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
1156875	Методы и системы обнаружения компьютерных атак

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Информационная безопасность телекоммуникационных систем	**Код ОП** 1. 10.05.02/22.01
Направление подготовки 1. Информационная безопасность телекоммуникационных систем	**Код направления и уровня подготовки** 1. 10.05.02

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	Старший преподаватель	
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 Методы и системы обнаружения компьютерных атак

1.1. Аннотация содержания модуля

Рассматриваются основные этапы применения систем обнаружения атак разработке и эксплуатации. Изучаются понятия сетевых компьютерных атак. Проводится анализ основных типов систем обнаружения атак, применяемых на практике в настоящее время, описаны математические модели, используемые в качестве базы для алгоритма обнаружения компьютерных атак.

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	Аппаратные средства вычислительной техники	4
2	Методы и средства противодействия вредоносному программному обеспечению	4
3	Методы обнаружения и противодействия компьютерным атакам	3
	ИТОГО по модулю:	11

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Основы технической защиты информации
Постреквизиты и кореквизиты модуля	1. Технические средства и методы защиты информации 2. Проектирование защищенных телекоммуникационных систем

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

Аппаратные средства вычислительной техники	ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	З-1 - Распознавать угрозы информационно-телекоммуникационной структуры З-2 - Объяснять модели угроз и оценивать их риски в информационно-телекоммуникационных инфраструктурах У-1 - Оценивать технические возможности обеспечения информационной безопасности У-2 - Анализировать возможные угрозы в информационно-телекоммуникационных инфраструктурах П-1 - Разрабатывать рекомендации по обеспечению информационной безопасности на элементном уровне информационно-телекоммуникационной инфраструктуры
Методы и средства противодействия вредоносному программному обеспечению	ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	З-1 - Распознавать угрозы информационно-телекоммуникационной структуры З-2 - Объяснять модели угроз и оценивать их риски в информационно-телекоммуникационных инфраструктурах У-1 - Оценивать технические возможности обеспечения информационной безопасности У-2 - Анализировать возможные угрозы в информационно-телекоммуникационных инфраструктурах П-1 - Разрабатывать рекомендации по обеспечению информационной безопасности на элементном уровне информационно-телекоммуникационной инфраструктуры
Методы обнаружения и противодействия компьютерным атакам	ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	З-1 - Распознавать угрозы информационно-телекоммуникационной структуры З-2 - Объяснять модели угроз и оценивать их риски в информационно-телекоммуникационных инфраструктурах У-1 - Оценивать технические возможности обеспечения информационной безопасности У-2 - Анализировать возможные угрозы в информационно-телекоммуникационных инфраструктурах П-1 - Разрабатывать рекомендации по обеспечению информационной

		безопасности на элементном уровне информационно-телекоммуникационной инфраструктуры

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Аппаратные средства вычислительной техники

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна		старший преподаватель	УНЦ ИБ
2	Поршнев Сергей Владимирович	д.т.н, профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ
3	Ронкин Михаил Владимирович	кандидат наук, без ученого звания	Доцент	Кафедра департамент радиоэлектроники и связи

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

Протокол № _9_ от _21.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Пономарева Ольга Алексеевна, старший преподаватель, УНЦ ИБ**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**
- **Ронкин Михаил Владимирович, Доцент, Учебно-научный центр "Информационная безопасность"**

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	Схемотехника электронных цифровых устройств	Базовые схемы логических элементов (ЛЭ). Триггеры. Регистры памяти и сдвига. Счетчики импульсов. Комбинационные логические элементы в составе серий ИС. Формирователи импульсов. Мультивибраторы
2	Микропроцессоры в телекоммуникационных системах	Микропроцессоры как новая технологическая база построения различных устройств телекоммуникационных систем. Основные понятия, виды архитектур, типы микропроцессоров. Состояние, перспективы и тенденции развития универсальных и специализированных микропроцессоров и их использование для построения элементов сетей передачи данных
3	Коммуникационные микропроцессоры	Классификация, показатели и архитектура коммуникационных микропроцессоров. Память, параллельные порты ввода/вывода и протоколы последовательного обмена. АЦП, ЦАП, таймеры и процессоры событий. Современные коммуникационные микропроцессоры и их использование в оборудовании сетей связи
4	Сигнальные микропроцессоры	Классификация, характеристики и архитектура цифровых сигнальных микропроцессоров. Память и арифметические узлы. Система команд. Состав команд арифметических и логических операций, операций передачи данных, управления

		и вызова подпрограмм. Способы адресации. Средства программирования отладки программ. Программная модель сигнального микропроцессора. Типы современных цифровых сигнальных микропроцессоров и их использование в оборудовании сетей связи.

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	ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	З-2 - Объяснять модели угроз и оценивать их риски в информационно-телекоммуникационных инфраструктурах

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аппаратные средства вычислительной техники

Электронные ресурсы (издания)

1. Семенов, Ю. А.; Алгоритмы телекоммуникационных сетей : учебное пособие. 2. Протоколы и алгоритмы маршрутизации в Internet; Интернет-Университет Информационных Технологий (ИНТУИТ)|Бином. Лаборатория знаний, Москва; 2007; https://biblioclub.ru/index.php?page=book&id=233325 (Электронное издание)

Печатные издания

1. Хартов, В. Я.; Микропроцессорные системы : учеб. пособие для студентов вузов, обучающихся по направлению "Информатика и вычисл. техника", специальности "Вычисл. машины, комплексы,

системы и сети".; Академия, Москва; 2010 (10 экз.)

2. Калашников, В. И., Раннев, Г. Г.; Электроника и микропроцессорная техника : учебник для студентов вузов, обучающихся по направлению подготовки бакалавров "Приборостроение".; Академия, Москва; 2012 (1 экз.)

3. Зиатдинов, С. И.; Схемотехника телекоммуникационных устройств : учебник для студентов [вузов], обучающихся по направлению подготовки 21070 "Инфокоммуникационные технологии и системы связи".; Академия, Москва; 2013 (1 экз.)

4. Гусев, В. Г., Гусев, Ю. М.; Электроника и микропроцессорная техника : учебник для студентов вузов, обучающихся по направлению подгот. бакалавров и магистров "Биомед. инженерия" и по направлению подгот. дипломир. специалистов "Биомед. техника".; Высшая школа, Москва; 2005 (90 экз.)

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.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

Аппаратные средства вычислительной техники

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	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя 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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
3	Самостоятельная работа студентов	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		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	
5	Текущий контроль и промежуточная аттестация	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы и средства противодействия вредоносному программному обеспечению

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Гибилинда Роман Владимирович	кандидат технических наук, без ученого звания	Ассистент	
2	Пономарева Ольга Алексеевна		старший преподаватель	УНЦ ИБ
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 № _9_ от _21.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Гибилинда Роман Владимирович, Ассистент,**
- **Пономарева Ольга Алексеевна, старший преподаватель, УНЦ ИБ**
- **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	Информационные и компьютерные преступления	Понятие об информационных и компьютерных преступлениях. Особенности и причины информационных преступлений. Особенности компьютерных преступлений. Преступления в сфере компьютерной информации. Место компьютерных систем в преступной деятельности. Компьютер как непосредственное орудие преступления. Компьютер как средство преступления и хранилище информации о преступной деятельности. Компьютер как предмет преступления. Особенности подготовки компьютерных преступлений.
2	Понятие об опасной компьютерной информации	Создание и использование компьютерных программ как деятельность, представляющая повышенную общественную опасность. Уровни представления опасной компьютерной информации. Понятие компьютерных программ и команд. Программы и данные как объективная форма представления компьютерной информации. Машинный код. Ассемблерные команды. Опасные системные вызовы. Опасные системные команды. Инструментарий для разработки, отладки и модификации вредоносных программ.
3	Классификация и технические возможности вредоносных программ	Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам. Классификация программ по степени опасности для защищаемой информации и компьютерной системы.

		Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и сетевые фильтры.
4	Уязвимые места программного обеспечения ЭВМ, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ.	Потенциально опасные функции и элементы операционной системы. Возможности использования уязвимостей ОС и штатного программного обеспечения с целью удаления, модификации, блокирования или копирования информации без уведомления и согласия ее владельца или пользователя. Защита компьютерных систем от вредоносного программного воздействия. Понятие об опасных и вредоносных программах. Характеристика компьютерной программы как вида информационного нарушителя. Классификация вредоносных программ. Демаскирующие признаки опасного программного воздействия. Основные организационные и программные меры антивирусной защиты.
5	Изучение функциональных возможностей вредоносных программ	Основные признаки и возможности макровирусов, сетевых «червей», программ «удаленного администрирования». Способы проникновения вредоносных программ в локальные и сетевые ЭВМ. Способы выявления деструктивной активности вредоносных программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Понятие о механизмах скрытности вредоносных программ. Демаскирующие признаки вредоносного программного кода. Полиморфизм программного кода. Программы-«невидимки». Способы сокрытия файловых объектов и процессов на уровне ядра операционной системы. Возможности программ-«руткитов»

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	ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с	З-2 - Объяснять модели угроз и оценивать их риски в информационно-телекоммуникационных инфраструктурах

			учетом обеспечения требований информационной безопасности	

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы и средства противодействия вредоносному программному обеспечению

Электронные ресурсы (издания)

1. Пушкарев, , В. В.; Уголовное преследование по уголовным делам о преступлениях, посягающих на системы и ресурсы банковского сектора : монография.; Прометей, Москва; 2019; http://www.iprbookshop.ru/94562.html (Электронное издание)

Печатные издания

1. Айков, Д., Воропаев, В. И., Трехалин, Г. Г.; Компьютерные преступления : Рук. по борьбе с компьютерными преступлениями.; Мир, Москва; 1999 (1 экз.)

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

Профессиональные базы данных, информационно-справочные системы

http://lib.urfu.ru/mod/data/view.php?id=1379]

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

Методы и средства противодействия вредоносному программному обеспечению

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	Office 365 EDUA5 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 Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA5 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 Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Самостоятельная работа студентов	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
5	Текущий контроль и промежуточная аттестация	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	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы обнаружения и противодействия компьютерным атакам

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Агафонов Алексей Владимирович	кандидат технических наук, без ученого звания	Доцент	
2	Пономарева Ольга Алексеевна		старший преподаватель	УНЦ ИБ
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 № _9_ от _21.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Агафонов Алексей Владимирович, Доцент,**
- **Пономарева Ольга Алексеевна, старший преподаватель, УНЦ ИБ**
- **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	Основы компьютерных сетей	Введение в основы компьютерных сетей. Основные протоколы прикладного уровня стека TCP/IP. Основные протоколы транспортного, сетевого и канального уровня стека TCP/IP. Сетевое оборудование, принципы работы. Vlan и Vpn, принципы построения сетей. Передача пакетов на сетевом и канальном уровнях.
2	Мониторинг событий информационной безопасности	Виды систем защиты информации. Принципы работы и использования систем защиты информации: Host IDS, Network IDS/IPS, Antivirus, Data Loss Prevention, Web Application Firewall, Proxy, Firewall, Vulnerability Scanner, Sandbox, SIEM. Принципы выявления атак на основе модели Cyber-Kill Chain. События ИБ и их анализ для выявления атак. Инциденты ИБ. Способы реагирования на инциденты ИБ.
3	Технические средства обнаружения вторжений	Архитектура и общее описание стека технологий ELK. Изучение агентов для сбора информации с ОС Windows, Linux. Логирование ОС Windows, политики аудита. Изучение возможностей Sysmon. Изучение возможностей системы Network IDS Suricata. Принципы работы с консолью Kibana для поиска и анализа событий ИБ. Разработка запросов на языке Query DSL. Изучение принципов разработки панелей визуализации событий. Изучение общих принципов

		разворачивания инструментов для мониторинга и диагностики неисправностей.
4	Методы автоматизации выявления инцидентов ИБ.	Изучение принципов автоматизации выявления инцидентов ИБ, применяемых в SIEM системах. Разработка правил автоматизированного выявления на примере подсистемы «Сигнал».

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	ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	З-2 - Объяснять модели угроз и оценивать их риски в информационно-телекоммуникационных инфраструктурах

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы обнаружения и противодействия компьютерным атакам

Электронные ресурсы (издания)

1. Пушкарев, , В. В.; Уголовное преследование по уголовным делам о преступлениях, посягающих на системы и ресурсы банковского сектора : монография.; Прометей, Москва; 2019; http://www.iprbookshop.ru/94562.html (Электронное издание)

Печатные издания

1. Соломон, Соломон Д., Руссинович, Руссинович М.; Внутреннее устройство Microsoft Windows 2000 : Мастер-класс : Пер. с англ..; Русская редакция : Питер, Москва; СПб.; Харьков; Минск; 2001 (0 экз.)

2. Уорд, Б., Райтман, М.; Внутреннее устройство Linux; Питер, Санкт-Петербург; 2016 (1 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

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

Методы обнаружения и противодействия компьютерным атакам

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	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		санитарными правилами и нормами	
2	Лабораторные занятия	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	Office 365 EDUA5 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 Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
5	Текущий контроль и промежуточная аттестация	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 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES