**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Бредихин А.В./

28.08.2025 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## «Информационные операции и атаки в кибернетических системах и сетях»

**Специальность** 10.05.02 Информационная безопасность телекоммуникационных систем

**Специализация** специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

**Квалификация выпускника** специалист по защите информации

**Нормативный период обучения** 5 лет и 6 м.

**Форма обучения** очная

**Год начала подготовки** 2025

Автор программы _____ А.Е. Дешина

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ С.С. Куликов

Воронеж 2025

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

**1.1. Цели дисциплины** является приобретение студентами знаний о структуре действий, предпринимаемые для достижения информационного пре-восходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным ук-реплением и защитой собственной информации и информационных систем и инфраструктуры.

**1.2. Задачи освоения дисциплины**

- сформировать у будущего специалиста в области безопасности теле-коммуникационных систем знания, умения и навыки в области формализация описания информационных конфликтов социотехнических систем, стратегии и тактики информационных операций и атак, реализуемых в социотехнических системах. Стратегии реализации информационных операций и атак;
- предоставить возможность изучения технологии поиска и анализа следов информационных операций и атак и инцидентов, прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационные операции и атаки в кибернетических системах и сетях» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационные операции и атаки в кибернетических системах и сетях» направлен на формирование следующих компетенций:

ПК-9.1 - Способен проводить экспертизу при расследовании компьютерных преступлений и исследовании эффективности способов, средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи.

ПК-9.4 - Способен разрабатывать средства и системы защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи ЗТКС

| Компетенция | Результаты обучения, характеризующие сформированность компетенции |
|---|---|
| ПК-9.1 | **Знать**: методы проведения компьютерно-технической экспертизы; признаки компьютерных атак и инцидентов; подходы к исследованию эффективности средств и систем защиты информации.<br>**Уметь**: выполнять анализ цифровых следов, проводить экспертизу при расследовании |

| | |
|---|---|
| | инцидентов, оценивать эффективность применяемых средств защиты от несанкционированного доступа и атак.<br>**Владеть**: навыками использования инструментальных средств цифровой криминалистики и оформления экспертных заключений. |
| ПК-9.4 | **Знать**: особенности построения защищённых телекоммуникационных комплексов; принципы обнаружения признаков компьютерных атак в высокоскоростных сетях.<br>**Уметь**: разрабатывать системы и средства защиты телекоммуникационных комплексов, включая шлюзы безопасности и системы обнаружения вторжений.<br>**Владеть**: навыками создания интегрированных решений для защиты сетей электросвязи с повышенными требованиями к безопасности. |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационные операции и атаки в кибернетических системах и сетях» составляет 7 з.е.

Распределение трудоемкости дисциплины по видам занятий

**очная форма обучения**

| Виды учебной работы | Всего часов | Семестры |
|---|---|---|
| | | 10 |
| **Аудиторные занятия (всего)** | 72 | 72 |
| В том числе: | | |
| Лекции | 36 | 36 |
| Лабораторные работы (ЛР) | 36 | 36 |
| **Самостоятельная работа** | 135 | 135 |
| **Курсовой проект** | | |
| Часы на контроль | 45 | 45 |
| Виды промежуточной аттестации - экзамен | + | + |
| Общая трудоемкость:<br>академические часы<br>зач.ед. | <br>252<br>7 | <br>252<br>7 |

## 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 | Социотехнические системы как среда реализации информационных операций и атак | Анализ подходов к определению понятия “социотехническая система”. Общесистемные закономерности в информационном аспекте функционирования социотехнических систем: энтропийная компенсация, динамическое равновесие или баланс; колебательные и циклические принципы функционирования; зависимость потенциала системы от структуры и характера взаимодействия ее элементов; фоновая закономерность; организация, ограничение, опережение, неполное использование, искажение, принудительное отчуждение и обобществление информации; обратимость процессов и явлений; энергоинформационный обмен; нелинейное синергетическое опосредование; идеальность нематериальных предметов; закон двадцати и восьмидесяти процентов | 6 | 6 | 22 | 34 |
| 2 | *Опасности социотехнических систем* | Опасности в информационно-психологическом пространстве; опасности в информационно-кибернетическом пространстве; безопасность социотехнических систем | 6 | 6 | 22 | 34 |
| 3 | *Специфика реализации информационных операций и атак в социотехнических системах* | Формализация описания информационных конфликтов социотехнических систем. Стратегии и тактики информационных операций и атак, реализуемых в социотехнических системах. Стратегии реализации информационных операций и атак. Тактики реализации информационных операций и атак. Простейшие информационные операции, реализуемые в социотехнических системах. Простейшие информационно-кибернетические операции. Простейшие информационно-психологические операции Специфика применения информационного оружия: средства информационного оружия, субъекты применения информационного оружия, объекты назначения информационного оружия, предметы воздействия информационного оружия. Типология, виды и сценарии информационных операций и атак | 6 | 6 | 22 | 34 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | *Организационные аспекты в контексте информационных операций и атак* | Организационный механизм реализации информационных операций и атак. Процесс реализации информационных операций и атак: мероприятия по планированию информационных операций и атак, мероприятия по подготовке информационных операций и атак, этапы непосредственной реализации информационных операций и атак. Иллюстрации организационных аспектов на примерах реализации операций и атак террористического характера: сценарные модели для атаки Центра международной торговли в г. Нью-Йорке, сценарные модели для операции в Беслане | 6 | 6 | 22 | 34 |
| 5 | *Правовые аспекты в контексте информационных операций и атак* | Правовая основа информационной безопасности: рисковый режим развития и системная проекция информационного права, правовая проекция информационных операций и атак на вероятные объекты деструктивного воздействия в технической подсистеме, | 6 | 6 | 22 | 34 |
| | | правовой режим информации как особого объекта назначения и средств информационного оружия, правовая проекция атак киберпреступников, правовой режим психотропных веществ в информационно-психологическом пространстве. | | | | |
| 6 | *Организационно-правовые аспекты обеспечения безопасности социотехнических систем в условиях противодействия информационным операциям и атакам* | Организационный механизм противодействия: структура и стадии противодействия, управление оборонительными средствами, этапы обеспечения рискового режима безопасности. Оценка эффективности противодействия информационным операциям и атакам. Региональный аспект противодействия. Международный аспект противодействия | 6 | 6 | 25 | 37 |
| | | **Итого** | **36** | **36** | **135** | **207** |

### 5.2 Перечень лабораторных работ

1. Оценка степени поражения информационным оружием при мониторинге сетевого пространства на предмет выявления информационных операций.
2. Оценка эффективности перепрограммирования субъектов информационного воздействия при мониторинге сетевого пространства на предмет выявления информационных операций.
3. Математическая модель распространения слухов и понятие «реальное время» информационной операции.
4. Формальная постановка задачи на формирование плана информационной операции
5. Планирование информационной операции
6. Моделирование информационной операции

## 6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ)

## И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 9 семестре для очной формы обучения.

Примерная тематика курсового проекта: «Анализ сетевых структур при выявлении информационных операций».

Задачи, решаемые при выполнении курсового проекта:

- исследование статистических свойств, которые характеризуют поведение сетей;
- создание моделей сетей;
- предсказание поведения сетей при изменении структурных свойств.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

## 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».

| Компетенция | Результаты обучения, характеризующие сформированность компетенции | Критерии оценивания | Аттестован | Не аттестован |
|---|---|---|---|---|
| ПК-9.1 | Знать: методы проведения компьютерно-технической экспертизы; признаки компьютерных атак и инцидентов; подходы к исследованию эффективности средств и систем защиты информации.<br>Уметь: выполнять анализ цифровых следов, проводить экспертизу при расследовании инцидентов, оценивать эффективность применяемых средств защиты от несанкционированного доступа и атак.<br>Владеть: навыками использования инструментальных средств цифровой криминалистики и оформления экспертных заключений. | Знание методов проведения компьютерно-технической экспертизы; признаки компьютерных атак и инцидентов; подходы к исследованию эффективности средств и систем защиты информации.<br>Умение выполнять анализ цифровых следов, проводить экспертизу при расследовании инцидентов, оценивать эффективность применяемых средств защиты от несанкционированного доступа и атак.<br>Владение навыками использования инструментальных средств цифровой криминалистики и оформления экспертных заключений. | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-9.4 | Знать: особенности построения защищённых телекоммуникационных комплексов; принципы обнаружения признаков компьютерных атак в высокоскоростных сетях.<br>Уметь: разрабатывать системы и средства защиты телекоммуникационных комплексов, включая шлюзы безопасности и системы обнаружения вторжений.<br>Владеть: навыками создания интегрированных решений для защиты сетей электросвязи с повышенными требованиями к безопасности. | Знает особенности построения защищённых телекоммуникационных комплексов; принципы обнаружения признаков компьютерных атак в высокоскоростных сетях.<br>Умеет разрабатывать системы и средства защиты телекоммуникационных комплексов, включая шлюзы безопасности и системы обнаружения вторжений.<br>Владеет навыками создания интегрированных решений для защиты сетей электросвязи с повышенными требованиями к безопасности. | 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 10 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

| Компетенция | Результаты обучения, характеризующие сформированность компетенции | Критерии оценивания | Отлично | Хорошо | Удовл. | Неудовл. |
|---|---|---|---|---|---|---|
| ПК-9.1 | Знает методы проведения компьютерно-технической экспертизы; признаки компьютерных атак и инцидентов; подходы к исследованию эффективности средств и систем защиты информации | Тест | Выполнение теста на 90- 100% | Выполнение теста на 80- 90% | Выполнение теста на 70-80% | В тесте менее 70% правильных ответов |
| | Умеет выполнять анализ цифровых следов, проводить экспертизу при расследовании инцидентов, оценивать эффективность применяемых средств защиты от несанкционированного доступа и атак. | Решение стандартных практических задач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстр ирован верный ход решения в большинстве задач | Задачи не решены |
| | Владеет навыками использования инструментальных средств цифровой криминалистики и оформления экспертных заключений. | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные от- | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех | Продемонстр ирован верный ход решения в большинстве задач | Задачи не решены |
| ПК-9.4 | Знает особенности построения защищённых телекоммуникационных комплексов; принципы обнаружения признаков компьютерных атак в высокоскоростных сетях.<br><br>Умеет разрабатывать системы и средства защиты телекоммуникационных комплексов, включая шлюзы безопасности и системы обнаружения вторжений.<br><br>Владеет навыками создания интегрированных решений для защиты сетей электросвязи с повышенными требованиями к безопасности. | Тест<br><br>Решение стандартных практических задач<br><br>Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстр ирован верный ход решения в большинстве задач | Задачи не решены |

**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. Что относится к основным категориям атак?

**атаки на отказ в обслуживании**

атаки прохода

атаки трансформации

2. Что такое атака доступа?

**попытка получения злоумышленником информации, для просмотра которой у него нет разрешений**

попытка неправомочного изменения информации

атака, запрещающая легальному пользователю использование системы, информации или возможностей компьютеров

попытка дать неверную информацию о реальном событии или транзакции

3. На что направлена атака доступа?

уничтожение информации

уничтожение компьютера

**нарушение конфиденциальности информации**

4. Где возможна атака доступа?

только в сети интернет только в локальных сетях

**везде, где существует информация и средства ее передачи**

5. Что такое подсматривание?

**просмотр файлов и документов для поиска информации**

получение информации из чужого разговора захват информации в процессе ее передачи

6. Что такое атака модификации?

попытка получения злоумышленником информации, для просмотра которой у него нет разрешений

**попытка неправомочного изменения информации**

атака, запрещающая легальному пользователю использование сис- темы, информации или возможностей компьютеров

попытка дать неверную информацию о реальном событии или транзакции

7. Какие разновидности атак модификации существуют?

**замена**

**удаление**

**добавление**

перемещение копирование

8. Где возможна атака модификации?

только в сети интернет

только в локальных сетях

**везде, где существует информация и средства ее передачи**

9. Что такое атака на отказ в обслуживании?

попытка получения злоумышленником информации, для просмотра которой у него нет разрешений

попытка неправомочного изменения информации

**атака, запрещающая легальному пользователю использование системы, информации или возможностей компьютеров**

попытка дать неверную информацию о реальном событии или транзакции

10. На что направлена атака на отказ в доступе к системе?

**вывод из строя компьютерной системы блокирование каналов связи**

уничтожение информации

приложения обработки информации

**7.2.2 Примерный перечень заданий для решения стандартных задач**

1. На что направлена атака на отказ в доступе к информации? блокирование информации

блокирование каналов связи

**уничтожение информации**

приложения обработки информации

2. Что такое атака на отказ от обязательств?

попытка получения злоумышленником информации, для просмотра которой у него нет разрешений

попытка неправомочного изменения информации

атака, запрещающая легальному пользователю использование системы, информации или возможностей компьютеров

**попытка дать неверную информацию о реальном событии или транзакции**

3. Как называется выполнение действий от имени другого пользователя?

отрицание события

**маскарад**

скрытие

4. Как называется отказ от факта совершения операции?

**отрицание события**

маскарад

скрытие

5. Какие из этих видов атак относятся к атакам доступа?

подсматривание

**подслушивание**

замена

6. Какой из этих видов атак не относится к атакам модификации?

замена

**подслушивание**

**добавление**

удаление

7. Какие из этих видов атак относятся к атакам на отказ в обслуживании?

**отказ в доступе к информации**

**отказ в доступе к приложениям**

подслушивание

добавление

8. Какой из этих видов атак относится к атаке на отказ от обязательств?

**маскарад**

**DoS-атаки против Интернета**

**отрицание события**

9. Какой из этих видов атак относится к атаке на отказ от обязательств?

замена

подслушивание

удаление

**и одна из выше перечисленных**

10. От чего зависит сложность организации атаки на отказ от обязательств?

**от мер предосторожности, принятых в организации**

от стабильности работы системы

от качества канала связи

### 7.2.3 Примерный перечень заданий для решения прикладных задач

1) В каком случае проще осуществить атаку на отказ от обязательств?

**(1)** в случае бумажных документов

**(2) когда информация передается в электронном виде**

**(3)** в обоих случаях сложность одинакова

2) Какой способ проведения DoS-атаки на канал связи является самым простым с точки зрения его осуществления?

**(1)** посылка большого объема трафика через атакуемый канал

**(2) перерезание кабеля**

**(3)** организовать атаку указанными способами одинакового сложно

3) Где может храниться информация в электронном виде?

**(1) на рабочих станциях**

**(2) на серверах**

**(3)** на бумажных носителях

4) Какой аспект информационной безопасности был нарушен, если в результате атаки на сайт авторизованные пользователи не могут получить доступ к необходимым данным?

**(1)** конфиденциальность

**(2) доступность**

**(3)** целостность

5) К каким типам удаленного воздействия по характеру воздействия и цели реализации относится DOS-атака?

**(1)** пассивное воздействие; нарушение целостности информации

**(2)** активное воздействие; нарушение конфиденциальности информации

**(3)** пассивное воздействие; нарушение конфиденциальности информации

**(4) активное воздействие; нарушение доступности информации**

6) Какую атаку осуществляет злоумышленник, если он ждет от потенциального объекта атаки передачи ARP-запроса?

**(1)** безусловная атака

**(2) атака по запросу от атакуемого объекта**

**(3)** атака по наступлению ожидаемого события на атакуемом объекте

7) Злоумышленник благодаря использованию ложных ARP-пакетов в сегменте Ethernet стал «человеком в середине» между двумя легитим-ными пользователями. Какую атаку он реализовал?

**(1)** анализ сетевого трафика

**(2) ложный объект сети**

**(3)** отказ в обслуживании

8) Благодаря чему стало возможным реализация атак типа «ложный объект сети»?

