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
1157113	Методы расследования преступлений в сфере информационных технологий

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Информационная безопасность телекоммуникационных систем 2. Информационно-аналитические системы безопасности	**Код ОП** 1. 10.05.02/22.01 2. 10.05.04/22.01
Направление подготовки 1. Информационная безопасность телекоммуникационных систем; 2. Информационно-аналитические системы безопасности	**Код направления и уровня подготовки** 1. 10.05.02; 2. 10.05.04

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	
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 расследования преступлений в сфере информационных технологий

1.1. Аннотация содержания модуля

Модуль «Методы расследования преступлений в сфере информационных технологий» предназначен для теоретического и практического обучения студентов с комплексом методов и средств по раскрытию возможных преступлений совершенных с применением информационных технологий.

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	Методы расследования компьютерных преступлений	6
2	Методы расследования финансовых преступлений в сфере информационных технологий	3
	ИТОГО по модулю:	9

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Основы информационной безопасности
Постреквизиты и кореквизиты модуля	1. Методы и средства компьютерной криминалистики

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
Методы расследования компьютерных преступлений	УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению	З-1 - Описывать основные права и обязанности человека и гражданина и способы воспитания нетерпимого отношения к коррупции в различных областях жизнедеятельности

		З-2 - Характеризовать законодательные нормы, направленные на борьбу с коррупционным поведением, манипулятивные технологии формирования ложных и антиправовых действий У-1 - Распознавать признаки коррупционного поведения в различных областях жизнедеятельности и определять свою жизненную позицию на основе гражданских ценностей, социальной ответственности и нетерпимости к коррупции У-2 - Оценивать политические и социально-экономические события и ситуации, выявлять действия, направленные на манипулирование людьми, и определять способы противостояния психологической манипуляции П-1 - Иметь опыт решения проблемных ситуаций, связанных с коррупционным поведением граждан, нарушением гражданских прав, применением манипулятивных технологий формирования ложных и антиправовых действий, опираясь на законодательные нормы и собственную позицию нетерпимого отношения к коррупции
	ПК-2 - Способен проводить финансовые расследования в целях ПОД/ФТ в организации **(Информационно-аналитические системы безопасности)**	З-1 - Характеризовать методы сбора, обработки и анализа информации З-2 - Перечислить инструменты для проведения анализа З-3 - Перечислить программное обеспечение, используемое в аналитической деятельности З-4 - Описать типологии отмывания денег З-5 - Перечислить признаки наличия преступления по ОД/ФТ З-6 - Описать уязвимости финансовых продуктов и услуг в отношении ОД/ФТ У-1 - Анализировать информацию о подозрительных операциях и сделках

		У-2 - Проверять соблюдение всех установленных процедур в рамках используемых методов У-3 - Осуществлять сбор информации У-4 - Прогнозировать развитие событий и их последствия У-5 - Формулировать выявленные закономерности и полученные результаты У-6 - Подготавливать аналитические и отчетные материалы П-1 - Иметь опыт разработки документов, рекомендаций, методических материалов по направлению деятельности П-2 - Иметь опыт проверки полученной информации о возможных фактах ОД/ФТ по результатам выявления в организации операций (сделок), подлежащих контролю в целях ПОД/ФТ
	ПК-3 - Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов **(Информационная безопасность телекоммуникационных систем)**	З-1 - Различать виды компьютерных преступлений, правонарушений и инцидентов З-2 - Объяснять принципиальные различия между компьютерным преступлением, правонарушением и инцидентом У-1 - Составлять план проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов П-1 - Осуществлять сбор, обработку и анализ информации при расследовании компьютерных преступлений, правонарушений и инцидентов
Методы расследования финансовых преступлений в сфере информационных технологий	УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению	З-1 - Описывать основные права и обязанности человека и гражданина и способы воспитания нетерпимого отношения к коррупции в различных областях жизнедеятельности З-2 - Характеризовать законодательные нормы, направленные на борьбу с коррупционным поведением, манипулятивные технологии формирования ложных и антиправовых действий

		У-1 - Распознавать признаки коррупционного поведения в различных областях жизнедеятельности и определять свою жизненную позицию на основе гражданских ценностей, социальной ответственности и нетерпимости к коррупции У-2 - Оценивать политические и социально-экономические события и ситуации, выявлять действия, направленные на манипулирование людьми, и определять способы противостояния психологической манипуляции П-1 - Иметь опыт решения проблемных ситуаций, связанных с коррупционным поведением граждан, нарушением гражданских прав, применением манипулятивных технологий формирования ложных и антиправовых действий, опираясь на законодательные нормы и собственную позицию нетерпимого отношения к коррупции
	ПК-2 - Способен проводить финансовые расследования в целях ПОД/ФТ в организации **(Информационно-аналитические системы безопасности)**	З-1 - Характеризовать методы сбора, обработки и анализа информации З-2 - Перечислить инструменты для проведения анализа З-3 - Перечислить программное обеспечение, используемое в аналитической деятельности З-4 - Описать типологии отмывания денег З-5 - Перечислить признаки наличия преступления по ОД/ФТ З-6 - Описать уязвимости финансовых продуктов и услуг в отношении ОД/ФТ У-1 - Анализировать информацию о подозрительных операциях и сделках У-2 - Проверять соблюдение всех установленных процедур в рамках используемых методов У-3 - Осуществлять сбор информации У-4 - Прогнозировать развитие событий и их последствия

		У-5 - Формулировать выявленные закономерности и полученные результаты У-6 - Подготавливать аналитические и отчетные материалы П-1 - Иметь опыт разработки документов, рекомендаций, методических материалов по направлению деятельности П-2 - Иметь опыт проверки полученной информации о возможных фактах ОД/ФТ по результатам выявления в организации операций (сделок), подлежащих контролю в целях ПОД/ФТ
	ПК-3 - Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов **(Информационная безопасность телекоммуникационных систем)**	З-1 - Различать виды компьютерных преступлений, правонарушений и инцидентов З-2 - Объяснять принципиальные различия между компьютерным преступлением, правонарушением и инцидентом У-1 - Составлять план проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов П-1 - Осуществлять сбор, обработку и анализ информации при расследовании компьютерных преступлений, правонарушений и инцидентов

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы расследования компьютерных преступлений

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Искакова Ксения Орестовна	без ученой степени, без ученого звания	Старший преподаватель	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	

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

Протокол № _9_ от _21.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Искакова Ксения Орестовна, Старший преподаватель,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Понятие, виды и особенности компьютерных преступлений	Понятие об информационных и компьютерных преступлениях. Особенности и причины информационных преступлений. Понятие о неправомерном обороте информации. Составы информационных преступлений, предусмотренные Уголовным кодексом РФ. Преступления в форме незаконного распространения, разглашения и передачи информации. Незаконное воспрепятствование доступу к информации. Незаконное хранение и использование конфиденциальной информации. Формы информационной фальсификации. Компьютерные мошенничества. 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.
2	Криминалистическая характеристика преступлений в сфере компьютерной информации	Особенности подготовки компьютерных преступлений. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Виды ЭВМ по отношению к преступной деятельности. Способы нарушения работы ЭВМ, системы ЭВМ и их сети. Формы несанкционированного копирования, удаления, модификации и блокирования защищаемой законом компьютерной информации. Ответственность за совершение преступлений, предусмотренных ст. 272 – 274 УК РФ. Ст. 138 УК РФ - нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений – характеристика и ответственность за совершение преступления. Ст. 159, п. 6 УК РФ - мошенничество в сфере компьютерной информации. – характеристика и ответственность за совершение преступления. Ст. 183 УК РФ - незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну - характеристика и ответственность за совершение преступления
3	Следовая картина компьютерных преступлений	Машинные носители информации как место нахождения компьютерной информации. Следы криминальной деятельности на машинных носителях. Признаки воздействия на информацию.
4	Организация расследования	Составляющие части расследования. Краткая характеристика составляющих частей расследования. Особенности расследования компьютерных преступлений. Программа расследования на первоначальном этапе. Тактические особенности

		проведения ОМП. Программа расследования на последующем и завершающем этапах.
5	Следственные ситуации и их разрешения в ходе предварительного расследования	Классификация следственных ситуаций по источнику информации. Классификация следственных ситуаций по объему информации, имеющийся в распоряжении следствия. Ход проведений предварительной и основной проверок. Схемы проведений проверок.
6	Организация и проведение осмотра происшествия	Понятие осмотра места происшествия. Организация осмотра места происшествия. Тактические приемы осмотра места происшествия. Фиксация хода и результатов осмотра места происшествия. Оперативно-розыскные мероприятия примыкающие к осмотру места происшествия.
7	Осмотр средств компьютерной техники	Протокол осмотра средств компьютерной техники. Требования при осмотре средств компьютерной техники. Интересующие сведения при осмотре компьютерной техники. Правила обращения с компьютерной техникой. Цели осмотра компьютерной техники. Осмотр документов учета работы на компьютерной технике.
8	Производство обыска и выемки средств компьютерной техники	Криминалистические цели и задачи производства обыска и выемки в процессе расследования преступлений в сфере компьютерной безопасности. Тактика подготовки к производству обыска и выемки в процессе расследования преступлений в сфере компьютерной безопасности. Тактика производства обыска и выемки в процессе расследования преступлений в сфере компьютерной безопасности. Фиксация хода и результатов обыска и выемки в процессе расследования преступлений в сфере компьютерной безопасности
9	Использование специальных познаний.	Компетенции эксперта в области информационной безопасности. Классификация объектов компьютерной экспертизы. Аппаратные,

	Судебная компьютернотехническая экспертиза.	программные и информационные объекты. Методика экспертизы аппаратных, программных и информационных объектов. Методика экспертизы целостной компьютерной системы, устройства. Виды компьютернотехнической экспертизы специальных средств
10	Допрос подозреваемых, обвиняемых и свидетелей по делам о компьютерных преступлениях	Понятие, сущность и задачи и значение допроса по делам о компьютерных преступлениях. Организация вызова свидетелей для производства следственных действий. Подготовка к допросу. Составление плана проведения следственного действия. Классификация тактических приемов допроса. Тактические приемы допроса подозреваемого и свидетеля. Фиксация хода и результатов допроса
11	Судебные ситуации и их разрешение в ходе судебного следствия по компьютерным преступлениям	Понятие судебной ситуации. Специфика и роль судебных ситуаций в криминалистике. Виды судебных ситуаций и алгоритмы их разрешения. Типичные и конкретные судебные ситуации.
12	Криминалистическое предупреждение компьютерных преступлений. Меры обеспечения криминалистического предупреждения	Понятие криминалистического предупреждения компьютерных преступлений. Задачи криминалистического предупреждения криминалистических преступлений. Разработка средств, приемов и методов предупреждения компьютерных преступлений. Классификация обстоятельств, способствующих совершению преступлений в сфере компьютерной информации. Обстоятельства, способствующие к неправомерному доступу к компьютерной информации. Обстоятельства, способствующие созданию, использованию и распространению вредоносных программ для ЭВМ. Анализ материалов уголовного дела, оперативных данных и другой имеющейся информации. Классификация мер предупреждения компьютерных преступлений. Правовые меры предупреждения. Меры предупреждения

		организационно-технического характера. Криминалистические меры предупреждения. Организационные мероприятия по предупреждению криминалистических преступлений. Методы регистрации попыток НСД.

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	ПК-3 - Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	З-1 - Различать виды компьютерных преступлений, правонарушений и инцидентов З-2 - Объяснять принципиальные различия между компьютерным преступлением, правонарушением и инцидентом У-1 - Составлять план проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов П-1 - Осуществлять сбор, обработку и анализ информации при расследовании компьютерных преступлений, правонарушений и инцидентов

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы расследования компьютерных преступлений

Электронные ресурсы (издания)

1. ; Математические модели новых физических эффектов в скрещенных полях и их практические приложения : монография.; Саратовский государственный технический университет имени Ю.А. Гагарина, ЭБС АСВ, Саратов; 2020; http://www.iprbookshop.ru/108692.html (Электронное издание)

Печатные издания

1. Кэрриэ, Кэрриэ Б.; Криминалистический анализ файловых систем : [пер. с англ.].; Питер, Москва ; Санкт-Петербург ; Нижний Новгород [и др.]; 2007 (2 экз.)

2. Романец, Ю. В., Тимофеев, П. А., Шаньгин, В. Ф.; Защита информации в компьютерных системах и сетях; Радио и связь, Москва; 1999 (1 экз.)

3. Айков, Айков Д., Воропаев, В. И., Сейгер, Сейгер К., Трехалин, Г. Г., Фонсторх, Фонсторх У.; Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями; Мир, Москва; 1999 (0 экз.)

4. Брэгг, Брэгг Р., Соловченко, А. Е.; Безопасность сети на основе Microsoft Windows Server 2003. Учебный курс Microsoft: экзамен 70-298 MCSE : офиц. пособие для самоподготовки.; Русская Редакция : Питер, Москва ; Санкт-Петербург ; Нижний Новгород [и др.]; 2005 (1 экз.)

5. Бакланов, В. В.; Введение в информационную безопасность. Направления информационной защиты : курс лекций.; Изд-во Уральского университета, Екатеринбург; 2007 (3 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 расследования компьютерных преступлений

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	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 Подключение к сети Интернет	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	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 Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES

3	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 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES
4	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 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES

		Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы расследования финансовых преступлений в сфере информационных технологий

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Князева Наталия Сергеевна	кандидат технических наук, без ученого звания	Доцент	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	

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

Протокол № _9_ от _21.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Князева Наталия Сергеевна, Старший преподаватель,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**

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	Информационная безопасность в системе национальной безопасности Российской Федерации	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства
2	Информационная война, методы и средства ее ведения	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы общества в

		информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. средств и систем, как уже развернутых, так и создаваемых на территории России. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.
3	Платежные терминалы	Классификация платежных терминалов по функциональным возможностям. Агентская и банковская схемы функционирования. Функциональные части и их назначение. Корпус платежного терминала, модем для организации обмена информацией между платежным терминалом и сервером электронной платежной системы. Конструктивные особенности Безопасность платежных терминалов. Этапы работы платежных терминалов.
4	Основные виды угроз в отношении Банкоматов и платежных терминалов	Общие критерии формирования модели нарушителя. Типология нарушителей. Категории нарушителей и виды совершаемых преступлений. Цели нарушителей. Оценка опасности нарушителя

		исходя из степени его осведомленности, оснащенности и подготовленности, типология нарушителей по подготовленности к преодолению системы охраны. Категории нарушителей и виды совершаемых ими преступлений, связанных с незаконным проникновением в зону размещения банкоматов и 7 платежных терминалов, криминальными посягательствами и конфиденциальную информацию банкоматов, а также на пользователей платежных терминалов и банкоматов, инкассаторов и обслуживающий персонал. Квалификация преступления. Угрозы держателю карты, обслуживающему персоналу. Нападение. Неправомерный доступ к Персональным данным. Угрозы банковской карте, ее реквизитам. Скимминг. Шимминг. Траппинг. Угрозы банкоматам и платежным терминалам. Несанкционированное проникновение на территорию, в здание, где установлены платежные терминалы и банкоматы. Вскрытие банкоматов. Хищение, срыв с места установки.
5	Обеспечение безопасности платежных терминалов и банкоматов	Требования Положения ЦБ РФ по обеспечению безопасной эксплуатации платежных терминалов и банкоматов. Основные организационные и технические меры по защите информации банкоматов и платежных терминалов. Выбор мест размещения банковских устройств самообслуживания. Влияние категории на место размещения. Анализ уязвимостей программного обеспечения банкоматов и терминалов. Обеспечение фиксации. Инженерно-техническая укрепленность и оборудование техническими средствами охраны банковских устройств самообслуживания и мест их размещения.

		Регулирование и установка порядков срока хранения информации, обновления версий, работы с клиентами. Оценка времени взлома. Минимальные требования по устойчивости к взлому сейфов. Системы удаленного мониторинга состояния устройства, обеспечивающие контроль надлежащего функционирования защитного оборудования и специального программного обеспечения. Требования к системе передачи тревожных сообщений для защиты банкоматов и платежных терминалов. Фиксация фактов атак и попыток их совершения. Информирование Банка России. Информирование населения.

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	ПК-3 - Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	З-1 - Различать виды компьютерных преступлений, правонарушений и инцидентов З-2 - Объяснять принципиальные различия между компьютерным преступлением, правонарушением и инцидентом У-1 - Составлять план проведения экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов П-1 - Осуществлять

				сбор, обработку и анализ информации при расследовании компьютерных преступлений, правонарушений и инцидентов

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы расследования финансовых преступлений в сфере информационных технологий

Электронные ресурсы (издания)

1. ; Мошенничество в платежной сфере: бизнес-энциклопедия : энциклопедия.; Интеллектуальная Литература, Москва; 2016; https://biblioclub.ru/index.php?page=book&id=430951 (Электронное издание)

2. 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)

3. Аверченков, В. И.; Аудит информационной безопасности : учебное пособие.; ФЛИНТА, Москва; 2021; https://biblioclub.ru/index.php?page=book&id=93245 (Электронное издание)

4. Башлы, П. Н.; Информационная безопасность: учебно-практическое пособие : учебное пособие.; Евразийский открытый институт, Москва; 2011; https://biblioclub.ru/index.php?page=book&id=90539 (Электронное издание)

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

Методы расследования финансовых преступлений в сфере информационных технологий

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES
2	Практические 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 Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr 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 Подключение к сети Интернет	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES
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 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
5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES

		Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	