Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

УТВЕРЖДАЮ
директор УрТИСИ СибГУТИ
_____ Минина Е.А.
«27» декабря 2024 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ
2.1.3.3(Ф) Кибербезопасность

Группа научных специальностей **2.2 Электроника, фотоника, приборостроение и связь**

Научная специальность **2.2.15 Сети, системы и устройства телекоммуникации**

Форма обучения: **очная**

Год набора: 2025

Разработчик (-и):
доцент _____ / В.А. Зацепин /
подпись

Оценочные средства обсуждены и утверждены на заседании информационных систем и технологий (ИСТ)
Протокол от 26.11.2024 г. № 4
Заведующий кафедрой _____ / В.А. Зацепин /
подпись

Екатеринбург, 2024

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

УТВЕРЖДАЮ
директор УрТИСИ СибГУТИ
_____Минина Е.А.
«27» декабря 2024 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ
2.1.3.3(Ф) Кибербезопасность

Группа научных специальностей **2.2 Электроника, фотоника, приборостроение и связь**

Научная специальность **2.2.15 Сети, системы и устройства телекоммуникации**

Форма обучения: **очная**

Год набора: 2025

Разработчик (-и):
доцент _____ / В.А. Зацепин /
подпись

Оценочные средства обсуждены и утверждены на заседании информационных систем и технологий (ИСТ)
Протокол от 26.11.2024 г. № 4
Заведующий кафедрой _____ / В.А. Зацепин /
подпись

Екатеринбург, 2024

1.Перечень результатов обучения (компетенций)

В результате освоения дисциплины (модуля) обучающийся должен обладать компетенциями, представленными в таблице:

Индекс	Наименование компетенции	Этап	Предшествующие этапы (с указанием дисциплин)
ОПК-3	Способен применять методы исследования и представлять полученные результаты научно-исследовательской деятельности в соответствии с научной специальностью на высоком уровне	2	Этап 1 - «Искусственный интеллект и машинное взаимодействие»

Форма(ы) промежуточной аттестации по дисциплине (модулю): зачет 6 семестр.

2.Показатели, критерии и шкалы оценивания компетенций

2.1.Показателем оценивания компетенций на этапе их формирования при изучении дисциплины (модуля) является уровень их освоения.

Шкала оценивания	Результат обучения	Критерий оценивания
ОПК- 3 Способен применять методы исследования и представлять полученные результаты научно-исследовательской деятельности в соответствии с научной специальностью на высоком уровне		
Низкий (пороговый) уровень	**Знает:** - основные угрозы информационной безопасности; - основы криптографии и сетевой безопасности;	- при ответе на вопросы допускает значительные ошибки, не в полной мере связывает рассматриваемые принципы работы с теоретическими и практическими вопросами информатики как науки о семантической информации и их связь с семиотикой.
	Умеет: - реализовывать поиск и устранение уязвимостей; - настраивать программные и аппаратные средства фильтрации трафика;	умение формулировать выводы по полученным результатам, сравнение предварительно рассчитанных характеристик с характеристиками, полученными в ходе практической работы по теории информации для решения задач криптографии и стеганографии, но при ответе на вопросы допускает значительные ошибки

	Владеет: - навыками настройки межсетевых экранов и операционных систем; - навыками аудита и управления корпоративной безопасностью внешних и внутренних угроз.	допускает значительные ошибки при исследовании
Средний уровень	**Знает:** - основные угрозы информационной безопасности; - основы криптографии и сетевой безопасности;	-при ответе на вопросы допускает незначительные ошибки, не в полной мере связывает рассматриваемые принципы работы с теоретическими и практическими вопросами информатики как науки о семантической информации и их связь с семиотикой.
	Умеет: - реализовывать поиск и устранение уязвимостей; - настраивать программные и аппаратные средства фильтрации трафика;	умение формулировать выводы по полученным результатам, сравнение предварительно рассчитанных характеристик с характеристиками, полученными в ходе практической работы по теории информации для решения задач криптографии и стеганографии, но при ответе на вопросы допускает незначительные ошибки
	Владеет: - навыками настройки межсетевых экранов и операционных систем; - навыками аудита и управления корпоративной безопасностью внешних и внутренних угроз.	допускает незначительные ошибки при исследовании
Высокий уровень	**Знает:** - основные угрозы информационной безопасности; - основы криптографии и сетевой безопасности;	в полной мере связывает рассматриваемые принципы работы с теоретическими и практическими вопросами информатики как науки о семантической информации и их связь с семиотикой.