**(1)** слишком большое количество узлов в сети Интернет привело к нехватке места в таблицах маршрутизации

**(2)** на клиентских машинах сети не установлено антивирусное программное обеспечение

**(3) уязвимости, присущие протоколам различных уровней стека TCP/IP**

**(4)** ограниченные возможности системных ресурсов конечных узлов сети

9) Как называется атака, направленная на исчерпание критичных системных ресурсов, что приводит к прекращению или нарушению функционирования системы и невозможности доступа к серверу удаленных пользователей?

**(1)** анализ сетевого трафика

**(2)** ложный объект сети

**(3)** подмена доверенного объекта сети

**(4) отказ в обслуживании**

10) Как называется атака, при которой атакующий передает сообщения от имени легального объекта сети?

**(1)** анализ сетевого трафика

**(2) подмена доверенного объекта сети**

**(3)** отказ в обслуживании

**7.2.4 Примерный перечень вопросов для подготовки к зачету**

Не предусмотрено учебным планом

**7.2.5 Примерный перечень заданий для решения прикладных задач**

Анализ подходов к определению понятия “социотехническая система”.

Общесистемные закономерности в информационном аспекте функ-ционирования социотехнических систем: энтропийная компенсация, дина-мическое равновесие или баланс;
колебательные и циклические принципы функционирования; зависи-мость потенциала системы от структуры и характера взаимодействия ее эле-ментов; фоновая закономерность; организация, ограничение, опережение, неполное использование, искажение, принудительное отчуждение и обобще-ствление информации; обратимость процессов и явлений; энергоинформа-ционный обмен; нелинейное синергетическое опосредование; идеальность нематери-альных предметов; закон двадцати и восьмидесяти процентов
Опасности в информационно-психологическом пространстве; опасно-сти в информационно-кибернетическом пространстве; безопасность со-цио-технических систем
Формализация описания информационных конфликтов социотехниче-ских систем. Стратегии и тактики информационных операций и атак, реа-лизуемых в социотехнических системах. Стратегии реализации информаци-онных опе-раций и атак.
Тактики реализации информационных операций и атак. Простейшие инфор-мационные операции, реализуемые в социотехнических системах. Простейшие информационно-кибернетические операции. Простейшие ин-формационно-психологические операции
Специфика применения информационного оружия: средства ин-фор-мационного оружия, субъекты применения информационного оружия, объ-екты назначения информационного оружия, предметы воздействия ин-фор-мационного оружия. Типология, виды и сценарии информационных опе-раций и атак
Организационный механизм реализации информационных операций и атак. Процесс реализации информационных операций и атак: мероприятия по пла-нированию информационных операций и атак, мероприятия по подготовке информационных операций и атак, этапы непосредственной реализации ин-формационных операций и атак. Иллюстрации организационных аспектов на примерах реализации операций и атак террористического характера: сце-нарные модели для атаки Центра международной торговли в г. Нью-Йорке, сценарные модели для операции в Беслане
Правовая основа информационной безопасности: рисковый режим развития и системная проекция информационного права, правовая проекция информа-ционных операций и атак на вероятные объекты деструктивного воздействия в технической подсистеме, правовой режим информации как особого объекта назначения и средств информационного оружия, правовая проекция атак ки-берпреступников, правовой режим психотропных веществ в информацион-

**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 до 10 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 | Социотехнические системы как среда реализации информационных операций и атак | ПК-9.1 | Тест, защита лабораторных работ, требования к курсовому проекту |
| 2 | Опасности социотехнических систем | ПК-9.1 | Тест, защита лабораторных работ, требования к курсовому проекту |
| 3 | Специфика реализации информационных операций и атак в социотехнических системах | ПК-9.1 | Тест, защита лабораторных работ, требования к курсовому проекту |
| 4 | Организационные аспекты в контексте информационных операций и атак | ПК-9.1 | Тест, защита лабораторных работ, требования к курсовому проекту |
| 5 | Правовые аспекты в контексте информационных операций и атак | ПК-9.1 | Тест, защита лабораторных работ, требования к курсовому проекту |
| 6 | Организационно-правовые аспекты обеспечения безопасности социотехнических систем в условиях противодействия информационным операциям и атакам | ПК-9.1 | Тест, защита лабораторных работ, требования к курсовому проекту |

**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 ме-

тодики 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.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

## 8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

### 8.1 Перечень учебной литературы, необходимой для освоения дисциплины

*Основная литература*

1. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101992.html

2. Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600

3. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: методические указания / Д. В. Фомин. — Благовещенск: АмГУ, 2017. — 240 с. — Текст: электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494.

