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
1157330	Криптографические методы защиты информации

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Математические методы защиты информации	**Код ОП** 1. 10.05.01/22.01
Направление подготовки 1. Компьютерная безопасность	**Код направления и уровня подготовки** 1. 10.05.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Ананичев Дмитрий Сергеевич	кандидат физико-математических наук, доцент	Доцент	алгебры и фундаментальной информатики

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Криптографические методы защиты информации

1.1. Аннотация содержания модуля

Модуль состоит из одной дисциплины: «Основы построения защищённых баз данных». Цель дисциплины – освоение принципов проектирования и управления защищенными базами данных, что позволит сформировать необходимую базу для изучения дисциплин продолжающих данное направление (проектирование интерфейсов, анализ данных, хранилища данных), даст необходимые знания и навыки работы с современными системами разработки на основе различных программных продуктов

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	Криптографические методы защиты информации	7
	ИТОГО по модулю:	7

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Не предусмотрены
Постреквизиты и кореквизиты модуля	1. Средства и методы 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
Криптографические методы защиты информации	ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения	З-1 - Описывать математические методы, необходимые для решения задач профессиональной деятельности У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности

	задач профессиональной деятельности	П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности
	ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	З-1 - Описывать основные перспективы развития науки и техники в области профессиональной деятельности У-1 - Формулировать задачи исследования, выбирать методы и средства их решения П-1 - Иметь практический опыт решения теоретических задач в областях математики
	ОПК-10 - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	З-1 - Классифицировать и дать общую характеристику основных типов криптографических протоколов З-3 - Описывать способы решения основных задач современной криптографии З-4 - Описывать основные конструкции, используемые в построении современных симметричных шифров и криптографических хеш-функций, и их свойства З-5 - Описывать устройство современных блочных шифров, поточных шифров и криптографических хэш-функций З-6 - Сформулировать основные понятия современной криптологии У-1 - Оценивать механизмы защиты, реализующие криптографические протоколы У-2 - Оценивать и контролировать эффективность криптографических протоколов У-3 - Производить анализ шифра на совершенство и имитостойкость У-4 - Реализовывать алгоритмы для работы с современными асимметричными криптосистемами и подписями на их основе У-5 - Реализовывать алгоритмы идентификации с нулевым разглашением П-1 - Разрабатывать компоненты криптографических протоколов

		П-2 - Иметь практический опыт криптоанализа базовых исторических шифров, и выработки пар ключей в ассиметричных криптосистемах
	ОПК-18 - Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	З-3 - Описывать понятия временной и пространственной сложности алгоритма, его зависимость от модели вычисления З-5 - Классифицировать и дать общую характеристику основных типов криптографических протоколов З-7 - Описывать способы решения основных задач современной криптографии З-8 - Описывать основные конструкции, используемые в построении современных симметричных шифров и криптографических хеш-функций, и их свойства З-9 - Описывать устройство современных блочных шифров, поточных шифров и криптографических хэш-функций З-10 - Сформулировать основные понятия современной криптологии У-1 - Оценивать механизмы защиты, реализующие криптографические протоколы У-3 - Производить анализ шифра на совершенство и имитостойкость У-4 - Реализовывать алгоритмы для работы с современными асимметричными криптосистемами и подписями на их основе У-5 - Реализовывать алгоритмы идентификации с нулевым разглашением П-1 - Иметь практический опыт деятельности по оценке вычислительной сложности алгоритмических проблем П-2 - Разрабатывать компоненты криптографических протоколов П-3 - Иметь практический опыт криптоанализа базовых исторических шифров, и выработки пар ключей в ассиметричных криптосистемах

	ОПК-19 - Способен разрабатывать и анализировать математические модели механизмов защиты информации	З-1 - Сформулировать основные понятия современной криптологии З-2 - Классифицировать и дать общую характеристику основных типов криптографических протоколов З-3 - Описывать способы решения основных задач современной криптографии З-4 - Описывать основные конструкции, используемые в построении современных симметричных шифров и криптографических хеш-функций, и их свойства З-5 - Описывать устройство современных блочных шифров, поточных шифров и криптографических хэш-функций У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности
	ПК-3 - Способен проводить анализ безопасности компьютерных систем	З-3 - Объяснять криптографические методы защиты информации
	ПК-5 - Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	З-16 - Описывать криптографические алгоритмы и особенности их программной реализации

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические методы защиты информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Ананичев Дмитрий Сергеевич	кандидат физико-математических наук, доцент	Доцент	алгебры и фундаментальной информатики

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Ананичев Дмитрий Сергеевич, Доцент, алгебры и фундаментальной информатики**

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
Р1.1	История, основные понятия и задачи криптографии.	Способы защиты информации (защита носителя, стеганография, криптография). Понятие криптоситемы (шифра). Шифр перестановки. Шифр «скитала». Маршрутные транспозиции. Столбцовые перестановки. Решетки Кардано и Ришелье. Шифр замены. Квадрат Полибия. Шифр Цезаря. Многоалфавитная замена. Диск Алберти. Таблица Тритемия и шифр Виженера. Самоключевой шифр Кардано. Диаграммный шифр Уитстона-Плэйфера. Блочные шифры Хилла. Шифр Вернама (одноразовый щит). Дисковые шифраторы. Понятие криптоанализа. Классификация атак. Частотный криптоанализ. Криптоанализ шифра замены, шифра перестановки и шифра Виженера (метод Казиски и методы Фридмана).
Р1.2	Теория Шеннона.	Информация и энтропия, свойства энтропии. Условная энтропия. Взаимная информация. Взаимная информация между открытым текстом и криптограммой. Остаточная

		неопределенность ключа и сообщения. Совершенная секретность (абсолютная стойкость) шифра. Описание эндоморфных совершенных криптосистем. Типичные и редкие последовательности в стационарной модели открытого текста. Избыточность языка. Расстояние единственности шифра. Имитостойкость шифра.
Р1.3	Помехоустойчивые шифры.	Эндоморфные шифры не распространяющие искажений типа “замена” (Теорема Маркова). Эндоморфные шифры не распространяющие искажений типа “пропуск” (Теорема Глухова).
Р1.4	Блочные шифры.	Понятие. Усложнение и рассеивание, Конструкция Файстеля. DES. ГОСТ-28147-89. IDEA. AES. Понятия линейного и дифференциального криптоанализа. Уровень нелинейности булевой функции. Булевы функции, удовлетворяющие строгому лавинному критерию. Режимы использования блочных шифров.
Р2.1	Поточные шифры.	Общая схема поточного шифра. Требования к управляющему блоку. Линейные регистры сдвига и линейные рекуррентные последовательности (ЛРП). Характеристическая матрица и характеристический многочлен однородной ЛРП. Финально-периодические последовательности. Вычисление минимального многочлена и периода ЛРП. ЛРП максимального периода. Их статистические свойства. Усложнения линейных регистров сдвига. Шифр А5. Алгоритм RC4.
Р2.2	Асимметричные криптосиситемы.	Новые задачи криптографии и недостаточность традиционных криптосистем. Общие принципы построения криптосистем с открытым ключом. Создание односторонней функции ловушки из сложной задачи на примере рюкзач- 7 ной криптосистемы. RSA: построение, связь параметров, бит-безопасность, известные виды атак. КС Рабина (Доказательство надежности). КС Блюма-Голдвассер, КС Голдвассер-Микали, КС Мак-Элиса. КС Эль-Гамаля. Подписи: RSA, Эль-Гамаля, Ниберга-Руппеля, DSS,

		ГОСТ 34.10-94, ГОСТ 34.10-2012.
Р3.1	Хеш-функции.	Понятие и мотивы использования в подписи. Требования к криптографической хеш-функции. Из взаимосвязь. Итерационная схема построения. Усиление Меркля-Дамгарда, конструкции Матиаса-Мейера-Осеаса, Девиса-Мейера и Миягучи-Пренеля. Примеры: MDC-2,MDC-4, MD4,MD5, SHA, ГОСТ Р 34.11-94. Парадокс дней рождений и предельная устойчивость к коллизиям. Атаки на криптографические хеш-функции. Проблема защиты целостности и способы ее решения. Ключевые хеш-функции. Способы построения ключевых хеш-функций из бесключевых.
Р3.2	Идентификация.	Протокол идентификации. Пароли. Многоразовые: атаки, правила использования, способы хранения. Одноразовые: обновляемый, запасаемые, схема Лампорта. Проблемы при использовании. Идентификация типа запрос-ответ. Классификация по требованиям и применяемым средствам. Атаки, роль меток времени и случайных чисел. Протоколы с нулевым разглашением. Протокол Фиата-Шамира. Протокол Гвиллоу-Квискватера. Протокол Шнорра. Протокол без установки.
Р3.3	Распределение ключей.	Распределение ключей с помощью симметричных криптосистем. Бесключевой протокол Шамира. Распределение ключей с помощью асимметричных криптосистем. Роль доверенных центров. X.509. STS. Распределение ключей Диффи-Хеллмана. Атаки с противником посередине. Протоколы Мацумото-Такашима-Имаи. Предварительное распределение ключей в сети. Схема Блома. Теорема Блома. Схема на основе пересечений множеств. Оценка параметров на основе леммы Шпернера.
Р3.4	Разделение секрета.	Задача разделения секрета. Структура доступа и схема разделения секрета. Общая конструкция и матричная форма схемы разделения секрета. Пороговые схемы. Схема Шамира. Пороговые схемы с лгунами. Визуальное

		разделение секрета. Примеры. Проблема расширяющего множителя. Конструкция на основе квадратичных вычетов.

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-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-3 - Способен проводить анализ безопасности компьютерных систем	З-3 - Объяснять криптографические методы защиты информации

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Электронные ресурсы (издания)

1. Аграновский, А. В.; Практическая криптография: алгоритмы и их программирование : учебное пособие.; СОЛОН-ПРЕСС, Москва; 2009; https://biblioclub.ru/index.php?page=book&id=117663 (Электронное издание)

Печатные издания

1. Тилборг, Х. К. А. ван, Хенк К. А. ван, Коряков, И. О., Ананичев, Д. С.; Основы криптологии. Профессиональное руководство и интерактивный учебник; Мир, Москва; 2006 (51 экз.)

2. Баричев, С. Г., Гончаров, В. В., Серов, Р. Е.; Основы современной криптографии : Учеб. курс.; Горячая линия-Телеком, Москва; 2002 (15 экз.)

Профессиональные базы данных, информационно-справочные системы

Menezes A., van Oorschot P. Handbook of cryptography. CRC Press, 1997.

http://math.fau.edu/bkhadka/Syllabi/A%20handbook%20of%20applied%20cryptography.pdf

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

Общероссийский математический портал http://www.mathnet.ru/

Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/

Сайт издательства Elsevier http://www.sciencedirect.com/

Сайт кафедры: http://kma.imkn.urfu.ru

Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические методы 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 Периферийное устройство Подключение к сети Интернет	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome
2	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
3	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
4	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		соответствии с количеством студентов Подключение к сети Интернет	Свободное ПО:Google Crome
5	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**