

Приложение 1 к рабочей программе

по дисциплине

«Защита информации»

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

2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине «Защита информации»

для основной профессиональной образовательной программы по направлению

09.03.01 «Информатика и вычислительная техника»

направленность (профиль) – Программное обеспечение средств вычислительной техники и

автоматизированных систем

квалификация – бакалавр

форма обучения – очная, заочная

год начала подготовки (по учебному плану) – 2022

Екатеринбург 2022

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

« ____ » _____ 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине «**Защита информации**»

для основной профессиональной образовательной программы по направлению

09.03.01 «Информатика и вычислительная техника»

направленность (профиль) – Программное обеспечение средств вычислительной техники и

автоматизированных систем

квалификация – бакалавр

форма обучения – очная, заочная

год начала подготовки (по учебному плану) – 2022

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)
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	7	Этап 5: Архитектура ЭВМ Этап 6: Менеджмент
	ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
	ОПК-3.3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.		
ОПК-9. Способен осваивать методики использования программных средств для решения практических задач	ОПК-9.1. Знать: методики использования программных средств для решения практических задач	7	Этап 1: Информатика Этап 3,4: Электротехника, электроника и схемотехника Этап 7: Базы данных
	ОПК-9.2. Уметь: использовать программные средства для решения практических задач		
	ОПК-9.3. Иметь навыки: использования программных средств для решения практических задач		

Формы промежуточной аттестации по дисциплине: экзамен (7 семестр), РГР (7 семестр).

2. Показатели, критерии и шкалы оценивания компетенций

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

Шкала оценивания	Результаты обучения	Дескрипторы уровней освоения компетенций
ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		
Низкий (пороговый) уровень	Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Имеет представление о способах защиты информации от несанкционированного доступа
Средний уровень		Владеет понятийным аппаратом защиты информации.
Высокий уровень		Свободно владеет понятийным аппаратом защиты информации, обладает навыками по организации защиты информации в вычислительной сети.
ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
Низкий (пороговый) уровень	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Владеет минимально необходимым набором навыков по обеспечению защиты информации
Средний уровень		Владеет набором навыков по обеспечению защиты информации с помощью специализированного ПО
Высокий уровень		Владеет набором навыков по обеспечению защиты информации, способен самостоятельно разработать ПО для защиты информации в вычислительной сети.
ОПК-3.3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.		
Низкий (пороговый) уровень	Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Ориентируется в основных понятиях и концепциях обеспечения защиты информации.
Средний уровень		Ориентируется в специальных понятиях и расширенных концепциях обеспечения защиты информации.
Высокий уровень		Способен разработать концепцию обеспечения защиты информации на основе общеизвестных моделей защиты информации.
ОПК-9.1. Знать: методики использования программных средств для решения практических задач		
Низкий (пороговый) уровень	Знать: методики использования программных средств для решения практических задач	Владеет минимально необходимым набором навыков по работе с ПО защиты информации

Средний уровень		Владеет набором навыков по обеспечению защиты информации с помощью с помощью специализированного ПО
Высокий уровень		Владеет набором навыков по обеспечению защиты информации, способен самостоятельно разработать ПО для защиты информации в вычислительной сети.
ОПК-9.2. Уметь: использовать программные средства для решения практических задач		
Низкий (пороговый) уровень	Уметь: использовать программные средства для решения практических задач	Владеет минимально необходимым набором навыков по работе с ПО защиты информации
Средний уровень		Владеет набором навыков по обеспечению защиты информации с помощью с помощью специализированного ПО
Высокий уровень		Владеет набором навыков по обеспечению защиты информации, способен самостоятельно разработать ПО для защиты информации в вычислительной сети.
ОПК-9.3. Иметь навыки: использования программных средств для решения практических задач		
Низкий (пороговый) уровень	Иметь навыки: использования программных средств для решения практических задач	Владеет минимально необходимым набором навыков по работе с ПО защиты информации
Средний уровень		Владеет набором навыков по обеспечению защиты информации с помощью с помощью специализированного ПО
Высокий уровень		Владеет набором навыков по обеспечению защиты информации, способен самостоятельно разработать ПО для защиты информации в вычислительной сети.

2.2 Таблица соответствия результатов промежуточной аттестации по дисциплине уровню этапа формирования компетенций

Форма контроля	Шкала оценивания	Код индикатора достижения компетенций	Уровень освоения компетенции
РГР	удовлетворительно	ОПК-3.1,2,3	низкий
		ОПК-9.1,2,3	низкий
	хорошо	ОПК-3.1,2,3	средний
		ОПК-9.1,2,3	средний
	отлично	ОПК-3.1,2,3	высокий
		ОПК-9.1,2,3	высокий
Экзамен	удовлетворительно	ОПК-3.1,2,3	низкий
		ОПК-9.1,2,3	низкий
	хорошо	ОПК-3.1,2,3	средний
		ОПК-9.1,2,3	средний
	отлично	ОПК-3.1,2,3	высокий
		ОПК-9.1,2,3	высокий

3. Методические материалы, определяющие процедуры оценивания

Процесс оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, представлен в таблицах по формам обучения:

Тип занятия	Тема (раздел)	Оценочные средства
<p>ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p> <p>ОПК-9.1. Знать: методики использования программных средств для решения практических задач</p>		
Лекция	Комплексный подход к обеспечению информационной безопасности Защита от несанкционированного доступа к информации в компьютерных системах Криптографические методы защиты информации Защита от вредоносных программ	Конспект лекций Дискуссии РГР Экзамен
Практическое занятие	Защита информации с помощью пароля Исследование стандартов защиты Wi-Fi сетей Анализ сетевого трафика Исследование уязвимостей сетевых служб на примере OWASP Mutillidae и Metasploitable	Отчет по практическим занятиям Экзамен
Самостоятельная работа	Аудит безопасности информационной системы	РГР Экзамен
<p>ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>ОПК-9.2. Уметь: использовать программные средства для решения практических задач</p>		
Практическое занятие	Основы стеганографии Практическое применение хэш-функций Практическое применение симметричных шифров	Отчет по практическим занятиям РГР
Самостоятельная работа	Основы вирусологии Изучение уязвимостей антивирусного ПО Основы криптоанализа	Отчет по практическим занятиям РГР
<p>ОПК-3.3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.</p> <p>ОПК-9.3. Иметь навыки: использования программных средств для решения практических задач</p>		
Практическое занятие	Основы вирусологии Изучение уязвимостей антивирусного ПО Основы криптоанализа	Отчет по практическим занятиям РГР

Самостоятельная работа	Основы вирусологии Изучение уязвимостей антивирусного ПО Основы криптоанализа	Отчет по практическим занятиям РГР Экзамен
------------------------	---	--

4. Типовые контрольные задания

Примеры задания по каждому типу оценочных средств для каждой компетенции, формируемой данной дисциплиной.

4.1 Типовое задание дискуссий по дисциплине:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Каким образом возможно защитить паролем данные любого типа?
2. Как возможно защититься от кражи личных и персональных данных посредством сниффинга?

ОПК-9. Способен осваивать методики использования программных средств для решения практических задач

1. Какие способы устранения уязвимостей веб-приложений вы знаете?
2. Как выявляются уязвимости веб-приложений? Как в этом процессе могут быть задействованы стратегии тестирования (черного/белого ящика)?

4.2 Типовое задание для практических занятий по дисциплине:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Какие способы устранения уязвимостей сетевых служб вы знаете?
2. Каким образом возможно использовать брандмауэры для защиты от атак на сетевые службы?

ОПК-9. Способен осваивать методики использования программных средств для решения практических задач

1. Какие способы устранения уязвимостей сетевых служб вы знаете?
2. Каким образом возможно использовать брандмауэры для защиты от атак на сетевые службы?

4.3 Типовое задание для самостоятельной работе по дисциплине:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Какие способы устранения уязвимостей сетевых служб вы знаете?
2. Каким образом возможно использовать брандмауэры для защиты от атак на сетевые службы?

ОПК-9. Способен осваивать методики использования программных средств для решения практических задач

1. Какие способы устранения уязвимостей сетевых служб вы знаете?

2. Каким образом возможно использовать брандмауэры для защиты от атак на сетевые службы?

4.4 Пример билета на устном экзамене по дисциплине:

ТИПОВОЙ ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ:

Уральский технический институт связи и информатики (филиал) ФГОБУ ВПО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ)

Утверждаю:

зав. кафедрой ИСТ _____

подпись

«__» _____ 20__ г.

Экзаменационный билет № 1
Факультет ИИиУ Курс 4 Семестр 7
Дисциплина Защита информации

1. Какие алгоритмы шифрования используется в стандарте WEP?
2. Как возможно защититься от кражи личных и персональных данных посредством сниффинга?
3. Каковы принципиальные отличия WEP от WPA, WPA от WPA2, WPA2 от WPA3?

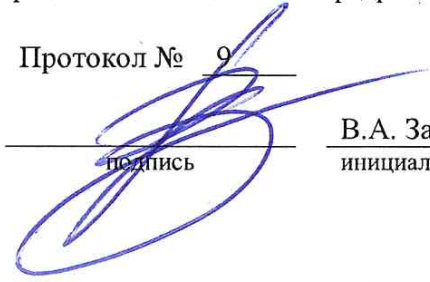
5. Банк контрольных заданий и иных материалов, используемых в процессе процедур текущего контроля и промежуточной аттестации

Банк представлен в локальной сети кафедры ИСТ и доступен по URL: <http://www.aup.uisi.ru>. После авторизации необходимо выбрать следующий путь: \Обучение \ИСТ \ФГОС ВО 3++ \ выбирается направление, профиль обучения, название дисциплины, указанные на титульном листе.

Оценочные средства рассмотрены и утверждены на заседании кафедры ИСТ

16.05.2022 г. Протокол № 9

Заведующий кафедрой (разработчика)



подпись

В.А. Зацепин
инициалы, фамилия

16.05.2022 г.

Оценочные средства рассмотрены и утверждены на заседании кафедры [ИСТ]

16.05.2022 г. Протокол № 9

Заведующий кафедрой (разработчика)

подпись

В.А. Зацепин

инициалы, фамилия

16.05.2022 г.