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
1159156	Информационная безопасность и цифровая культура

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Метрология и метрологическое обеспечение 2. Управление исследованиями и разработками	**Код ОП** 1. 27.03.01/33.01 2. 27.03.05/33.01
Направление подготовки 1. Стандартизация и метрология; 2. Инноватика	**Код направления и уровня подготовки** 1. 27.03.01; 2. 27.03.05

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Островский Андрей Борисович	без ученой степени, без ученого звания	Старший преподаватель	астрономии, геодезии, экологии и мониторинга окружающей среды

Согласовано:

Управление образовательных программ Е.С. Комарова

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Информационная безопасность и цифровая культура

1.1. Аннотация содержания модуля

В курсе «Информационная безопасность и цифровая культура» рассматриваются основные методы защиты информации. Основное внимание уделяется современным криптографическим методам и протоколам их корректного использования. Студенты знакомятся с математическими основами современной криптографии, изучают классические и современные симметричные и асимметричные криптосистемы. Студенты получают навыки использования безопасных протоколов обмена информацией, распределения ключей и формирования цифровых подписей. Кроме того, у студентов формируются навыки цифровой культуры.

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	Информационная безопасность и цифровая культура	3
	ИТОГО по модулю:	3

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Информационные технологии и сервисы 2. Основы информатики
Постреквизиты и кореквизиты модуля	Не предусмотрены

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
Информационная безопасность и цифровая культура	УК-1 - Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач, в	З-3 - Объяснять основные принципы критического мышления, методы анализа и оценки достижений современной цивилизации, включая достижения глобальной цифровизации

	том числе в цифровой среде	З-7 - Излагать принципы и обосновывать методы системного подхода для постановки целей, задач и реализации основных стадий проектной деятельности, в том числе с использованием цифровых инструментов У-2 - Критически анализировать информацию, формировать собственное мнение и формулировать аргументы для защиты своей позиции У-3 - Определять достоверность и обоснованность выводов, выявлять и анализировать типовые ошибки в рассуждениях и когнитивные искажения в работе с информацией У-5 - Критически оценивать надежность источников информации в условиях неопределенности и избытка/недостатка информации для решения поставленных задач, в том числе в цифровой среде У-7 - Оценивать достижения современной цивилизации, основные тенденции общественного и научно-технического развития и глобальной цифровизации, используя методы критического анализа П-2 - Определять пути решения поставленных задач, в том числе в цифровой среде, опираясь на методики поиска, системного анализа и коррекции информации П-6 - Работая в команде или самостоятельно решать поставленные задачи проектной деятельности на основе системного анализа и с использованием цифровых инструментов Д-2 - Демонстрировать умение нестандартно мыслить, в том числе в новой цифровой парадигме

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность и цифровая культура

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Островский Андрей Борисович	без ученой степени, без ученого звания	Старший преподаватель	астрономии, геодезии, экологии и мониторинга окружающей среды

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _3_ от _17.03.2022_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Островский Андрей Борисович, Старший преподаватель, астрономии, геодезии, экологии и мониторинга окружающей среды**

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	Введение	Информационная безопасность. Общие вопросы. Основные понятия. Терминология.
Р2	Математические основы	Теория информации. Энтропия и неопределенность. Норма языка. Безопасность криптосистемы. Теория сложности. Теория чисел. Арифметика вычетов. Обратные значения по модулю. Методы вычисления обратных величин. Малая теорема Ферма. Функция Эйлера. Китайская теорема об остатках. Генерация простого числа.
Р3	Протоколы	Передача информации с использованием симметричной криптографии. Однонаправленные функции. Однонаправленные хэш-функции. Передача информации с использованием криптографии с открытыми ключами. Цифровые подписи. Генерация случайных и псевдослучайных последовательностей. Обмен ключами. Удостоверение подлинности. Криптография с несколькими открытыми ключами. Разделение секрета. Совместное использование секрета. Криптографическая защита баз данных. Управление ключами. Генерация ключей. Нелинейные пространства ключей. Передача ключей. Проверка ключей. Использование ключей. Время жизни ключей. Управление открытыми ключами.
Р4	Классические симметричные криптосистемы	Классификация криптографических методов. Перестановочные шифры. Подстановочные шифры. Системы подстановок.

Р5	Современные симметричные криптосистемы	Криптосистемы на основе сети Фейстеля. Стандарт шифрования данных DES. Безопасность DES. Варианты DES. ГОСТ 28147-89. Стандарт AES.
Р6	Типы алгоритмов и криптографические режимы	Режим электронной шифровальной книги. Режим сцепления блоков шифра. Потоковые шифры. Самосинхронизирующиеся потоковые шифры. Режим обратной связи по шифру. Синхронные потоковые шифры. Режим выходной обратной связи. Выбор режима шифра.
Р7	Алгоритмы с открытыми ключами	Безопасность алгоритмов с открытыми ключами. Алгоритмы «рюкзака». Алгоритм RSA. Однонаправленная хэш-функция SHA-1.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Воспитание навыков жизнедеятельности в условиях глобальных вызовов и неопределенностей	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	УК-1 - Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач, в том числе в цифровой среде	З-3 - Объяснять основные принципы критического мышления, методы анализа и оценки достижений современной цивилизации, включая достижения глобальной цифровизации У-7 - Оценивать достижения современной цивилизации, основные тенденции общественного и научно-технического развития и глобальной цифровизации, используя методы критического анализа

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Информационная безопасность и цифровая культура

Электронные ресурсы (издания)

1. Бабенко, Л. И.; Параллельные алгоритмы для решения задач защиты информации : монография.; Горячая линия – Телеком, Москва; 2014; https://biblioclub.ru/index.php?page=book&id=466903 (Электронное издание)

2. Петров, , А. А.; Компьютерная безопасность. Криптографические методы защиты; Профобразование, Саратов; 2019; http://www.iprbookshop.ru/87998.html (Электронное издание)

Печатные издания

1. Бабенко, Л. К.; Параллельные алгоритмы для решения задач защиты информации : [монография].; Горячая линия - Телеком, Москва; 2014 (3 экз.)

2. Петров, А. А.; Компьютерная безопасность. Криптографические методы защиты; ДМК, Москва; 2000 (6 экз.)

3. Васильев, В. И.; Интеллектуальные системы защиты информации : учебное пособие для студентов вузов, обучающихся по специальности "Комплексное обеспечение информационной безопасности автоматизированных систем".; Машиностроение, Москва; 2013 (5 экз.)

4. Де Касто, В.; Просто криптография; Страта, Санкт-Петербург; 2014 (2 экз.)

5. Шнайер, Шнайер Б., Диффи, У., Семьянов, В. П.; Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си; Триумф, Москва; 2003 (5 экз.)

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

7. Соколов, А. В., Степанюк, О. М.; Защита от компьютерного терроризма : Справ. пособие.; БХВ-Петербург : Арлит, Санкт-Петербург; 2002 (2 экз.)

8. Ярочкин, В. И.; Информационная безопасность : учебник для студентов вузов, обучающихся по гуманитар. и соц.-экон. специальностям.; Академический Проект : Трикста, Москва; 2005 (16 экз.)

9. Гринберг, А. С., Горбачев, Н. Н., Тепляков, А. А.; Защита информационных ресурсов государственного управления : Учеб. пособие для студентов вузов, обучающихся по специальностям "Информатика" и "Гос. и муницип. упр. ".; ЮНИТИ-ДАНА, Москва; 2003 (11 экз.)

Профессиональные базы данных, информационно-справочные системы

1. ADS. http://adsabs.harvard.edu/abstract_service.html

2. SCIRUS. http://www.scirus.com/?PTS/

3. Электронная научная библиотека. https://elibrary.ru

4. Университетская библиотека онлайн. http://biblioclub.ru

5. Зональная научная библиотека УрФУ. URL: http://lib.urfu.ru

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

1. Российская государственная библиотека. URL: http://www.rsl.ru

2. Государственная публичная научно-техническая библиотека России. URL: http://www.gpntb.ru

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Информационная безопасность и цифровая культура

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 Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	Office Professional 2003 Win32 Russian CD-ROM Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся	Office Professional 2003 Win32 Russian CD-ROM Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES