Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра информационных технологий и систем безопасности

Рабочая программа дисциплины

Информационная безопасность в интернете

Основная профессиональная образовательная программа
высшего образования по направлению подготовки

09.03.03 Прикладная информатика

Направленность (профиль):

Прикладные информационные системы и технологии

Уровень:
Бакалавриат

Форма обучения
Очная

Согласовано
Руководитель ОПОП
_____ **Яготинцева Н.В.**

Утверждаю
Председатель УМС _____ **И.И. Палкин**

Рекомендована решением
Учебно-методического совета
11 06 **2019 г., протокол №** 7

Рассмотрена и утверждена на заседании кафедры
07 июня **2019 г., протокол №** 5
Зав. кафедрой _____

Авторы-разработчики:
_____ **/ Богданов П.Ю.**

Санкт-Петербург 2019

1. Цель и задачи освоения дисциплины

Цель дисциплины – изучение студентами основных угроз безопасности сети Интернет, методов обеспечения информационной безопасности, приобретение навыков применения средств защиты информации

Основные задачи дисциплины:

- изучить угрозы информационной безопасности.
- ознакомится с основными методами обеспечения информационной безопасности.
- изучить технологии обеспечения информационной безопасности в локальных и распределенных сетях.
- овладеть программным обеспечением для защиты информации.
- ознакомится с современными инструментами защиты информации в России и в мире

То есть, задачами дисциплины является изучение понятийного аппарата дисциплины, основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач.

2. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к дисциплинам по выбору Б1.В.ДВ.7. Изучение дисциплины требует входных компетенций, знаний, умений и навыков, предусмотренных следующими курсами:

- Информатика и программирование
- Операционные и телекоммуникационные системы
- Информационные системы и технологии

3. Перечень планируемых результатов обучения

Процесс изучения дисциплины направлен на формирование компетенции ПК-5 ; ПК-6

Таблица 1.

Категория общепрофессиональных компетенций	**Код и наименование общепрофессиональной компетенции**	**Код и наименование индикатора достижения общепрофессиональной компетенции**
	ПК-5. Способен разрабатывать техническое задание на основе выявленных и согласованных требований к системе и подсистеме	ИДПК-5.1. Применять стандарты оформления технических заданий ИДПК-5.2. Разрабатывать и описывать порядок работ по созданию и сдаче системы ИДПК-5.3. Представлять и защищать технического задания на систему ИДПК-5.4. Описывать объект, автоматизируемой системой, общих требований к системе
	ПК-6. Способен выявлять риски на основе проведенного анализа требований к системе	ИДПК-6.1 Проверять качество разработанных требований к системе и подсистеме ИДПК-6.2 Анализировать возможные позитивные и негативные события, последствия и обстоятельства ИДПК-6.3 Применять основы теории управления рисками

4. Структура и содержание дисциплины

4.1. Объем дисциплины

Объем дисциплины составляет 8 зачетных единиц, 288 академических часов.

Таблица 2.

Объем дисциплины по видам учебных занятий в академических часах

Объём дисциплины	**Всего часов**
	Очная форма обучения
Объем дисциплины	**288**
Контактная работа обучающихся с преподавателем (по видам аудиторных учебных занятий) – всего:	**112**
в том числе:	**-**
лекции	**56**
занятия семинарского типа:	**56**
лабораторные занятия	
Самостоятельная работа (далее – СРС) – всего:	**176**
в том числе:	**-**
курсовая работа	
контрольная работа	
Вид промежуточной аттестации	**Зачет, экзамен**

4.2. Структура дисциплины

Таблица 3.

Структура дисциплины для очной формы обучения

№	**Раздел дисциплины**	**Семестр**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемости**	**Формируемые компетенции**	**Индикаторы достижения компетенций**
			Лекции	**Практические занятия**	**СРС**			
1	**Локальные и глобальные сети**	7	6	6	22	Доклад Практическая работа	**ПК-5** **ПК-6**	ИДПК-5.4 ИДПК-6.1
2	**Теоретические основы информационной**	7	8	8	22	Доклад Практическая работа	**ПК-5** **ПК-6**	ИДПК-5.1 ИДПК-6.2

	безопасности							
3	**Угрозы информационной безопасности в сети Интернет**	7	6	6	22	Доклад Практическая работа	**ПК-5 ПК-6**	ИДПК-5.3 ИДПК-6.2
4	**Основы криптографии**	7	8	8	22	Доклад Практическая работа	**ПК-5 ПК-6**	ИДПК-5.3 ИДПК-6.3
5	**Методы и абстрактные модели защиты информации**	8	10	10	22	Доклад Практическая работа	**ПК-5 ПК-6**	ИДПК-5.2 ИДПК-6.1
6	**Защита информации в IP-сетях**	8	6	6	22	Доклад Практическая работа	**ПК-5 ПК-6**	ИДПК-5.2 ИДПК-6.2
7	**Классические и новые протоколы верхних уровней для работы с мультимедийным траффиком в сети Интернет**	8	6	6	22	Доклад Практическая работа	**ПК-5 ПК-6**	ИДПК-5.4 ИДПК-6.1
8	**Анализ и управление рисками в сфере информационной безопасности**	8	6	6	22	Доклад Практическая работа	**ПК-5 ПК-6**	ИДПК-5.1 ИДПК-6.3.
	ИТОГО	**-**	**56**	**56**	**176**	-	-	-

4.3. Содержание разделов дисциплины

Раздел 1. Локальные и глобальные сети

- Применение компьютерных сетей;
- Сетевое оборудование и программное обеспечение;
- Эталонные модели;
- Примеры сетей;
- Стандартизация сетей;

Раздел 2. Теоретические основы информационной безопасности

- Общая схема процесса обеспечения безопасности;
- Идентификация, аутентификация, управление доступом;
- Защита от несанкционированного доступа;
- Модели безопасности;
- Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408.

Раздел 3. Угрозы информационной безопасности в сети Интернет

- Классификация угроз безопасности;
- Интерпретация угрозы атаки;
- Понятие надежности безопасности, параметры и характеристики безопасности;
- Классификация угроз уязвимостей и уровней защиты (защищенности);
- Объекты защиты и объекты моделирования;

Раздел 4. Основы криптографии

- Основные понятия;
- Исторические шифры;
- Симметричные шифры;
- Управление криптографическими ключами для симметричных шифров;
- Асимметричные шифры;
- Хеш-функции;
- Инфраструктура открытых ключей. Цифровые сертификаты;

Раздел 5. Методы и абстрактные модели защиты информации

- Абстрактные модели контроля доступа к защищенным режимам обработки информации;
- Модели и методы ролевого и сессионного контроля доступа. Вопросы идентификации ролей и сессий;
- Задачи построения системы защиты информации;
- Альтернативные методы защиты информации;

Раздел 6. Защита информации в IP-сетях

- Протокол защиты электронной почты S/MIME;
- Протоколы SSL и TLS;
- Протоколы IPSec и распределение ключей;
- Межсетевые экраны;

Раздел 7. Классические и новые протоколы верхних уровней для работы с мультимедийным траффиком в сети Интернет

- Мультимедийный трафик и его классификация;
- Интерактивные потоковые аудио и видео приложения;
- Классические протоколы транспортного уровня;
- Управление потоком и перегрузками в протоколе TCP;

Раздел 8. Анализ и управление рисками в сфере информационной безопасности

- Введение в проблему;
- Управление рисками. Модель безопасности с полным перекрытием;
- Управление информационной безопасностью. Стандарты ISO/IEC 17799.27002 и 27001;
- Методики построения систем защиты информации;
- Методики и программные продукты для оценки рисков;
- Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель»

4.4. Содержание практических работ

Таблица 4.

Содержание практических занятий для очной формы обучения

№ темы дисциплины	Тематика практических занятий	Всего часов
1	Работа с сетевыми утилитами	2
1	Работа с анализатором протоколов wireshark	2

2	Управление доступом к файлам на NTFS	2
2	Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer	2
3	Использование сканеров безопасности для получения информации о хостах в сети	4
3	Встроенный межсетевой экран Windows Server	4
4	Шифры замены	4
4	Потоковые шифры	4
5	Использование цифровых сертификатов	4
5	Создание центра сертификации в Windows Server	4
6	Шифрование данных при хранении	4
6	Настройка протокола IPSec в Windows Server	4
7	Использование Microsoft Security Assessment Tool	4
7	Матричный подход к анализу рисков	4
8	Разработка политики информационной безопасности организации	4
8	Анализ рисков на основе ПО «Риск Детектор»	4

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Таблица 5.

№ раздела курса и темы самостоятельного изучения	Содержание вопросов и заданий для самостоятельного изучения
Локальные и глобальные сети	Современная защита сетей
Теоретические основы информационной безопасности	Нормативное обеспечение информационной безопасности
Угрозы информационной безопасности в сети Интернет	Угрозы интернет сегодняшнего дня
Основы криптографии	Квантовая криптография

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

6.1. Текущий контроль

Текущий контроль проводиться в форме доклада и выполнения практических работ.

Примерные темы к докладу:

1) Интеллектуальная собственность в условиях рыночной экономики
2) Теория и практика охраны авторского права законами государства

3) Обеспечение информационной безопасности на предприятии
4) Современный промышленный шпионаж
5) Средства борьбы с промышленным шпионажем
6) Системы криптографии данных
7) Программная защита при передаче данных
8) Программная защита интеллектуальной собственности
9) Электронная подпись
10) Обнаружение хакерских атак
11) Использование защит для отражения хакерских атак

Критерии оценки докладов

Доклад **зачтен**, если:

1. Качество доклада:
   1.1. – производит выдающееся впечатление, сопровождается иллюстративным материалом;
   1.2. – четко выстроен;
2. Использование демонстрационного материала:
   2.1. – автор представил демонстрационный материал и прекрасно в нем ориентировался;
   2.2. – использовался в докладе, хорошо оформлен, но есть неточности;
3. Качество ответов на вопросы:
   3.1. – отвечает на вопросы;
   3.2. – не может ответить на большинство вопросов;
4. Четкость выводов:
   4.1. – полностью характеризуют работу;
   4.2. – нечетки;

Доклад **не зачтен**, если:

1. Качество доклада:
   1.1. – рассказывается, но не объясняется суть работы;
   1.2. – зачитывается.
2. Использование демонстрационного материала:
   3.1. – представленный демонстрационный материал не использовался докладчиком или был оформлен плохо, неграмотно.
3. Качество ответов на вопросы:
   3.1. – не может четко ответить на вопросы.
4. Четкость выводов:
   4.1. – имеются, но не доказаны.

Примерное задание на практическую работу:

Практическая работа №1. «Работа с сетевыми утилитами».

Цель: Получение базовых навыков по работе с утилитами ping, traceroute, mtr и tracemap

Задание: Ознакомиться с работой сетевых утилит

Ход работы.

1. С помощью утилиты ping проверить состояние связи с узлами.

2. При помощи утилиты traceroute произвести трассировку узлов.

3. Получить маршрут прохождения пакетов до одного из заданных в варианте узлов при помощи утилиты ping.

4. Определить маршрут прохождения пакетов до узла при помощи утилиты mtr.

5. Построить графическую карту трассировки к заданным узлам при помощи утилиты tracemap.

В отчет по выполнению практической работы включить результаты хода выполнения работы, скриншоты результатов выполнения основных команд.

Практическая работа №2. «Работа с анализатором протоколов wireshark».

Цель: Получение базовых навыков по работе с анализатором протоколов wireshark.

