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
1163600	Спецкурс 2

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	Карпушин Андрей Валерьевич	без ученой степени, без ученого звания	Старший преподаватель	интеллектуальных информационных технологий
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
3	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Спецкурс 2

1.1. Аннотация содержания модуля

Целью модуля является приобретение знаний, умений и практических навыков в области проведения оценки соответствия систем управления обеспечения информационной безопасности организаций согласно требованиям современных источников нормативно-правового и технического регулирования. В рамках модуля проходит освоение: глоссария, подходов и метрик проведения аудитов в разных системах технического и нормативно-правового регулирования; корпоративных коммуникаций; особенностей методов управления и организации информационной безопасности в современной корпоративной среде; подходов к описанию систем управления и обеспечения информационной безопасности, оценке рисков информационной безопасности, мер и средств контроля и управления такими рисками.

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	Спецкурс 2	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
Спецкурс 2	ПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства

	современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности У-1 - Определять оптимальные методы обеспечения информационной безопасности П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности
	ПК-2 - Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	З-1 - Изложить состав, классификацию, особенности функционирования программных средств системного и прикладного назначений У-1 - Рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности П-1 - Иметь навыки использования системного программного обеспечения для решения задач профессиональной деятельности П-2 - Иметь навыки использования прикладного программного обеспечения для решения задач профессиональной деятельности
	ПК-3 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	З-1 - Изложить состав и содержание Российских и международных нормативных правовых актов, нормативных и методических документов, межгосударственных и международных стандартов, регламентирующих деятельность по защите информации З-2 - Изложить методологию управления информационной безопасностью, основанную на нормативных и методических документах У-1 - Применять действующую нормативную базу, нормативные правовые

		акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации П-1 - Осуществлять обоснованный выбор методов поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации П-2 - Разрабатывать проекты нормативно-правовых актов и организационно-распорядительных документов, регламентирующих деятельность по защите информации
	ПК-9 - Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	З-1 - Описать основные методы администрирования и контроля функционирования средств и систем защиты информации телекоммуникационных систем З-2 - Описать основные методы инструментального мониторинга и аудита защищенности телекоммуникационных систем У-1 - Администрировать средства и системы защиты информации телекоммуникационных систем П-1 - Иметь практический опыт выбора средств контроля функционирования средств и систем управления информационной безопасностью телекоммуникационных систем

1.5. Форма обучения

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Спецкурс 2

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Карпушин Андрей Валерьевич	без ученой степени, без ученого звания	Старший преподаватель	интеллектуальных информационных технологий
2	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”

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

Протокол № _6_ от _26.05.2023_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Карпушин Андрей Валерьевич, Старший преподаватель, интеллектуальных информационных технологий**
- **Поршнев Сергей Владимирович, Профессор, 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	OSINT и Киберразведка	1. Методы используемые OSINT 2. Приватность и анонимность - Windows или Linux. Оценка защищенности и приватности данных JC 3. Whonixˆ - принципы работы, настройка параметров конфигурации - слабые места 4. Настройка рабочего места, урок 1: - Установка и настройка ОС с точки зрения безопасности - Настройка Хоста - Настройка сети 5. Настройка рабочего места, урок 2: - VPN - оптимальные коммерческие решения - VPN - своими руками - Безопасное общение (мессенджеры, почтовые клиенты) - Виртуальные машины

		6. Блок схемы Michael Bazell: - Поиск по Email - Поиск по Username - Поиск по ФИО - Поиск по телефонному номеру - Поиск по доменному имени - Поиск геолокации 7. Использование поисковых систем (ClearNet): - Поисковые операторы - Дорки поисковых систем - Сервисные дорки (Shodan, GitHub) - Принцип работы robots.txt 8. Поиск в DarkNet 9. Сбор информации о ФЛ 10. Сбор информации о ЮЛ 11. CounterOSINT - ФЛ 12. CounterOSINT - ЮЛ 13. Методы поиска по изображению 14. Open - source инструменты OSINT урок 1: - Сбор информации по IP - Сбор информации по Email - Обзор утечек (боты и сервисы) 15. Open - source инструменты урок 2: - OS Kali linux - SpiderFoot - OsintSan 16. Создаем свою ПС используя сервисы Google 17. GEOINT - Принципы поиска и определения координат объекта по изображению - Разбор кейсов
2	Реагирование	1) КА, КИ, обнаружение, регистрация, реагирование 2) CyberKillChain 3) MITRE&ATTACK (ч1) 4) MITRE&ATTACK (ч2)

		5) PoP (Pyramid of Pain) 6) Threat Hunting 7) Процесс обнаружения инцидента (ч1). Сбор данных об инфраструктуре (SIEM, XDR, EDR, NDR, NTA, NGFW, Sysmon). 8) Процесс обнаружения инцидента (ч2). Агрегация данный и формирование инцидентов. 9) Оркестрация процессов реагирования (IRP/SOAR) 10) Момент инцидента и первые действия (проверка на ЛПС, приоритезация, сбор информации, эскалация) 11) Реагирование средствами AD 12) Реагирование средствами сетевого оборудования 13) Реагирование средствами XDR 14) Физическое реагирование 15) Ликвидация последствий (восстановление) 16) Нарушение политик информационной безопасности
3	Цифровая криминалистика	1) Методологии DFIR 2) Сбор энергонезависимой информации в ОС Windows 3) Сбор энергонезависимой информации в ОС Linux 4) Поиск следов компрометации в ОС Windows 5) Поиск следов запуска программного обеспечения в ОС Windows 6) Поиск следов закрепления в ОС Windows 7) Поиск следов горизонтального продвижения в ОС Windows 8) Поиск следов компрометации в ОС Linux 9) Поиск следов закрепления в ОС Linux 10) Поиск следов горизонтального продвижения в ОС Linux 11) Методология сетевого криминалистического анализа 12) Средства сбора и анализа журналов (ELK-стэк) для сетевого криминалистического анализа 13) Анализ журналов МЭ, DNS, DHCP 14) Исследование сетевого трафика 15) Кейс 1: Заражение вирусом-шифровальщиком 16) Кейс 2: Подделка платежных поручений 17) Кейс 3: Анализ утечки конфиденциальных данных

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-2 - Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	У-1 - Рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Спецкурс 2

Электронные ресурсы (издания)

1. Дубровин, В. В.; Программирование на С : учебное пособие. 1. ; Тамбовский государственный технический университет (ТГТУ), Тамбов; 2017; https://biblioclub.ru/index.php?page=book&id=499439 (Электронное издание)

2. Литвиненко, В. А.; Программирование на С++ задач на графах : учебное пособие.; Южный федеральный университет, Таганрог; 2016; https://biblioclub.ru/index.php?page=book&id=493220 (Электронное издание)

3. ; Основы информационной безопасности : учебник.; Юнити-Дана|Закон и право, Москва; 2018; https://biblioclub.ru/index.php?page=book&id=562348 (Электронное издание)

4. Вострецова, Е. В.; Основы информационной безопасности : учебное пособие.; Издательство Уральского университета, Екатеринбург; 2019; https://biblioclub.ru/index.php?page=book&id=697636 (Электронное издание)

Печатные издания

1. , Семкин, С. Н., Беляков, Э. В., Гребнев, С. В., Козачок, В. И.; Основы организационного обеспечения информационной безопасности объектов информатизации : учеб. пособие по специальностям в обл. информ. безопасности.; Гелиос АРВ, Москва; 2005 (16 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

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

Спецкурс 2

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 Professional 2003 Win32 Russian CD-ROM Windows Server Datacenter 2012R2 Single MVL 2Proc A Each Academic
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в	Office Professional 2003 Win32 Russian CD-ROM

		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	Windows Server Datacenter 2012R2 Single MVL 2Proc A Each Academic
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 Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Windows Server Datacenter 2012R2 Single MVL 2Proc A Each Academic
4	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	Office Professional 2003 Win32 Russian CD-ROM Windows Server Datacenter 2012R2 Single MVL 2Proc A Each Academic

		Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством 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 Professional 2003 Win32 Russian CD-ROM Windows Server Datacenter 2012R2 Single MVL 2Proc A Each Academic