ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

ФТД.В.02 Криптографические протоколы

рабочая программа дисциплины (модуля)

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

Учебный план 10.03.01 ИБ-2020.plx
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) "Организация и технология защиты информации (на транспорте)"

Направленность (профиль) направленность (профиль) N 2 "Организация и технология 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	РПД	УП	РПД
Лекции	8	8	8	8
Практические	10	10	10	10
Контактная работа	18	18	18	18
Итого ауд.	18	18	18	18
Сам. работа	18	18	18	18
Итого	36	36	36	36

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Основной целью дисциплины «Криптографические протоколы» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП	
Цикл (раздел) ОП:	ФТД.В

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)
Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач	
Знать:	
Уровень 1	основные задачи и понятия криптографии, требования основные характеристики криптографических протоколов
Уровень 2	модели криптографических протоколов и математические методы их исследования, принципы построения криптографических протоколов
Уровень 3	криптографические стандарты и методы их использования в информационных системах
Уметь:	
Уровень 1	пользоваться научно-технической литературой в области криптографии
Уровень 2	применять частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки
Уровень 3	применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
Владеть:	
Уровень 1	криптографической терминологией
Уровень 2	навыками использования типовых криптографических протоколов
Уровень 3	навыками использования ПЭВМ в анализе простейших шифров, навыками математического моделирования в криптографии

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
Знать:	
Уровень 1	классификацию защищаемой информации
Уровень 2	классификацию угроз защищаемой информации
Уровень 3	возможные методы и пути реализации угроз защищаемой информации
Уметь:	
Уровень 1	выявлять угрозы информационной безопасности объекта
Уровень 2	анализировать угрозы информационной безопасности объекта
Уровень 3	оценивать угрозы информационной безопасности объекта
Владеть:	
Уровень 1	-
Уровень 2	-
Уровень 3	-

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
Знать:	
Уровень 1	общие представления об основных задачах и понятий криптографии, требованиях к шифрам и основных характеристик шифров, моделях шифров и математических методах их исследования, принципах построения криптографических алгоритмов
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	применять частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки
Уровень 2	-
Уровень 3	-
Владеть:	
Уровень 1	криптографической терминологией, навыками использования типовых криптографических алгоритмов, навыками использования ПЭВМ в анализе простейших шифров, навыками математического моделирования в криптографии
Уровень 2	-
Уровень 3	-

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	ОПК-2 ОПК-7 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Э1	
1.2	Цифровые подписи. Цифровые подписи и шифрование. Генерация случайных и псевдослучайных последовательностей /Лек/	7	2	ОПК-2 ОПК-7 ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Э1	
1.3	Практический семинар /Пр/	7	5	ОПК-2 ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1Л3.1 Э1	Групповая дискуссия
1.4	Изучение учебной и научно-технической литературы по тематике раздела. Подготовка к практическому семинару /Ср/	7	6	ОПК-2 ОПК-7	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л3.1 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	ОПК-2 ОПК-7 ПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Э1	
2.2	Криптография с несколькими открытыми ключами. Разделение секрета. Совместное использование секрета /Лек/	7	2	ОПК-2 ОПК-7 ПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Э1	
2.3	Практический семинар /Пр/	7	5	ОПК-2 ОПК-7 ПК-1	Л1.1 Л1.3 Л2.1Л3.1 Э1	Групповая дискуссия
2.4	Изучение учебной и научно-технической литературы по тематике раздела. Подготовка к практическому семинару /Ср/	7	6	ОПК-2 ОПК-7	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л3.1 Л3.2 Э1	
2.5	Подготовка к промежуточной аттестации /Ср/	7	6	ОПК-2 ОПК-7 ПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л3.2 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	Бабаш А. В.	Криптографические методы защиты информации. Том 3: Учебно-методическое пособие	Москва: Издательский Центр РИО, 2014	http://znanium.com
Л1.2	Романьков В. А.	Введение в криптографию: Курс лекций	Москва: Издательство "ФОРУМ", 2018	http://znanium.com
Л1.3	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/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2018	http://znanium.com

Л2.2		Защита информации. Инсайд: специализированное отечественное периодическое издание	Издательский Дом «Афина»	https://elibrary.ru/title_about.asp?id=25917
Л2.3		Вестник УрФО. Безопасность в информационной сфере: специализированное отечественное периодическое издание	Изд-во ЮУрГУ	https://elibrary.ru/title_about.asp?id=32751
Л2.4		Безопасность информационных технологий: специализированное отечественное периодическое издание	Изд-во Национального исследовательского ядерного университета «МИФИ»	https://elibrary.ru/title_about.asp?id=8429
Л2.5		Information and Computer Security: специализированное зарубежное периодическое издание	Emerald	https://www.scopus.com/sourceid/21100421900?origin=resultslist
Л2.6		Information Security Journal: специализированное зарубежное периодическое издание	Taylor & Francis	https://www.scopus.com/sourceid/19700187807?origin=resultslist

Официальные, справочно-библиографические и специализированные, в том числе правовые нормативные акты и нормативные методические документы в области информационной безопасности при изучении данной дисциплины не используются

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/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
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/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

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.
Студенту 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 студентов 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.
Формы самостоятельной работы студентов по данной дисциплине разнообразны. Они включают в себя:
- изучение лекционного и дополнительного материала (учебной, научной, методической литературы, материалов периодических изданий);
- подготовку к занятиям, предусмотренных РПД, мероприятиям текущего контроля и промежуточной аттестации
Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности.
При выполнении самостоятельной работы студент должен руководствоваться методическими указаниями, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для СРС по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".
Перечень 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).