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
_____ Е.А. Минина
«28» 11 2025 г.

Оценочные материалы текущего контроля и промежуточной аттестации
по учебной дисциплине

ОП.12 ЗАЩИТА ИНФОРМАЦИИ

для специальности:
09.02.12 Техническая эксплуатация и сопровождение
информационных систем

Квалификация: специалист по технической эксплуатации и
сопровождению информационных систем

Год начала подготовки: 2026

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
_____ Е.А. Минина
«___» _____ 2025 г.

Оценочные материалы текущего контроля и промежуточной аттестации
по учебной дисциплине

ОП.12 ЗАЩИТА ИНФОРМАЦИИ

для специальности:
09.02.12 Техническая эксплуатация и сопровождение
информационных систем

Квалификация: специалист по технической эксплуатации и
сопровождению информационных систем

Год начала подготовки: 2026

Екатеринбург
2025

Оценочные материалы составил:
Тупицын К.М. - преподаватель ЦК ИТиАСУ кафедры ИСТ

Одобрено цикловой комиссией
Информационных технологий и АСУ
кафедры Информационных систем и
технологий.
Протокол 3 от 27.11.25
Председатель цикловой комиссии
_____ О.М. Ермоленко

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

Оценочные материалы составил:
Тупицын К.М. - преподаватель ЦК ИТиАСУ кафедры ИСТ

Одобрено цикловой комиссией
Информационных технологий и АСУ
кафедры Информационных систем и
технологий.
Протокол ___ от _____
Председатель цикловой комиссии
_____ О.М. Ермоленко

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

1 Структура матрицы компетенций по дисциплине

В результате освоения дисциплины «Защита информации» обучающийся должен обладать, предусмотренными ФГОС СПО по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем, умениями, знаниями, навыками:

уметь:

- устанавливать программное обеспечение, необходимое для функционирования ИС;
- деинсталлировать программное обеспечение, необходимое для функционирования ИС;
- работать с записями по качеству (в том числе с корректирующими действиями, предупреждающими действиями, запросами на исправление несоответствий) при выполнении технической поддержки процессов создания (модификации) и сопровождения ИС;
- отличать штатное состояние БД от работы БД в нештатном режиме;
- описывать работу БД и отклонения от штатного режима работы;
- идентифицировать и устранять типичные причины отклонений от штатного режима работы БД;

знать:

- основы системного администрирования;
- основы администрирования баз данных;
- коммуникационное оборудование;
- сетевые протоколы;
- основы современных операционных систем;
- основы современных СУБД;
- устройство и функционирование современных ИС;
- основы архитектуры мультиарендного программного обеспечения;
- основы ИБ организации;
- источники информации, необходимой для профессиональной деятельности в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
- лучшие практики создания (модификации) и сопровождения ИС в экономике;
- типичные ошибки, возникающие при работе БД, признаки их проявления при работе БД;
- средства и методы организации контроля функционирования БД;
- технологии передачи данных и обмена данными в компьютерных сетях;
- методы предотвращения потери данных;
- термины и определения в области информационных технологий;
- регламенты взаимодействия сотрудников при обнаружении отклонений от штатной работы БД;

- основные технические характеристики оборудования и архитектура БД;
- нормы и правила ведения технической документации, принятые в организации;

***владеть навыками*:**

- проверки соответствия рабочих мест ИС требованиям ИС к оборудованию и программному обеспечению в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
- инсталляции ИС на рабочих местах заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
- верификации правильности установки ИС на рабочих местах заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
- фиксирования результатов развертывания рабочих мест ИС у заказчика в системе учета организации в рамках технической поддержки процессов создания (модификации) и сопровождения ИС.
- наблюдения за работой БД;
- обнаружения отклонений от штатного режима работы БД;
- ведения журнала мониторинга событий работы БД;
- устранения типичных причин отклонений от штатного режима работы БД.

Указанные умения и знания формируют общие и профессиональные компетенции, представленные в виде структурной матрицы (Таблица 1).

Таблица 1

Индекс компетенции	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.
ПК 1.6	Развертывать рабочие места информационных систем у заказчика.
ПК 2.4	Выполнять мониторинг событий, возникающих в процессе функционирования баз данных.

Формой промежуточной аттестации по дисциплине «Защита информации» является дифференцированный зачет.

2 Оценка освоения дисциплины

2.1 Формы и методы оценивания

Предметом оценки служат знания, умения и навыки, предусмотренные ФГОС СПО по дисциплине «Защита информации», направленные на формирование общих и профессиональных компетенций.

2.2 Контроль и оценка освоения дисциплины

Таблица 2

№ п/п	Элементы дисциплины (темы/разделы)	Индекс компетенции	Форма и методы контроля	Макс. балл
1.	Комплексный подход к обеспечению информационной безопасности.	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ПК 1.6, ПК 2.4	Проверка отчетов по практическим занятиям 1,2.	5
			Тестирование по разделу.	5
2.	Защита от несанкционированного доступа к информации в компьютерных системах.	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ПК 1.6, ПК 2.4	Проверка отчетов по практическим занятиям 3-5	5
			Контроль самостоятельной работы обучающегося.	Зачет
			Тестирование по разделу.	5
3.	Криптографические методы защиты информации.	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ПК 1.6, ПК 2.4	Проверка отчетов по практическим занятиям 6-12	5
			Контроль самостоятельной работы обучающегося.	Зачет
			Тестирование по разделу.	5
4.	Защита от вредоносных программ.	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ПК 1.6, ПК 2.4	Проверка отчетов по практическим занятиям 13-17.	5
			Тестирование по разделу.	5

2.3 Формы и методы текущего контроля знаний и умений

В ходе текущего контроля знаний и умений по дисциплине применяются следующие формы и методы контроля и оценки:

- проверка отчетов по практическим занятиям;
- проверка выполнения самостоятельных работ;
- проверка теоретических знаний по дисциплине в форме тестирования.

2.3.1 Практические занятия

Практическое занятие 1 «Сертификация защищенности систем».

Практическое занятие 2 «Государственные и международные стандарты безопасности».

Практическое занятие 3 «Защитные механизмы при аутентификации».

Практическое занятие 4,5 «Разграничение доступа при работе с приложениями».

Практическое занятие 6,7 «Криптография и криптоанализ».

Практическое занятие 8 «Стеганография».

Практическое занятие 9,10 «Алгоритмы шифрования».

Практическое занятие 11,12 «Алгоритмы электронной цифровой подписи».

Практическое занятие 13 «Вирусология».

Практическое занятие 14,15 «Исследование уязвимостей сетевых устройств на примере Metasploitable».

Практическое занятие 16,17 «Исследование уязвимостей веб-приложений на примере OWASP Mutillidae».

Критерии оценки освоения

Объем и качество освоения обучающимися практического занятия, уровень сформированности компетенций оцениваются по результатам его защиты и ответов на контрольные вопросы.

Оценка «*отлично*» ставится в том случае, если:

- практическая работа выполнена в полном объеме с соблюдением необходимой последовательности решений задач, присутствуют ответы на контрольные вопросы.

Оценка «*хорошо*» ставится в том случае, если:

- в представленном отчете по практической работе допущены недочеты или ошибки в решении задач, но не более чем в 20% от всех заданий.

Оценка «*удовлетворительно*» ставится в том случае, если:

- практическая работа выполнена не полностью, но объем правильно выполненной части более 50% от всех заданий.

Оценка «*неудовлетворительно*» ставится в том случае, если:

- работа выполнена не полностью, и объем правильно выполненной части работы менее 50% от всех предложенных заданий.

2.3.2 Самостоятельная работа

Самостоятельная работа по теме 2.1 «Способы несанкционированного доступа к информации»: написание реферата по теме «Аутентификация, авторизация и аутентификация. Различия между понятиями. Способы защиты от несанкционированного доступа к информации».

Самостоятельная работа по теме 3.2 «Симметричные и несимметричные алгоритмы шифрования»: написание реферата по теме «Симметричные и несимметричные алгоритмы шифрования».

Критерии оценки освоения

Объем и качество освоения обучающимися самостоятельной работы, уровень сформированности компетенций оцениваются по результатам проверки рефератов, выступлений с докладами по темам рефератов, ответов на вопросы.

Результатом успешного выполнения самостоятельной работы является «зачет».

Таблица 3 - Критерии оценки реферата

«Зачет»	Реферативная работа выполнена в полном объеме. Работа отличается глубиной проработки всех разделов содержательной части, оформлена с соблюдением установленных правил; обучающийся твердо владеет теоретическим материалом, может применять его самостоятельно или по указанию преподавателя; на большинство вопросов даны правильные ответы, защищает свою точку зрения достаточно обосновано.
«Незачет»	Работа выполнена частично. Качество оформления печатного материала не соответствует предъявляемым требованиям. Обучающийся не может защитить свои решения и выводы, допускает грубые фактические ошибки при ответах на поставленные вопросы или вовсе не отвечает на них.

2.3.3 Тестирование обучающихся

Тестовые задания по разделу 1 «Комплексный подход к обеспечению информационной безопасности».

Тестовые задания по разделу 2 «Защита от несанкционированного доступа к информации в компьютерных системах».

Тестовые задания по теме 3 «Криптографические методы защиты информации».

Тестовые задания по теме 4 «Защита от вредоносных программ».

Критерии оценки освоения

За правильный ответ на вопрос тестового задания выставляется положительная оценка - 1 балл.

За неправильный ответ на вопрос тестового задания выставляется отрицательная оценка - 0 баллов.

Таблица 4 - Шкала оценки

Процент результативности (правильных ответов на вопросы тестового задания)	Оценка уровня подготовки
90 - 100	отлично
80 - 89	хорошо
65 - 79	удовлетворительно
менее 65	неудовлетворительно

2.4 Формы и методы промежуточной аттестации

Промежуточная аттестация по дисциплине осуществляется в форме дифференцированного зачета.

Вопросы для подготовки обучающихся к дифференцированному зачету:

1 Понятие информационной среды. Составляющие информационной среды. Классификация информации по степени конфиденциальности. Доступ к информации.

2 Факторы, влияющие на достоверность и актуальность информационного наполнения информационных систем. Источники атак на информацию. Типы

рисков потери достоверности информационного наполнения систем. Ограничение доступа к информации.

3 Комплексный подход к защите информации. Понятие политики безопасности. Типы политик безопасности. Классификация методов защиты информации. Организационные методы защиты информации.

4 Стандарты безопасности. Криптографические модели. Модели безопасности основных ОС. Государственные и международные стандарты безопасности. Сертификация защищенности систем.

5 Способы несанкционированного доступа к информации. Основные защитные механизмы: идентификация и аутентификация.

6 Разграничение доступа. Контроль целостности.

7 Понятия аутентификации и авторизации. Аппаратные методы аутентификации. Оборудование аутентификации. Информационно-программные методы аутентификации. Методы хранения аутентификационных данных. Защита информации в сетях. Аутентификация и авторизация в сетях. Сертификаты безопасности. Защита сетей от несанкционированного подключения и проникновения. Защита от прослушиваний трафика. Защита от подмены пакетов. Защита от несанкционированных изменений структуры и топологии сети. Туннельные протоколы.

8 Требования к алгоритмам шифрования. Понятие ключа. Требования к ключам. Алгоритмы подстановки. Алгоритмы перестановки. Гаммирование. Методы шифрования, основанные на односторонних и близких к ним функциях.

9 Симметричные и несимметричные алгоритмы шифрования. Методы генерации и обмена ключами. Функции хэширования. Электронная цифровая подпись. Компьютерная стеганография и ее применение.

10 Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и защита от них.

Критерии оценки освоения

Оценка «*неудовлетворительно*» ставится обучающемуся, не овладевшему ни одним из элементов компетенции, т.е. обнаружившему существенные пробелы в знании основного программного материала по дисциплине, допустившему принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине.

Оценка «*удовлетворительно*» ставится обучающемуся, овладевшему элементами компетенции «знать», т.е. проявившему знания основного программного материала по дисциплине в объеме, необходимом для последующего обучения и предстоящей практической деятельности, знакомому с основной рекомендованной литературой, допустившему неточности в ответе на дифференцированном зачете, но в основном обладающему необходимыми знаниями для их устранения при корректировке со стороны преподавателя.

Оценка «*хорошо*» ставится обучающемуся, овладевшему элементами компетенции «знать» и «уметь», проявившему полное знание программного материала по дисциплине, освоившему основную рекомендованную литературу, обнаружившему стабильный характер знаний и умений и способному к их самостоятельному применению и обновлению в ходе последующего обучения и практической деятельности.

Оценка «*отлично*» ставится обучающемуся, овладевшему элементами компетенции «знать», «уметь» и «владеть», проявившему всесторонние и глубокие знания программного материала по дисциплине, освоившему основную и дополнительную литературу, обнаружившему творческие способности в понимании, изложении и практическом использовании усвоенных знаний.

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.

Литература

1 Основные печатные и/или электронные издания:

1. Горюнов, В. Е. Защита информации: учебное пособие для СПО / В. Е. Горюнов. — Москва: Ай Пи Ар Медиа, 2025. — 353 с. — ISBN 978-5-4497-4317-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/149923.html — Режим доступа: для авторизир. пользователей.

2. Ларионова, Е. И. Криптографическая защита информации: практикум / Е. И. Ларионова, Ю. Д. Фот, К. Р. Джукашев. — Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2025. — 110 с. — ISBN 978-5-7410-3365-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/153198.html — Режим доступа: для авторизир. пользователей.

2 Дополнительные издания:

1. Прокопенко, Е. В. Техническая защита информации: учебное пособие / Е. В. Прокопенко, В. О. Коротин. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2024. — 131 с. — ISBN 978-5-00137-494-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/148668.html — Режим доступа: для авторизир. пользователей.