**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**
**ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ**
**ОТДЕЛЕНИЕ ПРИКЛАДНОЙ ИНФОРМАТИКИ**

**кафедра Системного анализа и информатики**

УТВЕРЖДЕНА

решением кафедры Системного анализа и информатики

Протокол №6 от «2» сентября 2019г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
# Б1.В.12 ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

направление подготовки
**09.03.03 Прикладная информатика**
направленность (профиль)
**«Прикладная информатика в информационной безопасности»**
квалификация
**бакалавр**
очная форма обучения

Год набора – 2020

Москва, 2020 г.

**Автор–составитель:** к.т.н.
преподаватель кафедры Системного анализа и информатики Каширская Е.Н.

Заведующий кафедрой
Системного анализа и информатики Маруев С.А.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы
2. Объем и место дисциплины в структуре ОП ВО
3. Содержание и структура дисциплины
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине
4.1. Формы и методы текущего контроля успеваемости.
4.2. Материалы текущего контроля успеваемости обучающихся
4.3. Оценочные средства для промежуточной аттестации
4.4. Методические материалы
5. Методические указания для обучающихся по освоению дисциплины
5.1. Методические указания по вопросам на понимание лекционного материала
5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов
5.3.Методические рекомендации по подготовке к экзамену по дисциплине
6. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине
6.1. Основная литература.
6.2. Дополнительная литература.
6.3. Учебно-методическое обеспечение самостоятельной работы.
6.4. Нормативные правовые документы
6.6. Иные источники.
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина «Организация безопасности корпоративных сетей» обеспечивает овладение следующими компетенциями:

| Код компетенции | Наименование компетенции | Код этапа освоения компетенции | Наименование этапа освоения компетенции |
|---|---|---|---|
| ПК-18 | способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью | ПК-18.2 | Способен определять основные требования стандартов ИБ и различать угрозы ИБ применительно к функционированию ИС |
| ПК-20 | способен осуществлять и обосновывать выбор проектных решений по видам обеспечения информационных систем | ПК-20.2 | Способен обосновывать выбор проектных решений по видам обеспечения информационных систем |
| ПК-22 | способен анализировать рынок программно-технических средств, информационных продуктов и услуг для создания и модификации информационных систем | ПК-22.1 | Способен выбирать операционные системы, системы управления базами данных, прикладное программное обеспечение, прочие услуги для функционирования ИС в соответствии с заданными требованиями |

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

| ОТФ/ТФ (при наличии профстандарта) | Код этапа освоения компетенции | Результаты обучения |
|---|---|---|
| | ПК-18.2 | на уровне знаний: знать виды угроз безопасности, методы и средства обеспечения информационной безопасности, подходы к организации ИТ - инфраструктуры; |
| | | на уровне умений: уметь организовывать защиту информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); |
| | | на уровне навыков: иметь навыки обеспечения информационной безопасности и защиты информации, организации ИТ – инфраструктуры. |
| | ПК-20.2 | на уровне знаний: знать современные проектные решения для математического, программного и лингвистического обеспечения информационных систем; |
| | | на уровне умений: уметь выбирать проектные решения |

| | | |
|---|---|---|
| | ПК-22.1 | для конкретной информационной системы под нужную предметную область; |
| | | на уровне навыков: иметь навык анализа проектных решений для широкого спектра информационных систем. |
| | | на уровне знаний: знать актуальные на момент исследования операционных систем, системы управления базами данных, прикладного программного обеспечение; |
| | | на уровне умений: уметь принимать решения по использованию в процессе разработки или модификации ИС тех или иных программных продуктов; |
| | | на уровне навыков: иметь навык выбора поставщиков необходимого программного обеспечения и услуг. |

## 2. Объем и место дисциплины в структуре ОП ВО

### Объем дисциплины

Объем дисциплины в ЗЕ и академических/астрономических часах– 4 ЗЕ (144/108 ч).
Количество академических/астрономических часов, выделенных на контактную работу по очной форме обучения – 48/36 часа (в т.ч. лекц.-16 ч., практ.-32 ч.); на самостоятельную работу обучающихся на очной форме – 96/72 часов.

### Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.12 «Организация безопасности корпоративных сетей» относится к обязательным дисциплинам вариативной части учебного плана по направлению подготовки 09.03.03 Прикладная информатика.
Дисциплина изучается на 4 курсе в 7 семестре (очная форма)
Дисциплины опирается на объём знаний области информатики, вычислительных систем, теории систем и системного анализа, баз данных, операционных систем, проектирования интерфейсов.
Форма промежуточной аттестации – зачет с оценкой

## 3. Содержание и структура дисциплины

Очная форма обучения

| № п/п | Наименование тем (разделов) | Объем дисциплины (модуля), час. | | | | | | Форма текущего контроля успеваемости*, промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|
| | | Всего | Контактная работа обучающихся с преподавателем по видам учебных занятий | | | | СР | |
| | | | Л | ЛР | ПЗ | КСР | | |
| Тема 1 | Элементы корпоративной модели информации | 18 | 2 | | 4 | | 12 | О |

| № п/п | Наименование тем (разделов) | Объем дисциплины (модуля), час. | | | | | | Форма текущего контроля успеваемости*, промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|
| | | Всего | Контактная работа обучающихся с преподавателем по видам учебных занятий | | | | СР | |
| | | | Л | ЛР | ПЗ | КСР | | |
| Тема 2 | Введение в безопасность корпоративных сетей | 18 | 2 | | 4 | | 12 | О |
| Тема 3 | Анализ уровня защищенности корпоративной информационной системы. | 29 | 3 | | 6 | | 20 | О |
| Тема 4 | Современные технологии защиты корпоративных сетей. | 29 | 3 | | 6 | | 20 | О |
| Тема 5 | Внутренние злоумышленники в корпоративных сетях. | 25 | 3 | | 6 | | 16 | О |
| Тема 6 | Защита корпоративных сетей от внутренних злоумышленников | 25 | 3 | | 6 | | 16 | О |
| Промежуточная аттестация | | | | | | | | Зачет с оценкой |
| **Всего академ./астроном.часов:** | | **144/108** | **16/12** | | **32/24** | | **96/72** | |

Примечание* – формы текущего контроля успеваемости: опрос (О), тестирование (Т).

**Содержание дисциплины**

| **№ п/п** | **Название темы** | **Основные вопросы и положения, раскрывающие содержание темы** |
|---|---|---|
| Тема 1. | Элементы корпоративной модели информации | Введение. Понятие корпорации, ресурсов, системы.<br>Языковые связи и шифрование.<br>Защищенное распределение ключей.<br>Соотношение времен жизни популяции, корпорации и индивидуумов.<br>Ценность корпоративной информации. Аспекты практической защиты. |
| Тема 2 | Введение в безопасность корпоративных сетей | Проблемы безопасности современных корпоративных сетей.<br>Комплексный подход к обеспечению информационной безопасности.<br>Основные принципы обеспечения информационной безопасности. Концепция информационной безопасности.<br>Введение.<br>Общие положения. Определение корпоративной сети.<br>Особенности корпоративных Сетей.<br>Классификационные признаки корпоративных сетей.<br>Обобщенная структура корпоративной сети, общие |

