Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1157413	Методы и средства криптографической защиты информации

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Безопасность компьютерных систем	**Код ОП** 1. 10.03.01/33.01
Направление подготовки 1. Информационная безопасность	**Код направления и уровня подготовки** 1. 10.03.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Домуховский Николай Анатольевич	без ученой степени, без ученого звания	Старший преподаватель	алгебры и фундаментальной информатики
2	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Методы и средства криптографической защиты информации

1.1. Аннотация содержания модуля

В модуле «Методы и средства криптографической защиты информации» изучаются криптографических алгоритмы построения и применения для обеспечения защиты информации.

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Методы и средства криптографической защиты информации	4
	ИТОГО по модулю:	4

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Методы и средства криптографической защиты информации
Постреквизиты и кореквизиты модуля	1. Методы и средства криптографической защиты информации 2. Методы и средства криптографической защиты информации

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Методы и средства криптографической защиты информации	ПК-7 - Способен применять средства криптографической и технической защиты информации для решения задач	З-1 - Различать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в телекоммуникационных системах З-2 - Различать особенности применения криптографических методов и средств

	профессиональной деятельности	защиты информации для защиты систем электронного документооборота У-1 - Анализировать программные модели средств криптографической защиты информации П-1 - Иметь опыт использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной и очно-заочной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы и средства криптографической защиты информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Домуховский Николай Анатольевич	без ученой степени, без ученого звания	Старший преподаватель	алгебры и фундаментальной информатики
2	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _6_ от _26.05.2023_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Домуховский Николай Анатольевич, Старший преподаватель, алгебры и фундаментальной информатики**
- **Поршнев Сергей Владимирович, Профессор, Учебно-научный центр ”Информационная безопасность”**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Введение в криптографию	Краткая история криптографии. Основные термины и определения. Классификация криптографических алгоритмов. Классические шифры. Совершенная криптостойкость. Правило Керкгоффса. Принципы Шеннона.
2	Симметричные криптосистемы	Симметричные криптосистемы. Шифры подстановок и перестановок. Характеристики открытых текстов. Вероятностный подход. Теоретико- информационный подход. Блочные шифры. Примитивные операции (XOR, сложение и вычитание по модулю 2□, циклический сдвиг, конкатенация, кодирование). Сеть Фейстеля, SP-сеть. Стандарт шифрования DES. Стандарт шифрования ГОСТ 28147-89, ГОСТ 34.12-2018 («Кузнечик», «Магма»). Стандарт шифрования AES. Режимы работы блочных шифров. Аутентифицированное шифрование (AEAD) . Легковесная криптография. Шифр Present.

		Поточные шифры. Регистры сдвига с обратной связью. Линейные рекуррентные Последовательности. Шифр RC4. Алгоритм A5/1.
3	Асимметричные криптосистемы	Математические основы асимметричной криптографии (булевы функции, группы, конечные поля, дискретный логарифм). Теоремы асимметричной криптографии. Алгоритм Диффи-Хеллмана, Криптосистема RSA. Криптосистема Эль-Гамаля (шифрование). Эллиптические кривые. Алгоритм Диффи-Хеллмана на эллиптических кривых. Инфраструктура открытых ключей.
4	Хэш-функции	Хэш-функции. Стандарт ГОСТ Р 34.11-2012 («Стрибог»). Алгоритм SHA (1, 2, 3). Аутентификация информации. Коды аутентификации сообщений (CBC-MAC, HMAC, GMAC).
5	Электронная подпись	Электронная подпись. Стандарт ГОСТ 34.10-2018. Digital Signature Algorithm (DSA), схема Эль-Гамаля (подпись).
6	Криптоанализ	Введение в криптоанализ. Парадокс дней рождения. Метод «встречи посередине». Линейный криптоанализ. Дифференциальный криптоанализ. Криптоанализ на связанных ключах. Нелинейные булевы функции в Криптографии.
7	Криптографические протоколы и алгоритмы	Схемы разделения секрета. Управление криптографическими ключами. Доказательство с нулевым разглашением, протокол Фиата-Шамира. Блокчейн, криптографические протоколы VPN, TLS.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательск	Технология формирования уверенности и готовности к	ПК-7 - Способен применять средства криптографической и технической	П-1 - Иметь опыт использования и исследования криптографически

	ая целенаправленная работа с информацией для использования в практических целях	самостоятельной успешной профессиональной деятельности Технология самостоятельной работы	защиты информации для решения задач профессиональной деятельности	х средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации

Электронные ресурсы (издания)

1. Кирпичников, А. П.; Криптографические методы защиты компьютерной информации : учебное пособие.; Казанский национальный исследовательский технологический университет (КНИТУ), Казань; 2016; https://biblioclub.ru/index.php?page=book&id=560536 (Электронное издание)

2. Гатченко, , Н. А.; Криптографическая защита информации; Университет ИТМО, Санкт-Петербург; 2012; http://www.iprbookshop.ru/68658.html (Электронное издание)

3. Кукина, , Е. Г.; Введение в криптографию : сборник задач и упражнений.; Омский государственный университет им. Ф.М. Достоевского, Омск; 2013; http://www.iprbookshop.ru/24876.html (Электронное издание)

Печатные издания

1. Фергюсон, Фергюсон Н., Шнайер, Шнайер Б., Селина, Н. Н., Журавлев, А. В.; Практическая криптография; Диалектика, Москва ; Санкт-Петербург ; Киев; 2005 (17 экз.)

2. Тилборг, ван Х. К. А, ван Х. К. А., Ананичев, Д. С., Коряков, И. О.; Основы криптологии. Профессиональное руководство и интерактивный учебник; Мир, Москва; 2006 (1 экз.)

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Среда электронного обучения BlackBoard Learn (http://bb.usurt.ru)

Официальный сайт Международной студенческой олимпиады по криптографии (https://nsucrypto.nsu.ru)

Среда вычислений Wolfram alpha (https://www.wolframalpha.com/)

Справочно-правовая система КонсультантПлюс

Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)

Международная реферативная база данных научных изданий Scopus

Международная реферативная база данных научных изданий eLIBRARY.RU

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc Office Professional 2003 Win32 Russian CD-ROM
2	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с	Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc Office Professional 2003 Win32 Russian CD-ROM

		санитарными правилами и нормами Подключение к сети Интернет	
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Windows Server Datacenter 2012R2 Single MVL 2Proc A Each Academic
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Windows Server Datacenter 2012R2 Single MVL 2Proc A Each Academic
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Доска аудиторная	Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc Office Professional 2003 Win32 Russian CD-ROM

		Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	