Задание: Захватить и проанализировать пакеты

Ход работы.

1. Захватить 5-7 пакетов широковещательного трафика. Результат сохранить в текстовый файл.

2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.

Практическая работа №3. «Управление доступом к файлам на NTFS».

Цель: Приобретение практических навыков настройки разрешений на доступ к файлам в операционных системах семейства Windows.

Задание: Исследовать настройки разрешения доступа к файлам

Ход работы.

1. В своей папке на диске виртуальной машины создайте текстовый файл с произвольным содержанием. Посмотрите его разрешения на вкладке «Безопасность». Проанализируйте текущие разрешения

2. Ознакомьтесь с разрешениями. Которые можно давать на папку или файл в Windows.

3. Посмотрите разрешения на папку Program Files. Опишите в отчете, каким группам какие разрешения даются на эту папку, куда по умолчанию устанавливаются программы.

4.С помощью утилиты icals.exe или cals.exe сохраните текущий ACL выбранного вами файла в текстовый файл. Предоставьте пользователю Student разрешение на изменение данного файла.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №4. «Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer».

Цель: Приобретение практических навыков выявления уязвимостей в ПО производства компании Microsoft с помощью специализированного программного средства Baseline Security Analyzer

Задание: Проверить уровень безопасности установленной конфигурации операционной системы Windows

Ход работы.

1. Оценить уровень уязвимости компьютера

2. Описать какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей.

3. Описать наиболее серьезные уязвимости каждого типа, выявленные на компьютере В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №5. «Использование сканеров безопасности для получения информации о хостах в сети

Цель: Приобретение практических навыков определения работающих сетевых приложений с помощью сетевого сканера безопсности.

Задание: провести исследование для виртуальных машин с помощью утилиты nmap.

Ход работы.

1. Выполните сканирование при включенном межсетевом экране виртуальной машины, потом при отключенном.

2. Опишите и проанализируйте полученные результаты. Какие сетевые службы запущены на виртуальных машинах?.

3. Установите виртуальную машину роль «Web-сервер», повторно выполните сканирование.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №6. «Встроенный межсетевой экран Windows Server».

Цель: Приобретение практических навыков настройки межсетевого экрана.

Задание: настроить межсетевой экран

Ход работы.

1. Открыть окно управления межсетевым экраном. Описать действующие настройки. Создать новое правило.

2. Найти правило, разрешающее отсылку ICMP-пакетов echo request. Проверить его работу для узла из локальной или внешней сети.

3. Создать правило, запрещающее отправку ICMP-пакетов на данный узел. Проверить его работу.

4. Активировать ведение журнала. Выполнить команду ping для проверки доступности узла, для которого создавалось блокирующее правило. Проверить содержимое файла журнала.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №7. «Шифры замены».

Цель: получить практические навыки криптоанализа шифра простой замены.

Задание: дешифровать текст зашифрованный методом простой замены

Ход работы.

1. Получить у преподавателя зашифрованный текст.

2. Найти относительную частоту встречаемости символов зашифрованного текста.

3. Используя метод частотного анализа и особенности русского языка дешифровать текст.

4. В файле отчета представить зашифрованный текст, таблицу замены символов и дешифрованный текст.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №8. «Потоковые шифры».

Цель: приобрести практические навыки шифрования и дешифрования потоковых шифров.

Задание: зашифровать текст с помощью сдвиговых регистров с обратной связью

Ход работы.

1. Получить схему регистра сдвига, текст сообщения и ключ..

2. Вычислить гуммирующую последовательность.

3. Зашифровать сообщение с помощью гаммы и передать его напарнику.

4. Получить от напарника зашифрованное сообщение, ключ и схему регистра сдвига.

5 Произвести дешифрацию полученного зашифрованного сообщения

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №9 Использование цифровых сертификатов.

Цель: Ознакомление с порядком использования цифровых сертификатов X.509 в протоколах защиты данных SSL/TLS S/MIME

Задание: рассмотреть вопросы использования цифровых сертификатов

Ход работы:

1 Посмотреть параметры сертификата какого-либо защищенного сайта. Описать кем, на какой срок, для какого субъекта сертификат был выдан.

2 Рассмотреть как хранятся сертификаты. Выполнить в консоли mmc.

3. Получите сертификат X.509 и добавьте его в почтовый клиент

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №10 Создание центра сертификации в Windows Server

Цель: Приобретение практических навыков развертывания и настройки центра сертификации встроенными средствами Windows Server

Задание: Создать центр сертификации

Ход работы:

1. Добавить серверу роль Active Directory Certificate Service
2. Определить тип центра сертификации
3. Настроить роль Active Directory Certificate Services
4. Описать какие шаблоны сертификатов определены, для каких целей служит каждый тип сертификатов.
5. Запросить сертификат одного из пользователей и изучить его.
6. Выполнить экспорт сертификата.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №11. Шифрование данных при хранении.

Цель работы: Приобретение практических навыков защиты данных при хранении с помощью шифрования встроенными средствами ОС Windows.

Задание: Изучить сертификаты, проверить возможность дешифрации зашифрованных файлов.

Ход работы:

1. Запросить сертификат, зашифровать папку.
2. Зайти в систему под учетной записью администратора и расшифровать папку.
3. Отредактировать политику таким образом, чтобы убрать из системы агента восстановления. Убедиться что теперь только пользователь зашифровавший файл может его расшифровать.
4. Зашифровать файл, предоставить другому пользователю возможность расшифровать данные (пользователь не является агентом восстановления).

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №12 Настройка протокола IPSec в Windows Server.

Цель работы: В практической работе рассматривается порядок настройки защищенного с помощью протокола IPSec соединения между клиентом и сервером.

Задание: настроить протокол IPSec для шифрования данных, передаваемых между сервером и рабочей станцией.

Ход работы:

1 Создать политику IPSec.

2 Применить политику.

3 Проверить соединение между компьютерами.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №13 Использование Microsoft Security Assessment Tool

Цель работы: Приобретение практических навыков оценки рисков организации, связанных с информационной безопасностью, с использованием ПО Microsoft Security Assessment Tool (MSAT).

Задание: Ознакомиться с программой для оценки рисков, связанных с безопасностью – Microsoft Security Assessment Tool

Ход работы:

1 Подробно описать малое предприятие: сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства.

2. С помощью программы MSAT провести оценку рисков для предприятия.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №14 Матричный подход к анализу рисков информационной безопасности.

Цель работы: изучить основные понятия СМИБ

Задание: Выявить активы, уязвимости, угрозы и средства управления в соответствии с вариантом задания. Разработать соответствующие матрицы и рассчитать соответствующие им формулы.

Ход работы:

1. Определение ценностей активов.
2. Разработка матриц

3 Оформить выводы по практической работе и ответы на контрольные вопросы.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №15. Разработка Политики информационной безопасности организации.

Цель работы: изучить основные аспекты, включаемые в политику информационной безопасности.

Задание: Разработать политику информационной безопасности организации.

Ход работы:

1. Изучить политику информационной безопасности «Газпромбанк»
2. Разработать политику информационной безопасности организации в соответствии с вариантом.

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Практическая работа №16 Анализ рисков на основе ПО «РискДетектор».

Цель работы: ознакомление и работа с автоматизированной системой управления рисками Риск Детектор.

Задание: Рассчитать риски при помощи ПО «РискДетектор»

Ход работы:

1 Выполнить пробный вариант.

2 Внести данные в программный комплекс.

3 Сохранить отчет о проделанной работе

В отчет по выполнению практической работы включить результаты анализа хода выполнения работы скриншоты результатов выполнения основных команд.

Критерии оценивания:

Практическая работа принимается в формате зачтено/ не зачтено.

