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
1153518	Противодействие вредоносным программам

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	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
2	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Противодействие вредоносным программам

1.1. Аннотация содержания модуля

В модуле «Противодействие вредоносным программам» изучаются основополагающие принципы защиты компьютерной информации от вредоносных программ, возможности и отличительные признаки различных видов вредоносных программ для ЭВМ, порядок применения антивирусного программного обеспечения.

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	Противодействие вредоносным программам	3
	ИТОГО по модулю:	3

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Организационно-правовые основы информационной безопасности
Постреквизиты и кореквизиты модуля	1. Защита информации от утечки по техническим каналам 2. Комплексное обеспечение защиты информации объекта информатизации

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
Противодействие вредоносным программам	ПК-14 - Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и	З-1 - Описать принципы построения антивирусного программного обеспечения З-2 - Сделать обзор основных средств и методов анализа программных реализаций З-3 - Описать нормативные правовые акты в области защиты информации

	корпоративными требованиями	З-4 - Описать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации У-1 - Анализировать угрозы безопасности информации программного обеспечения У-2 - Формулировать правила безопасной эксплуатации программного обеспечения У-3 - Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия П-1 - Определять состав применяемых программно-аппаратных средств защиты информации в операционных системах П-2 - Определять порядок применения программно-аппаратных средств защиты информации в операционных системах П-3 - Иметь практический опыт формирования шаблонов установки программно-аппаратных средств защиты информации в операционных системах П-4 - Определять конфигурацию программно-аппаратных средств защиты информации в операционных системах

1.5. Форма обучения

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Противодействие вредоносным программам

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Куц Дмитрий Владимирович	без ученой степени, без ученого звания	Старший преподаватель	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

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

Протокол № _6_ от _26.05.2023_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Куц Дмитрий Владимирович, Старший преподаватель,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

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	Понятие «вредоносное программное обеспечение», классификация. Возможности, механизмы действия вредоносного программного обеспечения	Понятие об опасных компьютерных программах и данных. Оценка опасностей, связанных с разработкой и использованием программ для ЭВМ. Состав вредоносных программ и команд. Классификация вредоносных программ по основным свойствам и признакам. Основные признаки и возможности компьютерных вирусов, программных закладок, «логических бомб», сетевых «червей», программ «удаленного администрирования» и иных видов опасных программ. Инструментарий, используемый вирмейкерами для создания вредоносных программ. Изучение функциональных возможностей вредоносных программ. Программные воздействия, заведомо приводящие к опасным последствиям. Сущность вредоносных блокирования, удаления, модификации защищаемой компьютерной информации. Программно-управляемые формы несанкционированного копирования информации. Механизмы вирусного заражения. Виды и формы программно-управляемого нарушения работы ЭВМ. Способы несанкционированного запуска опасных программ и команд. Способы внедрения и запуска вредоносных программ. Уязвимые места программного обеспечения автоматизированных систем, способствующие внедрению, запуску, сокрытию, и распространению вредоносных программ. Способы проникновения вредоносных программ в

		локальные и сетевые ЭВМ. Потенциально опасные функции операционной системы. Уязвимости ОС и штатного программного обеспечения, способствующие распространению вредоносных программ. Понятие о случайном и безусловном запуске. Внедрение и запуск программного кода на этапах самотестирования ПЭВМ и загрузки операционной системы. Способы подготовки вредоносных программ к автоматическому запуску. Типичные варианты обмана пользователей, провоцирующих их на запуск неизвестных программ. Внедрение и запуск опасных программ с применением «троянских» оболочек. Возможности программ-«джойнеров».
2	Методы анализа возможностей и механизмов действия вредоносного программного обеспечения. Меры противодействия вредоносному программному обеспечению	Виды и возможности антивирусных программ. Меры по реализации изолированной программной среды. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного кода. Динамический анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScope и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ. Способы выявления деструктивной активности вредоносных программ. Понятие о сигнатуре вредоносного программного кода. Принципы антивирусного сканирования памяти ЭВМ. Понятие о механизмах скрытности вредоносных программ. Демаскирующие признаки вредоносного программного кода. Полиморфизм программного кода. «Stealth»-технологии. Способы сокрытия файловых объектов и процессов на уровне ядра операционной системы. Возможности программ- «руткитов». Мониторинг подозрительной активности программ. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного кода. Динамический анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScope и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональн	целенаправленна	Технология	ПК-14 - Способен	П-2 - Определять

ое воспитание	я работа с информацией для использования в практических целях	самостоятельной работы	оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	порядок применения программно-аппаратных средств защиты информации в операционных системах

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Противодействие вредоносным программам

Электронные ресурсы (издания)

1. , Синадский, , Н. И.; Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие.; Уральский федеральный университет, ЭБС АСВ, Екатеринбург; 2014; http://www.iprbookshop.ru/65983.html (Электронное издание)

Печатные издания

1. Бакланов, В. В.; Введение в информационную безопасность. Направления информационной защиты : курс лекций.; Изд-во Уральского университета, Екатеринбург; 2007 (3 экз.)

2. Бакланов, В. В., Гайдамакин, Н. А.; Защита компьютерной информации в клиентских приложениях : учеб. пособие [для вузов].; [УГТУ-УПИ], Екатеринбург; 2006 (3 экз.)

3. , Андрончик, А. Н., Богданов, В. В., Домуховский, Н. А., Коллеров, А. С., Синадский, Н. И., Хорьков, Д. А., Щербаков, М. Ю.; Защита информации в компьютерных сетях. Практический курс : учебное пособие для студентов вузов, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 - "Информационная безопасность телекоммуникационных систем".; УГТУ-УПИ, Екатеринбург; 2008 (1 экз.)

Профессиональные базы данных, информационно-справочные системы

Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.ru

Банк данных угроз безопасности информации - Официальный сайт Федеральной службы по техническому и экспортному контролю http://www.fstec.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

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование_ (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https://elar.urfu.ru)

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Противодействие вредоносным программам

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 Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Периферийное устройство Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	
3	Текущий контроль и промежуточная аттестация	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	**Не требуется**
4	Самостоятельная работа студентов	Периферийное устройство Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES