

Приложение 1 к рабочей программе
по дисциплине «Основы информационной безопасности»
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)



ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине «Основы информационной безопасности»
для основной профессиональной образовательной программы по направлению
11.03.02 «Инфокоммуникационные технологии и системы связи»
направленность (профиль) – Транспортные сети и системы связи
квалификация – бакалавр
форма обучения – очная, заочная
год начала подготовки (по учебному плану) – 2022

Екатеринбург 2022

Приложение 1 к рабочей программе
по дисциплине «Основы информационной безопасности»
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 **«Основы информационной безопасности»**
для основной профессиональной образовательной программы по направлению
11.03.02 «Инфокоммуникационные технологии и системы связи»
направленность (профиль) – Транспортные сети и системы связи
квалификация – бакалавр
форма обучения – очная, заочная
год начала подготовки (по учебному плану) – 2022

Екатеринбург 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 применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационно й безопасности | ОПК-3.5- Владеет методами и навыками обеспечения информационной безопасности | 7 | - |

Формы промежуточной аттестации по дисциплине: зачет (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-3.5- Владеет методами и навыками обеспечения информационной безопасности | | |
| Низкий (пороговый) уровень | Владеть: методами и навыками обеспечения 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. |

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

| Форма контроля | Шкала оценивания | Код индикатора достижения компетенций | Уровень освоения компетенции |
|----------------|-------------------|---------------------------------------|------------------------------|
| Зачет | удовлетворительно | ОПК-3.5 | низкий |
| | хорошо | ОПК-3.5 | средний |
| | отлично | ОПК-3.5 | 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 |
|---|---|---|
| ОПК-3.5- Владеет методами и навыками обеспечения информационной безопасности | | |
| 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 |
| 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 Зачет |
| Самостоятельная работа | Аудит безопасности информационной системы | Отчет по практическим занятиям Зачет |

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?

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?

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?

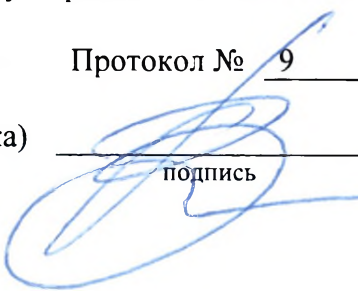
5. Банк контрольных заданий и иных материалов, используемых в процессе процедур текущего контроля и промежуточной аттестации

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)



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.