТЭК и его роль в обеспечении информационной безопасности в РФ. В Российской Федерации информационная безопасность обеспечивается соблюдением указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов ФСТЭК России и других нормативных документов.

Наиболее общие документы были рассмотрены ранее при изучении правовых основ информационной безопасности. В РФ с точки зрения стандартизации положений в сфере информа-

ционной безопасности первостепенное значение имеют руководящие документы (РД) ФСТЭК России, одной из задач которой является "проведение единой государственной политики в области технической защиты информации".

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

За 10 лет своего существования ФСТЭК разработала и довела до уровня национальных стандартов десятки документов, среди которых:

1. Руководящий документ "Положение по аттестации объектов информатизации по требованиям безопасности информации" (Утверждено Председателем ФСТЭК России 25.11.1994 г.).

2. Руководящий документ "Автоматизированные системы (АС). Защита от несанкционированного доступа (НСД) к информации. Классификация АС и требования к защите информации" (ФСТЭК России, 1997 г.).

3. Руководящий документ "Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации" (ФСТЭК России, 1992 г.).

4. Руководящий документ "Концепция защиты средств вычислительной техники от НСД к информации" (ФСТЭК России, 1992 г.).

5. Руководящий документ "Защита от НСД к информации. Термины и определения" (ФСТЭК России, 1992 г.).

6. Руководящий документ "Средства вычислительной техники (СВТ). Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" (ФСТЭК России, 1997 г.).

7. Руководящий документ "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей" (ФСТЭК России, 1999 г.).

8. Руководящий документ "Специальные требования и рекомендации по технической защите конфиденциальной информации" (ФСТЭК России, 2001 г.).

## **2 Механизмы безопасности**

В X.800 определены следующие сетевые механизмы безопасности:

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

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

"+" механизм используется для реализации данной функции безопасности;

"-" механизм не используется для реализации данной функции безопасности.

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

## **3 Администрирование средств безопасности**

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

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

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

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

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

Администрирование механизмов безопасности включает:

- управление криптографическими ключами (генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров);
- администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т. п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т. п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т. п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотариризацией (распространение информации о нотариальных службах, администрирование этих служб).

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

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

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

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

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

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

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

#### 4 Документы по оценке защищенности автоматизированных систем в РФ

Рассмотрим наиболее значимые из этих документов, определяющие критерии для оценки

защищенности автоматизированных систем.

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

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

- первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и включает только первый класс.

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

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС – коллективный или индивидуальный.

В документе определены девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

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

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

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

Всего выделяется пять показателей защищенности:

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

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

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

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию "Особой важности". Второму классу защищенности МЭ соответствует класс защи-

ценности АС 1Б, предназначенный для обработки "совершенно секретной" информации и т. п.

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

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

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

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

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС.

#### **1.4 Лекция №4**

**Тема: «Административный уровень обеспечения информационной безопасности.**

**Классификация угроз «Информационной безопасности»**

##### **1.4.1 Вопросы лекции:**

- 1 Цели, задачи и содержание административного уровня
- 2 Разработка политики информационной безопасности
- 3 Классы угроз информационной безопасности
- 4 Каналы несанкционированного доступа к информации

##### **1.4.2 Краткое содержание вопросов**

#### **1. Цели, задачи и содержание административного уровня**

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

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

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

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

Содержанием административного уровня являются следующие мероприятия:

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

#### **2 Разработка политики информационной безопасности**

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

**Политика безопасности** – это комплекс предупредительных мер по обеспечению инфор-



мационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Основные направления разработки политики безопасности:

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

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

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

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

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

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

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

В состав автоматизированной информационной системы входят следующие компоненты:

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

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

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

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

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

В зависимости от размеров организации, степени развитости ее информационной системы,

некоторые из перечисленных ролей могут отсутствовать вообще, а некоторые могут совмещаться одним и тем же физическим лицом.

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

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

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

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

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

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

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

### 3 Классы угроз информационной безопасности

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

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

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

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

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

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

Знание возможных угроз информационной безопасности, а также уязвимых мест системы

защиты, необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности.

Угрозы информационной безопасности классифицируются по нескольким признакам:

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

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

Рассмотрим угрозы **по характеру воздействия**.

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

Причинами *случайных воздействий* при эксплуатации могут быть:

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

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

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

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

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

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

#### **4 Каналы несанкционированного доступа к информации**

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

**Каналы НСД** классифицируются по компонентам автоматизированных информационных систем:

Через человека:

- хищение носителей информации;

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

Через программу:

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

Через аппаратуру:

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

## 1.5 Лекция №5 (2 часа)

**Тема: «Классификация компьютерных вирусов и характеристика вирусоподобных программ. Антивирусные программы и профилактика компьютерных вирусов»**

### 1.5.1 Вопросы лекции:

- 1 Компьютерные вирусы и информационная безопасность
- 2 Характерные черты компьютерных вирусов
- 3 Классификация компьютерных вирусов по среде обитания
- 4 Классификация компьютерных вирусов по особенностям алгоритма работы
- 5 Классификация компьютерных вирусов по деструктивным возможностям
- 6 Виды "вирусоподобных" программ
- 7 Характеристика "вирусоподобных" программ. "Троянские" программы (логические бомбы)
- 8 Утилиты скрытого администрирования
- 9 "Intended"-вирусы
- 10 Особенности работы антивирусных программ
- 11 Классификация антивирусных программ
- 12 Факторы, определяющие качество антивирусных программ
- 13 Характеристика путей проникновения вирусов в компьютеры
- 14 Правила защиты от компьютерных вирусов
- 15 Обнаружение загрузочного вируса
- 16 Обнаружение резидентного вируса
- 17 Обнаружение макровируса
- 18 Общий алгоритм обнаружения вируса

### 1.5.2 Краткое содержание вопросов

#### 1 Компьютерные вирусы и информационная безопасность

Компьютерные вирусы одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

Современный компьютерный вирус – это практически незаметный для обычного пользователя "враг", который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Вирусные эпидемии способны блокировать работу организаций и предприятий.

На тему борьбы с вирусами написаны десятки книг и сотни статей, борьбой с компьютерными вирусами профессионально занимаются тысячи специалистов в сотнях компаний. Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. Эти оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов.

В последнее время вирусные эпидемии стали настолько масштабными и угрожающими, что сообщения о них выходят на первое место в мировых новостях. При этом следует иметь в ви-

ду, что антивирусные программы и аппаратные средства не дают полной гарантии защиты от вирусов, а большинство пользователей не имеют даже основных навыков "защиты" от вирусов.

Е. Касперский в своей книге "Компьютерные вирусы" отмечает, что "Борьба с компьютерными вирусами является борьбой человека с человеческим же разумом. Эта борьба является борьбой умов, поскольку задачи, стоящие перед вирусологами, ставят такие же люди :".

## **2 Характерные черты компьютерных вирусов**

Термин "компьютерный вирус" появился в середине 80-х годов, на одной из конференций по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако, строгого определения компьютерного вируса так и нет.

Трудность, возникающая при попытках сформулировать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и др.) либо присущи другим программам, которые никакого отношения не имеют к вирусам, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

Основная особенность компьютерных вирусов заключается в возможности их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые не являются вирусами, но именно эта особенность является обязательным (необходимым) свойством компьютерного вируса. К более полной характеристике современного компьютерного вируса следует добавить способность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТе Р 51275-2006 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения".

**Программный вирус** – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Невозможность четкой формулировки определения компьютерного вируса сама по себе не является проблемой. Главная проблема, которая следует из этого, заключается в том, что нет четких (однозначных) признаков, по которым можно отличить различные файлы от "вирусов", что не позволяет в полной мере устранить их влияние.

Несмотря на все усилия разработчиков антивирусного программного обеспечения до сегодняшнего дня нет достаточно надежных антивирусных средств и, скорее всего, противостояние "вирусописателей" и их оппонентов будет постоянным.

Исходя из этого, необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной "компьютерной гигиены".

## **3 Классификация компьютерных вирусов по среде обитания**

По среде "обитания" вирусы делятся на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

**Файловые вирусы** внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

**Загрузочные вирусы** записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.

**Макровирусы** заражают файлы-документы и электронные таблицы популярных офисных

приложений.

**Сетевые вирусы** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний – например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс- и полиморфик-технологии. Другой пример такого сочетания – сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая операционная система является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS – DOS, Windows, и т. д. Макровирусы заражают файлы форматов Word, Excel, пакета Office. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

#### **4 Классификация компьютерных вирусов по особенностям алгоритма работы**

По особенностям алгоритма работы вирусы делятся на:

- резидентные;
- стелс-вирусы;
- полиморфик-вирусы;
- вирусы, использующие нестандартные приемы.

**Резидентный** вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. К резидентным относятся макровирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие "перезагрузка операционной системы" трактуется как выход из редактора.

В многозадачных операционных системах время "жизни" резидентного DOS-вируса также может быть ограничено моментом закрытия зараженного DOS-окна, а активность загрузочных вирусов в некоторых операционных системах ограничивается моментом инсталляции дисковых драйверов ОС.

Использование **стелс-алгоритмов** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо "подставляют" вместо себя незараженные участки информации. В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов.

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования (обнаружения) вируса. **Полиморфик-вирусы (polymorphic)** – это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные **нестандартные приемы** часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т. д.

#### **5 Классификация компьютерных вирусов по деструктивным возможностям**

По деструктивным возможностям вирусы можно разделить на:

- **безвредные**, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- **неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске;

- **опасные вирусы**, которые могут привести к серьезным сбоям в работе компьютера;
- **очень опасные**, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже повредить аппаратные средства компьютера.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия, поскольку вирус, ка

## **6 Виды "вирусоподобных" программ**

К "вредным программам", помимо вирусов, относятся:

- "троянские программы" (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- "intended"-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

## **7 Характеристика "вирусоподобных" программ. "Троянские" программы (логические бомбы)**

К "троянским" программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Например, уничтожение информации на дисках при каждом запуске или по определенному графику и т. д. Большинство известных "троянских" программ являются программами, которые маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по электронным конференциям. По сравнению с вирусами "троянские" программы не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем. К "троянским" программам также относятся так называемые "дроперы" вирусов – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют присутствие вируса в файле. Например, файл шифруется или упаковывается неизвестным архиватором, что не позволяет антивирусу "увидеть" заражение.

Отметим еще один тип программ (программы – "злые шутки"), которые используются для устрашения пользователя, о заражении вирусом или о каких-либо предстоящих действиях с этим связанных, т. е. сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям. Например, к "злым шуткам" относятся программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. К категории "злых шуток" можно отнести также заведомо ложные сообщения о новых "супер-вирусах". Такие сообщения периодически появляются в Интернете и обычно вызывают панику среди пользователей.

## **8 Утилиты скрытого администрирования**

Утилиты скрытого администрирования являются разновидностью "логических бомб" ("троянских программ"), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные "троянские" программы: отсутствие предупреждения об установке и запуске. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке активных приложений. В результате пользователь может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать/отсылать файлы, запускать и уничто-

жать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. В результате эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т. п.

## **9 "Intended"-вирусы**

К таким вирусам относятся программы, которые, на первый взгляд, являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении не помещает в начало файла команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (в большинстве приводит к "зависанию" компьютера) и т. д. К категории "intended" также относятся вирусы, которые по приведенным выше причинам размножаются только один раз – из "авторской" копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению. Появляются "intended"-вирусы чаще всего из-за неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

## **Конструкторы вирусов**

К данному виду "вредных" программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макро-вирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т. п.

## **Полиморфные генераторы**

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфные генераторы распространяются в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор.

## **10 Особенности работы антивирусных программ**

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения. **Антивирусная программа** – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Вместе с тем необходимо признать, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При работе с антивирусными программами необходимо знать некоторые понятия:

**Ложное срабатывание** – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

**Пропуск вируса** – недетектирование вируса в зараженном объекте.

**Сканирование по запросу** – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

**Сканирование налету** – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т. п.). В этом режиме антивирус постоянно активен, он присутствует в памяти "резидентно" и проверяет объекты без

## **11 Классификация антивирусных программ**

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры, CRC-сканеры (ревизоры). Существуют также антивирусы блокировщики и иммунизаторы.

**Сканеры.** Принцип работы антивирусных сканеров основан на проверке файлов, секторов



и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые "маски". Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфно-вирусов.

Во многих сканерах используются также алгоритмы "эвристического сканирования", т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории – "универсальные" и "специализированные". Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Сканеры также делятся на "резидентные" (мониторы), производящие сканирование "на лету", и "нерезидентные", обеспечивающие проверку системы только по запросу. Как правило, "резидентные" сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как "нерезидентный" сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам – размеры антивирусных баз, которые сканерам приходится хранить и пополнять, и относительно небольшая скорость поиска вирусов.

**CRC-сканеры.** Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т. д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие "анти-стелс" алгоритмы реагируют практически на 100 % вирусов сразу после появления изменений на компьютере. Характерный недостаток этих антивирусов заключается в невозможности обнаружения вируса с момента его появления и до тех пор, пока не будут произведены изменения на компьютере. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в восстанавливаемых файлах или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

**Блокировщики.** Антивирусные блокировщики – это резидентные программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю. К "вирусоопасным" относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочный сектор диска и др., которые характерны для вирусов в моменты их размножения.

К достоинствам блокировщиков относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно активизируется.

**Иммунизаторы.** Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

## **12 Факторы, определяющие качество антивирусных программ**

Качество антивирусной программы определяется несколькими факторами. Перечислим их по степени важности:

1. Надежность и удобство работы – отсутствие "зависаний" антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
2. Качество обнаружения вирусов всех распространенных типов, сканирование внутри

файлов-документов/таблиц, упакованных и архивированных файлов. Отсутствие "ложных срабатываний". Возможность лечения зараженных объектов.

3. Существование версий антивируса под все популярные платформы (DOS, Windows, Linux и т. д.).
4. Возможность сканирование "налету".
5. Существование серверных версий с возможностью администрирования сети.
6. Скорость работы.

### **13 Характеристика путей проникновения вирусов в компьютеры**

Рассмотрим основные пути проникновения вирусов в компьютеры пользователей:

1. Глобальные сети – электронная почта.
2. Электронные конференции, файл-серверы ftp.
3. Пиратское программное обеспечение.
4. Локальные сети.
5. Персональные компьютеры "общего пользования".
6. Сервисные службы.

#### **Глобальные сети – электронная почта**

Основным источником вирусов на сегодняшний день является глобальная сеть Интернет, такова расплата за возможность доступа к массовым информационным ресурсам и службам. Наибольшее число заражений вирусом происходит при обмене электронными письмами через почтовые серверы E-mail. Пользователь получает электронное письмо с вирусом, который активизируется (причем, как правило, незаметно для пользователя) после просмотра файла-вложения электронного письма. После этого вирус (стелс) выполняет свои функции. В первую очередь вирус "заботится" о своем размножении, для этого формируются электронные письма от имени пользователя по всем адресам адресной книги. Далее идет цепная реакция.

Для полноты картины приведем характеристику (вирусные новости "Лаборатории Касперского") наиболее распространенного на 1 марта 2004 г. сетевого червя "Netsky. D".

"Netsky. D" распространяется через письма электронной почты. Зараженные сообщения могут иметь самый разный внешний вид: червь случайным образом выбирает заголовок из 25 вариантов, текст письма (6 вариантов), имя вложенного файла (21 вариант). Вложенный файл имеет фиктивное расширение. PIF, в действительности представляя собой обычную EXE-программу (размер около 17 Кб). Если пользователь имел неосторожность запустить этот файл, то червь устанавливает себя в систему и запускает процедуры распространения. При установке "Netsky. D" копирует себя с именем WINLOGON. EXE в каталог Windows и регистрирует этот файл в ключе автозапуска системного реестра. Таким образом, он обеспечивает свою активизацию при каждой загрузке операционной системы. Для дальнейшей рассылки червь сканирует файлы наиболее распространенных интернет-приложений (например, WAB, EML, DOC, HTML, MSGи др.), считывает из них адреса электронной почты и незаметно для владельца компьютера отправляет на них свои копии. Важно отметить, что рассылка писем осуществляется в обход установленного на компьютере почтового клиента, но с использованием встроенной SMTP-подпрограммы. С ее помощью "Netsky. D" распространяется через 23 прокси-сервера, расположенных в разных концах мира. Червь имеет ряд побочных действий. В частности, он удаляет из системного реестра ключи другого сетевого червя – "Mydoom", а также пытается нарушить работу антивируса Касперского.

#### **Локальные сети**

Другой путь "быстрого заражения" – локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере. Далее пользователи при очередном подключении к сети запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.

#### **Персональные компьютеры "общего пользования"**

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из студентов принес на своих дискетах вирус и заразил какой-либо учебный компьютер, то очередной вирус будет гулять по всему учебному заведению, включая домашние компьютеры студентов и сотрудников.

#### **Пиратское программное обеспечение**

Нелегальные копии программного обеспечения, как это было всегда, являются одной из

основных "зон риска". Часто пиратские копии на дискетах и даже на CD-дисках содержат файлы, зараженные самыми разнообразными типами вирусов. Необходимо помнить, что низкая стоимость программы может дорого обойтись при потере данных.

### **Сервисные службы**

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре в сервисных центрах.

## **14 Правила защиты от компьютерных вирусов**

Учитывая возможные пути проникновения вирусов, приведем основные **правила защиты от вирусов**.

1. Внимательно относитесь к программам и документам, которые получаете из глобальных сетей.
2. Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте его на наличие вирусов.
3. Используйте специализированные антивирусы – для проверки "на лету" (например, SplDer Guard из пакета Dr. Web и др.) всех файлов, приходящих по электронной почте (и из Интернета в целом).
4. Для уменьшения риска заразить файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети, такие как: ограничение прав пользователей; установку атрибутов "только на чтение" или "только на запуск" для всех выполняемых файлов (к сожалению, это не всегда оказывается возможным) и т. д.
5. Регулярно проверяйте сервер обычными антивирусными программами, для удобства и системности используйте планировщики заданий.
6. Целесообразно запустить новое программное обеспечение на тестовом компьютере, не подключенном к общей сети.
7. Используйте лицензионное программное обеспечение, приобретенное у официальных продавцов.
8. Дистрибутивы копий программного обеспечения (в том числе копий операционной системы) необходимо хранить на защищенных от записи дисках.
9. Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.
10. Постоянно обновляйте вирусные базы используемого антивируса.
11. Старайтесь не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.
12. Ограничьте (по возможности) круг лиц допущенных к работе на конкретном компьютере.
13. Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т. д.).
14. Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа.
15. При работе с Word/Excel включите защиту от макросов, которая сообщает о присутствии макроса в открываемом документе и предоставляет возможность запретить этот макрос. В результате макрос не только не выполняется, но и не виден средствами Word/Excel.

## **15 Обнаружение загрузочного вируса**

В загрузочных секторах дисков расположены, как правило, небольшие программы, назначение которых состоит в определении размеров и границ логических дисков (для MBR винчестера) или загрузке операционной системы (для boot-сектора).

В начале следует прочитать содержимое сектора, подозрительного на наличие вируса. Для этой цели удобно использовать DISKEDIT из "Нортоновских утилит". Некоторые загрузочные вирусы практически сразу можно обнаружить по наличию различных текстовых строк выводимых на экран при активизации вируса. Другие вирусы, поражающие boot-секторы дисков, наоборот, определяются по отсутствию строк, которые обязательно должны присутствовать в boot-

секторе. К таким строкам относятся имена системных файлов и строки сообщений об ошибках. Отсутствие или изменение строки-заголовка boot-сектора (строка, название фирмы-производителя программного обеспечения) также может служить сигналом о заражении вирусом.

Однако существуют вирусы, которые внедряются в загрузчик без изменения его текстовых строк и с минимальными изменениями кода загрузчика. Для того чтобы обнаружить такой вирус, в большинстве случаев достаточно отформатировать дискету на заведомо незараженном компьютере, сохранить в виде файла ее boot-сектор, затем некоторое время использовать ее на зараженном компьютере (записать/прочитать несколько файлов), а после этого на незараженном компьютере сравнить ее boot-сектор с оригинальным. Если в коде загрузочного сектора произошли изменения – вирус обнаружен.

## **16 Обнаружение резидентного вируса**

Если в компьютере обнаружены следы деятельности вируса, но видимых изменений в файлах и системных секторах дисков не наблюдается, то вполне возможно, что компьютер поражен одним из "стелс"-вирусов.

Обнаружение резидентного Windows-вируса является крайне сложной задачей. Вирус, находясь в среде Windows как приложение или VxD-драйвер, практически невидим, поскольку одновременно активны несколько десятков приложений и VxD, и вирус по внешним признакам от них ничем не отличается. Для того чтобы обнаружить программу-вирус в списках активных приложений и VxD, необходимо разбираться во всех тонкостях Windows и иметь полное представление о драйверах и приложениях, установленных на данном компьютере, поэтому приемлемый способ обнаружить резидентный Windows-вирус – загрузить DOS и проверить запускаемые файлы Windows.

## **17 Обнаружение макровируса**

Характерными проявлениями макровирусов являются:

- Word: невозможность конвертирования зараженного документа Word в другой формат.
- Word: зараженные файлы имеют формат Template (шаблон), поскольку при заражении Word-вирусы конвертируют файлы из формата Word Document в Template.
- Excel/Word: в STARTUP (Автозагрузка)-каталоге присутствуют "посторонние" файлы.
- Excel: наличие в Книге (Book) лишних и скрытых Листов (Sheets)..

Для проверки системы на предмет наличия вируса можно использовать пункт меню Сервис/макрос. Если обнаружены "чужие макросы", то они могут принадлежать вирусу. Однако этот метод не работает в случае стелс-вирусов, которые запрещают работу этого пункта меню, что, в свою очередь, является достаточным основанием считать систему зараженной.

Многие вирусы имеют ошибки или некорректно работают в различных версиях Word/Excel, в результате чего Word/Excel выдают сообщения об ошибке.

Если такое сообщение появляется при редактировании нового документа или таблицы и при этом заведомо не используются какие-либо пользовательские макросы, то это также может служить признаком заражения системы.

Сигналом о вирусе являются и изменения в файлах и системной конфигурации Word, Excel и Windows. Многие вирусы тем или иным образом меняют пункты меню, разрешают или запрещают некоторые функции, устанавливают на файлы пароль при их заражении. Большое количество вирусов создает новые секции и/или опции в файле конфигурации Windows (WIN. INI).

Естественно, что к проявлениям вируса относятся такие очевидные факты, как появление сообщений или диалогов с достаточно странным содержанием или на языке, не совпадающем с языком установленной версии Word/Excel.

## **18 Общий алгоритм обнаружения вируса**

При анализе алгоритма вируса необходимо выяснить:

- способ(ы) размножения вируса;
- характер возможных повреждений, которые вирус нанес информации, хранящейся на дисках;
- метод лечения оперативной памяти и зараженных файлов (секторов).

**При анализе файлового вируса** необходимо выяснить, какие файлы (COM, EXE, SYS) поражаются вирусом, в какое место (места) в файле записывается код вируса - в начало, конец или середину файла, в каком объеме возможно восстановление файла (полностью или частично), в каком месте вирус хранит восстанавливаемую информацию.

**При анализе загрузочного вируса** основной задачей является выяснение адреса (адресов) сектора, в котором вирус сохраняет первоначальный загрузочный сектор.

**Для резидентного вируса** требуется также выделить участок кода, создающий резидентную копию вируса. Необходимо также определить, каким образом и где в оперативной памяти вирус выделяет место для своей резидентной копии.

**Для анализа макровирусов** необходимо получить текст их макросов. Для нешифрованных ("не-стелс") вирусов это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует "стелс"-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов. Такие специализированные утилиты есть практически у каждой фирмы-производителя антивирусов, однако, они являются утилитами "внутреннего пользования" и не распространяются за пределы фирм.

В любом случае, если есть возможность, правильнее всего передавать зараженные файлы специалистам антивирусных лабораторий.

## 1.6 Лекция № 6 (2 часа)

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

### 1.6.1 Вопросы 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

### 1.6.2 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. Пер-

вые 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.

Использование 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 "Aranet", 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, предназначенную 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 в 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 Datagram 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 работоспособности 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, злоумышленник 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 (однаправленная 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 однаправленной удаленной атакой. Примером однаправленных 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).

## **1.7. Лекция № 7 (2 часа)**

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

### **1.7.1 Вопросы 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
- 6 Принципы построения защищенных вычислительных сетей

### **1.7.2 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 используются нестойкие алгоритмы идентификации удаленных объектов, то оказывается возможной типовой удаленной атакой, заключающейся 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, проходящего 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 ре-

сурсам 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, соответственно, 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 заикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы.

Типовая удаленная атака "отказ в обслуживании" является активным (класс 1.2) односторонним 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 се-

тей 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 широко-вещательный 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 широкополосной 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 широкополосной 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 широковебчатых 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).

## 1.8 Лекция № 8 (2 часа)

**Тема: «Идентификация и аутентификация. Криптография и шифрование.**

**Методы разграничение доступа»**

### 1.8.1 Вопросы лекции:

- 1 Определение понятий "идентификация" и "аутентификация"
- 2 Механизм идентификация и аутентификация пользователей

- 3 Структура криптосистемы
- 4 Классификация систем шифрования данных
- 5 Симметричные и асимметричные методы шифрования
- 6 Механизм электронной цифровой подписи
- 7 Методы разграничения доступа
- 8 Мандатное и дискретное управление доступом

## 1.8.2 Краткое содержание вопросов

### 1. Определение понятий "идентификация" и "аутентификация"

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Дадим определения этих понятий.

**Идентификация** – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

**Аутентификация** (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

- набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на **паролях** – конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

- методы, использующие постоянные (многократно используемые) пароли;
- методы, использующие одноразовые (динамично изменяющиеся) пароли.

Использование одноразовых или динамически меняющихся паролей является более надежным методом парольной защиты.

В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

- пассивные (карточки с памятью);
- активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить не-

санкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двукомпонентной аутентификацией.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, например, многоразовые пароли, динамически меняющиеся пароли.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100 % идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако эти методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться, требуют пока сложного и дорогостоящего оборудования. Это обуславливает их использование пока только на особо важных объектах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, по почерку, по тембру голоса и др.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что исключает их перехват. Такой метод аутентификации может быть использован в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

## **2. Механизм идентификация и аутентификация пользователей**

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем.

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

В целом аутентификация по уровню информационной безопасности делится на три категории:

1. Статическая аутентификация.
2. Устойчивая аутентификация.
3. Постоянная аутентификация.

Первая категория обеспечивает защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса работы прочесть аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Устойчивая аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе ко-

торых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

### 3. Структура криптосистемы

Самый надежный технический метод защиты информации основан на использовании криптосистем. Криптосистема включает:

- алгоритм шифрования;
- набор ключей (последовательность двоичных чисел), используемых для шифрования;
- систему управления ключами.

Общая схема работы криптосистемы показана рис. 15.

Криптосистемы решают такие проблемы информационной безопасности как обеспечение **конфиденциальности, целостности данных**, а также **аутентификацию данных и их источников**.

Криптографические методы защиты являются обязательным элементом безопасных информационных систем. Особое значение криптографические методы получили с развитием распределенных открытых сетей, в которых нет возможности обеспечить физическую защиту каналов связи.

### 4. Классификация систем шифрования данных

Основным классификационным признаком систем шифрования данных является способ их функционирования. По способу функционирования системы шифрования данных делят на два класса:

- системы "прозрачного" шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах "прозрачного" шифрования (шифрование "налету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование. Системы второго класса обычно представляют собой утилиты (программы), которые необходимо специально вызывать для выполнения шифрования.

Как уже отмечалось, особое значение криптографические преобразования имеют при передаче данных по распределенным вычислительным сетям. Для защиты данных в распределенных сетях используются два подхода: канальное шифрование и оконечное (абонентское) шифрование.

В случае **канального шифрования** защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством – встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы.

**Оконечное (абонентское) шифрование** позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся служебная информация остается открытой.

### 5. Симметричные и асимметричные методы шифрования

Классические криптографические методы делятся на два основных типа: **симметричные** (шифрование секретным ключом) и **асимметричные** (шифрование открытым ключом).

В **симметричных** методах для шифрования и расшифровывания используется один и тот же секретный ключ. Наиболее известным стандартом на симметричное шифрование с закрытым ключом является стандарт для обработки информации в государственных учреждениях США DES (Data Encryption Standard). Основной недостаток этого метода заключается в том, что ключ должен быть известен и отправителю, и получателю. Это существенно усложняет процедуру назначения и распределения ключей между пользователями. Указанный недостаток послужил при-

чиной разработки методов шифрования с открытым ключом – асимметричных методов.

**Асимметричные методы** используют два взаимосвязанных ключа: для шифрования и расшифрования. Один ключ является закрытым и известным только получателю. Его используют для расшифрования. Второй из ключей является открытым, т. е. он может быть общедоступным по сети и опубликован вместе с адресом пользователя. Его используют для выполнения шифрования. Схема функционирования данного типа криптосистемы показана на рис. 17.

В настоящее время наиболее известным и надежным является асимметричный алгоритм RSA (Rivest, Shamir, Adleman).

## 6. Механизм электронной цифровой подписи

Для контроля целостности передаваемых по сетям данных используется электронная цифровая подпись, которая реализуется по методу шифрования с открытым ключом.

**Электронная цифровая подпись** представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Идея технологии электронной подписи состоит в следующем. Отправитель передает два экземпляра одного сообщения: открытое и расшифрованное его закрытым ключом (т. е. обратно шифрованное). Получатель шифрует с помощью открытого ключа отправителя расшифрованный экземпляр. Если он совпадет с открытым вариантом, то личность и подпись отправителя считается установленной.

При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма – хэш, защищающая послание от нелегального изменения. Электронная подпись здесь гарантирует как целостность сообщения, так и удостоверяет личность отправителя.

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае **ненадежного управления** ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети. Различают следующие виды функций управления ключами: генерация, хранение и распределение ключей.

Способы генерации ключей для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами.

Функция хранения предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (т. е. мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключа является наиболее критическим вопросом криптозащиты.

**Распределение** – самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

## 7. Методы разграничения доступа

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются: **списком ресурсов**, доступным пользователю и **правами по доступу** к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

1. Разграничение доступа по спискам.
2. Использование матрицы установления полномочий.

3. Разграничение доступа по уровням секретности и категориям.

4. Парольное разграничение доступа.

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами – объекты (ресурсы) информационной системы. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Данный метод предоставляет более унифицированный и удобный подход, т. к. вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток – пустые).

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов информационной системы по уровням секретности и категориям.

При разграничении по степени секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем ему определен, например, пользователь имеющий доступ к данным "секретно", также имеет доступ к данным "конфиденциально" и "общий доступ".

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы информационной системы разделяются по уровням важности, причем определенному уровню соответствует категория пользователей. В качестве примера, где используются категории пользователей, приведем операционную систему Windows 2000, подсистема безопасности которой по умолчанию поддерживает следующие категории (группы) пользователей: "администратор", "опытный пользователь", "пользователь" и "гость". Каждая из категорий имеет определенный набор прав. Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения групповых политик безопасности.

Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

Разграничение прав доступа является обязательным элементом защищенной информационной системы. Напомним, что еще в "Оранжевой книге США" были введены понятия:

- произвольное управление доступом;
- принудительное управление доступом.

## **8. Мандатное и дискретное управление доступом**

В ГОСТе Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации" и в документах ФСТЭК России определены два вида (принципа) разграничения доступа:

- дискретное управление доступом;
- мандатное управление доступом.

**Дискретное управление** доступом представляет собой разграничение доступа между по-

именованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

**Мандатное управление доступом** основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть ничто иное, как произвольное управление доступом (по "Оранжевой книге США"), а мандатное управление реализует принудительное управление доступом.

## **1.9.Лекция № 9 (2 часа)**

**Тема: «Регистрация и аудит. Межсетевое экранирование.**

**Технология виртуальных частных сетей (VPN)»**

### **1.9.1Вопросы лекции:**

- 1 Определение и содержание регистрации и аудита информационных систем
- 2 Этапы регистрации и методы аудита событий информационной системы
- 3 Классификация межсетевых экранов
- 4 Характеристика межсетевых экранов
- 5 Сущность и содержание технологии виртуальных частных сетей
- 6 Понятие "туннеля" при передаче данных в сетях

### **1.9.2.Краткое содержание вопросов:**

#### **1. Определение и содержание регистрации и аудита информационных систем**

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т. д.

Для сертифицируемых по безопасности информационных систем список контролируемых событий определен рабочим документом ФСТЭК России: "Положение о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации".

Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

**Аудит** – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Рассматриваемые механизмы регистрации и аудита являются сильным психологическим средством, напоминая потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные критические ошибки.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемого админи-

стратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

**Регистрационный журнал** – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Обнаружение попыток нарушений информационной безопасности входит в функции активного аудита, задачами которого является оперативное выявление подозрительной активности и предоставление средств для автоматического реагирования на нее.

Под **подозрительной активностью** понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Например, подсистема аудита, отслеживая процедуру входа (регистрации) пользователя в систему подсчитывает количество неудачных попыток входа. В случае превышения установленного порога таких попыток подсистема аудита формирует сигнал о блокировке учетной записи данного пользователя.

## 2 Этапы регистрации и методы аудита событий информационной системы

Организация регистрации событий, связанных с безопасностью информационной системы включает как минимум три этапа:

1. Сбор и хранение информации о событиях.
2. Защита содержимого журнала регистрации.
3. Анализ содержимого журнала регистрации.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место и средства хранения журнала, возможность регистрации шифрованной информации и др.

Регистрируемые данные должны быть защищены, в первую очередь, от несанкционированной модификации и, возможно, раскрытия.

Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления несанкционированных действий.

**Статистические методы** основаны на накоплении среднестатистических параметров функционирования подсистем и сравнении текущих параметров с ними. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз.

**Эвристические методы** используют модели сценариев несанкционированных действий, которые описываются логическими правилами или модели действий, по совокупности приводящие к несанкционированным действиям.

## 3 Классификация межсетевых экранов

Одним из эффективных механизмов обеспечения информационной безопасности распределенных вычислительных сетей является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет **межсетевой экран** или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

- по месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;



- по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов, например, при использовании сетевой операционной системы Novell Netware, следует принимать во внимание протокол SPX/IPX.

#### 4 Характеристика межсетевых экранов

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;
- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

**Межсетевые экраны с фильтрацией пакетов** представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

**Шлюзы сеансового уровня** контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым, исключая подмену IP-адреса. Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

**Шлюзы прикладного уровня** проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип меж сетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, Telnet и т. д.) и служат для проверки сетевых пакетов на наличие достоверных данных.

Шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Интернет при работе по низкоскоростным каналам, но существенно при работе во внутренней сети.

Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И, наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами

данных, что теоретически должно обеспечить более эффективную фильтрацию пакетов.

## 5 Сущность и содержание технологии виртуальных частных сетей

Технология виртуальных частных сетей (VPN - Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

- шифрования (с использованием инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);

- экранирования (с использованием межсетевых экранов);

- туннелирования.

Сущность технологии VPN заключается в следующем (рис. 22):

1. На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливается VPN-агент, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

2. Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

- анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут, поддерживая одновременно несколько алгоритмов шифрования и контроля целостности). Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;

- вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;

- пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);

- формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

3. При получении IP-пакета выполняются обратные действия:

- из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);

- согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);

- после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

## 6. Понятие "туннеля" при передаче данных в сетях

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется "туннелем", а технология его создания называется "туннелированием"). Вся информация передается по туннелю в зашифрованном виде.

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Фильтрация пакетов реализуется в соответствии с настройками VPN-агента, совокупность которых образует

политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

## **2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ**

### **2.1 Лабораторная работа №1 (4 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 го-

да

#### **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 (4 часа).**

**Тема:** «Административный уровень обеспечения информационной безопасности. Классификация угроз «Информационной безопасности»»

**2.2.1 Цель работы:** Разработка политики информационной безопасности

**2.2.2 Задачи работы:**

1. Изучить классы угроз информационной безопасности
2. Изучить каналы несанкционированного доступа к информации

**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:**

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

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

**Каналы несанкционированного доступа к информации**

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

**Каналы НСД** классифицируются по компонентам автоматизированных информационных систем:

Через человека:

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

Через программу:

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

Через аппаратуру:

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

**2.3 Лабораторная работа №3 (4 часа).**

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

**2.3.1 Цель работы:** рассмотреть принципы организации обмена данными в вычислительных сетях

**2.3.2 Задачи работы:**

## 1. Специфика средств защиты в компьютерных сетях

### 2. Понятие протокола передачи данных

#### 2.1.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютеры Pentium Core2 1,6GHz,
2. Мониторы LCD 17" Acer.

#### 2.3.4 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.

### 2.4 Лабораторная работа №4 (4 часа).

**Тема:** «Идентификация и аутентификация. Криптография и шифрование. Методы разграничения доступа»

**2.4.1 Цель работы:** Изучить методы разграничения доступа и механизм электронной цифровой подписи

#### 2.4.2 Задачи работы:

1. Рассмотреть механизм идентификации и аутентификации пользователей
2. Рассмотреть структуру криптосистемы
3. Рассмотреть классификацию систем шифрования данных
4. Рассмотреть симметричные и асимметричные методы шифрования

#### 2.4.3 Перечень приборов, материалов, используемых в лабораторной работе:

1. Компьютеры Pentium Core2 1,6GHz,
2. Мониторы LCD 17" Acer .....

#### 2.4.4 Описание (ход) работы:

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем.

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защи-

ценных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Самый надежный технический метод защиты информации основан на использовании криптосистем. Криптосистема включает:

- алгоритм шифрования;
- набор ключей (последовательность двоичных чисел), используемых для шифрования;
- систему управления ключами.

Криптосистемы решают такие проблемы информационной безопасности как обеспечение **конфиденциальности, целостности данных**, а также **аутентификацию данных и их источников**.

Основным классификационным признаком систем шифрования данных является способ их функционирования. По способу функционирования системы шифрования данных делят на два класса:

- системы "прозрачного" шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах "прозрачного" шифрования (шифрование "налету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование. Системы второго класса обычно представляют собой утилиты (программы), которые необходимо специально вызывать для выполнения шифрования.

### **3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ**

#### **3.1 Практическое 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.

#### **Практическое занятие №2 (4 часа)**

**Тема: «Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ»**

##### **3.2.1 Задание для работы**

- 1 Сервисы безопасности в вычислительных сетях

2 Механизмы безопасности

3 Администрирование средств безопасности

4 Документы по оценке защищенности автоматизированных систем в РФ

### **3.2.2. Краткое описание проводимого занятия**

1.Ознакомление с механизмами безопасности

2.Рассмотреть вопросы, связанные с администрированием средств безопасности

3.С помощью устного опроса и (или) тестирования оценить уровень усвоения студентами изученного материала.

### **3.2.3.Результаты и выводы**

Усвоение студентами знаний по теме практического занятия.

### **3.3. Практическое занятие № 3 (4 часа)**

**Тема: «Классификация компьютерных вирусов и характеристика вирусоподобных программ. Антивирусные программы и профилактика компьютерных вирусов»**

#### **3.3.1 Задание для работы**

1 Компьютерные вирусы и информационная безопасность

2 Характерные черты компьютерных вирусов

3 Классификация компьютерных вирусов по среде обитания

4 Классификация компьютерных вирусов по особенностям алгоритма работы

5 Классификация компьютерных вирусов по деструктивным возможностям

6 Виды "вирусоподобных" программ

7 Характеристика "вирусоподобных" программ. "Троянские" программы (логические бомбы)

8 Утилиты скрытого администрирования

9 "Intended"-вирусы

10 Особенности работы антивирусных программ

11 Классификация антивирусных программ

12 Факторы, определяющие качество антивирусных программ

13 Характеристика путей проникновения вирусов в компьютеры

14 Правила защиты от компьютерных вирусов

15 Обнаружение загрузочного вируса

16 Обнаружение резидентного вируса

17 Обнаружение макровируса

18 Общий алгоритм обнаружения вируса

#### **3.3.2. Краткое описание проводимого занятия**

1.Ознакомление с компьютерными вирусами и информационной безопасностью

2.Рассмотреть вопросы, связанные с особенностями работы антивирусных программ

3.С помощью устного опроса и (или) тестирования оценить уровень усвоения студентами изученного материала.

#### **3.3.3.Результаты и выводы**

Усвоение студентами знаний по теме практического занятия.

### **3.4 Практическое занятие № 7 (4 часа)**

**Тема: «Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.№**

#### **3.4.1. Задание для работы**

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

6 Принципы построения защищенных вычислительных сетей

### **3.4.2. Краткое описание проводимого занятия**

1. Ознакомление с причинами успешной реализации удаленных угроз в вычислительных сетях.
2. Рассмотреть вопросы, связанные с принципами построения защищенных вычислительных сетей
3. С помощью устного опроса и (или) тестирования оценить уровень усвоения студентами изученного материала.

### **3.4.3. Результаты и выводы**

Усвоение студентами знаний по теме практического занятия.

### **3.5 Практическое занятие № 5 (4 часа)**

**Тема: Регистрация и аудит. Межсетевое экранирование.**

**Технология виртуальных частных сетей (VPN)**

#### **3.5.1. Задание для работы**

1. Определение и содержание регистрации и аудита информационных систем
2. Этапы регистрации и методы аудита событий информационной системы
3. Классификация межсетевых экранов
4. Характеристика межсетевых экранов
5. Сущность и содержание технологии виртуальных частных сетей
6. Понятие "туннеля" при передаче данных в сетях

### **3.5.2. Краткое описание проводимого занятия**

1. Ознакомление с определением и содержанием регистрации и аудита информационных систем.
2. Рассмотреть вопросы, связанные с характеристиками межсетевых экранов
3. С помощью устного опроса и (или) тестирования оценить уровень усвоения студентами изученного материала.

### **3.5.3. Результаты и выводы**

Усвоение студентами знаний по теме практического занятия.

Разработал(а): \_\_\_\_\_

О.Я. Набокина