	Умеет: - реализовывать поиск и устранение уязвимостей; - настраивать программные и аппаратные средства фильтрации трафика;	умение формулировать выводы по полученным результатам, сравнение предварительно рассчитанных характеристик с характеристиками, полученными в ходе практической работы по теории информации для решения задач криптографии и стеганографии.
	Владеет: - навыками настройки межсетевых экранов и операционных систем; - навыками аудита и управления корпоративной безопасностью внешних и внутренних угроз.	не допускает ошибки в научно-исследовательской деятельности

2.2 Таблица соответствия уровня формирования компетенций результатам промежуточной аттестации

Форма контроля	Шкала оценивания	Индекс компетенции	Уровень освоения (низкий (пороговый), средний, высокий)
Зачет	Зачтено	ОПК-3	низкий
			средний
			высокий

3 Методические материалы, определяющие процедуры оценивания

Процесс оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций представлен в таблице

Тип занятия	Тема (раздел)	Оценочные средства
ОПК- 3 Способностью к разработке новых методов исследования и их применению в самостоятельной профессиональной научно-исследовательской деятельности в области профессиональной деятельности		
Лекция	Введение в кибербезопасность	зачет
Лекция	Угрозы информационной безопасности	зачет
Лекция	Криптография и защита данных	зачет
Лекция	Сетевая безопасность	зачет
Лекция	Защита операционных систем	зачет
Лекция	Защита приложений и веб-безопасность	зачет
Лекция	Управление и аудит безопасности	зачет
Лекция	Социальная инженерия и анализ уязвимостей	зачет
Лекция	Законодательные аспекты кибербезопасности	зачет
Практическая работа	Настройка безопасности сетевых устройств	зачет
Практическая работа	Настройка фильтрации трафика в ОС Windows и Linux	зачет
Практическая работа	Разработка политики безопасности предприятия	зачет
Самостоятельная работа	Разработка политики безопасности предприятия	Выполнение практического индивидуального задания, зачет

4.Типовые контрольные задания:

4.1 Типовое задание дискуссий и докладов по дисциплине:

1. Презентация на тему «Сетевая безопасность».

По вопросам:

- Основы сетей и протоколов
- Фильтрация трафика и межсетевые экраны
- Защита от DDoS-атак

2. Презентация на тему «Защита приложений и веб-безопасность».

По вопросам:

- Уязвимости веб-приложений
- SQL-инъекции и XSS-атаки
- Безопасное программирование

Типовые темы докладов и лекций представлены в электронно-информационной образовательной среде и доступны по URL: \\aup.uisi.ru\

4.2.Практические работы по дисциплине (модулю):

Практические занятия № 1 Настройка безопасности сетевых устройств.

Практическое занятие №2 Настройка фильтрации трафика в ОС Windows и Linux.

Практическое занятие №3 Разработка политики безопасности предприятия.

Задания на выполнение практических работ представлены в электронно-информационной образовательной среде и доступны по URL: \\aup.uisi.ru\

4.3.Перечень вопросов на зачет:

Вопросы к зачету по дисциплине
“Кибербезопасность”

1. Что такое кибербезопасность, и почему она важна?
2. Какие основные виды угроз существуют в сфере кибербезопасности?
3. Какие шаги можно предпринять для защиты своих персональных данных в интернете?
4. Что такое аутентификация и авторизация в контексте кибербезопасности?
5. Какие методы атак используют хакеры для взлома паролей?
6. Что такое фишинг и какие меры можно принять для защиты от него?
7. Каковы основные принципы создания безопасных паролей?
8. Что такое многофакторная аутентификация (MFA) и почему она важна?
9. Какие основные методы защиты компьютерных сетей от несанкционированного доступа?
10. Какие виды вредоносных программ (вирусов) существуют, и как они работают?

11. Что такое ботнет и какие цели могут преследовать злоумышленники, создавая их?
12. Какие меры можно предпринять для защиты своего компьютера от вредоносных программ?
13. Что такое DDoS-атака и какие её последствия могут быть для организации?
14. Какие меры обеспечивают конфиденциальность и целостность данных в сети?
15. Что такое шифрование и как оно используется в кибербезопасности?
16. Какие основные принципы безопасности следует соблюдать при работе с электронной почтой?
17. Какие меры безопасности необходимо предпринимать при использовании общественных Wi-Fi-сетей?
18. Что такое баг иран и почему это важный аспект кибербезопасности?
19. Какие меры следует предпринимать для обеспечения безопасности мобильных устройств?
20. Какие законы и регуляции регулируют область кибербезопасности в вашей стране?
21. Приведите настройку фильтрации пакетов в среде Windows.
22. Приведите настройку фильтрации пакетов в среде Linux.
23. Произведите настройку безопасности межсетевого экрана.
24. Разработайте политику безопасности предприятия по представленному плану.

5. Банк контрольных заданий и иных материалов, используемых в процессе процедур текущего контроля и промежуточной аттестации

Представлен в электронной информационно-образовательной среде по URI: http://aup.uisi.ru/