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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.06 Информационная безопасность

Направление подготовки 38.04.01 Экономика

Профиль подготовки Экономическая безопасность

Квалификация (степень) выпускника магистр

Форма обучения заочная

Содержание

1. КОНСПЕКТ ЛЕКЦИЙ

ЛЕКЦИЯ № 1: (2 часа)

Тема: Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ

Вопросы лекции

1 Сервисы безопасности в вычислительных сетях

2 Механизмы безопасности

3 Администрирование средств безопасности

4 Документы по оценке защищенности автоматизированных систем в РФ

Краткое содержание вопросов

Наименование вопроса № 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 соблюдение указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов ФСТЭК России и других нормативных документов.

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

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

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 недекларированных возможностей" (ФСТЭК России, 1999 г.).

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

Наименование вопроса № 2 Механизмы безопасности

В X.800 определены следующие сетевые механизмы безопасности:

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

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

Таблица 1 - Взаимосвязь функций и механизмов безопасности

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

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Неотказуемость	-	+	-	+	-	-	-	+

"+" механизм используется для реализации данной функцию безопасности;

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

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

Наименование вопроса № 3 Администрирование средств безопасности

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

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

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

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

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

Администрирование механизмов безопасности включает:

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

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

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

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

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

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

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

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

Наименование вопроса № 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.

В таб. 2 приведены классы защищенности АС и требования для их обеспечения.

Таблица 2 - Требования к защищенности автоматизированных систем

Подсистемы и требования	**Классы**

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

По существу в таб. 2 систематизированы минимальные требования, которым необходимо следовать, чтобы обеспечить конфиденциальность информации.

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

Руководящий документ "СВТ. Межсетевые экраны. Защита от НСД к информации. Пока-

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

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

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

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

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

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

Лекция № 2 (2 часа)

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

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

Краткое содержание вопросов

Наименование вопроса № **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 меха-

низма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

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

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

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

- целостности данных;
- конфиденциальности данных;
- доступности данных.

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

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

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

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

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

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

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

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными на протоколах TCP/IP, и предоставляющих аналогичные сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признан-

ным на международном уровне. Национальные границы, законы, стандарты не должны препятствовать защите потоков данных между клиентами и серверами.

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

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

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

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

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

Наименование вопроса № **2 Специфика средств защиты в компьютерных сетях**

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

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

Вопросы реализации таких методов защиты будут рассмотрены далее.

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

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

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

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

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

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

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

Наименование вопроса № **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 исследо-

ванию 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.

Наименование вопроса № 4 Принципы организации обмена данными в вычислительных сетях

Существуют два принципа организации обмена данными:

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

Установление виртуального соединения или создание виртуального канала является более надежным способом обмена информацией. Поэтому он более предпочтителен при передаче данных на большие расстояния и (или) по физическим каналам, в которых возможны помехи. При

виртуальном соединении пункт приема информации уведомляет отправителя о правильном или неправильном приеме каждого пакета. Если какой-то пакет принят неправильно, отправитель повторяет его передачу. Так длится до тех пор, пока все сообщение не будет успешно передано. На время передачи информации между двумя пунктами коммутируется канал, подобный каналу при телефонном разговоре. Виртуальным его называют потому, что в отличие от телефонного коммутированного канала обмен информацией может идти по различным физическим путям даже в процессе передачи одного сообщения.

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

Наименование вопроса № **5 Транспортный протокол TCP и модель TCP/IP**

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

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

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

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

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

Таблица 4 – Уровни модели

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

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

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

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

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

Как уже отмечалось ранее, в сетях с коммутацией пакетов, а модель TCP/IP относится к таким, для передачи по сети сообщение (сформированное на прикладном уровне) разбивается на

пакеты или датаграммы. **Пакет или датаграмма** – это часть сообщения с добавленным заголовком пакета или датаграммы.

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

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

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

Наименование вопроса № **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, злоумышленик ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Internet служат DNS-запросы. Отметим, что данный тип удаленных атак наиболее характерен для распределенных вычислительных сетей.

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

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

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

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

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

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

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

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

Рассмотрим ряд определений:

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

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

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

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

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу рас-

полагаются 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).

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие 1 (ПЗ-1)

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

1 Задание для работы

Вопросы к занятию:

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

Типовые тесты (для контроля знаний)

1. Защита информации от непреднамеренного воздействия это деятельность по предотвращению:

a)получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

b)воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

c)воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

d)неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

e)несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

2.Защита информации от разглашения это деятельность по предотвращению:

a)получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

b)воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а

также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

2. Краткое описание проводимого занятия

1. Ознакомление с правовыми основами информационной безопасности общества
2. Рассмотреть вопросы, связанные с основными положениями важнейших законодательных актов РФ в области информационной безопасности и защиты информации
3. С помощью устного опроса и (или) тестирования оценить уровень усвоения студентами изученного материала.

3.Результаты и выводы

1. Усвоение студентами знаний и закрепление навыков по теме практического занятия.
2. Формирование у студентов практических умений, развитие навыков командной работы, коммуникативной компетентности.

Практическое занятие 2 (ПЗ-2) Административный уровень обеспечения информационной безопасности. Классификация угроз «Информационной безопасности»

1 Задание для работы

Вопросы к занятию

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

Типовые тесты (для контроля знаний)

1. Носитель информации это:
a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

2. Собственник информации это:
a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;
e) участник правоотношений в информационных процессах.

3 Владелец информации это:

a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

d) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;

e) участник правоотношений в информационных процессах.

2. Краткое описание проводимого занятия

1. Устный опрос и (или) тестирование по теме занятия.

2. Обсуждение ситуационных (проблемных) вопросов по теме занятия.

3. При обсуждении ситуационных (проблемных) вопросов по теме занятия необходимо акцентировать внимание на следующем:

4. Обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным вопросам темы.

5. Формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности.

6. Выработка таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

3.Результаты и выводы

1. Усвоение студентами знаний и закрепление навыков по теме практического занятия.

2. Формирование у студентов практических умений, развитие навыков командной работы, коммуникативной компетентности.

Практическое занятие 3 (ПЗ-3) Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей

1. Задание для работы

Вопросы к занятию

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

Типовые тесты (для контроля знаний)

1. Доступ к информации это:

a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

2. Защита информации от утечки это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установлен-

ных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

3.Защита информации от несанкционированного воздействия это деятельность по предотвращению:
a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

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.Результаты и выводы

1. Усвоение студентами знаний и закрепление навыков по теме практического занятия.

2. Формирование у студентов практических умений, развитие навыков командной работы, коммуникативной компетентности.

Практическое занятие 4 (ПЗ-4) Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа.

1. Задание для работы

Вопросы к занятию

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

Типовые тесты (для контроля знаний)

1.Защита информации от непреднамеренного воздействия это деятельность по предотвращению:
a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил дос-

тупа к защищаемой информации;
b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

2.Защита информации от разглашения это деятельность по предотвращению:
a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

2. Краткое описание проводимого занятия

1. Устный опрос и (или) тестирование по теме занятия.

2. Обсуждение ситуационных (проблемных) вопросов по теме занятия.

3. При обсуждении ситуационных (проблемных) вопросов по теме занятия необходимо акцентировать внимание на следующем:

4. Обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным вопросам темы.

5. Формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности.

6. Выработка таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

3.Результаты и выводы

1. Усвоение студентами знаний и закрепление навыков по теме практического занятия.

2. Формирование у студентов практических умений, развитие навыков командной работы, коммуникативной компетентности.