Подписано и утверждено в СЭД 02.02.2022 20:03:47ИД задачи 2567583

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
1156422	Теоретические аспекты информационной безопасности

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Математика и компьютерные науки 2. Математическое обеспечение и администрирование информационных систем	**Код ОП** 1. 02.03.01/33.01 2. 02.03.03/33.01
Направление подготовки 1. Математика и компьютерные науки; 2. Математическое обеспечение и администрирование информационных систем	**Код направления и уровня подготовки** 1. 02.03.01; 2. 02.03.03

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Баранский Виталий Анатольевич	доктор физико-математических наук, профессор	Профессор	алгебры и фундаментальной информатики
2	Копейцев Вячеслав Ефимович	без ученой степени, без ученого звания	Ассистент	Департамент математики, механики и компьютерных наук

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Теоретические аспекты информационной безопасности

1.1. Аннотация содержания модуля

Модуль состоит из одноименной дисциплины. Цель данной дисциплины состоит в получении слушателями теоретических основ защиты информационных систем. В результате прохождения курса студенты должны знать основные методы и средства защиты информации, а также получить теоретические сведения по использованию специализированных средств защиты информации, а также возможностей обеспечения информационной безопасности в программных средствах общего назначения

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	Теоретические аспекты информационной безопасности	3
	ИТОГО по модулю:	3

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Основания информатики и программирования 2. Фундаментальная математика
Постреквизиты и кореквизиты модуля	1. Практические аспекты информационной 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
Теоретические аспекты информационной безопасности	ПК-2 - Способен математически корректно ставить естественнонаучные задачи, обрабатывать научную информацию и	З-3 - Классифицировать основные методы решения прикладных задач, современные методы информационных технологий

	результаты исследований, определять закономерности предметной области **(Математика и компьютерные науки)**	Д-2 - Демонстрировать умения анализировать и обобщать информацию, делать логические умозаключения
	ПК-4 - Способен разрабатывать и реализовывать алгоритмы на базе современных языков программирования и пакетов прикладных программ, осуществлять обоснованный выбор программно-аппаратных средств **(Математика и компьютерные науки)**	У-3 - Определять оптимальные методы обеспечения защиты информации П-3 - Осуществлять обоснованный выбор используемых методов защиты информации
	ПК-4 - Готовность к разработке алгоритмов и реализации их на базе языков программирования и пакетов прикладных программ, осуществлять выбор программно-аппаратных средств **(Математическое обеспечение и администрирование информационных систем)**	У-3 - Определять оптимальные методы обеспечения защиты информации П-3 - Осуществлять обоснованный выбор используемых методов защиты информации
	ПК-5 - Способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям **(Математическое обеспечение и администрирование**	З-3 - Классифицировать основные методы решения прикладных задач, современные методы информационных технологий Д-2 - Демонстрировать умения анализировать и обобщать информацию, делать логические умозаключения

	информационных систем)	

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Теоретические аспекты информационной безопасности

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Баранский Виталий Анатольевич	доктор физико-математических наук, профессор	Профессор	алгебры и фундаментальной информатики
2	Копейцев Вячеслав Ефимович	без ученой степени, без ученого звания	Ассистент	Департамент математики, механики и компьютерных наук

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _2_ от _13.04.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Баранский Виталий Анатольевич, Профессор, алгебры и фундаментальной информатики**
- **Копейцев Вячеслав Ефимович, Ассистент, Департамент математики, механики и компьютерных наук**

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	Основы сетевых технологий	Разбор принципов работы сетевых протоколов транспортного уровня TCP и UDP. Возможные проблемы безопасности, возникающие при использовании каждого из протоколов. Разбор протокола сетевого уровня ICMP и протокола прикладного уровня HTTP.
2	Проблемы информационной безопасности в сетевых технологиях	Основные принципы работы Wi-Fi сетей, использования различных прокси-серверов, как на локальном компьютере, так и на удалённом, а также проблем информационной безопасности, связанных с перехватом сетевого трафика. Методы аутентификации на удалённых ресурсах и проблемы безопасности, связанные с передачей данных по незащищённому каналу. Разбор общих принципов работы протокола DNS и проблем безопасности, связанных с ним.
3	Алгоритмы шифрования	История алгоритмов шифрования от древности до наших дней. Рассмотрение симметричных алгоритмов шифрования. Шифры замены и шифры перестановок. Шифр Цезаря, Xor, алгоритм Blowfish. Блочные алгоритмы: RC5, DES, AES. История создания и принципы работы. Методы анализа криптостойкости алгоритмов. Методы нахождения ключа расшифровки. Ассиметричные алгоритмы

		шифрования. Алгоритм Диффи-Хеллмана. Рассмотрение принципа работы алгоритма RSA
4	Безопасные протоколы прикладного уровня	Применение ассиметричного шифрования в задаче передачи данных по незащищённому сетевому каналу. Принцип работы протокола HTTPS. Сертификаты, их виды и центры сертифика- ции, доверенные корневые центры сертификации. Создание собственного сертификата. Криптографический протокол SSL, криптографический протокол TLS. Проблемы информационной безопасности, связанные с подменой сертификата на промежуточном узле связи (так называемые, техники man-in-the-middle).
5	Безопасность веб-сервера.	Рассмотрение основных методов аудита безопасности веб-сервера. Сканирование портов, обнаружение скрытых страниц и поддоменов. Техники и приёмы анализа протоколов взаимодействия клиента и сервера, в частности: файлов cookie, передаваемых параметров, генерируемых страниц и т.д. Безопасность при работе с базами данных, так называемые атаки SQL Injection. Методы модификации кода страниц сервера, XSS уязвимости. Атаки, направленные на уязвимости в программном обеспечении сервера, эксплойты. Атаки, направленные на отказ в обслуживании, рассмотрение различных типов DDoS атак, а также методов защиты от них
6	Методы скрытого хранения информации	Рассмотрение основных методов стеганографии. Скрытое хранение информации в изображениях, аудиофайлах, других файлов различных типов, без повреждения и модификации основ- ного содержимого файла. Рассмотрение методов скрытого хранения данных на носителях информации с учётом специфики современных файловых систем. Анализ существующих техник обнаружения скрытого хранения информации
7	Работа исполняемых файлов в современных операционных системах	Рассмотрение формата исполняемых файлов Portable Executable, работающих под управлением операционной системы Windows. Обзор формата исполняемых файлов ELF, работающих под управлением операционных систем семейства Unix. Общие методы ручного и автоматического анализа исполняемых файлов. Обзор механизмов, используемых операционной системой для загрузки, создания контекста и исполнения данных файлов.
8	Методы статического анализа исполняемых файлов	Основы использования интерактивного дизассемблера IDA. Применение автоматических средств анализа кода. Техники нахождения основных участков кода, характеризующих основ- ной функционал анализируемого программного обеспечения. Использование скриптового движка IDA Script. Рассмотрение

		основных техник анализа кода исполняемого файла, в частности, анализа вредоносного программного обеспечения, с целью проведения криминалистических действий
9	Методы динамического анализа исполняемых файлов	Основы использования локального отладчика интерактивного дизассемблера IDA. Обсуждение основных принципов отладки приложений. Проблемы безопасности, связанные с локальной отладкой и переход к удалённой отладке приложения. Настройка подключения к удалённой системе. Особенности проведения удалённой отладки приложений. Рассмотрение основных принципов работы с отладчиком OllyDbg. Использование отладчика для подключения к уже запущенному процессу. Методы противодействия обнаружения отладчика со стороны приложения
10	Различные проблемы безопасности исполняемых файлов	Рассмотрение уязвимостей, которые может содержать исполняемый файл и техник, применяемых для эксплуатации данных уязвимостей. Техники переполнения буфера, используемые для получения управления произвольным кодом. Использование так называемых ROP методов. Методы противодействия, в частности, рандомизация стека. Рассмотрение примеров эксплуатации уязвимости известных приложений на примерах Internet Explorer, Java, Adobe Flash и других
11	Методы противодействия проникновению в систему	Анализ современных методов проведения атак, в том числе таргетированных т.е. специально подготовленных для атаки на конкретную систему. Рассмотрение различных примеров фишинговых писем. Эксплойтов для легитимного программного обеспечения. Приёмы социальной инженерии. Атаки, производящиеся с использованием сменных носителей. Рассмотрение различных методов защиты от всех вышеописанных техник как с использованием различного программного обеспечения, так и в условиях ручной работы специалиста
12	Принципы работы современного антивирусного ПО.	История развития вредоносного ПО и антивирусного ПО. Классификация вредоносного ПО. Простейшие сигнатурные сканеры, их преимущества и недостатки. Эвристические сканеры, основанные на различных анализаторах кода и эмуляторах, их преимущества и недостатки. Поведенческие анализаторы, допускающие исполнение программного обеспечения, их преимущества и недостатки. Классификаторы приложений. Сетевые экраны. Антиспам фильтры, основные принципы работы, рассмотрение алгоритма Байеса. Применение облачных технологий в методах защиты от вредоносного программного обеспечения

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-4 - Способен разрабатывать и реализовывать алгоритмы на базе современных языков программирования и пакетов прикладных программ, осуществлять обоснованный выбор программно-аппаратных средств	У-3 - Определять оптимальные методы обеспечения защиты информации П-3 - Осуществлять обоснованный выбор используемых методов защиты информации

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теоретические аспекты информационной безопасности

Электронные ресурсы (издания)

1. Смирнов, В. И.; Защита информации: лабораторный практикум : практикум.; Поволжский государственный технологический университет, Йошкар-Ола; 2017; https://biblioclub.ru/index.php?page=book&id=476512 (Электронное издание)

2. Пильщиков, В. Н.; Программирование на языке ассемблера IBM PC : учебное пособие.; Диалог-МИФИ, Москва; 2014; https://biblioclub.ru/index.php?page=book&id=447687 (Электронное издание)

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

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.urfu.ru –портал информационно-образовательных ресурсов УрФУ http://lib.urfu.ru - Зональная научная библиотека ФГАОУ ВО УрФУ

http://lib.urfu.ru/mod/resource/view.php?id=2320 - Списки рекомендованной литературы от ЗНБ

http://biblioclub.ru - портал-библиотека электронных книг

http://lib.urfu.ru/course/view.php?id=81 - заказ литературы из электронного каталога

http://ustu.antiplagiat.ru/index.aspx - Пакет «Антиплагиат.ВУЗ»

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теоретические аспекты информационной 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 Professional 2003 Win32 Russian CD-ROM Google Chrome
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Подключение к сети Интернет	Google Chrome
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Подключение к сети Интернет	Google Chrome
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя	Google Chrome

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