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
1156044	Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Защита информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры	**Код ОП** 1. 10.04.01/22.01
Направление подготовки 1. Информационная безопасность	**Код направления и уровня подготовки** 1. 10.04.01

Программа модуля 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	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
3	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)

1.1. Аннотация содержания модуля

Целью модуля является формирование знаний и умений в области противодействия компьютерной преступности, решения задач в области в области установки, настройки и эксплуатации систем обнаружения компьютерных атак на значимых объектах критической информационной инфраструктуры (далее КИИ), реагирования на компьютерные инциденты на значимых объектах КИИ, а также проектирования базы правил для обнаружения и предупреждения направленных компьютерных атак, формирование рекомендаций по принятию мер, направленных на недопущение повторений подобных инцидентов в будущем. В модуле изучаются основные подходы к организации экспертно-аналитической деятельности в сфере обеспечения безопасности объектов КИИ; принципы аналитической работы с системами обнаружения атак (далее — СОА) при помощи систем управления базами данных (далее — СУБД); стандарты и нормативные правовые акты, описывающие порядок реагирования на компьютерные инциденты на значимых объектах КИИ; требования, предъявляемые к системам обнаружения компьютерных атак при защите значимых объектов КИИ; механизмы компьютерного следообразования; принципы функционирования и построения систем обнаружения компьютерных атак; ликвидация последствий компьютерного инцидента и совершенствование применяемых мер защиты. В модуль входят: - Эксплуатация систем обнаружения компьютерных атак на объектах КИИ; - Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ; - Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ.

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	Эксплуатация систем обнаружения компьютерных атак на объектах КИИ	4
2	Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ	4
3	Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ	4
	ИТОГО по модулю:	12

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Защищенные информационные системы
Постреквизиты и кореквизиты модуля	1. Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и

	ликвидации последствий компьютерных атак (ГосСОПКА)

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
Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ	ПК-5 - Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа	З-1 - Различать стандарты ЕСКД, ЕСТД и ЕСПД З-3 - Использовать способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах З-5 - Понимать методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее З-6 - Использовать программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее З-7 - Использовать методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий З-8 - Использовать средства контроля защищенности информации от несанкционированного доступа З-9 - Различать методики контроля защищенности информации от несанкционированного доступа У-1 - Разрабатывать техническое задание на создание программно-технического

		средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-3 - Разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-1 - Разрабатывать технический (эскизный) проект программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-3 - Разрабатывать рабочую и эксплуатационную документацию на техническое средство защиты П-4 - Применять информацию от несанкционированного доступа и специальных воздействий на нее
Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ	ПК-5 - Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа	З-8 - Использовать средства контроля защищенности информации от несанкционированного доступа З-9 - Различать методики контроля защищенности информации от несанкционированного доступа З-10 - Различать средства проектирования электронных схем У-1 - Разрабатывать техническое задание на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-3 - Разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-1 - Разрабатывать технический (эскизный) проект программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее

		П-3 - Разрабатывать рабочую и эксплуатационную документацию на техническое средство защиты
Эксплуатация систем обнаружения компьютерных атак на объектах КИИ	ПК-5 - Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа	З-1 - Различать стандарты ЕСКД, ЕСТД и ЕСПД З-2 - Использовать современные информационные технологии (операционные системы, базы данных, вычислительные сети) З-3 - Использовать способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах З-4 - Различать основные классы и виды уязвимостей программного обеспечения З-6 - Использовать программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее З-8 - Использовать средства контроля защищенности информации от несанкционированного доступа З-10 - Различать средства проектирования электронных схем У-1 - Разрабатывать техническое задание на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-2 - Разрабатывать проектно-сметную документацию на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-3 - Разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-1 - Разрабатывать технический (эскизный) проект программно-

		технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-2 - Испытывать программно-технические средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-3 - Разрабатывать рабочую и эксплуатационную документацию на техническое средство защиты П-4 - Применять информацию от несанкционированного доступа и специальных воздействий на нее

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Эксплуатация систем обнаружения компьютерных атак на объектах КИИ

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	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
3	Пономарева Ольга Алексеевна	-, -	старший преподаватель	УНЦ ИБ

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

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Гибилинда Роман Владимирович, Ассистент,**
- **Коллеров Андрей Сергеевич, доцент, УНЦ ИБ**
- **Пономарева Ольга Алексеевна, старший преподаватель, 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
Р1	Подходы к организации экспертноаналитической деятельности в центрах мониторинга	Центр мониторинга информационной безопасности (Security Operation Center); Обзор методики CRAMM; Обзор методологии COBIT for Risk Реестр уязвимостей БДУ ФСТЭК России; MITRE CVE и база данных NVD; OSVDB; Secunia Advisory and Vulnerability Database; VND от CERT/CC; Exploit Database; Агрегаторы информации об уязвимостях Регламентирование в российской нормативной базе деятельности по анализу угроз; Сценарии Cyber Kill Chain; Применение ATT&CK для моделирования угроз Автоматическое извлечение и сканирование файлов; Автоматическое назначение имени хоста

		и подсети; CIDR подсети для сопоставления имени сегмента сети через конфигурационный файл; Определение интерфейса имени хоста и имен подсетей CIDR; Elasticsearch; Способы установки Malcolm; Анализ конфигурации узлов сети; Исключения стандартов CIS
Р2	Аналитическая работа с СОА при помощи СУБД	Оператор SELECT; Проекция; Выбор; Соединения; Выбор столбцов; SQL-операторы; Заголовки столбцов; Использование арифметических операторов; Использование псевдонимов; Структура таблицы Ограничение строк выборки; Символьные строки и даты в предложении WHERE; Операторы сравнения; Подстановочные символы; Идентификатор ESCAPE; Примеры сортировки Функции SQL; Однострочные и многострочные функции; Символьные и числовые функции; Виды функций; Таблица DUAL; Работа с датами Функции преобразования; Неявное и явное 17 преобразование; Инструкции; Вложенные функции; Условное выражение CASE

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Эксплуатация систем обнаружения компьютерных атак на объектах КИИ

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. Мартишин, С. А.; Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench. Методы и средства проектирования информационных систем и технологий. Инструментальные средства информационных систем : учеб. пособие для студентов вузов, обучающихся по направлению 230400 "Информ. системы и технологии".; ФОРУМ, Москва; 2012 (1 экз.)

2. Просис, К., Труфанов, О., Головко, А.; Расследование компьютерных преступлений; Лори, Москва; 2013 (1 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

Эксплуатация систем обнаружения компьютерных атак на объектах КИИ

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	1 Лекции Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		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	
2	Практические занятия	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
3	Консультации	1 Лекции 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 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	Самостоятельная работа студентов	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
2	Пономарева Ольга Алексеевна	-, -	старший преподаватель	УНЦ ИБ

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

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Коллеров Андрей Сергеевич, доцент, УНЦ ИБ**
- **Пономарева Ольга Алексеевна, старший преподаватель, 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
Р1, Т1	Подходы к организации экспертно-аналитической деятельности в центрах мониторинга	Центр мониторинга информационной безопасности (Security Operation Center); Обзор методики CRAMM; Обзор методологии COBIT for Risk Нормативное регулирование деятельности центров ГосСОПКА; подключение к ГосСОПКА; реагирование на инцидент Реестр уязвимостей БДУ ФСТЭК России; MITRE CVE и база данных NVD; OSVDB; Secunia Advisory and Vulnerability Database; VND от CERT/CC; Exploit Database; Агрегаторы информации об уязвимостях Автоматическое извлечение и сканирование файлов; Автоматическое назначение имени хоста и подсети; CIDR подсети для сопоставления имени сегмента сети через конфигурационный файл; Определение интерфейса имени хоста и имен подсетей CIDR; Elasticsearch; Способы установки Malcolm; Анализ

		конфигурации узлов сети; Исключения стандартов CIS
Р2, Т1	Аналитическая работа с СОА при помощи СУБД	Оператор SELECT; Проекция; Выбор; Соединения; Выбор столбцов; SQL-операторы; Заголовки столбцов; Использование арифметических операторов; Использование псевдонимов; Структура таблицы Ограничение строк выборки; Символьные строки и даты в предложении WHERE; Операторы сравнения; Подстановочные символы; Идентификатор ESCAPE; Примеры сортировки Функции SQL; Однострочные и многострочные функции; Символьные и числовые функции; Виды функций; Таблица DUAL; Работа с датами Функции преобразования; Неявное и явное преобразование; Инструкции; Вложенные функции; Условное выражение CASE.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ

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. , Синадский, Н. И.; Защита информации в компьютерных сетях : практ. курс.; УГТУ-УПИ, Екатеринбург; 2008 (2 экз.)

2. Просис, К., Труфанов, О., Головко, А.; Расследование компьютерных преступлений; Лори, Москва;

2013 (1 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

Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ

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	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	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 Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	
2	Практические занятия	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
3	Консультации	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	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		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	Самостоятельная работа студентов	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
2	Пономарева Ольга Алексеевна	-, -	старший преподаватель	УНЦ ИБ

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

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Коллеров Андрей Сергеевич, доцент, УНЦ ИБ**
- **Пономарева Ольга Алексеевна, старший преподаватель, 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
Р1, Т1	Подходы к организации экспертно-аналитической деятельности в центрах мониторинга	Центр мониторинга информационной безопасности (Security Operation Center); Обзор методики CRAMM; Обзор методологии COBIT for Risk Нормативное регулирование деятельности центров ГосСОПКА; подключение к ГосСОПКА; реагирование на инцидент Реестр уязвимостей БДУ ФСТЭК России; MITRE CVE и база данных NVD; OSVDB; Secunia Advisory and Vulnerability Database; VND от CERT/CC; Exploit Database; Агрегаторы информации об уязвимостях Автоматическое извлечение и сканирование файлов; Автоматическое назначение имени хоста и подсети; CIDR подсети для сопоставления имени сегмента сети через конфигурационный файл; Определение интерфейса имени хоста и имен подсетей CIDR; Elasticsearch; Способы установки Malcolm; Анализ

		конфигурации узлов сети; Исключения стандартов CIS
Р2, Т1	Аналитическая работа с СОА при помощи СУБД	Оператор SELECT; Проекция; Выбор; Соединения; Выбор столбцов; SQL-операторы; Заголовки столбцов; Использование арифметических операторов; Использование псевдонимов; Структура таблицы Ограничение строк выборки; Символьные строки и даты в предложении WHERE; Операторы сравнения; Подстановочные символы; Идентификатор ESCAPE; Примеры сортировки Функции SQL; Однострочные и многострочные функции; Символьные и числовые функции; Виды функций; Таблица DUAL; Работа с датами Функции преобразования; Неявное и явное преобразование; Инструкции; Вложенные функции; Условное выражение CASE.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ

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. , 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.)

2. , Синадский, Н. И.; Защита информации в компьютерных сетях : практ. курс.; УГТУ-УПИ, Екатеринбург; 2008 (2 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

Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ

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	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	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	
2	Практические занятия	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
3	Консультации	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	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 Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	
4	Самостоятельная работа студентов	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 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES