ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.Б.19 Методы и средства криптографической защиты информации

рабочая программа дисциплины (модуля)

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

Учебный план 10.03.01 ИБ-2023.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) **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 54
самостоятельная работа 54
часов на контроль 36

Промежуточная аттестация и формы контроля:
экзамен 4

Часов контактной работы всего, в том числе: 60,1
аудиторная работа 54
текущие консультации по лабораторным занятиям 1,8
текущие консультации по практическим занятиям 1,8
консультации перед экзаменом 2
прием экзамена 0,5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Практические	18	18	18	18
Элект	36	36	36	36
Итого ауд.	54	54	54	54
Контактная работа	90	90	90	90
Сам. работа	54	54	54	54
Часы на контроль	36	36	36	36
Итого	180	180	180	180

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины: приобретение знаний и умений в области криптографической защиты информации; формирование мировоззрения и системного мышления.
1.2	Задачи дисциплины: Изложение основополагающих принципов защиты информации с помощью криптографических методов; применение на практике криптоглафических методов и средств защиты информации.

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)
Комплексные системы защиты информации на транспорте

Защита информационных процессов на транспорте
Производственная практика (преддипломная практика)
Подготовка к процедуре защиты и защита выпускной квалификационной работы
Подготовка к сдаче и сдача государственного экзамена

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
ОПК-2.3: Осуществляет меры противодействия нарушениям информационной безопасности с использованием различных программных и аппаратных средств защиты информации
ОПК-2.1: Знает аппаратные средства вычислительной техники, принципы построения информационных систем и сетей, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-5.2: Применяет нормативные правовые акты и нормативные методические документы по информационной безопасности в профессиональной деятельности
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;
ОПК-9.2: Применяет отечественные и зарубежные стандартизированные алгоритмы в области методов криптографической защиты информации
ОПК-9.1: Знает основные задачи и понятия криптографии, принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах
ОПК-9.3: Применяет программные и программно-аппаратные средства криптографической защиты информации для решения задач профессиональной деятельности
ОПК-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ОПК(п)-2.3.3: Разрабатывает, внедряет и сопровождает комплекс мер по обеспечению безопасности объектов защиты различных видов

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/	4	1	ОПК-9.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
1.2	Решение задач на тему "Методы и алгоритмы классической симметричной криптографии" /Пр/	4	4	ОПК-9.2	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	Работа в группе. Изучение алгоритмов
1.3	Изучение лекционного материала по тематике раздела /Ср/	4	10	ОПК-9.1 ОПК-9.2	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
	Раздел 2. Симметричные криптосистемы					
2.1	Симметричные криптосистемы. Шифры подстановок и перестановок /Лек/	4	2	ОПК-9.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
2.2	Характеристики открытых текстов. Вероятностный подход /Лек/	4	1	ОПК-9.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
2.3	Характеристики открытых текстов. Теоретико-информационный подход /Лек/	4	1	ОПК-9.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
2.4	Современные симметричные криптосистемы /Лек/	4	1	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-2.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
2.5	Поточные шифры /Лек/	4	2	ОПК-9.1 ОПК-9.2	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
2.6	Решение задач на тему "Симметричные поточные криптографические алгоритмы" /Пр/	4	4	ОПК-9.2	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	Работа в группе. Изучение алгоритмов
2.7	Блочные шифры /Лек/	4	2	ОПК-9.1 ОПК-9.2	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
2.8	Решение задач на тему "Симметричные блочные криптографические алгоритмы" /Пр/	4	4	ОПК-9.2	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	Работа в группе. Изучение алгоритмов
2.9	Изучение лекционного материала по тематике раздела /Ср/	4	10	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-2.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	

	Раздел 3. Асимметричные криптосистемы					
3.1	Математические основы асимметричной криптографии /Лек/	4	2	ОПК-9.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
3.2	Теоремы асимметричной криптографии /Лек/	4	2	ОПК-9.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
3.3	Аутентификация инормации. Подверждение целостности информации /Лек/	4	1	ОПК-5.2 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
3.4	Аутентификация информации. Подтверждение подлинности источника информации /Лек/	4	1	ОПК-5.2 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
3.5	Управление криптографическими ключами /Лек/	4	2	ОПК-5.2 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
3.6	Решение задач на тему "Методы и алгоритмы асимметричной криптографии" /Пр/	4	6	ОПК-9.2	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	Работа в группе. Изучение алгоритмов
3.7	Изучение лекционного материала по тематике раздела /Ср/	4	10	ОПК-5.2 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
	Раздел 4. Средства криптографической защиты информации					
4.1	Аппаратно-программный комплекс шифрования "Континент" /Лаб/	4	4	ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
4.2	Тест портов персонального компьютера для работы с АПКШ "Континент" /Лаб/	4	4	ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
4.3	Организация межсетевого взаимодейтсвия при помощи АПКШ "Континент" /Лаб/	4	4	ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
4.4	Организация межсетевого экранирования при помощи АПКШ "Континент" /Лаб/	4	6	ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
4.5	Подготовка к лабораторным работам /Ср/	4	10	ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
4.6	Взаимодействие с обучающимися по вопросам текущего контроля в электронной информационно-образовательной среде: выполнение контрольных заданий и промежуточных тестов /Элект/	4	36	ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	
4.7	Подготовка к промежуточной аттестации /Ср/	4	14	ОПК-5.2 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	

4.8	Промежуточная аттестация /Экзамен/	4	36	ОПК-5.2 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-2.1 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине (модулю), состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине. Оценочные материалы размещаются 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 методы защиты информации: курс лекций для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru

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□, 2020	http://znanium.com

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	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
Л3.2	Зырянова Т. Ю.	Криптографические методы защиты информации: методические рекомендации по организации самостоятельной работы студентов по дисциплине «Криптографические методы защиты информации» для 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	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». Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (практических занятий, лабораторных занятий), курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Специализированная мебель Лабораторное оборудование: Аппаратно-программный комплекс шифрования "Континент" Программно-аппаратный комплекс защиты информации ViPNet Custom, включающий в том числе киптографические средства" Оборудование для центра защиты информации, включающее в том числе интегрированную систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппартные средства аутетификации 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. 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. 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).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)".
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.