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.
«28» 11 2025 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ
Б1.О.22 Основы информационной безопасности

Направление подготовки / специальность: **11.03.02 «Инфокоммуникационные технологии и системы связи»**

Направленность (профиль) /специализация: **Инженерия телекоммуникаций**

Форма обучения: **очная**

Год набора: 2026

Разработчик (-и):
старший преподаватель _____ /А.Е. Каменсков/
подпись

к.т.н. доцент _____ /Д.В. Кусайкин/
подпись

Оценочные средства обсуждены и утверждены на заседании информационных систем и технологий (ИСиТ)
Протокол от 27.11.2025 г. № 3
Заведующий кафедрой _____ / Д.И. Бурумбаев/
подпись

Екатеринбург, 2025

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.
«____» _____2025 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ
Б1.О.22 Основы информационной безопасности

Направление подготовки / специальность: **11.03.02 «Инфокоммуникационные технологии и системы связи»**

Направленность (профиль) /специализация: **Инженерия телекоммуникаций**

Форма обучения: **очная**

Год набора: 2026

Разработчик (-и):
старший преподаватель _____ /А.Е. Каменсков/
подпись

к.т.н. доцент _____ /Д.В. Кусайкин/
подпись

Оценочные средства обсуждены и утверждены на заседании информационных систем и технологий (ИСиТ)
Протокол от 27.11.2025 г. № 3
Заведующий кафедрой _____ / Д.И. Бурумбаев/
подпись

Екатеринбург, 2025

1. Перечень компетенций и индикаторов их достижения

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенций	Этап	Предшествующие этапы (с указанием дисциплин/практик)
ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.3 Умеет решать задачи анализа, обработки данных с помощью современных средств цифровой вычислительной техники, их представления в требуемом формате, соблюдая при этом основные требования информационной безопасности	-	-

Форма промежуточной аттестации по дисциплине – зачет

2. Показатели, критерии и шкалы оценивания компетенций

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

Индикатор освоения компетенции	**Показатель оценивания**	**Критерий оценивания**
ОПК-3.3 Умеет решать задачи анализа, обработки данных с помощью современных средств цифровой вычислительной техники, их представления в требуемом формате, соблюдая при этом основные требования информационной безопасности	Умеет решать задачи анализа, обработки данных с помощью современных средств цифровой вычислительной техники, их представления в требуемом формате, соблюдая при этом основные требования информационной безопасности	Свободно умеет решать задачи анализа, обработки данных с помощью современных средств цифровой вычислительной техники, их представления в требуемом формате, соблюдая при этом основные требования информационной безопасности

Шкала оценивания.

Зачет

Шкала оценивания	**Критерии оценки**
«зачет»	На экзаменационные вопросы даны полные аргументированные ответы. Студент демонстрирует сформированность дисциплинарных компетенций на итоговом уровне, обнаруживает всестороннее, систематическое и глубокое знание учебного материала по тематике: комплексный подход к обеспечению информационной безопасности, защита от

	несанкционированного доступа к информации в компьютерных системах, криптографические методы защиты информации, защита от вредоносных программ. Студент усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, свободно оперирует приобретенными знаниями, умениями, применяет их при выполнении заданий.
«незачет»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового, проявляется недостаточность знаний. Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний по темам дисциплины, отсутствуют навыки решения задач.

3. Методические материалы, определяющие процедуры оценивания по дисциплине

3.1. В ходе реализации дисциплины используются следующие формы и методы текущего контроля

Тема и/или раздел	**Формы/методы текущего контроля успеваемости**
ОПК-3.3 Умеет решать задачи анализа, обработки данных с помощью современных средств цифровой вычислительной техники, их представления в требуемом формате, соблюдая при этом основные требования информационной безопасности	
Комплексный подход к обеспечению информационной безопасности	Лекция
Защита от несанкционированного доступа к информации в компьютерных системах	Лекция
Криптографические методы защиты информации	Лекция
Защита от вредоносных программ	Лекция
Защита информации с помощью пароля	Практическое занятие
Реализация сетевой сегментации и настройка межсетевого экрана	Практическое занятие
Исследование уязвимостей сетевых служб на примере OWASP Mutillidae и Metasploitable	Практическое занятие

3.2. Типовые материалы текущего контроля успеваемости обучающихся

ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности

Пример задания на практическое занятие

Практическое занятие 1
Защита информации с помощью пароля

1. **Цель работы:**
   1.1. Исследовать защиту данных с применением пароля.
   1.2. Исследовать методы противодействия атакам на пароль.

2. **Вопросы допуска:**
   2.1. Какие типы данных могут быть защищены паролем?
   2.2. Каким образом возможно защитить паролем данные любого типа?
   2.3. Какие из существующих форматов сжатия поддерживают парольную защиту?
   2.4. Какие существуют утилиты для подбора пароля к защищенным архивам? Какие способы подбора пароля к защищенным архивам они используют?

3. **Порядок подготовки рабочего места:**
   3.1. В качестве инструмента проверки безопасности парольной защиты архивов в данной работе рассматривается утилиты hashcat в связке с John the Ripper совместимые с Windows и Linux. Перед выполнением работы необходимо подготовить рабочее место согласно следующему порядку:
   3.2. Скачать утилиту John the Ripper
   3.3. Скачать утилиту Hashcat
   3.4. Установить необходимое ПО для работы Hashcat.
   3.5. Проверить корректность установки запуском hashcat.exe с ключем -b (benchmark)

4. **Задание**
   4.1. Используя Hashcat произвести атаку перебором по маске (-a 3) на зашифрованный файл second.rar если известно что пароль состоит из одной строчной латинской буквы и четырех цифр.
      4.1.1. С формировать хэш-сумму для целевого архива с помощью John the Ripper.
      4.1.2. За пустить подбор пароля по маске для полученного хеша. Скриншот команды
      4.1.3. П роверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым. Скриншот содержимого.
   4.2. Используя Hashcat произвести атаку по словарю (-a 0). Архив выбрать из папки Задание 3 соответственно номеру по журналу. Пароль является осмысленным словом английского языка. К отчету приложить скриншот команды Hashcat и раскрытый пароль. Вывод?
   4.3. Используя Hashcat раскрыть пароль от архива используя опцию инкремента. Пароль может являться числом от 0 до 100000000. Архив выбрать из папки Задание 4 соответственно номеру по журналу. К отчету приложить скриншот команды Hashcat и раскрытый пароль.
   4.4. Зная фактическую длину пароля повторить атаку в режиме атаки по маске. Сравнить разницу во времени для случаев атаки в режиме инкремента и атаке при известной длине пароля, сделать вывод о существенности/несущественности изменения продолжительности атаки.

5. **Требования к отчету:**
   5.1. Выполнение требований оформления
   5.2. Ответы на вопросы допуска
   5.3. Скриншоты основных этапов выполнения задания.
   5.4. Выводы по работе / пунктам. Выводы должны быть разумными и понятными
   5.5. Способность студента объяснить написанное в любой части отчета

3.3. Типовые материалы для проведения промежуточной аттестации обучающихся

Типовые вопросы и задания к экзамену:

1. Раскройте понятие "информационная безопасность". В чем разница между понятиями "конфиденциальность", "целостность" и "доступность" (триада CIA)? Приведите примеры нарушения каждого из свойств.

2. Дайте определение понятиям "актив", "угроза", "уязвимость" и "риск" в контексте ИБ. Какова взаимосвязь между ними?
3. Опишите основные этапы процесса управления рисками информационной безопасности. В чем разница между качественной и количественной оценкой рисков?
4. Какие существуют стратегии обработки рисков (уклонение, снижение, передача, принятие)? В каких случаях применяется каждая из них?
5. Что такое политика информационной безопасности? Какие уровни документов обычно входят в комплект документации по ИБ организации?
6. Для чего нужны стандарты и спецификации в области ИБ (ISO/IEC 27000, ГОСТ Р 57580, стандарты ФСТЭК)? Чем стандарты отличаются от законов?
7. Какие основные законодательные акты РФ регулируют отношения в области информационной безопасности? (Назовите и кратко охарактеризуйте не менее двух, например, ФЗ "О персональных данных" и "Об информации, информационных технологиях и о защите информации").
8. Что такое Система менеджмента информационной безопасности (СМИБ)? Объясните суть процессного подхода и цикла PDCA (Plan-Do-Check-Act) в контексте СМИБ.
9. Что означает принцип комплексного подхода к обеспечению ИБ? Почему недостаточно использовать только технические средства защиты?
10. Какие виды ответственности (дисциплинарная, административная, уголовная) предусмотрены за нарушения в сфере информационной безопасности? Приведите примеры.
11. Дайте определение дискреционной (мандатной, ролевой) модели управления доступом. В чем их принципиальные отличия?
12. Раскройте содержание четырех этапов модели IAAA: Идентификация, Аутентификация, Авторизация, Аудит.
13. Перечислите основные факторы (методы) аутентификации (то, что мы знаем, имеем, чем являемся). Приведите примеры и сравните их надежность.
14. Для чего нужны межсетевые экраны (Firewalls)? Объясните принципы фильтрации трафика на основе портов и протоколов (статистический анализ).
15. Что такое сегментация сети? Какие цели преследует разделение корпоративной сети на VLAN'ы или изолированные подсети? Как сегментация помогает сдержать атаку?
16. Какие основные меры необходимо предпринять для обеспечения безопасности операционной системы (Windows или Linux) после ее установки? (Обновления, политики паролей, отключение ненужных служб и т.д.).
17. Что такое привилегии пользователя и принцип минимальных привилегий (PoLP)? Почему опасно работать в системе с правами администратора?
18. Какая информация фиксируется в журналах аудита (лог-файлах) событий безопасности? С какой целью эти журналы анализируются?
19. Какие средства инженерно-технической защиты информации относятся к физическим преградам, а какие — к средствам охраны и наблюдения (СКУД, видеонаблюдение)?
20. Что понимается под "несанкционированным доступом"? Каковы основные каналы НСД к информации в компьютерной системе?
21. Дайте определения основным криптографическим примитивам: шифрование, хеширование, электронная подпись. Какую задачу решает каждый из них?
22. В чем заключался основной недостаток классических шифров (например, шифра Цезаря или Виженера) по сравнению с современными алгоритмами?
23. Опишите принцип работы симметричного шифрования. В чем его главное преимущество и главный недостаток (проблема распространения ключей)?
24. Опишите принцип работы асимметричного шифрования. Для решения какой фундаментальной проблемы криптографии были созданы эти системы?
25. Сравните симметричные и асимметричные криптосистемы по скорости работы, длине ключа и области применения (где что лучше использовать?).

26. Какие существуют основные проблемы при управлении криптографическими ключами (генерация, хранение, распространение, уничтожение)?
27. Что такое инфраструктура открытых ключей (PKI)? Из каких компонентов она состоит (Удостоверяющий центр, регистратура, конечные пользователи, сертификаты)?
28. Что представляет собой цифровой сертификат (например, X.509)? Какая информация в нем содержится и какую роль играет подпись Удостоверяющего центра?
29. Для чего используется протокол SSL/TLS? Какую роль он играет в безопасности интернета (например, при работе с сайтами по HTTPS)?
30. Где, помимо шифрования дисков и HTTPS, применяется криптография в повседневной жизни? (Электронная почта, мессенджеры, ЭЦП в документах, блокчейн).
31. Дайте определение понятию "вредоносная программа". Перечислите основные типы вредоносного ПО (вирусы, черви, трояны, шпионское ПО, руткиты) и кратко охарактеризуйте каждый тип.
32. Как менялись цели создания вредоносных программ от первых компьютерных вирусов до современных угроз (от хулиганства до финансового мошенничества и кибершпионажа)?
33. Что такое руткит (rootkit)? Какие техники скрытия вредоносного ПО в системе вы знаете (маскировка процессов, файлов, записей реестра)?
34. В чем разница между сигнатурным (реактивным) и эвристическим (поведенческим) методами обнаружения вредоносных программ? В чем преимущества и недостатки каждого?
35. Что такое "песочница" (sandbox) в контексте антивирусной защиты? Как она помогает обнаружить неизвестное вредоносное ПО?
36. Опишите принцип действия программ-вымогателей (шифровальщиков). Какой тип криптографии они обычно используют для быстрого шифрования файлов жертвы и почему?
37. Какие основные меры профилактики позволяют минимизировать ущерб от атаки программы-вымогателя (резервное копирование, сегментация сети, привилегии доступа)?
38. Перечислите основные способы проникновения вредоносного ПО на компьютер пользователя (электронная почта, съемные носители, зараженные сайты, уязвимости ПО).
39. Что такое статический анализ вредоносного ПО и что можно узнать о файле, не запуская его (хэши, строки, импортируемые библиотеки)?
40. Что такое динамический анализ вредоносного ПО? В чем заключается главное правило безопасности при его проведении? (Использование изолированной среды/песочницы).

3.4. Методические материалы проведения текущего контроля и промежуточной аттестации обучающихся

Перечень методических материалов для подготовки к текущему контролю и промежуточной аттестации:

1. Методические указания по выполнению практических занятий по дисциплине «Основы информационной безопасности». –URL: https://aup.uisi.ru/4171753/