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
1156492	Основы компьютерной безопасности

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Математическое обеспечение и администрирование информационных систем	**Код ОП** 1. 02.03.03/33.01
Направление подготовки 1. Математическое обеспечение и администрирование информационных систем	**Код направления и уровня подготовки** 1. 02.03.03

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бродская Лариса Игоревна	без ученой степени, без ученого звания	Старший преподаватель	Департамент математики, механики и компьютерных наук
2	Пьянзина Елена Сергеевна	кандидат физико-математических наук, без ученого звания	Доцент	Кафедра теоретической и математической физики

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Основы компьютерной безопасности

1.1. Аннотация содержания модуля

Состоит из одноименной дисциплины, дающей необходимые для профессионального программирования и системного администрирования знания и навыки по широкому спектру проблем компьютерной безопасности, от криптографии до обратного инжиниринга

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	Основы компьютерной безопасности	6
	ИТОГО по модулю:	6

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Основания информатики и программирования
Постреквизиты и кореквизиты модуля	1. Практикум по компьютерной безопасности

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
Основы компьютерной безопасности	ПК-4 - Готовность к разработке алгоритмов и реализации их на базе языков программирования и пакетов прикладных программ, осуществлять выбор программно-аппаратных средств	У-3 - Определять оптимальные методы обеспечения защиты информации П-3 - Осуществлять обоснованный выбор используемых методов защиты информации Д-1 - Проявлять умения анализировать и систематизировать информацию

	ПК-5 - Способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям	З-1 - Сформулировать математически корректную постановку задачи

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы компьютерной безопасности

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бродская Лариса Игоревна	без ученой степени, без ученого звания	Старший преподаватель	Департамент математики, механики и компьютерных наук
2	Пьянзина Елена Сергеевна	кандидат физико-математических наук, без ученого звания	Доцент	Кафедра теоретической и математической физики

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _2_ от _13.04.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Бродская Лариса Игоревна, Старший преподаватель, Департамент математики, механики и компьютерных наук**
- **Пьянзина Елена Сергеевна, Доцент, Кафедра теоретической и математической физики**

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	Криптография и стеганография	История криптографии. Понятие шифрования. Симметричное и ассиметричное шифрование. Открытый и закрытый ключи. Алгоритм Диффи-Хеллмана. Алгоритм RSA с доказательством корректности. Электронно-цифровая подпись. Хеш-функция. Криптографическая хеш-функция. Хеш-функция MD5. Коллизии первого и второго рода. Архитектура и экономика криптовалюты Bitcoin. История стеганографии. Компьютерная стеганография. Текстовая стеганография. Стеганография в изображениях, звуковом и видеофайле. Стеганография в форматах с потерями (на примере JPEG). Стегоанализ. Цифровые водяные знаки.
2	Компьютерные сети	Стек протоколов ISO/OSI. Стек протоколов TCP IP. Физический уровень. Канальный уровень: протокол Ethernet. Протокол DHCP. Протокол ARP. Сетевой уровень: протокол IP. IP-маршрутизация. IPv4 итIPv6. Протоколы прикладного уровня. Протокол DNS. Иерархия NS-серверов. Отравление кеша DNS.

		Протокол FTP. Протокол SMTP. Туннелирование. Построение частных сетей VPN. История протокола HTTP. Структура HTTP-запроса и ответа.URL. Методы HTTP. Заголовки HTTP. Авторизация и аутенфикация посредством HTTP. Протоколы HTTPS, SSL и TLS.
3	Инъекции. Безопасность веб-приложений	Инъекции. SQL-инъекции. Синтаксис SQL. UNION. Экранирование символов при инъекции. Множественные запросы. Слепые SQL-инъекции. NoSQL-инъекции. LDAP-инъекции. XPath-инъекции. Инъекции в командах операционных систем.
4	Операционные системы. GNU Linux	Операционные системы. GNU и FSF. Стандарт POSIX. История ядра Linux. Дистрибутивы Linux. Unix Way. Загрузка системы. GRUB. Пользователи в Linux. Командная строка. Виртуальные машины. Сброс пароля.
5	Низкоуровневое программирование. Обратный инжиниринг	Архитектура компьютера. Принципы фон Неймана. Регистры процессора. Ассемблер. Команда MOV. Арифметические и логические команды. Знаковые и беззнаковые числа. Условный и безусловные переходы. Управление выполнение программы. Функции. Структура исполняемого файла. Обратный инжиниринг. Форматы исполняемых файлов. Формат PE. Шаблоны исполняемого кода. Шаблоны объектно-ориентированного программирования. Пакеты. Антиотладка. Введение в бинарные уязвимости. Отладчик. GDB. Переполнение стека. Переполнение кучи. Исполнение кода, шеллкод. OpenSSL Heartbleed. Уязвимость форматной строки.

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 профессиональн	ПК-4 - Готовность к разработке алгоритмов и реализации их на базе языков программирования и пакетов прикладных	У-3 - Определять оптимальные методы обеспечения защиты информации П-3 -

		ой деятельности	программ, осуществлять выбор программно-аппаратных средств	Осуществлять обоснованный выбор используемых методов защиты информации Д-1 - Проявлять умения анализировать и систематизировать информацию

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основы компьютерной безопасности

Электронные ресурсы (издания)

1. Падалкин, И. М.; Междисциплинарный элективный курс по теме "Элементы криптографии" : студенческая научная работа.; б.и., Воронеж; 2020; https://biblioclub.ru/index.php?page=book&id=594606 (Электронное издание)

Печатные издания

1. , Ященко, В. В.; Введение в криптографию : Учебник.; МЦНМО : Питер, СПб.; Москва; Харьков; Минск; 2001 (11 экз.)

2. Нечаев, В. И., Садовничий, В. А.; Элементы криптографии. (Основы теории защиты информации : Учеб. пособие для вузов.; Высш. шк., Москва; 1999 (79 экз.)

3. , Аграновский, А. В., Девятин, П. Н., Хади, Р. А., Черемушкин, А. В.; Основы компьютерной стеганографии : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютер. безопасность" и "Комплексное обеспечение информ. безопасности автоматизир. систем".; Радио и связь, Москва; 2003 (4 экз.)

4. ; Основы криптографии : Учеб. пособие для вузов.; Гелиос АРВ, Москва; 2001 (4 экз.)

5. Таненбаум, Э., Леонтьев, А.; Современные операционные системы; Питер, Москва; СПб.; Н. Новгород и др.; 2002 (4 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

lib.urfu.ru

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основы компьютерной безопасности

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 Chrome
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Подключение к сети Интернет	Свободное ПО: Google Chrome
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Подключение к сети Интернет	Свободное ПО: Google Chrome
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Подключение к сети Интернет	Свободное ПО: Google Chrome

5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Подключение к сети Интернет	Свободное ПО: Google Chrome