МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Гусев П.Ю./

_____ 202_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность вычислительных сетей»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ С.С. Куликов

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ А.Г. Остапенко

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Формирование компетенций, позволяющих обеспечить безопасность информации, обрабатываемой в компьютерных сетях, с учетом их структурных и функциональных особенностей, а также применяемых технических средств и технологий обработки информации.

1.2. Задачи освоения дисциплины

1) Научить оценивать актуальность угроз безопасности информации, характерных для структурных и функциональных особенностей компьютерных сетей, а также применяемых технических средств и технологий обработки информации.

2) Научить проектировать архитектуру компьютерных сетей с учетом требований по обеспечению безопасности информации.

3) Научить применять технические средства и технологии обеспечения безопасности информации при сетевом взаимодействии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность вычислительных сетей» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Безопасность вычислительных сетей» направлен на формирование следующих компетенций:

ОПК-11 - Способен разрабатывать компоненты систем защиты информации автоматизированных систем;

ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем.

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-11	знать методы, способы, средства, последовательность и содержание этапов разработки систем защиты информационной автоматизированных систем
	уметь проектировать защищенные автоматизированные системы с учетом действующих нормативных и методических документов
	владеть средствами защиты информации
ОПК-12	знать принципы построения и функционирования локальных и глобальных вычислительных сетей

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Безопасность вычислительных сетей» составляет 13 з.е.

Распределение трудоемкости дисциплины по видам занятий.

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		8	9
Аудиторные занятия (всего)	180	72	108
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	108	36	72
Самостоятельная работа	252	180	72
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы, зач.ед.	468 13	252 7	216 6

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и	12	18	42	72

		протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений. Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратно-программных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.				
2	Обнаружение компьютерных атак	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.	12	18	42	72
3	Технология	Стратегии и средства межсетевого	12	18	42	72

	межсетевого экранирования	экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows 2000-XP. Служба RRAS. Программа управления службой RRAS. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого.				
4	Организация виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения. Защита на транспортном уровне. Организация VPN средствами протокола SSL в WindowsServer 2003. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения. Организация VPN прикладного уровня средствами	12	18	42	72

		протокола S/MIME и СКЗИ КриптоПроCSP. Защищенный обмен электронной почтой.				
5	Технологии защищенной обработки информации	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС WindowsServer 2003. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Созданиеединого пространства безопасности на базе ActiveDirectory	12	18	42	72
6	Управление сетевой безопасностью	Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности. Основные понятия. Концепция глобального управления безопасностью. Глобальная и локальная политики безопасности. Функционирование системы управления средствами безопасности	12	18	42	72
		Итого	**72**	**108**	**252**	**432**

5.2 Перечень лабораторных работ

1. Классификация и анализ угроз информационной безопасности.
2. Передача шифрованных данных с помощью квантовой криптографии.
3. Модель OSI. Сетевые протоколы. Стек протоколов TCP/IP.
4. Автоматизация процесса создания учетных записей пользователей в операционных системах Windows. Создание скриптов автозапуска идентификационной информации.
5. Знакомство со средой виртуализации VMWare. Создание виртуальной сетевой инфраструктуры.
6. Доменная сеть на основе WindowsServer. Создание и настройка контроллеров домена.
7. Доменная сеть на основе WindowsServer создание и настройка клиентских машин.
8. Файловая система и локальные диски.
9. Создание динамического массива для хранения данных.RAID технологии.
10. Конфигурирование инфраструктуры DHCP на основе операционной системы WindowsServer.
11. Создание пользовательских групп посредством скриптов. Настройка безопасности сети и разграничение доступа к ресурсам.
12. Создание пользовательских групп посредством графического

интерфейса. Настройка безопасности сети и разграничение доступа к ресурсам.

13. Настройка политики паролей и блокировки.
14. Установка службы DNS.
15. Защита серверного и клиентского программного обеспечения посредством групповой политики безопасности.
16. Управление программным обеспечением с помощью групповой политики.
17. Перемещаемые профили, квотирование, блокировка файлов.
18. Репликация и разделы каталога.
19. Мониторинг сетевой структуры.
20. Защита сети посредством установки и настройки межсетевого экрана.
21. Создание VPN туннеля для удаленного подключения пользователей к защищенной сети.
22. Установка сервера обновлений WSUS+MSSQL сервер.
23. Установка и конфигурирование сервера антивирусной защиты локальной сети.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован,

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-11	знать методы, способы, средства, последовательность и содержание этапов	Обучающийся знает методы, способы, средства, последовательность и	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих

	разработки систем защиты информационной автоматизированных систем	содержание этапов разработки систем защиты информационной автоматизированных систем		программах
	уметь проектировать защищенные автоматизированные системы с учетом действующих нормативных и методических документов	Обучающийся умеет проектировать защищенные автоматизированные системы с учетом действующих нормативных и методических документов	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть средствами защиты информации	Обучающийся владеет средствами защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-12	знать принципы построения и функционирования локальных и глобальных вычислительных сетей	Обучающийся знает принципы построения и функционирования локальных и глобальных вычислительных сетей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8, 9 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Зачтено**	**Не зачтено**
ОПК-11	знать методы, способы, средства, последовательность и содержание этапов разработки систем защиты информационной автоматизированных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь проектировать защищенные автоматизированные системы с учетом действующих нормативных и	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	методических документов			
	Владеть средствами защиты информации	Решение прикладных практических задач	Продемонстрирован н верный ход решения в большинстве задач	Задачи не решены
ОПК-12	знать принципы построения и функционирования локальных и глобальных вычислительных сетей	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Установка и (или) запуск только разрешенного к использованию в ИСПДн ПО или исключение возможности установки и (или) запуска запрещенного к использованию в ИСПДн ПО обеспечиваются:

А) Идентификацией и аутентификацией субъектов доступа и объектов доступа.

Б) Управлением доступа субъектов доступа к объектам доступа.

В) Антивирусной защитой.

Г) Ограничениями программной среды.

2. Обнаружение в ИСПДн компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации СЗИ, а также реагирование на обнаружение этих программ и информации обеспечиваются:

А) Антивирусной защитой.

Б) Ограничениями программной среды.

В) Обнаружением (предотвращением) вторжений.

Г) Защитой среды виртуализации.

3. Обнаружение действий в ИСПДн, направленных на НСД к информации, специальные воздействия на ИСПДн и (или) ПДн в целях добывания, уничтожения, искажения и блокирования доступа к ПДн, а также

реагирование на эти действия обеспечиваются:

А) Антивирусной защитой.

Б) Обнаружением (предотвращением) вторжений.

В) Ограничениями программной среды.

Г) Идентификацией и аутентификацией субъектов доступа и объектов доступа.

4. Предоставление определѐнному лицу или группе лиц прав на выполнение определѐнных действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий называется:

А) Авторизацией.

Б) Аутентификацией.

В) Идентификацией.

Г) Управлением доступом.

5. Для обеспечения 4 уровня защищенности ПДн при их обработке в ИСПДн минимально допустимым является применение:

А) СВТ не ниже 6 класса, СОВ и САЗ не ниже 5 класса, МЭ 5 класса.

Б) СВТ не ниже 6 класса, СОВ и САЗ не ниже 5 класса, МЭ не ниже 4 класса.

В) СВТ не ниже 5 класса, СОВ и САЗ не ниже 4 класса, МЭ не ниже 4 класса.

Г) СВТ не ниже 5 класса, СОВ и САЗ не ниже 4 класса, МЭ не ниже 3 класса.

6. Для обеспечения 1 и 2 уровней защищенности ПДн при их обработке в ИСПДн минимально допустимым является применение:

А) СВТ 6 класса, СОВ и САЗ не ниже 5 класса, МЭ не ниже 4 класса.

Б) СВТ не ниже 5 класса, СОВ и САЗ не ниже 5 класса, МЭ не ниже 4 класса.

В) СВТ не ниже 5 класса, СОВ и САЗ не ниже 4 класса, МЭ не ниже 4 класса.

Г) СВТ не ниже 5 класса, СОВ и САЗ не ниже 4 класса, МЭ не ниже 3 класса.

7. Сетевой атакой, цель которой заключается в выявлении работающих в сети служб, открытых портов, активных сетевых сервисов, используемых протоколов, является:

А) Анализ сетевого трафика.

Б) Сканирование сети.

В) Подмена доверенного объекта сети.

Г) Атака «отказ в обслуживании».

8. Сетевой атакой, цель которой заключается в создании таких условий,

при которых легитимные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднѐн, является:

А) Анализ сетевого трафика.

Б) Сканирование сети.

В) Подмена доверенного объекта сети.

Г) Атака «отказ в обслуживании».

9. Неверным является утверждение:

А) Программное (программно-математическое) воздействие – это несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Б) Основными видами вредоносных программ являются: программные закладки, программные вирусы, сетевые черви, другие вредоносные программы, предназначенные для осуществления НСД.

В) Программная закладка – это исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

Г) Сетевой червь – это тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.

10. В общем случае система защиты информации от НСД состоит из четырех подсистем:

А) Управления доступом, регистрации и учета, криптографической, обеспечения целостности.

Б) Управления доступом, регистрации и учета, резервирования и восстановления, обеспечения целостности.

В) Идентификации и аутентификации, регистрации и учета, обнаружения и предотвращения вторжений, обеспечения целостности.

Г) Идентификации и аутентификации, регистрации и учета, антивирусной защиты, обеспечения целостности.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Разработайте политику для пакетного фильтра, Разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами сетевых фильтров.

2. Разработайте политику для пакетного фильтра, Разрешающего только получение и отправку электронной почты. Реализуйте политику средствами сетевых фильтров.

3. Разработайте и реализуйте политику для пакетного фильтра,

запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров.

4. Разработайте и реализуйте политику для пакетного фильтра, Запрещающего получение извне доступа к ресурсам компьютера за исключением двух доверенных узлов. Реализуйте политику средствами сетевых фильтров.

5. Разработайте и реализуйте политику для пакетного фильтра, Запрещающего получение доступа к Web-ресурсам определенного узла.Реализуйте политику средствами сетевых фильтров.

6. Разработайте и реализуйте политику для пакетного фильтра, Разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров.

7. Разработайте и реализуйте политику для пакетного фильтра, Разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами сетевых фильтров.

8. Разработайте политику для пакетного фильтра, Разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами протокола IPSec.

9. Разработайте политику для пакетного фильтра, Разрешающего только получение и отправку электронной почты. Реализуйте политику средствами протокола IPSec.

10. Разработайте и реализуйте политику для пакетного фильтра, Разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec.

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Осуществите криптографическую защиту сетевого трафика средствами протокола IPSec в ОС Windows. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

2. Осуществите криптографическую защиту сетевого трафика средствами СКЗИ StrongNet. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

3. Организовать защищенный обмен почтовой информацией между двумя пользователями. Шифрование почтовых сообщений выполнить с помощью алгоритма ГОСТ 28147-89, реализуемого средствами СКЗИ КриптоПро CSP. Выполнить с использованием образов ОС WindowsServer 2003 и Windows 2000.

4. Разработайте файл конфигурации и настройте СОА Snort на обнаружение тестирования внутренней структуры сети ICMP-запросами.

5. Разработайте файл конфигурациии настройте СОА Snort на обнаружение ICMP-пакетов большой длины.

6. Разработайте файл конфигурации и настройте СОА Snort на обнаружение устанавливаемых из внешней сети TCP-соединений.

7. Установить службут ерминального доступа. Выполнить настройки

службы MSTS, разрешающие доступ к ресурсам терминального сервера только для учетных записей, зарегистрированных в созданной по умолчанию группе «RemoteDesktopUsers».

8. Установить службу терминального доступа. Выполнить настройки протокола RDP, запрещающие использование ресурсов рабочей станции, включая буферобмена, принтеры и накопители.

9. Выявите сетевые узлы в локальном сетевом сегменте с использованием: утилиты fping; утилиты ping ишироковещательной ICMP-посылки; утилиты icmpush (тип ICMP-пакетов13 и 17); утилиты ping и многоадресной рассылки; утилиты arping; утилиты hping3 и методов TCP- и UDP-разведки; утилиты Ethereal и метода прослушивания сети.

10. С помощью утилиты nmap проведите сканирование портов сетевого узла. Сформируйте списки открытых TCP- и UDP-портов, идентифицируйте версии ОС из запущенных сервисов. По результатам сделайте вывод о возможности обнаружения открытых портов и идентификации типа иверсии ОС, а также сетевых сервисов.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.
2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
4. Создание защищенных сегментов сетей с использованием межсетевых экранов.
5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows.
6. Защита рабочих станций с использованием персональных сетевых фильтров.
7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
8. Электронные сертификаты. Понятие инфраструктуры открытых ключей.
9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация шифрование данных в протоколах SKIP и IPSec.
10. Протоколы PPTP, SSL. Назначение, область применения, Аутентификация и шифрование данных.

7.2.5 Примерный перечень заданий для решения прикладных задач

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.
2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.

3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.

4. Создание защищенных сегментов сетей с использованием межсетевых экранов.

5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows.

6.Защита рабочих станций с использованием персональных сетевых фильтров.

7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.

8. Электронные сертификаты.

Понятие инфраструктуры открытых ключей.

9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация шифрование данных в протоколах SKIP и IPSec.

10. Протоколы PPTP, SSL. Назначение, область применения, Аутентификация и шифрование данных.

11. Преимущества технологии терминального доступа. Обеспечение безопасности.

12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.

13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.

14. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространств абезопасности на базе ActiveDirectory.

15.Аудит безопасности компьютерных систем. Цели, стандарты,подходы.

16. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем.

17. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности.

Методика проведения инструментальных проверок.

18. Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799.

19. Виды требований безопасности согласно ГОСТРИСО/МЭК 15408-1-2002.

20. Назначение систем обнаружения атак.

Классификация систем обнаружения атак.

Использование системы обнаружения атак «Snort»

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10

вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ).

Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.
2. Оценка «Удовлетворительно» ставится в случае,если студент набрал от 6 до10 баллов
3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов
4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Аудит информационной безопасности в компьютерных сетях	ОПК-11, ОПК-12	Тест, защита лабораторных работ
2	Обнаружение компьютерных атак	ОПК-11, ОПК-12	Тест, защита лабораторных работ
3	Технология межсетевого экранирования	ОПК-11, ОПК-12	Тест, защита лабораторных работ
4	Организация виртуальных частных сетей	ОПК-11, ОПК-12	Тест, защита лабораторных работ
5	Технологии защищенной обработки информации	ОПК-11, ОПК-12	Тест, защита лабораторных работ
6	Управление сетевой безопасностью	ОПК-11, ОПК-12	Тест, защита лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется

проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Деревянко, В.Н. Безопасность вычислительных сетей [Электронный ресурс] : Учеб. пособие / В. Н. Деревянко, М. Ю. Киреев. - Электрон. текстовые дан. (1 588 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2009. - 1 файл. - 30-00.

2. Деревянко В.Н. Безопасность сетей ЭВМ [Электронный ресурс] : Учеб. пособие / В. Н. Деревянко. - Электрон. текстовые, граф. дан. (7,31 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.

3. Методические указания к практическим занятиям по дисциплине "Безопасность сетей ЭВМ" для студентов специальности 090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: А. Г. Остапенко, А. И. Мордовин. - Электрон. текстовые, граф. дан. (941 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.

Дополнительная литература:

1. Олифер, В.Г. Компьютерные сети : Принципы, технологии, протоколы : Учебник для вузов / В. Г. Олифер, Н. А. Олифер ; В.Г. Олифер, Н.А. Олифер. - 2-е изд. - СПб. : Питер, 2003. - 864 с. : ил. - ISBN 5-94723-478-5 : 212.00.

2. Деревянко В.Н. Вычислительные сети : учеб. пособие. Ч.2 / В. Н. Деревянко. - Воронеж : ВГТУ, 2004. - 257 с. - 30-00.

3. Эпидемии в телекоммуникационных сетях [Текст] / Остапенко Александр Григорьевич [и др.] ; под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2 : 736-00.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Не требуется.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Компьютерных класс с количеством персональных компьютеров из расчета 1 персональный компьютер на 2 обучающихся.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Безопасность вычислительных сетей» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад;

	- подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.