ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Уральский государственный университет путей сообщения"
(ФГБОУ ВО УрГУПС)

ФТД.03 Криптографические протоколы

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационные технологии и защита информации**

Учебный план 10.03.01 ИБ-2021.plx
10.03.01 Информационная безопасность

Направленность (профиль) Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **1 ЗЕТ**

Часов по учебному плану 36
в том числе:
аудиторные занятия 18
самостоятельная работа 18

Часов контактной работы всего, в том числе: 19
аудиторная работа 18
текущие консультации по практическим занятиям 1

Промежуточная аттестация и формы контроля:
зачет 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	8	8	8	8
Практические	10	10	10	10
Итого ауд.	18	18	18	18
Контактная работа	18	18	18	18
Сам. работа	18	18	18	18
Итого	36	36	36	36

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины: изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.
1.2	Задачи дисциплины: изучение принципов и методов разработки криптографических протоколов; применение на практике криптоглафических методов и средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП	
Цикл (раздел) ОП:	ФТД
2.1 Требования к предварительной подготовке обучающегося:	
Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные в ходе изучения дисциплин Математика, Дискретная математика. В результате освоения предшествующих дисциплин обучающийся должен знать: основные понятия и методы математического анализа, аналитической геометрии, линейной алгебры и теории алгебраических систем, математической логики и теории алгоритмов; основные методы помехоустойчивого кодирования и декодирования информации; основные параметры и характеристики помехоустойчивых кодов; уметь: использовать математические методы и модели для решения прикладных задач; применять знания о кодах, устраняющих избыточность и корректирующих ошибки; владеть: методами количественного анализа процессов обработки, поиска и передачи информации; навыками пользования библиотеками прикладных программ для решения прикладных математических задач.	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Производственная практика (эксплуатационная практика) Производственная практика (преддипломная практика)	

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-2: Способен администрировать средства защиты информации прикладного и системного программного обеспечения
ПК-2.2: Знает принципы функционирования программных средств криптографической и стеганографической защиты информации

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	сновные задачи и понятия криптографии; требования к криптографический протоколам и основные характеристики криптографических протоколов;
3.2	**Уметь:**
3.2.1	использовать криптографические протоколы для проектирования и разработки компьютерных систем; пользоваться научно-технической литературой в области криптографии.
3.3	**Владеть:**
3.3.1	криптографической терминологией; навыками использования типовых криптографических протоколов; навыками использования ПЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Элементы криптографических протоколов					
1.1	Введение в протоколы. Передача информации с использованием симметричной криптографии. Однонаправленные функции.Однонаправленные хэш функции. Передача информации с использованием криптографии с открытыми ключами /Лек/	7	2	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1 Э1	
1.2	Цифровые подписи. Цифровые подписи и шифрование. Генерация случайных и псевдослучайных последовательностей /Лек/	7	2	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1 Э1	

1.3	Практический семинар /Пр/	7	5	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1	Работа в группе. Групповая дискуссия
1.4	Изучение учебной и научно-технической литературы по тематике раздела. Подготовка к практическому семинару /Ср/	7	6	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Л3.2 Э1	
	Раздел 2. Основные криптографические протоколы					
2.1	Обмен ключами. Удостоверение подлинности. Удостоверение подлинности и обмен ключами. Формальный анализ протоколов проверки подлинности и обмена ключами /Лек/	7	2	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1 Э1	
2.2	Криптография с несколькими открытыми ключами. Разделение секрета. Совместное использование секрета /Лек/	7	2	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1 Э1	
2.3	Практический семинар /Пр/	7	5	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1	Работа в группе. Групповая дискуссия
2.4	Изучение учебной и научно-технической литературы по тематике раздела. Подготовка к практическому семинару /Ср/	7	6	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Л3.2 Э1	
2.5	Подготовка к промежуточной аттестации /Ср/	7	6	ПК-2.2	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Э1	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине, состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине и хранится на кафедре. Оценочные материалы дублируются на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося.

Фонд оценочных материалов для проведения промежуточной аттестации обучающихся по дисциплине (модулю), включая порядок проведения промежуточной аттестации, систему оценивания результатов промежуточной аттестации и критерии выставления оценок, примеры типовых заданий или иных материалов, необходимых для оценки знаний, умений, навыков, используемых для промежуточной аттестации по дисциплине, приведен в приложении 1 к рабочей программе дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1.1. Основная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	Зырянова Т. Ю.	Криптографические протоколы: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л1.2	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021	http://znanium.com
Л1.3	Романьков В. А.	Введение в криптографию: Учебное пособие	Москва: Издательство "ФОРУМ", 2021	http://znanium.com

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Бабаш А. В.	Криптографические методы защиты информации. Том 3: Учебно-методическое пособие	Москва: Издательский Центр РИО□, 2014	http://znanium.com

6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Зырянова Т. Ю.	Криптографические протоколы: методические рекомендации к практическим семинарам для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.2	Зырянова Т. Ю.	Криптографические протоколы: методические рекомендации по организации самостоятельной работы студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)	
Э1	Система электронной поддержки обучения Blackboard Learn (http:// bb.usurt.ru)

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем	
6.3.1 Перечень программного обеспечения	
6.3.1.1	Неисключительные права на ПО Windows
6.3.1.2	Неисключительные права на ПО Office
6.3.1.3	Система электронной поддержки обучения Blackboard Learn
6.3.2 Перечень информационных справочных систем и профессиональных баз данных	
6.3.2.1	Справочно-правовая система КонсультантПлюс
6.3.2.2	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.3	Международная реферативная база данных научных изданий Scopus
6.3.2.4	Международная реферативная база данных научных изданий eLIBRARY.RU

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)	
Назначение	Оснащение
Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель Демонстрационное оборудование - Комплект мультимедийного оборудования Учебно-наглядные пособия - презентационные материалы
Компьютерный класс - Учебная аудитория для самостоятельной работы студентов	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным пунктом 6.3.1 РПД, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Учебная аудитория для проведения групповых и индивидуальных консультаций	Специализированная мебель
Читальный зал Информационно-библиотечного центра ИБК УрГУПС - Аудитория для самостоятельной работы	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий, групповых и индивидуальных консультаций	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Технические средства обучения - Комплект мультимедийного оборудования

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) И

ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Эффективное освоение дисциплины предполагает регулярное посещение всех видов аудиторных занятий, выполнение плана самостоятельной работы в полном объеме и прохождение аттестации в соответствии с календарным учебным графиком. Обучающемуся рекомендуется ознакомиться со списком основной и дополнительной литературы и взять в библиотеке издания (необходимо иметь при себе персонифицированную электронную карту и уметь пользоваться электронным каталогом «ИРБИС»).Доступ к информационным ресурсам библиотеки и информационно-справочным системам сети «Интернет» организован в читальных залах библиотеки, в компьютерных классах, в помещениях для самостоятельной работы обучающихся со стационарных ПЭВМ, либо с личного ПЭВМ (ноутбука, планшетного компьютера или иного мобильного устройства) посредством беспроводного доступа при активации индивидуальной учетной записи. Пользование информационными ресурсами расширяет возможности освоения теоретического курса, выполнения самостоятельной работы и позволяет получить информацию для реализации творческих образовательных технологий. Комплект учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося. Методические материалы, разработанные для обеспечения образовательного процесса представлены в электронном каталоге УрГУПС. Для закрепления теоретического материала в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) размещены тестовые материалы. Число тренировочных попыток ограничено. Тестовые материалы сформированы в логической последовательности в соответствии с изученными темами. Совместная деятельность преподавателя и обучающихся по проверке выполнения мероприятий текущего контроля, предусмотренных рабочей программой дисциплины (модуля) организована в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru). Для корректной работы в системе обучающиеся в разделе "Личные сведения" должны ввести актуальный адрес своей электронной почты. Формы самостоятельной работы обучающихся по данной дисциплине разнообразны. Они включают в себя:- изучение теоретического материала (учебной, научной, методической литературы, материалов периодических изданий);- подготовку к занятиям, предусмотренным РПД, мероприятиям текущего контроля, промежуточной аттестации и т.д. Выполнять самостоятельную работу и отчитываться по ее результатам обучающийся должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности. При выполнении самостоятельной работы обучающемуся рекомендуется руководствоваться учебно-методическими материалами, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для самостоятельной работы по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".Перечень учебно-методических материалов (учебно-методического обеспечения) для самостоятельной работы обучающихся по дисциплине указан по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)", материалы размещены на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru).

При применении дистанционных образовательных технологий и электронного обучения освоение дисциплины (модуля) осуществляется в электронно-информационной образовательной среде (образовательная платформа электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru)) в рамках созданного курса, что позволяет реализовывать асинхронное и синхронное взаимодействие участников образовательных отношений.