Зачтено, если задание выполнено полностью, в представленном отчете обоснованно получено правильное выполненное задание.

Не зачтено, если задания выполнены частично или не выполнено.

6.2. Промежуточная аттестация

Форма промежуточной аттестации по дисциплине –**зачет, экзамен.**

Форма проведения зачета: *устно по вопросам*

Перечень вопросов для подготовки к зачету:

ПК-5, ПК-6

Зачет оценивается по двухбалльной шкале: «зачтено»/ «незачтено».

1) Что такое информация.
2) Государственная тайна
3) Коммерческая тайна

4) Персональные данные
5) Понятие Автоматизированная система
6) Информационная безопасность и ее составляющие
7) защита информации
8) методы обеспечения информационной безопасности
9) классификация угроз информационной безопасности
10) структура системы защиты от угроз нарушения конфиденциальности информации
11) организационные меры обеспечения иб
12) идентификация и аутентификация
13) методы хранения паролей
14) дискреционная модель разграничения доступа
15) мандатная модель разграничения доступа
16) симметричные криптосистемы
17) ассиметричные криптосистемы
18) межсетевое экранирование
19) модель ISO/OSI
20) классы межсетевых экранов
21) системы обнаружения вторжений
22) протоколирование и аудит
23) требования к регистрационным журналам
24) принципы обеспечения целостности
25) цифровая подпись
26) хэш-функция
27) методы резервного копирования информации

Оценка «Зачёт» ставится, если:
1. полно раскрыто содержание материала билета;
2. материал изложен грамотно, в определенной логической последовательности, точно используется терминология;
3. показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации;
4. продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков;
5. ответ прозвучал самостоятельно, без наводящих вопросов;
6. допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию.
7. в изложении допущены небольшие пробелы, не исказившие содержание ответа;

Оценка «Незачёт» ставится, если:
1. не раскрыто основное содержание учебного материала;
2. обнаружено незнание или непонимание большей или наиболее важной части учебного материала;
3. допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.
4. не сформированы компетенции, умения и навыки.

Перечень вопросов для подготовки к экзамену:

ПК-5, ПК-6

1) Что такое информация.
2) Государственная тайна
3) Коммерческая тайна
4) Персональные данные
5) Понятие Автоматизированная система
6) Информационная безопасность и ее составляющие
7) защита информации
8) методы обеспечения информационной безопасности

9) классификация угроз информационной безопасности
10) структура системы защиты от угроз нарушения конфиденциальности информации
11) организационные меры обеспечения иб
12) идентификация и аутентификация
13) методы хранения паролей
14) дискреционная модель разграничения доступа
15) мандатная модель разграничения доступа
16) симметричные криптосистемы
17) ассиметричные криптосистемы
18) межсетевое экранирование
19) модель ISO/OSI
20) классы межсетевых экранов
21) системы обнаружения вторжений
22) протоколирование и аудит
23) требования к регистрационным журналам
24) принципы обеспечения целостности
25) цифровая подпись
26) хэш-функция
27) методы резервного копирования информации

Экзамен оценивается по четырехбалльной шкале: «отлично» / «хорошо» / «удовлетворительно» / «неудовлетворительно».

Оценка «**отлично**» ставится студенту, ответ которого содержит:

- глубокое знание программного материала, а также основного содержания и новаций лекционного курса но сравнению с учебной литературой;
- знание концептуально-понятийного аппарата всего курса;

а также свидетельствует о способности:

- самостоятельно критически оценивать основные положения курса;
- увязывать теорию с практикой.

Оценка «отлично» не ставится в случаях систематических пропусков студентом семинарских и лекционных занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «**хорошо**» ставится студенту, ответ которого свидетельствует о полном знании материала по программе, а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка «**удовлетворительно**» ставится студенту, ответ которого содержит:

- поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии курса;
- стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

Оценка «**неудовлетворительно**» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

7. Методические указания для обучающихся по освоению дисциплины

7.1. Методические указания к занятиям лекционного типа

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. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

7.2. Методические указания к занятиям семинарского типа

Практические занятия

При подготовке к практическим работам необходимо заранее изучить методические рекомендации по его проведению. Обратить внимание на цель занятия, на основные вопросы для подготовки к занятию, на содержание темы занятия.