| | | |
|---|---|---|
| | | требования к администрированию сети. Структура управления эффективностью функционирования сети. Основные требования.<br>Структура управления безопасностью сети. Основные требования. |
| Тема 3 | Анализ уровня защищенности корпоративной информационной системы. | Понятие защищенности АС. Нормативная база анализа защищенности. ISO15408: Common Criteria for Information Technology Security<br>Evaluation. РД Гостехкомиссии России.<br>Методика анализа защищенности. Исходные данные по обследуемой АС. Анализ конфигурации средств защиты внешнего периметра ЛВС. Методы тестирования системы защиты. Сетевые сканеры. Механизмы работы сканеров безопасности. |
| Тема 4 | Современные технологии защиты корпоративных сетей. | Межсетевые экраны, системы обнаружения атак и виртуальные частные Сети. Классификация МЭ. Политика работы МЭ.<br>Схемы подключения МЭ. Системы обнаружения атак. Виртуальные частные сети. Концепция построения защищенных виртуальных частных сетей VPN. Функции и компоненты сети VPN.<br>Туннелирование. Классификация виртуальных частных сетей VPN. Классификация VPN по рабочему уровню ЭМВОС. Классификация VPN по архитектуре технического решения.<br>Классификация VPN по способу технической реализации. Технические и экономические преимущества внедрения технологий VPN в корпоративные сети. |
| Тема 5 | Внутренние злоумышленники в корпоративных сетях. | Модель внутреннего нарушителя. Модель типовой корпоративной сети. Методы воздействий нарушителя на корпоративную сеть. Пассивные методы воздействия. Прослушивание сетевого трафика. Активные методы воздействия. Сканеры уязвимостей. Сетевые атаки. Троянские программы. Утилиты для сокрытия факта компрометации системы (Rootkits). Вирусы и сетевые черви. Несанкционированная установка дополнительных технических<br>средств. |
| Тема 6 | Защита корпоративных сетей от внутренних злоумышленнико в | Противодействие пассивным методам воздействия. Противодействие угрозе прослушивания сетевого трафика. Методы, снижающие риск угрозы расшифрования паролей. Противодействие активным методам воздействия. Обнаружение сканирования. Противодействие эксплойтам. Противодействие троянским программам, сетевым червям и Вирусам. Обнаружение утилит для сокрытия факта компрометации системы. Противодействие несанкционированной установке модемов. Системы централизованного мониторинга безопасности. Виртуальные ловушки. Рекомендации по усилению защиты корпоративных сетей от внутренних нарушителей. |

## 4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

### 4.1. Формы и методы текущего контроля успеваемости.

4.1.1. В ходе реализации дисциплины «Организация безопасности корпоративных сетей» используются следующие методы текущего контроля успеваемости обучающихся:

| Тема (раздел) | Методы текущего контроля успеваемости |
|---|---|
| Тема 1 | Опрос |
| Тема 2 | Опрос |
| Тема 3 | Опрос |
| Тема 4 | Опрос |
| Тема 5 | Опрос |
| Тема 6 | Опрос |

4.1.2. Зачет с оценкой проводится в форме устного ответа на билеты (по 2 вопроса в билете, 1 вопрос теоретический, 2 вопрос практический).

### 4.2. Материалы текущего контроля успеваемости обучающихся

Текущий контроль успеваемости осуществляется непрерывно, на протяжении всего курса. Прежде всего, это устный опрос по ходу лекции, выполняемый для оперативной активизации внимания обучающихся и оценки их уровня восприятия. Помимо этого, контроль самостоятельной работы обучающихся осуществляется при опросе на практических занятиях. Проведение контрольных работ в соответствии с п.4.1.1

### 4.3. Оценочные средства для промежуточной аттестации

#### 4.3.1. Формируемые компетенции

| Код компетенции | Наименование компетенции | Код этапа освоения компетенции | Наименование этапа освоения компетенции |
|---|---|---|---|
| ПК-18 | способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью | ПК-18.2 | Способен определять основные требования стандартов ИБ и различать угрозы ИБ применительно к функционированию ИС |
| ПК-20 | способен осуществлять и обосновывать выбор проектных решений по видам обеспечения информационных систем | ПК-20.2 | Способен обосновывать выбор проектных решений по видам обеспечения информационных систем |
| ПК-22 | способен анализировать рынок программно-технических средств, | ПК-22.1 | Способен выбирать операционные системы, системы управления базами данных, прикладное |

| | | | |
|---|---|---|---|
| | информационных продуктов и услуг для создания и модификации информационных систем | | программное обеспечение, прочие услуги для функционирования ИС в соответствии с заданными требованиями |

4.3.2. Типовые оценочные средства

Промежуточный контроль проводится в форме устного опроса и заключительного теста по всем темам, устный ответ на вопросы по каждому изученному разделу в соответствии с п. 4.2

| Код и наименование этапа освоения компетенции | Результаты обучения | Оценочное средство |
|---|---|---|
| ПК-18.2 Способен определять основные требования стандартов ИБ и различать угрозы ИБ применительно к функционированию ИС | на уровне знаний: знать виды угроз безопасности, методы и средства обеспечения информационной безопасности, подходы к организации ИТ - инфраструктуры; | устный опрос |
| | на уровне умений: уметь организовывать защиту информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); | устный опрос |
| | на уровне навыков: иметь навыки обеспечения информационной безопасности и защиты информации, организации ИТ – инфраструктуры. | устный опрос |
| ПК-20.2 Способен обосновывать выбор проектных решений по видам обеспечения информационных систем | на уровне знаний: знать современные проектные решения для математического, программного и лингвистического обеспечения информационных систем; | устный опрос |
| | на уровне умений: уметь выбирать проектные решения для конкретной информационной системы под нужную предметную область; | устный опрос |
| | на уровне навыков: иметь навык анализа проектных решений для широкого спектра информационных систем. | устный опрос |
| ПК-22.1 Способен выбирать операционные системы, системы управления базами данных, прикладное программное обеспечение, прочие услуги для | на уровне знаний: знать актуальные на момент исследования операционных систем, системы управления базами данных, прикладного программного обеспечение; | устный опрос |
| | на уровне умений: уметь принимать решения по использованию в процессе разработки или модификации ИС тех или иных программных продуктов; | устный опрос |

| | | |
|---|---|---|
| функционирования ИС в соответствии с | на уровне навыков: иметь навык выбора поставщиков необходимого программного обеспечения и услуг. | устный опрос |

**Перечень вопросов к зачету с оценкой:**

1. Корпоративная теория информации. Понятие корпорации, ресурсов, системы, языковых связей. Понятие ценности корпоративной информации.
2. Проблемы безопасности корпоративных компьютерных систем.
3. Комплексный подход к обеспечению ИБ.
4. Принципы обеспечения ИБ.
5. Концепция обеспечения безопасности информационных ресурсов корпоративных сетей
6. Основные понятия корпоративной сети. Особенности корпоративных сетей
7. Особенности и классификационные признаки корпоративных сетей.
8. Обобщенная структура корпоративной сети.
9. Структура управления эффективностью корпоративной сети.
10. Структура управления безопасностью корпоративной сети.
11. Защищенность АС. Нормативная база анализа защищенности (Общие критерии, РД Гостехкомиссии, ISO17799).
12. Методика анализа защищенности. Исходные данные по обследуемой АС.
13. Анализ конфигурации средств защиты внешнего периметра ЛВС. Методы тестирования системы защиты. Сетевые сканеры. Механизмы работы сканеров безопасности.
14. Межсетевые экраны, классификация, политика работы, схемы подключения.
15. Системы обнаружения атак.
16. Виртуальные частные сети. Общий обзор.
17. Функции и компоненты сети VPN. Механизмы туннелирования и инкапсуляции.
18. Классификация VPN. Общий обзор
19. Классификация VPN по уровню модели OSI.
20. Классификация VPN по архитектуре технического решения. Классификация VPN по способу технического решения.
21. Технические и экономические преимущества внедрения технологий VPN в корпоративные сети.
22. Характеристика внутренних нарушителей. Классификация методов воздействия внутренних нарушителей на корпоративные сети.
23. Угрозы прослушивания сетевого трафика в корпоративных сетях на основе концентраторов и коммутаторов. Атаки ARP-spoofing, MACFlooding и MAC-Duplicating.
24. Последствия угрозы прослушивания сетевого трафика.
25. Использование внутренними злоумышленниками сканеров уязвимостей
26. Классификация сетевых атак. Сетевые атаки, основанные на использовании уязвимостей в ПО.
27. Троянские программы и утилиты для сокрытия фактов компрометации системы.
28. Вирусы и сетевые черви. Несанкционированная установка дополнительных программно-технических средств.

29. Методы противодействия угрозе прослушивания трафика. (обнаружение снифферов ARP- и Ping-методами не надо).
30. Методы, снижающие риск угрозы расшифрования паролей.
31. Обнаружение сканирования. Противодействие эксплойтам.
32. Противодействие троянским программам, сетевым червям и вирусам. Обнаружение утилит Rootkits.
33. Противодействие несанкционированной установке модемов.
34. Системы централизованного мониторинга безопасности и виртуальные ловушки.
35. Рекомендации по усилению защиты корпоративных сетей от внутренних нарушителей.

**4.4. Методические материалы**

4.4.1. Методические материалы, определяющие процедуру оценивания ответов обучающихся на вопросы на понимание лекционного материала

Критериями оценки ответа обучающихся на лекционном занятии выступают:

- правильность ответов на вопросы преподавателя по изученному материалу;
- полнота и лаконичность ответа;
- степень понимания тематики предмета;
- логика и аргументированность изложения материала;
- приведение примеров, демонстрирующих умение и владение полученными знаниями по темам предмета в раскрытии поставленных вопросов.

4.4.2. Методические материалы, определяющие процедуру оценивания при проведении опроса на практическом занятии

Оценки **"отлично"** заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание вопроса, умение свободно ориентироваться в теме, усвоивший основную, и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется обучающимся, усвоившим взаимосвязь основных понятий в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

Оценки **"хорошо"** заслуживает обучающийся, обнаруживший полное знание темы, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по пройденному материалу и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности;

Оценки **"удовлетворительно"** заслуживает обучающийся, обнаруживший знание основного материала в объеме, необходимом для дальнейшего усвоения материала и предстоящей работы по профессии, знакомый с основной литературой, рекомендованной программой.

Оценка **"неудовлетворительно"** выставляется обучающемуся, обнаружившему пробелы в знаниях основного материала темы, допустившему принципиальные ошибки в понимании и изложении учебного материала.

4.4.3.Методические материалы, определяющие процедуру оценивания промежуточной аттестации по дисциплине «Организация безопасности корпоративных сетей»

Экзамен принимается в устной форме, по билетам. Экзаменационный билет

включает два теоретических вопроса и один практический. Оценка знаний обучающегося на экзамене носит комплексный характер и определяется его:

- ответом на экзамене;
- учебными достижениями в семестровый период.

Знания, умения, навыки обучающегося на экзамене оцениваются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

**Оценивание студента на зачете с оценкой по дисциплине «Организация безопасности корпоративных сетей»**

| Оценка | Требования к знаниям |
|---|---|
| *Отлично* | Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает на экзамене, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение. Учебные достижения в семестровый период демонстрируют высокую степень овладения программным материалом. |
| *Хорошо* | Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.<br>Учебные достижения в семестровый период демонстрируют хорошую степень овладения программным материалом. |
| *Удовлетво-рительно* | Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.<br>Учебные достижения в семестровый период демонстрируют достаточную (удовлетворительную) степень овладения программным материалом. |
| *Неудовлет-ворительно* | Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.<br>Учебные достижения в семестровый период не демонстрировали достаточную степень овладения программным материалом на пороговом уровне. |

## 5. Методические указания для обучающихся по освоению дисциплины

### 5.1. Методические указания по вопросам на понимание лекционного материала

На лекциях рекомендуется слушать предлагаемый лектором материал, при этом параллельно конспектировать основные положения, поскольку это дает наибольший результат в усвоении материала. Предоставляется возможность задавать вопросы на уточнение понимания темы и принимать участие в ее обсуждении.

Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего обсуждения на семинарском занятии. В случае необходимости обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в разделе 6 программы.

### 5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов

Подготовка обучающегося к практическому занятию осуществляется на основании плана раскрытия темы практического занятия, которое разрабатывается преподавателем на основе рабочей программы и доводится до сведения обучающегося своевременно.

При подготовке к практическому занятию обучающемуся необходимо изучить внимательно основные вопросы темы семинара. Важным условием успешной подготовки к практическому занятию является четкая организация самостоятельной работы студентов по изучению учебной и дополнительной литературы. Умение анализировать и применять для ответов на вопросы и решения задач и заданий полученные знания при самостоятельной подготовке в значительной степени определяет успешность освоения материала по дисциплине и формирование у обучающихся соответствующих компетенций.

Подготовка вопросов для самостоятельного изучения включает: изучение необходимой литературы (обязательной, дополнительной литературы, специальных периодических изданий, Интернет-ресурсов), подготовку конспекта ответа, ответы на вопросы.

При подготовке к практическим занятиям важно:

– использовать достаточно широкий диапазон массива информации, провести обзор литературы и специальных изданий, составить каталог Интернет-ресурсов;

– представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;

– грамотно структурировать материал, ясно, четко и логично его излагать, приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики, диаграммы.

Вопросы для самостоятельной подготовки к занятиям практического (семинарского) типа указаны в разделе 4.2.

### 5.2.1. Учебно-методическое обеспечение самостоятельной работы.

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий или лабораторных работ, для выполнения

домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

### 5.3. Методические рекомендации по подготовке к зачету с оценкой по дисциплине

Ответ на зачете с оценкой предусматривает устный ответ на теоретические вопросы и решение практической задачи.

При подготовке к зачету с оценкой обучающийся обращается к пройденному материалу, сосредоточенному в конспектах лекций, учебниках и других источниках информации. Повторяя, обобщая, закрепляя и дополняя полученные знания, поднимает их на качественно-новый уровень — уровень системы совокупных данных, что позволяет ему понять логику всего предмета в целом. Новые знания обучающийся получает в ходе самостоятельного изучения того, что не было изложено в лекциях и на семинарских занятиях.

Зачет с оценкой как особая форма учебного процесса имеет свои особенности, специфические черты и некоторые аспекты, которые необходимо обучающемуся знать и учитывать в своей работе. Это, прежде всего:

- что и как запоминать при подготовке к зачету с оценкой;
- по каким источникам и как готовиться;
- на чем сосредоточить основное внимание;
- каким образом в максимальной степени использовать программу курса;
- что и как записать, а что выучить дословно и т. п.

На зачете с оценкой, как правило, проверяется не столько уровень запоминания обучающимся учебного материала, сколько то, насколько успешно он оперирует теми или иными научными понятиями и категориями, систематизирует факты, как умеет мыслить, аргументировано отстаивать определенную позицию, объясняет и пересказывает заученную информацию.

Программу курса необходимо максимально использовать как в ходе подготовки, так и на самом экзамене. Ведь она включает в себя разделы, темы и основные проблемы, в рамках которых и формируются вопросы для экзамена.

Оптимальным для подготовки к экзамену является вариант, когда обучающийся начинает подготовку к нему с первых занятий по данному курсу.

При подготовке к зачету с оценкой по наиболее сложным вопросам, ключевым проблемам и важнейшим понятиям необходимо сделать краткие письменные записи в виде тезисов, планов, определений. Особое внимание в ходе подготовки к экзамену следует уделять конспектам лекций, ибо они обладают рядом преимуществ по сравнению с печатной продукцией. Как правило, они более детальные, иллюстрированные, что позволяет оценивать современную ситуацию, отражать самую свежую научную и оперативную информацию, отвечать на вопросы, интересующие аудиторию, в данный момент, тогда как при написании и опубликовании печатной продукции проходит определенное время, и материал быстро устаревает.

В то же время подготовка по одним конспектам лекций недостаточна, необходимо использовать и иную учебную литературу. Не следует бояться дополнительных и уточняющих вопросов на зачете с оценкой. Они, как правило, задаются или помимо экзаменационного вопроса для выявления общей подготовленности, или в рамках билета для уточнения высказанной мысли.

## 6. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

**6.1. Основная литература.**

1. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — М. : Московский технический университет связи и информатики, 2015. — 35 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/61737.html
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. Учебное пособие**:** Форум, Инфра-М, 2010 – 594с.
3. Мэйволд Э. Безопасность сетей. М.: НОУ "Интуит", 2016 – 571с.
4. Биячуев Т.А, Безопасность корпоративных сетей. СПб: СПб ГУ ИТМО, 2004 – 163с.

**6.2. Дополнительная литература.**

1. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
2. Д. Скляров. Искусство защиты и взлома информации, БХВ-Петербург, 288 стр., 2004 г.
3. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. . –СПб.: БХВ-Петербург, 2008. – 318 с.
4. Осовецкий Л.Г., Немолочнов О.Ф., Твердый Л.В., Беляков Д.А. Основы корпоративной теории информации. СПб: СПбГУ ИТМО, 2004

.

**6.3. Нормативные правовые документы.**

1.Конституция РФ от 23 февраля 1996 года
2.Доктрина информационной безопасности РФ от 9 сентября 2000г.
3.Кодексы РФ
4.Законы РФ
5.Указы Президента РФ
6.Постановления Правительства РФ
7.Государственные стандарты в области защиты информации (ГОСТы)
8. Руководящие документы (РД)

**6.4.Интернет-ресурсы.**

Internet URL http://www.sans.org SANS Bulletin Why your switched network isn't secure
Internet URL http://www.sans.org Tom King Packet Sniffing In a Switched Environment, August 2002 SANS Institute

Internet URL http://www.securitylab.ru/33493.html arp_antidote - средство для активной борьбы с атаками типа arpoison

Internet URL http://www.securitylab.ru/34607.html IP Smart Spoofing - новый метод отравления ARP кэша, 27 ноября 2002 года

Д. Аникин Против кого работает служба безопасности? Безопасность.Достоверность.Информация. №3 2003 стр. 18-19

Internet URL http://www.securitylab.ru/29827.html Михаил Разумов «Десять мифов о паролях в Windows»

Internet URL http://www.securitylab.ru/40572.html «Сканирование. За и Против»
Internet URL http://www .infosec.ru НИП Информзащита «СЗИ Secret Net 2000. Принципы построения»

**6.5. Иные источники.**

Не предусмотрены.

## 7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

| **Название лаборатории/класса, оснащенного необходимым, в соответствии с требованиями ФГОС/ СУОС, оборудованием** | **Наименование оборудования** | **Перечень лицензионного программного обеспечения** |
|---|---|---|
| учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации | Рабочие места студентов: столы и стулья – соответственно количеству студентов. Рабочее место для инвалида и лиц с ОВЗ: парта с телескопической столешницей на электромеханическом приводе - 1 шт., кресло-коляска для инвалидов 18" - 1 шт., индукционная петля - 1 шт., компьютер с версией для слабовидящих - 1 шт., кнопка вызова сотрудников - 1 шт. Рабочее место преподавателя: стол – 1 шт., стул – 1 шт, кафедра - 1 шт. Доска меловая и маркерная. Экран, ноутбук Lenovo ideapad 100/15, проектор | Мультимедийный проектор КонсультантПлюс |
| информационно-аналитическая лаборатория - учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций | Рабочие места: столы компьютерные – в соответствии с количеством студентов, кресло Престиж Profi -B-20 Самба бордо в рубчик - 15 шт., подставка для ног Fellowes FS-48121 Standard черный - 15 шт. Рабочее место преподавателя: стол компьютерный - 1 шт., стул - 1 шт. Доска меловая или маркерная Персональные компьютеры | Мультимедийный проектор КонсультантПлюс |
| библиотека - помещение для самостоятельной работы | Рабочие места: столы и стулья. Рабочее место преподавателя: стол – 1 шт., стул - 1 шт., кафедра библиотечная - 1 шт. Телефон – 1 шт., цифровой многофункциональный копир - 1 шт., копировальный аппарат МФУ – 1 шт., принтер - 1 шт., сканер – 1 шт. Шкаф – 7 шт, стеллаж-33 шт, библиотечная стойка – 2 шт., стенд – 2 шт. Меловая или маркерная доска. Персональные компьютеры | Мультимедийный проектор<br><br>КонсультантПлюс |

**Программное обеспечение:**

В процессе лекционных и семинарских занятий используется следующее программное обеспечение:

- программы, обеспечивающие навигацию в сети Интернет: «Google chrome»;
- программы, демонстрации видео материалов: проигрыватель «Windows Media»;
- программы для демонстрации и создания презентаций: «Microsoft Power Point».

**Информационные справочные системы:**

Информационно-правовой портал «Консультант плюс» (правовая база данных). [Электронный ресурс]. – URL: http://www.consultant.ru/

Информационно-правовой портал «Гарант» (правовая база данных). [Электронный ресурс]. – URL: http://www.garant.ru/