Частное образовательное учреждение высшего образования
«Международный Институт Дизайна и Сервиса»
(ЧОУВО МИДиС)
Кафедра математики и информатики

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки: 09.03.03 Прикладная информатика
Направленность (профиль): Разработка компьютерных игр и приложений с виртуальной и дополненной реальностью
Квалификация выпускника: Бакалавр
Год набора: 2020

Автор-составитель: Чеботарев С.С.

Челябинск 2024

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

Код и наименование компетенций выпускника	Код и наименование индикатора достижения компетенций
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы

№ п/п	Код компетенции	Наименование компетенции	Этапы формирования компетенций
1.	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных	*1 Этап - Знать:* ОПК-3.1. Принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
			2 Этап - Уметь: ОПК-3.2. Решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-

		требований информационной безопасности	коммуникационных технологий с учетом основных требований информационной безопасности
			3 Этап - Владеть: ОПК-3.3. Навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
2.	ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	*1 Этап - Знать:* ОПК-4.1. Основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
			2 Этап - Уметь: ОПК-4.2. Применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
			3 Этап - Владеть: ОПК-4.3. Навыками составления технической документации на различных этапах жизненного цикла информационной системы

2. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

№ п/п	Код компетенции	Наименование компетенции	Критерии оценивания компетенций на различных этапах формирования	Шкала оценивания
1.	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информацион	*1 Этап - Знать:* ОПК-3.1. Принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	«ЗАЧТЕНО»: 1. Хорошее знание программного материала. 2. Хорошие навыки выполнения практических заданий 3. Точность и обоснованность выводов. 4. Логичное изложение вопроса, соответствие изложения научному стилю. 5. Правильные ответы на дополнительные

		но-коммуникационных технологий и с учетом основных требований информационной безопасности	*2 Этап - Уметь:* ОПК-3.2. Решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности	вопросы. «НЕ ЗАЧТЕНО»: 1. Поверхностное усвоение программного материала. 2. Неумение четко сформулировать выводы. 3. Отсутствие навыков научного стиля изложения. 4. Неточные ответы на дополнительные вопросы. 5. Незнание значительной части программного материала. 6. Неумение выделить главное, сделать выводы и обобщения.
			3 Этап - Владеть: ОПК-3.3. Навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	
2.	ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	*1 Этап - Знать:* ОПК-4.1. Основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	
			2 Этап - Уметь: ОПК-4.2. Применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	
			3 Этап - Владеть: ОПК-4.3. Навыками составления технической документации на различных этапах жизненного цикла информационной системы	

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1 ЭТАП – ЗНАТЬ

Устный опрос по темам:

ТЕМА 1.1. Основные положения теории информации

1. Виды информации, типы каналов связи.
2. Особенности и технические характеристики современных каналов передачи информации, использующих различные физические принципы (электрические, акустические, оптические, радиочастотные) с точки зрения безопасности.
3. Виды сигналов.
4. преимущества цифровых каналов перед аналоговыми с точки зрения защищённости передаваемой информации.

ТЕМА 1.2. Правовое регулирование информационных процессов в обществе

1. Классификация информации по степени ограниченности доступа к ней (открытая, конфиденциальная, секретная).
2. Понятие тайны (государственная, промышленная, коммерческая, финансовая, частная тайна).
3. Государство как гарант права граждан на защиту личной информации и интеллектуальной собственности.
4. Законы Российской Федерации о защите тайны и интеллектуальной собственности.

ТЕМА 1.3. Методы похищения, искажения, подмены, уничтожения информации

1. Виды информационных нападений (по месту воздействия).
2. Виды информационных нападений (по способу воздействия):пассивные, активные.
3. Традиционные методы с использованием подручных технических средств.

ТЕМА 1.4. Устройства двойного применения.

1. Использование возможностей современной техники для получения стабильного результата.
2. Использование свойств обратимости преобразователей информации.
3. Радиоэлектронные средства. Электронные устройства двойного применения.
4. Использование средств спецтехники.

ТЕМА 2.1. Информационная безопасность и современные информационные технологии.

1. Концепция информационной безопасности Российской Федерации в основных сферах: политической, экономической, военной, в сфере духовной жизни.
2. Классификация источников угроз информационной безопасности.
3. Основные объекты информационной безопасности и специфика угроз для них.
4. Комплекс мероприятий по обеспечению информационной безопасности объектов электронно-вычислительной техники.

ТЕМА 2.2. Общие принципы системного подхода к обеспечению безопасности информации

1. Организационные меры для выявления и предотвращения угроз информационной безопасности.
2. Понятие о сертификации информационных устройств.
3. Закрытие каналов передачи (шифрование).
4. Виды устройств шифрования (канальные, абонентские).

ТЕМА 2.3. Безопасность компьютерных систем.

1. Компьютерные вирусы.
2. Стандартные средства защиты (аппаратные и программные).
3. Организационные меры по защите информации на ЭВМ.
4. Стандарты шифрования. Электронная цифровая подпись - технология применения и защита.

ТЕМА 2.4. Противоправное использование компьютеров

1. Сущность компьютерных преступлений.

2. Классификация компьютерных преступлений.
3. Основные виды компьютерных преступлений.
4. "Электронные деньги" и безопасность платёжных систем с использованием пластиковых карт.

Поиск, анализ и обобщение информации, и ее представление в виде презентационного доклада по следующим темам:

1. История криптографии
2. Социальная инженерия
3. История хакеров
4. Файловые системы с шифрованием
5. Учетные записи в операционных системах
6. Защищенные среды передачи
7. Биометрические технологии
8. Многоядерные антивирусы
9. Операционные системы маршрутизаторов Cisco
10. Влияние электромагнитной совместимости
11. Влияние кэширования данных на безопасность
12. Безопасность в ОС Юникс
13. Безопасность в ОС Windows
14. Программные закладки
15. Кодификатор Интерпола по компьютерным преступлениям
16. Аттестация рабочих мест
17. Обзор ФЗ 152
18. Руткиты в ОС
19. Безопасность одиночной ЭВМ
20. Межсетевые экраны.

2 ЭТАП – УМЕТЬ

Комплект практических работ для формирования умений

Практическая работа№ 1. Международные стандарты информационного обмена. Понятие угрозы

Цель работы: Получение знаний о видах угроз, путей и каналов утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками.

Изучив тему, студент должен:

- знать закономерности возникновения угроз информационной безопасности;
- знать классификацию угроз информационной безопасности;
- знать пути и каналы утечки информации;
- знать виды удаленных атак на интрасеть;
- знать классические и современные методы взлома интрасетей.

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

угроза информационной безопасности, утечка информации, нарушение целостности информации, модификация информации, искажение информации, подделка информации, уничтожение информации, блокирование информации, побочное электромагнитное излучение, электромагнитная наводка, специальное электронное закладное устройство, внешнее воздействие на информационный ресурс.

Содержание работы:

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Виды атак и методы взлома интрасетей»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Основные закономерности возникновения и классификация угроз информационной безопасности.
2. Пути и каналы утечки информации.
3. Удаленные атаки на интрасети.
4. Классические методы взлома интрасетей.
5. Современные методы взлома интрасетей.

Контрольные вопросы по теме

1. Чем обусловлены угрозы безопасности информации?
2. Перечислите пути реализации угроз информационной безопасности.
3. Как классифицируются угрозы безопасности информации по базовым признакам?
4. В чем заключается пассивное и активное проникновение в систему?
5. Как классифицируются каналы утечки конфиденциальной информации?
6. Как классифицируются удаленные атаки на интрасети?
7. Какие вида сетевых устройств являются объектами удаленных атак на итрасети?
8. Какие методы взлома интрасетей относятся к классическим и как они осуществляются?
9. Перечислите современные методы взлома итрасетей и объясните на чем они основаны?

Форма представления отчета:

Студент должен продемонстрировать знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимое для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Предоставить отчет в письменном виде.

Практическая работа№ 2. Информационная безопасность в условиях функционирования в России глобальных сетей.

Цель работы: Получение статистических знаний об атаках, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины.

Изучив тему, студент должен:

- уметь объяснить необходимость изучения информационной безопасности;
- знать статистику проявления компьютерных преступлений и наносимый ими ущерб;
- знать классификацию пользователей и злоумышленников в Internet;
- знать причины уязвимости Internet;
- знать основные понятия и определения, используемые при изучении информационной безопасности.

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

безопасность информации, угроза безопасности информации, несанкционированный доступ, нарушитель, злоумышленник, защита информации, целостность информации, аутентификация, верификация, идентификация.

Содержание работы:

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Компьютерные преступления»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Что такое информационная безопасность?
2. Актуальность проблемы информационной безопасности.
3. Примеры взломов сетей и Web-узлов через Internet.
4. Пользователи и злоумышленники в Internet.
5. Причины уязвимости сети Internet.
6. Понятия и определения в информационной безопасности.

Контрольные вопросы по теме

1. Что такое информационная безопасность?
2. В чем заключается утечка информации?
3. Какова цель создания системы компьютерной безопасности?
4. Назовите виды компьютерных атак.
5. Откуда следует ожидать компьютерной атаки?
6. Приведите примеры взломов сетей и Web-узлов через Internet.
7. Перечислите и охарактеризуйте основных пользователей Internet.
8. Как классифицируются злоумышленники в Internet?
9. Какие факторы уязвимости Internet?
10. Дайте определения следующим понятиям: безопасность информации, угроза безопасности информации, несанкционированный доступ, нарушитель, злоумышленник, защита информации, целостность информации, аутентификация, верификация, идентификация.

Форма представления отчета:

Студент должен изучить понятия: безопасность информации, угроза безопасности информации, несанкционированный доступ, нарушитель, злоумышленник, защита информации, целостность информации, аутентификация, верификация, идентификация. Предоставить отчет в письменном виде.

Практическая работа№ 3. Виды противников или «нарушителей». Понятие о видах вируса.

Цель работы: Получение знаний о существующих «компьютерных вирусах» и об алгоритмах их работы.

Содержание работы:

Изучив тему, студент должен:

- знать, какие программы называются «компьютерными вирусами», и чем они отличаются от других вредных программ;
- знать классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации;
- знать алгоритмы работы «компьютерных вирусов» и пути их внедрения в систему;
- уметь по индивидуальным признакам различать «компьютерные вирусы»

различных классов;

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

«компьютерные вирусы», свойства «компьютерных вирусов», вредные программы, резидентность, самошифрование, полиморфичность, overwriting-вирусы, parasitig-вирусы, companion-вирусы, link-вирусы, файловые черви, макровирусы, сетевые вирусы, «троянские кони», логические бомбы.

Порядок изучения темы

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Компьютерные вирусы»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Классификация «компьютерных вирусов».
2. Файловые вирусы.
3. Загрузочные вирусы.
4. Макровирусы.
5. Сетевые вирусы.
6. Вредные программы.

Контрольные вопросы по теме

1. Какими основными свойствами обладают «компьютерные вирусы»?
2. По каким классам разделяются «компьютерные вирусы»?
3. Как классифицируются «компьютерные вирусы»?
4. Какие «компьютерные вирусы» относятся к файловым?
5. Как разделяются файловые «компьютерные вирусы» по способу размножения?
6. Объясните алгоритм работы файлового вируса.
7. Какие «компьютерные вирусы» относятся к загрузочным?
8. Объясните алгоритм работы загрузочного вируса.
9. Какие «компьютерные вирусы» относятся к макровирусам?
10. Объясните алгоритм работы макровируса.
11. Какие «компьютерные вирусы» относятся к сетевым?
12. Какие программы являются вредными и почему?

Форма представления отчета:

Студент должен изучить понятие сервиса безопасности, вопросы архитектурной безопасности, классификацию сервисов. Предоставить отчет в письменном виде.

Практическая работа№ 4. Три вида возможных нарушений информационной системы. Защита.

Цель работы: Получение знаний о правилах защиты от «компьютерных вирусов». Знать основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы

Содержание работы:

Изучив тему, студент должен:

- знать, откуда проникают в компьютерную систему «компьютерные вирусы»;
- знать правила защиты от «компьютерных вирусов»;
- уметь выбрать антивирусную программу;
- уметь правильно использовать антивирусную программу;
- знать основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

комплексный подход к информационной безопасности, законодательный уровень, государственная тайна, коммерческая тайна, лицензия, электронная цифровая подпись, нормативные документы.

Порядок изучения темы

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Законодательный уровень информационной безопасности.
2. Обзор российского законодательства.
3. Закон «Об информации, информатизации и защите информации».
4. О текущем состоянии российского законодательства.

Контрольные вопросы по теме

1. Что такое законодательный уровень ИБ?
2. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
3. Основные понятия закона «Об информации, информатизации и защите информации».
4. Другие законы и нормативные акты.
5. Обзор зарубежного законодательства в области ИБ.
6. Текущее состояние российского законодательства.
7. Стандарты в области информационной безопасности.

Форма представления отчета:

Студент должен изучить понятие сервиса безопасности, знать основные нормативные руководящие документы. Предоставить отчет в письменном виде.

Практическая работа№ 5. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы

Цель работы: Получение знаний о правилах защиты от «компьютерных вирусов». Знать основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы

Содержание работы:

Изучив тему, студент должен:

- знать, откуда проникают в компьютерную систему «компьютерные вирусы»;
- знать правила защиты от «компьютерных вирусов»;
- уметь выбрать антивирусную программу;
- уметь правильно использовать антивирусную программу;
- знать основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

комплексный подход к информационной безопасности, законодательный уровень, государственная тайна, коммерческая тайна, лицензия, электронная цифровая подпись, нормативные документы.

Порядок изучения темы

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;

- подготовка к участию в форуме по теме «Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Законодательный уровень информационной безопасности.
2. Обзор российского законодательства.
3. Закон «Об информации, информатизации и защите информации».
4. О текущем состоянии российского законодательства.

Контрольные вопросы по теме

1. Что такое законодательный уровень ИБ?
2. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
3. Основные понятия закона «Об информации, информатизации и защите информации».
4. Другие законы и нормативные акты.
5. Обзор зарубежного законодательства в области ИБ.
6. Текущее состояние российского законодательства.
7. Стандарты в области информационной безопасности.

Форма представления отчета:

Студент должен изучить понятие сервиса безопасности, знать основные нормативные руководящие документы. Предоставить отчет в письменном виде.

Практическая работа№ 6. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства

Цель работы: Получение знаний по критериям, с помощью которых оценивается защищенность вычислительных систем. Ознакомление со стандартом США «Оранжевая книга». Изучение руководящих документов Гостехкомиссии Российской Федерации.

Содержание работы:

Изучив тему, студент должен:

- знать руководящие документы Гостехкомиссии Российской Федерации;
- знать стандарт США «Оранжевая книга»;
- уметь классифицировать автоматизированные системы согласно руководящих документов Гостехкомиссии Российской Федерации.

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

стратегия, подотчетность, гарантии, минимальная защита, индивидуальная защита, мандатная защита, верифицированная защита, идентификация, шифрование.

Порядок изучения темы

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Руководящие документы Гостехкомиссии Российской Федерации»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Критерии безопасности компьютерных систем «Оранжевая книга».
2. Руководящие документы Гостехкомиссии Российской Федерации.

Контрольные вопросы по теме

1. Дайте полное наименование стандарта США «Оранжевая книга».

2. На какие группы разделены фундаментальные требования, которым должны удовлетворять вычислительные системы, предназначенные для обработки конфиденциальной информации?

3. На какие группы делятся автоматизированные системы, приведите их краткую характеристику?

4. Перечислите руководящие документы Гостехкомиссии Российской Федерации?

5. Назовите подсистемы, на которые разделяются механизмы защиты.

При изучении темы необходимо:

- читать литературу:

1. Гостехкомиссия России. Руководящий документ. «Защита от несанкционированногодоступа к информации, термины и определения».

2. Гостехкомиссия России. Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа кинформации».

3. Гостехкомиссия России. Руководящий документ. «Средства вычислительной техники.Защита от несанкционированного доступа к информации. Показатели защищенностиот несанкционированного доступа к информации».

4. Гостехкомиссия России. Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

5. Гостехкомиссия России. Руководящий документ. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средствзащиты секретной информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники».

- посетить сайты: www.sbcinfo/index.htm.

Форма представления отчета:

Студент должен изучить руководящие документы Гостехкомиссии Российской Федерации. Предоставить отчет в письменном виде.

Практическая работа № 7. Модели безопасности и их применение.

Цель работы: Получение знаний о методах защиты информации. Получение знаний и навыков по обеспечению информационной безопасности организации при ее подключении к Internet.

Содержание работы:

Изучив тему, студент должен:

- знать и уметь применять методы защиты информации;
- знать, как организовать информационную безопасность в организации;
- уметь подключить организацию к Internet с соблюдением требований информационной безопасности;

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры.

Порядок изучения темы

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Методы защиты информации»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Ограничение доступа.
2. Контроль доступа к аппаратуре.
3. Разграничение и контроль доступа к информации.
4. Разделение привилегий на доступ.
5. Идентификация и установление подлинности объекта (субъекта).
6. Криптографическое преобразование информации.

Контрольные вопросы по теме

1. В чем заключается ограничение доступа к компьютерным системам?
2. Как классифицируются системы тревожной сигнализации?
3. В чем заключается контроль доступа к аппаратуре?
4. От каких действий защищает контроль доступа к аппаратуре?
5. В чем заключается контроль доступа к информации?
6. В чем заключается разделение привилегий на доступ?
7. В чем заключается идентификация и установление подлинности объекта (субъекта)?
8. Что может быть объектом идентификации?

Форма представления отчета:

Студент должен изучить модели безопасности и их применение. Предоставить отчет в письменном виде.

Комплект типовых тем лабораторных работ

Порядок выполнения лабораторных работ

1) изучить теоретический материал по теме лабораторной работы;

2) составить программу на одном из алгоритмических языков программирования для заданного варианта задания;

3) выполнить отладку составленной программы и показать преподавателю;

4) составить и защитить отчет по лабораторной работе.

Лабораторные работы

1. Блочное симметричное шифрование
2. Изучение ППП систем криптографической защиты информации, классическая криптография и распределение ключей
3. Асимметричное шифрование
4. Электронная цифровая подпись (ЭЦП)
5. Практическое применение криптографии с открытым ключом. Пакет PGP
6. Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI

Контрольные вопросы к лабораторным работам

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?

10. Принципы, используемые для повышения стойкости шифра?
11. Приведите схему и объясните принцип работы блочного шифра.
12. Дайте характеристику шифра DES.
13. Дайте характеристику шифра ГОСТ 28147-89.
14. Перечислите основные различия между DES и ГОСТ 28147-89.
15. Что такое – режим применения блочного шифра?
16. Чем отличается поточное и блочное шифрование.
17. Дайте характеристику шифра RC4.
18. Основные свойства криптографических хеш-функций.
19. Принципы работы хеш-функции.
20. Особенности построение хеш-функции на базе блочного шифра.
21. Опишите операцию приведения по модулю.
22. Какими свойствами обладает операция приведения по модулю?
23. Приведите определение простого числа.
24. Какие два числа называются взаимно простыми?
25. Определите понятие обратного значения по модулю.
26. Сформулируйте малую теорему Ферма.
27. Дайте определение функции Эйлера.
28. Сформулируйте теорему Эйлера.
29. Перечислите свойства простых чисел.
30. Чем отличается криптография с открытым ключом от симметричных шифров?
31. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?
32. Опишите алгоритм Шамира.
33. Опишите алгоритм Эль-Гамаля.
34. Опишите алгоритм RSA. 35. Опишите алгоритм цифровой подписи RSA.
36. Опишите алгоритм цифровой подписи Эль-Гамаля.
37. Опишите алгоритм цифровой подписи DSA (DSS).

3 ЭТАП – ВЛАДЕТЬ

Задания для промежуточного контроля

1. Каковы операционные системы использует ВУЗ? Описать их возможности с точки зрения ИБ.
2. Привести пример системы резервного копирования серверов в компании.
3. Формирование защищенной виртуальной среды.
4. Способы оценки защищенности ОС.
5. Автоматизации обновления ОС.
6. Администрирование безопасности ОС Windows.
7. Администрирование безопасности ОС Линукс
8. Средства проверки и восстановления файловой системы.
9. Системы шифрования с открытым ключом.
10. Использование средств клонирования в задачах администрирования ОС.
11. Создание акростиха.
12. Безопасность систем с бездисковыми станциями.
13. Виды учетных записей в ОС.

Вопросы к зачету

1. Информация и её характеристики. Важность и ценность информации.
2. Виды информации, подлежащие защите. Классификация информации по степени ограниченности доступа к ней Понятие тайны.
3. Информационные ресурсы как объекты собственности. Права граждан на защиту личной информации и интеллектуальной собственности.

4. Законы Российской Федерации о защите тайны и интеллектуальной собственности.

5. Критерии в выборе средств защиты. Понятие комплексной защиты.

6. Источники конфиденциальной информации в информационных системах.

7. Технические средства информационных систем и их характеристики с точки зрения информационной безопасности.

8. Действия, приводящие к незаконному овладению КИ (разглашение, утечка, НСД).

9. Способы НСД к КИ. Обобщенная модель способов НСД к источникам КИ.

10. Каналы утечки информации ТС ИС. Общая картина образования опасных сигналов.

11. Причины и условия возникновения каналов утечки информации.

12. Способы НСД к КИ через ТС ИС. Активные и пассивные способы.

13. Техника промышленного шпионажа.

14. Угрозы ИС. Виды угроз. Виды потерь и их причины.

15. Модель нарушителя в ИС.

16. Оценка безопасности ИС. Требования к безопасности ИС. Показатели защищенности СВТ. Классы защищенности.

17. Защита одиночной ПЭВМ. Каналы утечки информации, методы защиты.

18. Влияние архитектуры ЭВМ на безопасность обрабатываемой информации. Понятие "защищённая архитектура".

19. Операционные системы, ориентированные на безопасность информации.

20. Безопасность компьютерных сетей - корпоративных и глобальных (общие принципы).

21. Вредоносные программы. Принципы защиты от их воздействия.

22. Организационные меры по защите информации на ЭВМ.

23. Стандартные средства защиты (аппаратные и программные).

24. Использование криптографических методов для защиты электронной документации.

25. Противоправное использование компьютеров. Сущность компьютерных преступлений.

26. Классификация компьютерных преступлений. Законы РФ о преступлениях в сфере компьютерной информации.

Тестирование

Вопрос № 1.
Вопрос: информация - это
Неверно: актуальность защиты
Неверно: персональные данные
Неверно: данные между началом и концом сетевого пакета
Неверно: интервал времени между посылкой пакетов в сеть
Верно: сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

Вопрос № 2.
Вопрос: Для удовлетворения законных прав и интересов субъектов для обеспечения их информационной безопасности необходимо постоянно поддерживать одно из следующих свойств информации и систем ее обработки:
Неверно: объем
Верно: целостность
Неверно: контрольную сумму

Неверно: матрицу доступа при пакетной передаче
Неверно: осмысленность

Вопрос № 3.
Вопрос: Информационная безопасность – это
Неверно: преграждение потоков ненужной вредной информации в персональной ЭВМ с помощью защитных программ
Верно: состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства
Неверно: шифрование данных при передаче по всем видам каналов связи
Неверно: безопасность средств обработки, копирования, считывания информации в автоматизированных системах
Неверно: применение всех видов и уровней охраны информации в автоматизированных и неавтоматизированных системах обработки информации

Вопрос № 4.
Вопрос: Доктрина информационной безопасности Российской Федерации - это
Неверно: доступность информации только определённому кругу лиц, гарантия существования информации в исходном виде, возможность получения информации авторизованным пользователем в нужное для него время.
Неверно: организация совокупности информационных процессов в автоматизированной системе для ее защиты
Неверно: деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
Верно: совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации

Вопрос № 5.
Вопрос: конфиденциальность – это
Неверно: гарантия существования информации в исходном виде
Верно: доступность информации только определённому кругу лиц
Неверно: возможность получение информации авторизованным пользователем в нужное для него время
Неверно: возможность установления автора информации
Неверно: возможность доказать, что автором является именно заявленный человек, и не никто другой

Вопрос № 6.
Вопрос: процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации – это ###
Верно: идентификация

Вопрос № 7.
Вопрос: Защита информации (ГОСТ 350922-96) - это
Неверно: информационная безопасность
Верно: деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
Неверно: возможность установления автора информации
Неверно: защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации

Неверно: состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства

Вопрос № 8.
Вопрос: Канал утечки информации – это
Неверно: ведение противостоящей стороной технической и агентурной разведки
Верно: совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя
Неверно: несоблюдение персоналом норм, требований, правил эксплуатации АС
Неверно: оценка реальной эффективности применяемых на предприятии мер защиты информации и предложения по их совершенствованию
Неверно: деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Вопрос № 9.
Вопрос: Параметрический канал утечки информации
Неверно: представляет вспомогательные средства, выходящие за пределы контролируемой зоны
Верно: формируется путем "высокочастотного облучения" ТСОИ, при взаимодействии электромагнитного поля которого с элементами ТСОИ происходит переизлучение электромагнитного поля, промодулированного информационным сигналом
Неверно: включает описание технологии обработки данных в защищаемой подсистеме, анализ угроз и оценку риска нанесения ущерба, правила эксплуатации системы, необходимый набор инструкций должностным лицам
Неверно: определяет общую систему взглядов в организации на проблему защиты информации в АС и пути решения этой проблемы с учетом накопленного опыта и современных тенденций ее развития
Неверно: определяет комплекс конкретных организационно-технических мер по защите информации, а также незаконного вмешательства в процесс функционирования конкретной АС
Неверно: развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере

Вопрос № 10.
Вопрос: сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления ###
Верно: информация

Вопрос № 11.
Вопрос: Концепция обеспечения информационной безопасности
Неверно: определяет комплекс конкретных организационно-технических мер по защите информации, а также незаконного вмешательства в процесс функционирования конкретной АС
Неверно: такого нет
Неверно: спасает владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые
Верно: определяет общую систему взглядов в организации на проблему защиты информации в АС и пути решения этой проблемы с учетом накопленного опыта и современных тенденций ее развития

Неверно: определяет правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение
Неверно: ни одно из перечисленных

Вопрос № 12.
Вопрос: Нарушитель – это
Неверно: индукционный канал перехвата, не требующий контактного подключения к каналам связи
Неверно: совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя
Неверно: комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки обрабатываемой или хранящейся информации
Верно: лицо, предпринявшее попытку выполнения запрещенных операций по ошибке, незнанию или осознанно со злым умыслом или без такового и использующее для этого различные возможности, методы и средства
Неверно: предоставление субъекту прав на доступ к объекту
Неверно: ни одно из перечисленных

Вопрос № 13.
Вопрос: Электрический канал перехвата информации
Неверно: не требует контактного подключения к каналам связи
Верно: предполагает контактное подключение к линиям связи
Неверно: формируется путем "высокочастотного облучения" ТСОИ, при взаимодействии электромагнитного поля которого с элементами ТСОИ происходит переизлучение электромагнитного поля, промодулированного информационным сигналом
Неверно: использует среду распространения воздух
Неверно: ни одно из перечисленных

Вопрос № 14.
Вопрос: Угроза – это
Неверно: проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы
Верно: потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам
Неверно: совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя
Неверно: вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся
Неверно: предположения о категориях лиц, к которым может принадлежать нарушитель

Вопрос № 15.
Вопрос: Биометрия - это
Верно: раздел науки, занимающийся количественными биологическими экспериментами с привлечением методов математической статистики
Неверно: дактилоскопия
Неверно: распознавания лица
Неверно: верификация подписи
Неверно: цифровой код

Вопрос № 16.
Вопрос: лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) ###
Верно: нарушитель

Вопрос № 17.
Вопрос: для сохранения голосового отпечатка требуется объем:
Неверно: 8 бит
Верно: 30 кбайт
Неверно: 300 мбайт
Неверно: 1 Гбайт
Неверно: 1 Кбит

Вопрос № 18.
Вопрос: статические методы биометрической идентификации -
Неверно: основываются на поведенческой характеристике человека — особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия
Неверно: обеспечивают постоянные характеристики определения идентификатора
Неверно: неизменные вероятности статистического метода
Неверно: ни одно из перечисленных
Верно: основываются на физиологической характеристике человека, то есть уникальном свойстве, данном ему от рождения и неотъемлемом от него

Вопрос № 19.
Вопрос: Программное размагничивание -
Неверно: удаление программ с помощью магнита
Неверно: не существует
Неверно: состоит из более чем трех или более логических частей
Неверно: ни одно из перечисленных
Верно: уничтожение данных на магнитном носителе путем многократной операции записи различными псевдослучайными кодами

Вопрос № 20.
Вопрос: Служба компьютерной безопасности – это
Неверно: формирование требований к системе защиты в процессе создания АС
Верно: штатное или нештатное подразделение, создаваемое для организации квалифицированной разработки системы защиты информации и обеспечения ее функционирования
Неверно: дополнительные неудобства, связанные с большим объемом рутинной формальной деятельности
Неверно: служба охраны, использующая в работе компьютеры для наблюдения и охраны
Неверно: охрана компьютерной техники предприятия службой безопасности
Неверно: ни одно из перечисленного

Вопрос № 21.
Вопрос: Аутентификация – это
Верно: проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы
Неверно: работа за гранью системы защиты предприятия
Неверно: передача прав пользования информацией другому лицу

Неверно: передача информации по защищенному каналу связи
Неверно: передача информации по незащищенному каналу связи

Вопрос № 22.
Вопрос: стеганография – это
Неверно: использование шифрования при передаче данных
Верно: наука о скрытой передаче информации путём сохранения в тайне самого факта передачи
Неверно: раздел науки о программных средствах закрытия информации
Неверно: аппаратное средство защиты информации
Неверно: перемешивание блоков текста для невозможности прочтения
Неверно: наука об исчезнувшей информации

Вопрос № 23.
Вопрос: модуляция – это
Неверно: изменение содержания информационного контейнера на новое нечитаемое
Неверно: процесс, обратный стеганографии
Неверно: выделение полезной информации из закодированного сообщения
Верно: процесс изменения одного или нескольких параметров высокочастотного модулируемого колебания по закону информационного низкочастотного сообщения
Неверно: применение методов программного стирания информации
Неверно: пересечение информационных потоков с целью сокрытия содержимого каждого из них
Неверно: распространение данных через шифрующее устройство

Вопрос № 24.
Вопрос: Самый верхний уровень защиты –
Неверно: технический
Неверно: смешанный
Неверно: программный
Верно: законодательный
Неверно: инженерный
Неверно: управляющий
Неверно: организационный

Вопрос № 25.
Вопрос: Злоумышленник – это
Неверно: пользователь ЭВМ, не соблюдающий правила пользования
Неверно: внутренний нарушитель автоматизированной системы обработки информации
Неверно: лицо, использующее программы для секретного копирования
Верно: пользователь или программа, неправомочно пытающиеся получить доступ к отдельному компьютеру или компьютерной сети
Неверно: нелегальный пользователь ЭВМ
Неверно: бывший сотрудник, имеющий права доступа к системе

Вопрос № 26.
Вопрос: вибрационный канал утечки информации имеет средой распространения
Неверно: воздух
Верно: конструкции зданий
Неверно: электромагнитные волны
Неверно: оптический луч
Неверно: ни одно из перечисленных

Вопрос № 27.
Вопрос: косвенные каналы проникновения в систему
Неверно: требуют проникновения в помещения, где расположены компоненты системы
Неверно: ни одно из перечисленных
Неверно: требуют наличия пароля для входа в систему
Неверно: используют совместное использование ресурсов АС
Верно: не требуют проникновения в помещения, где расположены компоненты системы
Неверно: ни одно из перечисленных

Вопрос № 28.
Вопрос: Целостность информации – это
Верно: способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения
Неверно: способ ограничения доступа пользователей к компьютерной системе или ее файлам с использованием метода паролирования
Неверно: предотвращение или существенное затруднение несанкционированного доступа
Неверно: уникальный признак субъекта или объекта доступа
Неверно: состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства
Неверно: разграничение доступа между поименованными субъектами и поименованными объектами

Вопрос № 29.
Вопрос: Модель нарушителя – это
Неверно: описание процесса взлома компьютерной системы
Неверно: характеристики взаимодействия информационных процессов при взломе системы
Неверно: описание действий по защите автоматизированной системы
Верно: абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа
Неверно: единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Вопрос № 30.
Вопрос: Обработка информации -
Неверно: изучение характеристик пользователей информационной системы
Неверно: кодирование и шифрование информационных потоков
Неверно: квантование процессов вычислительной системы
Неверно: разделяют вычислительное время главного сервера
Неверно: разделение доступа и полномочий в автоматизированной системе
Верно: сбор, хранение, обработка и воспроизведение данных средствами вычислительной техники

Вопрос № 31.
Вопрос: Действия, предпринимаемые криптоаналитиком с целью раскрытия секретного ключа - это ###
Верно: атака

Вопрос № 32.
Вопрос: Криптология состоит из двух частей: 1) криптография 2) ###

Верно: криптоанализ

Вопрос № 33.
Вопрос: Подслушивание со стороны противника называется
Неверно: активным перехватом сообщений
Верно: пассивным перехватом сообщений
Неверно: подсматриванием за сообщениями
Неверно: злоумышленным перехватом сообщений
Неверно: выделением информации из сообщения

Вопрос № 34.
Вопрос: прямое/обратное криптографическое преобразование, выполняемое в ходе шифрования открытого текста и дешифрования шифротекста – это ###
Верно: криптоалгоритм

Вопрос № 35.
Вопрос: Первый алгоритм для обобщенного шифрования с открытым ключом –
Неверно: хэш функция
Верно: алгоритм рюкзака
Неверно: алгоритм Эль Гамаля
Неверно: алгоритм Де Буараза
Неверно: DES

Вопрос № 36.
Вопрос: процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации – это
Верно: идентификация
Неверно: системотехника
Неверно: дискретизация
Неверно: реализация
Неверно: оцифровка
Неверно: отпечаток пальца

Вопрос № 37.
Вопрос: шифр, который при каждом шифровании превращает один и тот же бит или байт открытого текста в различные биты или байты шифротекста –
Неверно: блочный
Верно: потоковый
Неверно: кольцевой
Неверно: аналоговый
Неверно: цифровой

Вопрос № 38.
Вопрос: криптография с секретными ключами использует
Неверно: асимметричные алгоритмы шифрования
Верно: симметричные алгоритмы шифрования
Неверно: сверхсимметричные алгоритмы шифрования
Неверно: кольцевые алгоритмы шифрования
Неверно: плоские алгоритмы шифрования

Вопрос № 39.
Вопрос: получение открытого текста по наблюдаемому шифротексту –

Неверно: криптология
Верно: криптоанализ
Неверно: криптография
Неверно: криптосистема
Неверно: несанкционированный доступ
Неверно: криптоключ

Вопрос № 40.
Вопрос: сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления ###
Верно: информация

Вопрос № 41.
Вопрос: Заключается в замене каждой буквы на следующую за ней в алфавите через некоторое заданное число букв
Неверно: шифр Эль Гамаля
Неверно: шифр DES
Неверно: шифр Де Буазара
Верно: шифр Цезаря
Неверно: шифр 3DES
Неверно: ни одно из перечисленных

Вопрос № 42.
Вопрос: Криптостойкость – это
Неверно: возможность быстрого вскрытия шифра
Неверно: возможность долгой работы без утраты доверия
Неверно: свойство криптосистемы по надежному шифрованию
Верно: свойство криптосистемы выдерживать все разновидности атак
Неверно: свойство криптосистемы выдерживать все виды интеллектуальных атак
Неверно: ни одно из перечисленных

Вопрос № 43.
Вопрос: брандмауэр –
Неверно: антивирусное программное обеспечение
Верно: барьер, защищающий от попыток злоумышленников вторгнуться в сеть
Неверно: попытка проникновения в систему через компьютерную сеть
Неверно: использует среду распространения воздух
Неверно: программа для организации виртуальной «песочницы»

Вопрос № 44.
Вопрос: Анонимайзер – это
Неверно: проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы
Верно: программа, позволяющая замаскировать свой реальный IP-адрес, используя анонимные прокси-серверы
Неверно: совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя
Неверно: вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся
Неверно: предположения о категориях лиц, к которым может принадлежать нарушитель

Вопрос № 45.
Вопрос: Многофакторная аутентификация – это
Верно: способ аутентификации с использованием нескольких способов одновременно
Неверно: дактилоскопия и биометрия
Неверно: распознавание лица и отпечатков пальцев
Неверно: верификация подписи на основе алгоритма Шамаля
Неверно: цифровой код USB брелка

Вопрос № 46.
Вопрос: В системе UNIX имеет право на выполнение всех без исключения операций: ###
Верно: суперпользователь
Верно: root

Вопрос № 47.
Вопрос: Изолированная программная среда
Неверно: защищает от утечки конфиденциальной информации
Верно: не защищает от утечки конфиденциальной информации
Неверно: обычно применяется в совокупности с избирательным доступом
Неверно: не назначается субъектам, от имени которых выполняются системные процессы
Неверно: имеет гриф секретности объекта строго ниже уровня конфиденциальности процесса

Вопрос № 48.
Вопрос: Аутентификация -
Неверно: исключает прямое взаимодействие между авторизованным клиентом и внешним хостом
Неверно: осуществляется на основе информации, содержащейся в TCP- и IP- заголовках пакетов
Неверно: является маршрутизатором или компьютером, на котором работает программное обеспечение
Неверно: ни одно из перечисленных
Верно: средство, проверяющее, что пославший сообщение или запрос объект обладает необходимыми для этого правами

Вопрос № 49.
Вопрос: брандмауэры экспертного уровня
Неверно: используют идентификационную информацию, созданную при введении пароля
Неверно: не существуют
Неверно: состоят из более чем трех или более логических частей
Неверно: копируют пакеты в обоих направлениях, не осуществляя их фильтрации
Верно: оценивают содержимое каждого пакета в соответствии с политикой безопасности

Вопрос № 50.
Вопрос: Персональные данные – это
Неверно: служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами
Верно: сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность
Неверно: информация органов государственной власти, которую они передают в коммерческие структуры
Неверно: информация, не являющаяся государственными секретами
Неверно: перечень сведений конфиденциального характера

Неверно: ни одно из перечисленного

Вопрос № 51.
Вопрос: проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы: ###
Верно: аутентификация

Вопрос № 52.
Вопрос: Конфиденциальная информация – это
Неверно: отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах
Верно: документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
Неверно: сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность
Неверно: документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу
Неверно: зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
Неверно: документированная информация любого типа

Вопрос № 53.
Вопрос: Электронная цифровая подпись – это
Неверно: документ, в котором информация представлена в электронно-цифровой форме
Неверно: документ на бумажном носителе, выданный в соответствии с правилами системы сертификации
Неверно: документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра
Верно: реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки
Неверно: подпись в виде цифрового кода владельца
Неверно: удостоверяющий сертификат
Неверно: распространение данных через шифрующее устройство

Вопрос № 54.
Вопрос: демилитаризованная зона (DMZ) – это
Неверно: вспомогательная часть сети
Неверно: способ шифрования информации
Неверно: способ хранения секретного ключа
Верно: третий сегмент, защищенный извне, но и изолированный от остальной внутренней сети
Неверно: инженерный уровень защиты
Неверно: управляющий механизм аутентификации
Неверно: организационный канал защиты

Вопрос № 55.
Вопрос: Утечка информации – это
Неверно: несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
Верно: ознакомление постороннего лица с содержанием секретной информации
Неверно: потеря, хищение, разрушение или неполучение переданных данных
Неверно: перемещение данных в канале связи

Неверно: изготовление радиожучков

Вопрос № 56.
Вопрос: Уровень секретности – это
Неверно: воинское звание обработчика информации государственной тайны
Неверно: способ шифрования информации
Неверно: ответственность за модификацию и НСД информации
Верно: административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов
Неверно: инженерный уровень защиты

Вопрос № 57.
Вопрос: В чем заключается основная причина потерь информации, связанной с ПК?
Неверно: с глобальным хищением информации
Неверно: с появлением интернета
Неверно: с подкупом сотрудников
Верно: с недостаточной образованностью в области безопасности
Неверно: с низкой надежностью ПК

Вопрос № 58.
Вопрос: Что такое несанкционированный доступ (нсд)
Неверно: Создание резервных копий в организации
Неверно: Правила и положения, выработанные в организации для обхода парольной защиты
Неверно: Вход в систему без согласования с руководителем организации
Неверно: Удаление не нужной информации
Верно: Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
Неверно: доступ в запрещенное помещение

Вопрос № 59.
Вопрос: Угроза – это
Неверно: событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов
Неверно: набор способов обхода защиты
Неверно: несанкционированный доступ к информации
Неверно: Удаление нужной информации
Верно: возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов
Неверно: доступ в закрытый сайт

Вопрос № 60.
Вопрос: Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется
Неверно: политикой информации
Неверно: защитой информации
Неверно: организацией безопасности
Неверно: системой безопасности
Верно: политикой безопасности

Неверно: антивирусом

Вопрос № 61.
Вопрос: Что такое компьютерный вирус?
Неверно: Вирус в организме компьютерного специалиста
Верно: Разновидность программ, которые способны к размножению
Неверно: Разновидность программ, которые самоуничтожаются
Неверно: Разновидность программ, которые не работают
Неверно: Разновидность программ, которые плохо работают

Вопрос № 62.
Вопрос: Как подразделяются вирусы в зависимости от деструктивных возможностей?
Неверно: Сетевые, файловые, загрузочные, комбинированные
Верно: Безвредные, неопасные, опасные, очень опасные
Неверно: Резидентные, нерезидентные
Неверно: Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы
Неверно: Одновендорные и многовендорные

Вопрос № 63.
Вопрос: Надежным средством отвода наведенных сигналов на землю служит ###
Верно: заземление
Верно: экранирование

Вопрос № 64.
Вопрос: Какой из перечисленных алгоритмов шифрования разрешено использовать в органах государственной власти РФ:
Неверно: DES
Верно: ГОСТ 28147-89
Неверно: RSA
Неверно: ГОСТ Р 34.10-2001
Неверно: РС-5 283147-98

Вопрос № 65.
Вопрос: Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она
Неверно: не может самопроизвольно отключиться или перестать обрабатывать информацию
Верно: **с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды**
Неверно: с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
Неверно: способна противостоять только информационным угрозам, как внешним так и внутренним
Неверно: способна противостоять только внешним информационным угрозам

Вопрос № 66.
Вопрос: Суть компрометации информации:
Неверно: внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

Неверно: несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
Верно: **внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений**
Неверно: передача информации другому пользователю
Неверно: перешифрование информационных блоков базы данных

Вопрос № 67.
Вопрос: Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОА)
Неверно: Отличие по загрузочным функциям защиты
Верно: **МЭ были разработаны для активной или пассивной защиты, а СОА – для активного или пассивного обнаружения**
Неверно: МЭ были разработаны для активного или пассивного обнаружения, а СОА – для активной или пассивной защиты
Неверно: МЭ работают только на сетевом уровне, а СОА – еще и на физическом
Неверно: Принципиальных отличий нет

Вопрос № 68.
Вопрос: Под угрозой удаленного администрирования в компьютерной сети понимается угроза
Неверно: внедрения агрессивного программного кода в рамках активных объектов Web-страниц
Неверно: перехвата или подмены данных на путях транспортировки
Неверно: вмешательства в личную жизнь
Неверно: поставки неприемлемого содержания
Верно: **несанкционированного управления удаленным компьютером**

Вопрос № 69.
Вопрос: Наиболее эффективное средство для защиты от сетевых атак
Неверно: использование антивирусных программ
Неверно: посещение только «надёжных» Интернет-узлов
Неверно: использование только сертифицированных программ-броузеров при доступе к сети Интернет
Неверно: использование обновлений программного обеспечения и драйверов
Верно: **использование сетевых экранов или «firewall»**

Вопрос № 70.
Вопрос: Информация, составляющая государственную тайну не может иметь гриф
Неверно: «не вскрывать»
Верно: **«для служебного пользования»**
Неверно: «секретно»
Неверно: «совершенно секретно»
Неверно: «особой важности»

Вопрос № 71.
Вопрос: Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности

Неверно: рекомендации X.800
Неверно: **Красная книга**
Неверно: Закон «Об информации, информационных технологиях и о защите информации»
Верно: **Оранжевая книга**
Неверно: Политика безопасности

Вопрос № 72.
Вопрос: Концепция системы защиты от информационного оружия не должна включать
Неверно: рекомендации ITSU
Неверно: Закон «Об информации, информационных технологиях и о защите информации»
Верно: **средства нанесения контратаки с помощью информационного оружия**
Неверно: механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
Неверно: признаки, сигнализирующие о возможном нападении
процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

Вопрос № 73.
Вопрос: Средства защиты объектов файловой системы основаны на
Неверно: объектном подходе
Неверно: **концепции информационной безопасности**
Неверно: Законе «Об информации, информатизации и защите информации»
Верно: **определении прав пользователя на операции с файлами и каталогами**
Неверно: задании атрибутов файлов и каталогов, независящих от прав пользователей

Вопрос № 74.
Вопрос: Сложность обеспечения информационной безопасности является следствием
Неверно: злого умысла разработчиков информационных систем
Верно: объективных проблем современной технологии программирования
Неверно: происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы
Неверно: большого количества информации для обработки
Неверно: **определения прав пользователя на операции с файлами и каталогами**

Вопрос № 75.
Вопрос: Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование
Неверно: активная
Неверно: **инверсная**
Неверно: технологическая
Верно: **пассивная**
Неверно: прямая

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1 ЭТАП – ЗНАТЬ

Критерии оценки устных ответов студентов

Оценка	Правильность (ошибочность) выполнения задания

«отлично»	полно и аргументировано отвечает по содержанию задания; понимает материал, обосновывает свои суждения, применяет знания на практике, иллюстрирует ответ примерами не только по предложенной литературе; излагает материал последовательно и правильно.
«хорошо»	полно и аргументировано отвечает по содержанию задания; понимает материал, обосновывает свои суждения, применяет знания на практике, иллюстрирует ответ примерами не только по предложенной литературе; излагает материал последовательно и правильно, но допускает 1-2 ошибки, которые исправляет сам.
«удовлетворительно»	знает и понимает основные положения по содержанию задания; излагает материал неполно, но допускает неточности в определении понятий или формулировке правил; не достаточно глубоко и доказательно обосновать свои суждения иллюстрирует ответ примерами только по предложенной литературе; излагает материал непоследовательно и допускает 3-4 ошибки.
«неудовлетворительно»	допускает существенные ошибки в формулировке определений и правил, искажающие их смысл; излагает материал непоследовательно, неуверенно и не по существу задания; допускает существенные ошибки, не позволяющие раскрыть смысл задания, являющиеся серьезным препятствием к успешному овладению следующим материалом.

Критерии оценивания доклада с презентацией

	Минимальный ответ	Изложенный, раскрытый ответ	Законченный, полный ответ	Образцовый, примерный ответ
Раскрытие проблемы	Проблема не раскрыта. Отсутствуют выводы	Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы	Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы	Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы
Представление	Представляемая информация логически не связана. Не использованы профессиональные термины	Представляемая информация не систематизирована и/или не последовательна. использовано 1-2 профессиональных термина	Представляемая информация систематизирована и последовательна. Использовано более 2 профессиональных терминов	Представляемая информация систематизирована, последовательна и логически связана. Использовано более 5 профессиональных терминов

Оформление	Не использованы технологии Power Point. Больше 4 ошибок в представляемой информации	Использованы технологии Power Point частично. 3-4 ошибки в представляемой информации	Использованы технологии Power Point. Не более 2 ошибок в представляемой информации	Широко использованы технологии (Power Point и др.). Отсутствуют ошибки в представляемой информации
Ответы	Нет ответов на вопросы	Только ответы на элементарные вопросы	Ответы на вопросы полные и/или частично полные	Ответы на вопросы полные с привидением примеров и/или пояснений
Оценка	неудовлетворительно	удовлетворительно	хорошо	отлично

2 ЭТАП – УМЕТЬ

Критерии оценивания результатов практической работы

К работе должен быть приложен отчёт, содержащий
1. Титульный лист.
2. Цель работы.
3. Описание этапов проектирования
4. Выводы по работе.

Оценка	Критерии
«отлично»	работа выполнена полностью; в логических рассуждениях и обосновании решения нет пробелов и ошибок; в решении нет ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).
«хорошо»	работа выполнена полностью, но обоснования шагов решения недостаточны; допущена одна ошибка или два-три недочета в решении.
«удовлетворительно»	допущены более одной ошибки или более двух-трех недочетов в решении задачи, но учащийся владеет обязательными умениями по проверяемой теме.
«неудовлетворительно»	допущены существенные ошибки, показавшие, что учащийся не владеет обязательными умениями по данной теме в полной мере

Критерии оценивания результатов лабораторной работы

Оценка	Критерии
«отлично»	работа выполнена полностью; в логических рассуждениях и обосновании решения нет пробелов и ошибок; в решении нет ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

«хорошо»	работа выполнена полностью, но обоснования шагов решения недостаточны; допущена одна ошибка или два-три недочета в решении.
«удовлетворительно»	допущены более одной ошибки или более двух-трех недочетов в решении задачи, но учащийся владеет обязательными умениями по проверяемой теме.
«неудовлетворительно»	допущены существенные ошибки, показавшие, что учащийся не владеет обязательными умениями по данной теме в полной мере

3 ЭТАП –ВЛАДЕТЬ

Критерии оценивания знаний во время промежуточного контроля и на зачете

Оценка «ЗАЧТЕНО»:
1. Хорошее знание программного материала.
2. Хорошие навыки выполнения практических заданий
3. Точность и обоснованность выводов.
4. Логичное изложение вопроса, соответствие изложения научному стилю.
5. Правильные ответы на дополнительные вопросы.

Оценка «НЕ ЗАЧТЕНО»:
1. Поверхностное усвоение программного материала.
2. Неумение четко сформулировать выводы.
3. Отсутствие навыков научного стиля изложения.
4. Неточные ответы на дополнительные вопросы.
5. Незнание значительной части программного материала.
6. Неумение выделить главное, сделать выводы и обобщения.

Критерии оценивания теста:

Полная версия тестовых вопросов содержится в электронно-информационной системе вуза. Студенты проходят тестирование в компьютерном классе. Оценка успешности прохождения теста определяется следующей сеткой: от 0% до 29% – «неудовлетворительно», от 30% до 59% – «удовлетворительно»; 60% – 79 % – «хорошо»; 80% -100% – «отлично».