*Дополнительная литература*

1. Международная информационная безопасность: Теория и практика : сборник : в 3 томах / под общей редакцией А. В. Крутских. — Москва : Аспект Пресс, 2019 — Том 2 : Сборник документов (на русском языке) — 2019. — 784 с. — ISBN 978–5–7567–1032–8. — Текст : электронный // Лань : электрон-но-библиотечная система. — URL: https://e.lanbook.com/book/144114

2. Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. —

ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578

**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:**

Научная библиотека ВГТУ https://cchgeu.ru/university/library/

Электронный каталог научной библиотеки ВГТУ https://cchgeu.ru/university/library/elektronnyy-katalog/

Зональная научная библиотека ВГТУ https://lib.vsu.ru/

Профессиональные базы данных и информационные справочные системы

https://cchgeu.ru/university/library/prof-bd/index.php

Стандарты по информации, библиографии, библиотечному и издательскому делу (СИБИД)

https://cchgeu.ru/university/library/sibid/

ЭБС IPRBooks https://www.iprbookshop.ru/

ЭБС Лань https://e.lanbook.com/

ЭБС Университетская библиотека https://biblioclub.ru/

Методические и иные документы кафедры СИБ

https://cchgeu.ru/education/cafedras/kafsib/?docs

https://cchgeu.ru/education/programms/bksiss-3pp/?docs2021#md

https://cchgeu.ru/education/programms/ubtss-3pp/?docs2021#md

https://cchgeu.ru/education/programms/abis-3pp/?docs2021#mdhttp://e.lanbook.com/ (ЭБС Лань)
http://znanium.com/ (ЭБС Знаниум)
http://IPRbookshop.ru/ (ЭБС IPRbooks (Айбукс))

## 9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

В состав материально-технического обеспечения, необходимого для успешного прохождения практики на базе кафедры систем информационной безопасности входит следующее оборудование:

1. Система виброакустической и акустической защиты помещений «Соната АВ» в комплекте – 47190 – 1 шт
2. Системный телефон 2519-30 – 1 шт
3. Устройство защиты объектов информации «Соната-Р2»
4. Устройство защиты телефонных линий «МП-1Ц - 4212»
5. Устройство комбинированной защиты объектов «Соната РК-1» -19812

6. Частотомер Ч3-34А – 5 шт
7. Частотомер электронный счётный Ч3-33
8. Радиостанция 63 З21с-1 –
9. Измеритель модуляции СКЗ-43 – 2 шт.
10. Вольтметр В7-37 – 2 шт.
11. Вольтметр В7-26 – 5 шт.
12. Вольтметр В3-38Б – 4 шт.
13. Генератор Г3-112 – 4 шт.
14. Генератор Г4-102 – 6 шт.
15. Генератор Г3-112 – 4 шт.
16. Генератор Г3-116 – 2 шт.
17. Радиостанция ИП 1.100.074 «Лен-В» 1з21С-4 - 10 шт.
18. Индикатор поля камуфлированный «Редут» - 1 шт.
19. Осцилограф GOS-620FG – 2 шт.
20. Осцилограф С1-55 – 2 шт.
21. Паяльная станция LUKEY-852D+ - 2 шт.
22. Радиоприёмник З-399А - 3
23. Радиостанция 63 Р21с-1
24. Индикатор поля – 1 шт
25. Имитатор ИМФ-2

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

По дисциплине «Информационные операции и атаки в кибернетических системах и сетях» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

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.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

| 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:<br>- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;<br>- выполнение домашних заданий и расчетов;<br>- работа над темами для самостоятельного изучения;<br>- участие в работе студенческих научных конференций, олимпиад;<br>- 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 с оценкой, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала. |

## ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

| № п/п | Перечень вносимых изменений | Дата внесения изменений | Подпись заведующего кафедрой, ответственной за реализацию ОПОП |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |