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
1155863	Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Информатика и вычислительная техника 2. Прикладная информатика 3. Программная инженерия	**Код ОП** 1. 09.03.01/33.01 2. 09.03.03/33.01 3. 09.03.04/33.01
Направление подготовки 1. Информатика и вычислительная техника; 2. Прикладная информатика; 3. Программная инженерия	**Код направления и уровня подготовки** 1. 09.03.01; 2. 09.03.03; 3. 09.03.04

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Новиков Максим Юрьевич	к.п.н.	Доцент	Базовая кафедра «Аналитика больших данных и методы видеоанализа»

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)

1.1. Аннотация содержания модуля

Модуль «Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)» включает в себя обучение тестированию безопасности на проникновение, изучение комплекса мер, которые имитируют реальную атаку на сеть или приложение, а также направлен на получение студентами профессиональных навыков.

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	Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)	3
	ИТОГО по модулю:	3

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Не предусмотрены
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
Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)	ПК-3 - Способен обеспечить функционирование и безопасность программного обеспечения на уровне БД, оптимизировать БД, предотвращать потери и повреждение данных	З-3 - Перечислить основные угрозы безопасности БД, способы для их предотвращения и средства восстановления безопасности на уровне БД З-4 - Описать методы и средства обеспечения безопасности данных приработе с БД У-4 - Анализировать возможные угрозы для безопасности данных У-5 - Оценивать степень нагрузки различных инструментов обеспечения безопасности на

	(Информатика и вычислительная техника)	производительность БД П-3 - Осуществлять обоснованный выбор основных средств поддержки информационной безопасности на уровнеБД П-4 - Разрабатывать мероприятия по обеспечению безопасности на уровне БД
Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)	ПК-3 - Способен обеспечить функционирование и безопасность программного обеспечения на уровне БД, оптимизировать БД, предотвращать потери и повреждение данных **(Прикладная информатика)**	З-3 - Перечислить основные угрозы безопасности БД, способы для их предотвращения и средства восстановления безопасности на уровне БД З-4 - Описать методы и средства обеспечения безопасности данных приработе с БД У-4 - Анализировать возможные угрозы для безопасности данных У-5 - Оценивать степень нагрузки различных инструментов обеспечения безопасности на производительность БД П-3 - Осуществлять обоснованный выбор основных средств поддержки информационной безопасности на уровне БД П-4 - Разрабатывать мероприятия по обеспечению безопасности на уровне БД
Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)	ПК-3 - Способен обеспечить функционирование и безопасность программного обеспечения на уровне БД, оптимизировать БД, предотвращать потери и повреждение данных **(Программная инженерия)**	З-3 - Перечислить основные угрозы безопасности БД, способы для их предотвращения и средства восстановления безопасности на уровне БД З-4 - Описать методы и средства обеспечения безопасности данных приработе с БД У-4 - Анализировать возможные угрозы для безопасности данных У-5 - Оценивать степень нагрузки различных инструментов обеспечения безопасности на производительность БД П-3 - Осуществлять обоснованный выбор основных средств поддержки информационной безопасности на уровнеБД П-4 - Разрабатывать мероприятия по обеспечению безопасности на уровне БД

1.5. Форма обучения

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Профессиональный курс. Спецкурс 4
(Специалист по кибербезопасности)

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Новиков Максим Юрьевич	к.п.н.	Доцент	Базовая кафедра «Аналитика больших данных и методы видеоанализа»

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Новиков Максим Юрьевич, к.п.н., доцент, Базовая кафедра «Аналитика больших данных и методы видеоанализа»**

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	Введение в проблематику и методологию	Стандарты в пентесте. Базовое ПО для пентеста: ОС, приложения, пути развития. Создание стенда для тестирования и его настройка. Площадки для тестирования на проникновение в интернете.
2	Программирование на Python	Базовые понятия Python. Функции, переменные. Автоматизация на Python. Брутфорсер и кейлоггер на Python.
3	Веб-программирование	Основы веб-программирования и атак на системы управления контентом. HTML и CSS. Основы JavaScript. Основы PHP и XAMPP.
4	SQL и работа с базами данных	Реляционные и нереляционные базы данных. Установка и проектирование баз данных. Сканирование баз данных. Атаки на базы данных. SQLi.
5	Основы pentest в вебе	Методология и ПО для web-pentest. Применение BurpSuite. Устройства и приложения для упрощения работы.
6	Client Side Attacks	Уязвимости клиентской части: XSS, CSRF, CSP. Проведение client side-атак в вебе. Противодействие атакам на клиентскую часть.

7	Server Side Attacks	Уязвимости серверной части. Security Misconfiguration. Local File Inclusion. Remote Code Execution. HTTP Parameter Pollution, CRLF Injection. SQL Injection, Template Injections.
8	OS Linux	Введение в администрирование и архитектуру Linux. Управление пакетами. Bash и написание скриптов. Linux-сети. Сетевые сервисы. Принципы построения сетей, фильтрация трафика, маршрутизация. Аудит безопасности в OS Linux. Сбор логов и информации.
9	OS Windows	Введение в администрирование и архитектуру Windows. Active Directory. Аутентификация и сбор данных. Атаки бокового смещения: Pass the hash, Overpass the hash. Pass the ticket. Атаки на сетевые сервисы. Firewall, его настройка и обход. Администрирование с помощью Powershell. Powershell для пентеста.
10	Network Base	Основы сетевого взаимодействия TCP/IP. Основные сетевые протоколы. Исследование сетевого трафика. Средства обнаружения вторжения и утечек данных. Атаки на сетевое оборудование. Сетевые атаки MITM. Спуфинг.
11	Тестирование беспроводных сетей	Атаки на беспроводные сети. Методология, оборудование. Атаки на WPS, перехват handshake. Меры по противодействию атакам. Bluetooth, GSM, RFID.

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	профориентационная деятельность	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-3 - Способен обеспечить функционирование и безопасность программного обеспечения на уровне БД, оптимизировать БД, предотвращать потери и повреждение данных	З-3 - Перечислить основные угрозы безопасности БД, способы для их предотвращения и средства восстановления безопасности на уровне БД

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации.

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)

Электронные ресурсы (издания)

1. Суворова, , Г. М.; Основы информационной безопасности : учебное пособие для спо.; Профобразование, Саратов; 2021; http://www.iprbookshop.ru/108005.html (Электронное издание)

2. Моргунов, А. В.; Информационная безопасность : учебно-методическое пособие.; Новосибирский государственный технический университет, Новосибирск; 2019; https://biblioclub.ru/index.phppage=book&id=576726 (Электронное издание)

3. Ревнивых, , А. В.; Информационная безопасность в организациях : учебное пособие.; Ай Пи Ар Медиа, Москва; 2021; http://www.iprbookshop.ru/108227.html (Электронное издание)

4. Галатенко, , В. А.; Основы информационной безопасности : учебное пособие.; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, Москва; 2020; http://www.iprbookshop.ru/97562.html (Электронное издание)

5. Артемов, А. В.; Информационная безопасность: курс лекций : курс лекций.; Межрегиональная академия безопасности и выживания, Орел; 2014; https://biblioclub.ru/index.php?page=book&id=428605 (Электронное издание)

6. Прохорова, О. В.; Информационная безопасность и защита информации : учебник.; Самарский государственный архитектурно-строительный университет, Самара; 2014; https://biblioclub.ru/index.php?page=book&id=438331 (Электронное издание)

Профессиональные базы данных, информационно-справочные системы

1. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии http://window.edu.ru/catalog

2. Интернет-Университет Информационных Технологий http://www.intuit.ru/

3. Федеральный центр информационно-образовательных ресурсов http://eor.edu.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. Издательство "Лань" http://e.lanbook.com/
2. ЭБС Университетская библиотека онлайн «Директ-Медиа» http://www.biblioclub.ru/
3. ООО Научная электронная библиотека http://elibrary.ru

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)

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	Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc Office Professional 2003 Win32 Russian CD-ROM
2	Лабораторные 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	Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc Office Professional 2003 Win32 Russian CD-ROM
3	Самостоятельная работа студентов	Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc Office Professional 2003 Win32 Russian CD-ROM
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 Подключение к сети Интернет	Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc Office Professional 2003 Win32 Russian CD-ROM

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Профессиональный курс. Спецкурс 4
(Специалист по кибербезопасности)

Код модуля	**Модуль**
1155863(2)	Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Новиков Максим Юрьевич	к.п.н.	Доцент	Базовая кафедра «Аналитика больших данных и методы видеоанализа»

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Новиков Максим Юрьевич, к.п.н., доцент, Базовая кафедра «Аналитика больших данных и методы видеоанализа»**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)

1.	**Объем дисциплины в зачетных единицах**	3	
2.	**Виды аудиторных занятий**	Лекции Лабораторные занятия	
3.	**Промежуточная аттестация**	Зачет	
4.	**Текущая аттестация**	Контрольная работа Домашняя работа	1 1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Профессиональный курс. Спецкурс 4 (Специалист по кибербезопасности)

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ПК-3 - Способен обеспечить функционирование и безопасность программного обеспечения на уровне БД, оптимизировать БД, предотвращать потери и повреждение данных (Информатика и вычислительнаятехника)	З-3 - Перечислить основные угрозы безопасности БД, способы для их предотвращения и средства восстановлениябезопасности на уровне БД З-4 - Описать методы и средства обеспечения безопасности данных при работе с БД У-4 - Анализировать возможные угрозы длябезопасности данных У-5 - Оценивать степень нагрузки различных инструментов обеспечения безопасности на производительность БД П-3 - Осуществлять обоснованный выборосновных средств поддержки	Домашняя работа Зачет Лабораторные занятия Контрольная работа Лекции

	информационной безопасности на уровнеБД П-4 - Разрабатывать мероприятия по обеспечению безопасности на уровне БД	
ПК-3 - Способен обеспечить функционирование и безопасность программного обеспечения на уровне БД, оптимизировать БД, предотвращать потери и повреждение данных (Прикладная информатика)	З-3 - Перечислить основные угрозы безопасности БД, способы для их предотвращения и средства восстановлениябезопасности на уровне БД З-4 - Описать методы и средства обеспечения безопасности данных при работе с БД У-4 - Анализировать возможные угрозы длябезопасности данных У-5 - Оценивать степень нагрузки различных инструментов обеспечения безопасности на производительность БД П-3 - Осуществлять обоснованный выборосновных средств поддержки информационной безопасности на уровне БД П-4 - Разрабатывать мероприятия по обеспечению безопасности на уровне БД	Домашняя работа Зачет Лабораторные занятия Контрольная работа Лекции
ПК-3 - Способен обеспечить функционирование и безопасность программного обеспечения на уровне БД, оптимизировать БД, предотвращать потери и повреждение данных (Программнаяинженерия)	З-3 - Перечислить основные угрозы безопасности БД, способы для их предотвращения и средства восстановлениябезопасности на уровне БД З-4 - Описать методы и средства обеспечения безопасности данных при работе с БД У-4 - Анализировать возможные угрозы длябезопасности данных У-5 - Оценивать степень нагрузки различных инструментов обеспечения безопасности на производительность БД П-3 - Осуществлять обоснованный выборосновных средств поддержки информационной безопасности на уровнеБД	Домашняя работа Зачет Лабораторные занятия Контрольная работа Лекции

	П-4 - Разрабатывать мероприятия по обеспечению безопасности на уровне БД	

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	6, 4	*60*
домашняя работа	6, 13	*40*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0.4		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
выполнение и защита лабораторных работ	6,16	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		

Текущая аттестация на онлайн-занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	Сроки − семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Лабораторные занятия

Примерный перечень тем

1. Программирование на Python
2. Веб-программирование
3. SQL и работа с базами данных
4. Основы pentest в вебе

5. Client Side Attacks
6. Server Side Attacks
7. OS Linux
8. OS Windows
9. Network Base
10. Тестирование беспроводных сетей

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Законодательное регулирование в области кибербезопасности
2. Применение биометрических технологий для защиты данных
3. Развитие киберугроз и методы их предотвращения
4. Кибератаки на критическую инфраструктуру: угрозы и защита
5. Применение машинного обучения для обнаружения угроз в сети
6. Управление рисками в области кибербезопасности
7. Применение технологии облачных вычислений для обеспечения безопасности данных
8. Контроль за информационной безопасностью на уровне государства
9. Борьба с дезинформацией и фейками в цифровом пространстве
10. Разработка программ обучения по кибербезопасности для различных аудиторий
11. Применение методов шифрования для защиты конфиденциальной информации

Примерные задания:

1) Практическая задача: разработать модель машинного обучения для обнаружения угроз в сети с целью повышения безопасности системы.

Информация о данных: набор данных содержит информацию о сетевом трафике, событиях безопасности, логах аутентификации, атаках и других характеристиках сети. Данные могут быть представлены в виде структурированных или неструктурированных данных.

Цель: создать модель, способную автоматически обнаруживать потенциальные угрозы в сети, такие как DDoS-атаки и несанкционированный доступ.

2) Практическая задача: применение методов шифрования для защиты конфиденциальной информации с использованием симметричного и асимметричного шифрования. Необходимо зашифровать текстовое сообщение и передать другому студенту для дешифровки.

Данные: текстовые сообщения по вариантам.

Цель: практическое применение знаний о методах шифрования для защиты конфиденциальной информации. Использование методов симметричного и асимметричного шифрования.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Криптография и шифрование
2. Сетевая безопасность
3. Веб-безопасность
4. Форензика и анализ цифровых следов
5. Реверс-инжиниринг и обратная разработка
6. Стеганография и скрытые сообщения
7. Атаки на приложения и сервисы
8. Безопасность мобильных устройств
9. Атаки на операционные системы
10. Социальная инженерия и фишинг

Примерные задания

1) Практическое задание по теме "Атаки на операционные системы"
   Условие: вам предоставляется виртуальная машина с уязвимой операционной системой (например, Windows или Linux), на которой установлены различные сервисы и приложения. Ваша задача - провести атаку на данную систему, используя известные уязвимости и методы эксплойтов.
   Цель: практическое применение знаний о типах атак на операционные системы, их уязвимостях и методах защиты.
2) Практическое задание по теме "Реверс-инжиниринг"
   Условие: необходимо в одном из исполняемых файлов (например, исполняемый файл программы или драйвера) или образов памяти процесса, который содержит скрытую информацию и зашифрованные данные провести реверс-инжиниринг с целью извлечения скрытой информации или восстановления алгоритма шифрования.
   Цель: практическое применение знаний о методах реверс-инжиниринга, обратной разработке и анализе исполняемых файлов.

LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Зачет

Список примерных вопросов

1. Основы кибербезопасности
2. Анализ угроз кибербезопасности
3. Методы обнаружения и предотвращения кибератак
4. Криптография и ее роль в кибербезопасности
5. Защита сетей и систем от внешних угроз
6. Идентификация и аутентификация в киберпространстве
7. Методы защиты данных и конфиденциальной информации
8. Роль человеческого фактора в кибербезопасности
9. Управление доступом и привилегиями в информационных системах
10. Аудит безопасности информационных ресурсов
11. Защита мобильных устройств и приложений
12. Безопасность интернета вещей (IoT)
13. Применение искусственного интеллекта в кибербезопасности

14. Стандарты и сертификация в области кибербезопасности
15. Защита от социальной инженерии и фишинга
16. Борьба с вредоносным программным обеспечением

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Профессиональное воспитание	профориентационная деятельность	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-3	З-3	Домашняя работа Зачет Лабораторные занятия Контрольная работа Лекции