ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.Б.16 Криптографические методы защиты информации

рабочая программа дисциплины (модуля)

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

Учебный план 10.03.01 ИБ-2019.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) **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 36
самостоятельная работа 72

Часов контактной работы всего, в том числе: 37,8
аудиторная работа 36
текущие консультации по лабораторным занятиям 1,8

Промежуточная аттестация и формы контроля:
зачет 3

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Контактная работа	36	36	36	36
Итого ауд.	36	36	36	36
Сам. работа	72	72	72	72
Итого	108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Учебная дисциплина «Криптографические методы защиты информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления. Основной целью дисциплины «Криптографические методы защиты информации» 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:	Б1.Б

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:

Программно-аппаратные средства защиты информации
Безопасность сетей ЭВМ
Безопасность информационных процессов
Производственная практика (эксплуатационная практика)
Преддипломная практика
Комплексные системы защиты информации на транспорте
Защита информационных процессов на транспорте

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 к шифрам и основным характеристикам шифров
Уровень 2	модели шифров и математические методы их исследования, принципы построения криптографических алгоритмов
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 алгоритмов
Уровень 3	навыками использования ПЭВМ в анализе простейших шифров, навыками математического моделирования в криптографии

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, криптографических стандартов и их использовании в инфорационных системах
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	применять частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки, отечественные и зарубежные стандарты в области криптографических методов

	компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, пользование научно-технической литературой в области криптографии
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	основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования; принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах.
3.2	**Уметь:**
3.2.1	использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки; применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться научно-технической литературой в области криптографии.
3.3	**Владеть:**
3.3.1	криптографической терминологией; навыками использования типовых криптографических алгоритмов; 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. Введение в криптографию					
1.1	Место криптографии в сфере научных заний. Основные определения и историческая справка /Лек/	3	1	ОПК-2	Л1.1 Л1.2 Л1.3Л2.1 Э1	
1.2	Решение задач на тему "Методы и алгоритмы классической симметричной криптографии" /Лаб/	3	2	ОПК-2	Л1.1Л2.1Л3.2 Э2	Работа в группе, решение практико-ориентированных задач
1.3	Изучение лекционного материала по тематике раздела /Ср/	3	12	ОПК-2	Л1.1 Л1.3Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1	
	Раздел 2. Симметричные криптосистемы					
2.1	Симметричные криптосистемы. Шифры подстановок и перестановок /Лек/	3	2	ОПК-2	Л1.1 Л1.3Л2.1 Э1	
2.2	Характеристики открытых текстов. Вероятностный подход /Лек/	3	1	ОПК-2	Л1.1 Л1.3Л2.1 Э1	
2.3	Характеристики открытых текстов. Теоретико-информационный подход /Лек/	3	1	ОПК-2	Л1.1 Л1.3Л2.1 Э1	
2.4	Современные симметричные криптосистемы /Лек/	3	1	ОПК-2	Л1.1 Л1.3Л2.1 Э1	
2.5	Поточные шифры /Лек/	3	2	ОПК-2	Л1.1 Л1.3Л2.1 Э1	

2.6	Решение задач на тему "Симметричные поточные криптографические алгоритмы" /Лаб/	3	2	ОПК-2	Л1.1Л2.1Л3.2 Э1 Э2	Работа в группе, решение практико-ориентированных задач
2.7	Блочные шифры /Лек/	3	2	ОПК-2	Л1.1 Л1.3Л2.1 Э1	
2.8	Решение задач на тему "Симметричные блочные криптографические алгоритмы" /Лаб/	3	2	ОПК-2	Л1.1Л2.1Л3.2 Э1 Э2	Работа в группе, решение практико-ориентированных задач
2.9	Изучение лекционного материала по тематике раздела /Ср/	3	12	ОПК-2	Л1.1 Л1.3Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1	
	Раздел 3. Асимметричные криптосистемы					
3.1	Математические основы асимметричной криптографии /Лек/	3	2	ОПК-2	Л1.1 Л1.3Л2.1 Л2.2 Э1	
3.2	Теоремы асимметричной криптографии /Лек/	3	2	ОПК-2	Л1.1 Л1.3Л2.1 Л2.2 Э1	
3.3	Аутентификация инормации. Подверждение целостности информации /Лек/	3	1	ОПК-2	Л1.1 Л1.3Л2.1 Э1	
3.4	Аутентификация информации. Подтверждение подлинности источника информации /Лек/	3	1	ОПК-2	Л1.1 Л1.3Л2.1 Э1	
3.5	Управление ключами /Лек/	3	2	ОПК-2	Л1.1 Л1.3Л2.1 Э1	
3.6	Решение задач на тему "Методы и алгоритмы асимметричной криптографии" /Лаб/	3	2	ОПК-2	Л1.1Л2.1Л3.2 Э1 Э2	Работа в группе, решение практико-ориентированных задач
3.7	Изучение лекционного материала по тематике раздела /Ср/	3	12	ОПК-2	Л1.1 Л1.3Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Э1	
	Раздел 4. Средства криптографической защиты информации					
4.1	Аппаратно-программный комплекс шифрования "Континент" /Лаб/	3	2	ПК-1	Л1.1Л2.1Л3.1 Э1	Работа в группе, решение практико-ориентированных задач
4.2	Тест портов персонального компьютера для работы с АПКШ "Континент" /Лаб/	3	2	ПК-1	Л1.1Л2.1Л3.1 Э1	Работа в группе, решение практико-ориентированных задач
4.3	Организация межсетевого взаимодейтсвия при помощи АПКШ "Континент" /Лаб/	3	2	ПК-1	Л1.1Л2.1Л3.1 Э1	Работа в группе, решение практико-ориентированных задач
4.4	Организация межсетевого экранирования при помощи АПКШ "Континент" /Лаб/	3	4	ПК-1	Л1.1Л2.1Л3.1 Э1	Работа в группе, решение практико-ориентированных задач
4.5	Подготовка к лабораторным работам /Ср/	3	18	ПК-1	Л1.1Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л3.1 Э1	

4.6	Подготовка к промежуточной аттестации /Ср/	3	18	ОПК-2 ПК-1	Л1.1 Л1.3Л2.1Л3.1 Л3.2 Э1 Э2	

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	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2018	http://znanium.com
Л1.2	Ларин Д.А.	Криптографическая деятельность в России от Полтавы до Бородина: Монография	Москва: Издательский Центр РИО, 2018	http://znanium.com
Л1.3	Зырянова Т. Ю.	Криптографические методы защиты информации: курс 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	Гашков С. Б., Применко Э. А., Черепнев М. А.	Криптографические методы защиты информации: учебное пособие для студентов вузов, обучающихся по направлению "Прикладная математика и информатика" и "Информационные технологии"	Москва: Академия, 2010	
Л2.2	Новиков Ф. А.	Дискретная математика: для бакалавров и магистров : рекомендовано УМО по университетскому политехническому образованию в качестве учебника для студентов вузов, обучающихся по направлению подготовки "Системный анализ и управление"	Санкт-Петербург: Питер, 2013	
Л2.3		Защита информации. Инсайд: специализированное отечественное периодическое издание	Издательский Дом «Афина»	https://elibrary.ru/title_about.asp?id=25917
Л2.4		Вестник УрФО. Безопасность в информационной сфере: специализированное отечественное периодическое издание	Изд-во ЮУрГУ	https://elibrary.ru/title_about.asp?id=32751
Л2.5		Безопасность информационных технологий: специализированное отечественное периодическое издание	Изд-во Национального исследовательского ядерного университета «МИФИ»	https://elibrary.ru/title_about.asp?id=8429
Л2.6		Information and Computer Security: специализированное зарубежное периодическое издание	Emerald	https://www.scopus.com/sourceid/21100421900?origin=resultslist

Л2.7		Information Security Journal: специализированное зарубежное периодическое издание	Taylor & Francis	https://www.scopus.com/sourceid/19700187807?origin=resultslist

Официальные, справочно-библиографические, 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	Маслов А. К., Зырянова Т. Ю.	АПКШ «Континент 3.5»: методические рекомендации для выполнения лабораторных работ по дисциплине «Криптографические методы защиты информации» для студентов направления подготовки 10.03.01 «Информационная безопасность»	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 методы защиты информации: сборник задач и упражнений для студентов направления подготовки 10.03.01 «Информационная безопасность»	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	Среда электронного обучения BlackBoard Learn (http://bb.usurt.ru)
Э2	Официальный сайт Международной студенческой олимпиады по криптографии (https://nsucrypto.nsu.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
Лаборатория "Программно-аппаратные средства защищенных информационных систем". Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий	Специализированная мебель Лабораторное оборудование: Аппаратно-программный комплекс шифрования "Континент" Программно-аппаратный комплекс защиты информации ViPNet Custom, включающий в том числе криптографические средства" Оборудование для центра защиты информации, включающее в том числе интегрированную систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппаратные средства аутентификации пользователя 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 Технические средства обучения - Комплект мультимедийного оборудования
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

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
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

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).