Практическое занятие проходит в виде выполнения определенного задания на компьютере с использованием специального программного обеспечения. Студент должен сдавать практическую работу в виде наглядной демонстрации достигнутых результатов преподавателю.

Кроме того, на таких занятиях студенты представляют доклады, подготовленные во время самостоятельной работы. Тема доклада выбирается студентом самостоятельно, исходя из его интересов. Доклад представляется в виде презентации (PowerPoint или PDF).

7.3. Методические указания по организации самостоятельной работы

Материал, законспектированный на лекциях, необходимо регулярно прорабатывать и дополнять сведениями из других источников литературы, представленных не только в программе дисциплины, но и в периодических изданиях.

При изучении дисциплины сначала необходимо по каждой теме прочитать рекомендованную литературу и составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме для освоения последующих тем курса. Для расширения знания по дисциплине рекомендуется использовать Интернет-ресурсы; проводить поиски в различных системах и использовать материалы сайтов, рекомендованных преподавателем.

При ответе на зачете необходимо: продумать и четко изложить материал; дать определение основных понятий; дать краткое описание явлений; привести примеры. Ответ следует иллюстрировать схемами, рисунками и графиками.

8. Учебно-методическое и информационное обеспечение дисциплины обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1) Нестеров С.А. Информационная безопасность: учебник и практикум для академического бакалавриата. – М.: Издательство Юрайт, 2019.[Электронный ресурс] - Режим доступа: https://biblio-online.ru/book/informacionnaya-bezopasnost-434171
2) Запечников С.В., Казарин О.В. Криптографические методы защиты информации: учеб. Пособие для академического бакалавриата – М.: Издательство Юрайт, 2019. - 309с. Электронный ресурс. Режим доступа: https://biblio-online.ru/book/kriptograficheskie-metody-zaschity-informacii-433133

Дополнительная литература

3) Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование: учеб. Пособие для вузов – М. Издательство Юрайт, 2019. –220 с. Электронный ресурс. Режим доступа: https://biblio-online.ru/book/kriptograficheskaya-zaschita-informacii-simmetrichnoe-shifrovanie-437667
4) Лось А.Б., Нестеренко А.Ю., Рожков М. И.. Криптографические методы защиты информации для изучающих компьютерную безопасность.: учебник для

академического бакалавриата – М.: Издательство Юрайт, 2019 – 473 с. [Электронный ресурс]— Режим доступа: https://biblio-online.ru/book/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-447581

8.3. Перечень программного обеспечения

- Операционная система: Windows 7.
- Офисный пакет: Microsoft Office.
- Windows server
- Ubuntu
- Microsoft Baseline Security analyzer
- Nmap
- Active Directory Domain Services
- Active Directory Certificate Services
- Microsoft Security Assessment Tool
- РискДетектор
- Virtual Box

8.4. Перечень информационных справочных систем

- Электронная библиотека ЭБС «БИБЛИООНЛАЙН» [Электронный ресурс]. Режим доступа: https:// biblio-online.ru /

8.5. Перечень профессиональных баз данных

- Электронно-библиотечная система elibrary
- База данных Web of Science
- База данных Scopus

9. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение программы соответствует действующим санитарно-техническим и противопожарным правилам и нормам и обеспечивает проведение всех видов аудиторных занятий и самостоятельной работы студентов.

Учебная аудитории для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования.

Учебная лаборатория информационной безопасности.

Учебная аудитория для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и выходом в ЭИОС.

Помещение для хранения и профилактического обслуживания учебного оборудования.

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации.

10. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при

необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.