Общество с ограниченной ответственностью
«ЛАН-ПРОЕКТ»

«Утверждаю»

Генеральный директор
_____/Крохин С.Л.

« 02» июня 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Современные технологии извлечения и анализа данных из цифровых устройств»

Объем программы (трудоемкость): 56 академических часов.

Срок освоения: 3 учебных недели.

Форма обучения: очная.

Москва

2025 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Характеристика программы:

Дополнительная профессиональная программа повышения квалификации «Современные технологии извлечения и анализа данных из цифровых устройств» (далее – программа) является учебно-методическим нормативным документом, регламентирующим содержание, организационно-методические формы и трудоемкость обучения.

Дополнительная профессиональная программа повышения квалификации **«Современные технологии извлечения и анализа данных из цифровых устройств»** разработана в соответствии с нормами Федерального закона от 29 декабря 2012 г. № 273- ФЗ «Об образовании в Российской Федерации» с учетом требований приказа Минобрнауки России от 01.07.2013 № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», приказа Министерства науки и высшего образования Российской Федерации от 19 октября 2020 года № 1316 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности», профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (утв. приказом Министерства труда и социальной защиты РФ от 14 сентября 2022 года N 533н), Федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (утв. приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427).

1.2. Категория обучающихся: лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование; специалисты в области информационной безопасности и извлечения данных.

1.3. Объем программы (трудоемкость): общая трудоемкость 56 академических часов.

1.4. Срок освоения: 3 учебных недели.

1.5. Форма обучения: очная.

1.6. Документ, выдаваемый после завершения обучения: удостоверение о повышении квалификации установленного образца.

2. ЦЕЛИ И ЗАДАЧИ ПРОГРАММЫ

2.1. Цель программы заключается в получении теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы в области цифровой криминалистики, извлечения информации и информационной безопасности.

2.2. Задачи программы:
1. Формирование знаний методов извлечения и анализа данных из мобильных устройств и облачных сервисов.
2. Формирование знаний основ мобильной криминалистики.
3. Формирование знаний и навыков извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
4. Формирование знаний и навыков извлечения и анализа информации из iPhone и iPad.
5. Формирование знаний основ шифрования и анализа данных в криминалистике.
6. Формирование знаний и навыков в области техник и инструментов для извлечения данных.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

3.1. **Программа направлена** на совершенствование и приобретения новых компетенций в области цифровой криминалистики, извлечения информации и информационной безопасности, обеспечивающих качественную, безопасную и эффективную профессиональную деятельность в современных условиях.
3.2. В планируемых результатах обучения отражается связь с требованиями соответствующего профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (утв. приказом Министерства труда и социальной защиты РФ от 14 сентября 2022 года N 533н) и Федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (утв. приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427).

3.3. Программа направлена на совершенствование и получение слушателями универсальных, общепрофессиональных и профессиональных компетенций.

В результате освоения программы слушатели будут обладать *универсальными компетенциями* (УК), включающими в себя способность:

УК-1. Осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
УК-2. Определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.

В результате освоения программы слушатели будут обладать *общепрофессиональными компетенциями* (ОПК):

ОПК-1. Оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;
ОПК-2. Применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
ОПК-3. При решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-4. Использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;
ОПК-5. Применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

3.3. Планируемым результатом обучения является освоение как теоретических знаний, так и практических умений и навыков.

В результате освоения программы обучающиеся
будут знать:

- Архитектуру и пользовательские интерфейсы операционных систем;
- Типовые средства защиты информации в операционных системах;
- Общие принципы функционирования программно-аппаратных средств криптографической защиты информации;
- Форматы хранения информации в анализируемой системе
- Основные форматы файлов, используемые в компьютерных системах;
- Особенности хранения конфигурационной и системной информации в компьютерных системах;
- Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;
- Методы анализа остаточной информации;
- Криптографические алгоритмы и особенности их программной реализации;
- Методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Основ мобильной криминалистики.
- Особенности извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.

- Особенности извлечения и анализа информации из iPhone и iPad.
- Основы шифрования и анализа данных в криминалистике.
- Техники и инструменты для извлечения данных.
- Инструменты и решения от Elcomsoft для извлечения данных из устройств.

будут уметь:
- Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
- Настраивать компоненты подсистем защиты информации операционных систем;
- Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;
- Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;
- Анализировать структуру механизма возникновения и обстоятельства события;
- Выявлять возможные траектории состояний функционирования системы;
- Применять методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Осуществлять извлечение и анализ информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
- Осуществлять извлечение и анализ информации из iPhone и iPad.
- Применять техники и инструменты для извлечения данных.
- Применять инструменты и решения от Elcomsoft для извлечения данных из устройств.

4. УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы повышения квалификации «Современные технологии извлечения и анализа данных из цифровых устройств»

Цель обучения – заключается в получении теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы в области цифровой криминалистики, извлечения информации и информационной безопасности.

Категория слушателей – лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование; специалисты в области информационной безопасности и извлечения данных.
Трудоемкость обучения: 56 академических часов.

Форма обучения: очная

№ п/п	Наименование компонентов программы	Трудоемкость, ак. ч.[1]				Форма контроля
		Всего	Лекции	Практические занятия / Самостоятельная работа	Контроль	
1	**Модуль 1. Основы мобильной криминалистики**	**11**	**8**	**3**		
1.1	Тема 1.1. Мобильные устройства как объект криминалистического исследования: изучаем все аспекты	1	1			
1.2	Тема 1.2. Обзор ключевых мобильных платформ	1	1			
1.3	Тема 1.3. Алгоритм сохранения и извлечения данных	1	1			
1.4	Тема 1.4. Сравнительный анализ физических, логических и облачных методов исследования	1	1			
1.5	Тема 1.5. Основные принципы криминалистических исследований мобильных устройств: правила и общий порядок работы	1	1			
1.6	Тема 1.6. Инструменты для анализа информации с мобильных устройств	2	1	1		
1.7	Тема 1.7. Техники извлечения данных из мобильных устройств	2	1	1		
1.8	Тема 1.8. Способы получения данных из iOS-устройств с использованием продуктов Elcomsoft	2	1	1		
2	**Модуль 2. Низкоуровневое извлечение**	**16**	**10**	**6**		
2.1	Тема 2.1. Введение в основы низкоуровневого анализа	1	1			
2.2	Тема 2.2. Механизмы защиты мобильных	1	1			

[1] Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

	устройств и техники извлечения данных					
2.3	Тема 2.3. Понятие уязвимостей загрузчиков	1	1			
2.4	Тема 2.4. Извлечение данных из iPhone и iPad	1	1			
2.5	Тема 2.5. Физический анализ и джейлбрейк	2	1	1		
2.6	Тема 2.6. Установка и использование агента-экстрактора	2	1	1		
2.7	Тема 2.7. Препятствия при извлечении и расшифровке информации	2	1	1		
2.8	Тема 2.8. Методы получения данных с устройств Qualcomm	2	1	1		
2.9	Тема 2.9. Извлечение информации из чипсетов Spreadtrum и МТК	2	1	1		
2.10	Тема 2.10. Специфика чипов Samsung Exynos	2	1	1		
3	**Модуль 3. Низкоуровневое и логическое извлечение**	**6**	**3**	**3**		
3.1	Тема 3.1. Техники подбора паролей для расшифровки данных	2	1	1		
3.2	Тема 3.2. Способы извлечения данных из поврежденных устройств	2	1	1		
3.3	Тема 3.3. Кросс-платформенные методы извлечения данных	2	1	1		
4	**Модуль 4. Основы шифрования и анализа данных в криминалистике**	**8**	**6**	**2**		
4.1	Тема 4.1. Анализ данных мобильных приложений	1	1			
4.2	Тема 4.2. Основы шифрования и его значение в криминалистике	1	1			
4.3	Тема 4.3. Возможности восстановления удаленных данных	1	1			
4.4	Тема 4.4. Методы доступа к зашифрованной информации	1	1			
4.5	Тема 4.5. Структура Elcomsoft Premium Forensic Bundle	2	1	1		
4.6	Тема 4.6. Основные действия при извлечении информации	2	1	1		

	с цифровых носителей с целью их исследования					
5	**Модуль 5. Облачные технологии в криминалистике**	**13**	**8**	**5**		
5.1	Тема 5.1. Роль облачных сервисов в мобильной криминалистике	1	1			
5.2	Тема 5.2. Извлечение данных из облаков iCloud и Google Account	2	1	1		
5.3	Тема 5.3. Основы аутентификации и двухфакторной авторизации	1	1			
5.4	Тема 5.4. Роль токенов безопасности и маркеров аутентификации	2	1	1		
5.5	Тема 5.5. Уникальные аспекты защиты с использованием двухфакторной аутентификации	1	1			
5.6	Тема 5.6. Извлечение паролей от учетных записей и данных приложений	2	1	1		
5.7	Тема 5.7. Доступ к данным мессенджеров через облачные сервисы	2	1	1		
5.8	Тема 5.8. Получение информации из социальных сетей	2	1	1		
6	**Итоговая аттестация**	**2**			**2**	**Практическое задание**
7	**Итого**	**56**	**35**	**19**	**2**	

5. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК дополнительной профессиональной программы повышения квалификации «Современные технологии извлечения и анализа данных из цифровых устройств»

Календарный график обучения является примерным, составляется и утверждается для каждой группы.

Срок освоения программы — 3 учебных недели.

Начало обучения — по мере набора группы.

Примерный режим занятий: 3-5 раз в неделю по 3-4 академических часа в день[2].

Итоговая аттестация проводятся согласно графику.

[2] Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

№ п/п	Наименование компонентов программы	1 неделя	2 неделя	3 неделя
1	Модуль 1. Основы мобильной криминалистики	11		
2	Модуль 2. Низкоуровневое извлечение	9	7	
3	Модуль 3. Низкоуровневое и логическое извлечение		6	
4	Модуль 4. Основы шифрования и анализа данных в криминалистике		5	3
5	Модуль 5. Облачные технологии в криминалистике			13
6	Итоговая аттестация (зачет)			2
7	ВСЕГО	20	18	18

6. РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ МОДУЛЕЙ

6.1. Рабочая программа Модуля 1. Основы мобильной криминалистики

Цель программы заключается в получении теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы в области цифровой криминалистики, извлечения информации и информационной безопасности.

Задачи программы:
1. Формирование знаний методов извлечения и анализа данных из мобильных устройств и облачных сервисов.
2. Формирование знаний основ мобильной криминалистики.
3. Формирование знаний и навыков извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
4. Формирование знаний и навыков извлечения и анализа информации из iPhone и iPad.
5. Формирование знаний основ шифрования и анализа данных в криминалистике.
6. Формирование знаний и навыков в области техник и инструментов для извлечения данных.

Планируемые результаты изучения модуля

В результате освоения программы обучающиеся
будут знать:
- Архитектуру и пользовательские интерфейсы операционных систем;
- Типовые средства защиты информации в операционных системах;

- Общие принципы функционирования программно-аппаратных средств криптографической защиты информации;
- Форматы хранения информации в анализируемой системе
- Основные форматы файлов, используемые в компьютерных системах;
- Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;
- Методы анализа остаточной информации;
- Методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Основ мобильной криминалистики.
- Особенности извлечения и анализа информации из iPhone и iPad.
- Техники и инструменты для извлечения данных.
- Инструменты и решения от Elcomsoft для извлечения данных из устройств.

будут уметь:

- Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
- Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;
- Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;
- Анализировать структуру механизма возникновения и обстоятельства события;
- Выявлять возможные траектории состояний функционирования системы;
- Применять методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Осуществлять извлечение и анализ информации из iPhone и iPad.
- Применять техники и инструменты для извлечения данных.
- Применять инструменты и решения от Elcomsoft для извлечения данных из устройств.

Учебный план

№ п/п	Наименование компонентовпрограммы	Трудоемкость, ак. ч.[3]				Форма контроля
		Всего	Лекции	Практические занятия / Самостоятельная работа	Контроль	
1	**Модуль 1. Основы мобильной криминалистики**	**11**	**8**	**3**		
1.1	Тема 1.1. Мобильные	1	1			

[3] Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

	устройства как объект криминалистического исследования: изучаем все аспекты					
1.2	Тема 1.2. Обзор ключевых мобильных платформ	1	1			
1.3	Тема 1.3. Алгоритм сохранения и извлечения данных	1	1			
1.4	Тема 1.4. Сравнительный анализ физических, логических и облачных методов исследования	1	1			
1.5	Тема 1.5. Основные принципы криминалистических исследований мобильных устройств: правила и общий порядок работы	1	1			
1.6	Тема 1.6. Инструменты для анализа информации с мобильных устройств	2	1	1		
1.7	Тема 1.7. Техники извлечения данных из мобильных устройств	2	1	1		
1.8	Тема 1.8. Способы получения данных из iOS-устройств с использованием продуктов Elcomsoft	2	1	1		
2	**Итого**	**11**	**8**	**3**		

Содержание

Вид занятий	Количество часов	Наименование модуля, темы и содержание
Модуль 1. Основы мобильной криминалистики		

Лекция	1	**Тема 1.1. Мобильные устройства как объект криминалистического исследования: изучаем все аспекты:**
		• Введение в мобильную криминалистику: Определение понятия, его актуальность в современном правоприменении.
		• Структура мобильного устройства: Элементы архитектуры и функционирования: процессор, память, интерфейсы.
		• Типы хранимой информации:
		  • Текстовые сообщения: SMS, мессенджеры, их значение и возможности извлечения.
		  • Изображения и видео: источники данных для анализа, форматы и методы извлечения.

		• Контакты: важность информации о связях, хранение данных в облаке и на устройстве. • Метаданные: понимание и использование метаданных, как способа реконструкции событий. • Формирование полной картины преступления: Как данные помогают восстанавливать хронологию событий и выявлять связи между участниками.
Лекция	1	**Тема 1.2. Обзор ключевых мобильных платформ:** • Анализ архитектуры iOS: Общая структура, особенности системы, подходы к безопасности. • Изучение Android: Гибкость системы, разные версии, механизмы защиты данных. • Windows Phone: Характеристика платформы, её уникальные функции и ограничения. • Сравнительный анализ: Достоинства и недостатки каждой платформы с точки зрения криминалистического анализа, включая шифрование и доступ к данным.
Лекция	1	**Тема 1.3. Алгоритм сохранения и извлечения данных:** • Этапы извлечения данных: Подробный разбор последовательных действий для проведения исследования, начиная от подготовки до анализа. • Оценка состояния устройства: Как состояние мобильного устройства влияет на процесс извлечения данных и его результаты. • Методы создания образов данных: Используемые технологии для копирования и анализа информации с устройства. • Юридические нормы: Значение соблюдения протоколов и правовых аспектов при извлечении данных для обеспечения их допустимости в судебном разбирательстве.
Лекция	1	**Тема 1.4. Сравнительный анализ физических, логических и облачных методов исследования:** • Физические методы: Обзор техник прямого извлечения данных с устройства, их преимущества и недостатки. • Логические методы: Механизмы анализа через программное обеспечение, методы работы с резервными копиями и их использование в расследовании. • Облачные технологии: Применение облачных решений для извлечения данных, возможность взаимодействия с удалёнными серверами, преимущества и риски. • Выбор метода: Условия и ситуации, при которых каждый из методов может быть наиболее эффективным.
Лекция	1	**Тема 1.5. Основные принципы криминалистических исследований мобильных устройств: правила и общий порядок работы**:

		• Этические нормы: Значение этики в криминалистическом исследовании и защите прав граждан. • Протоколы и правила: Основные принципы работы, обеспечивающие качество и допустимость доказательств. • Документация: Формирование отчётов о проведении экспертизы, методах и результатах. • Безопасность исследований: Основные стандарты и протоколы, направленные на защиту данных и сведений, выявленных в ходе работы.
Лекция	1	**Тема 1.6. Инструменты для анализа информации с мобильных устройств:** • Обзор программного обеспечения • Оборудование для низкоуровневого доступа: Специальные устройства и технологии для физического извлечения данных. • Критерии выбора инструментов.
Практическое занятие	1	**Тема 1.6. Инструменты для анализа информации с мобильных устройств:** • Обзор программного обеспечения: Сравнение различных программ, используемых в мобильной криминалистике. • Критерии выбора инструментов: Как действовать в зависимости от типа устройства и характера поставленной задачи.
Лекция	1	**Тема 1.7. Техники извлечения данных из мобильных устройств:** • Методы программного и аппаратного извлечения: Углубленное изучение различных подходов к работе с данными. • Обход защитных механизмов: Техники преодоления блокировок и средств защиты информации.
Практическое занятие	1	**Тема 1.7. Техники извлечения данных из мобильных устройств:** Практическое применение: Рекомендации по реализации выработанных методов в условиях реального расследования, анализ реальных примеров. Техники преодоления блокировок и средств защиты информации.
Лекция	1	**Тема 1.8. Способы получения данных из iOS-устройств с использованием продуктов Elcomsoft:** • Инструменты Elcomsoft: Обзор доступных решений для работы с устройствами Apple. • Методы обхода ограничений системы.
Практическое занятие	1	**Тема 1.8. Способы получения данных из iOS-устройств с использованием продуктов Elcomsoft:** • Методы обхода ограничений системы: Практические аспекты работы с паролями
Всего	11	

Календарный учебный график

№ п/п	Наименование компонентов программы	1 неделя	2 неделя	3 неделя
1	Модуль 1. Основы мобильной криминалистики	11		
2	ВСЕГО	11		

Организационно-педагогические условия реализации модуля

Реализация модуля обеспечивает приобретение слушателями знаний и умений, необходимых для осуществления работы в области информационной безопасности и извлечения данных.

Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала необходимо вести в форме, доступной для понимания обучающихся, соблюдать единство терминологии, определений и условных обозначений, соответствующих международным договорам и нормативным правовым актам.

Практические занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы в ситуациях, максимально имитирующих реальные рабочие процессы.

Выбор методов обучения для каждого занятия определяется преподавателем в соответствии с составом и уровнем подготовленности обучающихся, степенью сложности излагаемого материала, наличием и состоянием учебного оборудования, технических средств обучения, местом и продолжительностью проведения занятий.

Кадровые (педагогические) условия. Реализация модуля обеспечивается педагогическими кадрами, имеющими соответствующее профессиональное образование и отвечающими квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам, в рамках изучаемого цикла.

Материально-технически условия реализации модуля

Образовательная организация располагает материально-технической базой, обеспечивающей проведение предусмотренных теоретических и практических занятий.

Материально-техническая база образовательной организации включает в себя учебные аудитории, оснащенные мебелью и учебным оборудованием:

Перечень учебного оборудования для занятий:

Комната 14

- Столы – 3 шт.
- Стулья – 6 шт.
- Проектор – 1 шт.
- Экран – 1 шт.

- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 15

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 20

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 8 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 21

- Столы – 5 шт.
- Стулья – 10 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 10 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Реализация модуля обеспечена учебно-методической и нормативно-правовой документацией, учебными и учебно-методическими изданиями, справочниками и т.д., формируемыми в соответствии с темами учебного плана.

Информационные и учебно-методические условия

Список литературы:

Список нормативных правовых документов:

1. Конституция Российской Федерации

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ

Список основной литературы:

1. Информационная безопасность компьютерных систем и сетей: учеб. пособие/ Шаньгин В. Ф. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.
2. Форензика – компьютерная криминалистика / Федотов Н.Н. – М.: Юридический Мир, 2007. – 360 с.
3. Форензика. Теория и практика расследования киберпреступлений / Шелупанов А.А., Смолина А.Р. – М.: Горячая линия-Телеком, 2020. – 104 с.
4. Информационная безопасность: учебное пособие / Макаренко С. И. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
5. Методическое руководство по извлечению данных из iPhone и других устройств Apple. – ЭлкомСофт, 2023. – 197 с.

6.2. Рабочая программа
Модуля 2. Низкоуровневое извлечение

Цель программы заключается в получении теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы в области цифровой криминалистики, извлечения информации и информационной безопасности.

Задачи программы:

1. Формирование знаний методов извлечения и анализа данных из мобильных устройств и облачных сервисов.
2. Формирование знаний основ мобильной криминалистики.
3. Формирование знаний и навыков извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
4. Формирование знаний и навыков извлечения и анализа информации из iPhone и iPad.
5. Формирование знаний основ шифрования и анализа данных в криминалистике.
6. Формирование знаний и навыков в области техник и инструментов для извлечения данных.

Планируемые результаты изучения модуля

В результате освоения программы обучающиеся
будут знать:

- Архитектуру и пользовательские интерфейсы операционных систем;

- Типовые средства защиты информации в операционных системах;
- Общие принципы функционирования программно-аппаратных средств криптографической защиты информации;
- Форматы хранения информации в анализируемой системе
- Основные форматы файлов, используемые в компьютерных системах;
- Особенности хранения конфигурационной и системной информации в компьютерных системах;
- Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;
- Методы анализа остаточной информации;
- Криптографические алгоритмы и особенности их программной реализации;
- Методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Основ мобильной криминалистики.
- Особенности извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
- Особенности извлечения и анализа информации из iPhone и iPad.
- Основы шифрования и анализа данных в криминалистике.
- Техники и инструменты для извлечения данных.
- Инструменты и решения от Elcomsoft для извлечения данных из устройств.

будут уметь:

- Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
- Настраивать компоненты подсистем защиты информации операционных систем;
- Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;
- Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;
- Анализировать структуру механизма возникновения и обстоятельства события;
- Выявлять возможные траектории состояний функционирования системы;
- Применять методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Осуществлять извлечение и анализ информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
- Осуществлять извлечение и анализ информации из iPhone и iPad.
- Применять техники и инструменты для извлечения данных.
- Применять инструменты и решения от Elcomsoft для извлечения данных из устройств.

Учебный план

№ п/п	Наименование компонентовпрограммы	Трудоемкость, ак. ч.[4]				Форма контроля
		Всего	Лекции	Практические занятия / Самостоятельная работа	Контроль	
1	**Модуль 2. Низкоуровневое извлечение**	**16**	**10**	**6**		
1.1	Тема 2.1. Введение в основы низкоуровневого анализа	1	1			
1.2	Тема 2.2. Механизмы защиты мобильных устройств и техники извлечения данных	1	1			
1.3	Тема 2.3. Понятие уязвимостей загрузчиков	1	1			
1.4	Тема 2.4. Извлечение данных из iPhone и iPad	1	1			
1.5	Тема 2.5. Физический анализ и джейлбрейк	2	1	1		
1.6	Тема 2.6. Установка и использование агента-экстрактора	2	1	1		
1.7	Тема 2.7. Препятствия при извлечении и расшифровке информации	2	1	1		
1.8	Тема 2.8. Методы получения данных с устройств Qualcomm	2	1	1		
1.9	Тема 2.9. Извлечение информации из чипсетов Spreadtrum и MTK	2	1	1		
1.10	Тема 2.10. Специфика чипов Samsung Exynos	2	1	1		
2	**Итого**	**16**	**10**	**6**		

Содержание

Вид занятий	Количество часов	Наименование модуля, темы и содержание
Модуль 2. Низкоуровневое извлечение		
Лекция	1	**Тема 2.1. Введение в основы низкоуровневого анализа:** • Понимание концепций и методов низкоуровневого анализа данных.

[4] Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

		• Изучение принципов работы с памятью мобильных устройств. • Невозможность полного учета различий между низкоуровневыми и высокоуровневыми методами.
Лекция	1	**Тема 2.2. Механизмы защиты мобильных устройств и техники извлечения данных:** • Изучение основных механизмов безопасности мобильных устройств. • Ознакомление с методами шифрования и аутентификации. • Исследование подходов к извлечению данных при наличии защиты.
Лекция	1	**Тема 2.3. Понятие уязвимостей загрузчиков:** • Анализ уязвимостей, связанных с загрузчиками мобильных устройств. • Ознакомление с типами загрузчиков и их ролью в безопасности. • Изучение методов эксплуатации уязвимостей для извлечения данных.
Лекция	1	**Тема 2.4. Извлечение данных из iPhone и iPad:** • Освоение решений от Elcomsoft для извлечения данных из устройств Apple. • Понимание работы с учетными записями iCloud и резервными копиями.
Лекция	1	**Тема 2.5. Физический анализ и джейлбрейк:** • Изучение физических методов анализа, включая джейлбрейк. • Оценка преимуществ и недостатков применения этих методов.
Практическое занятие	1	**Тема 2.5. Физический анализ и джейлбрейк:** • Физические методы анализа, включая джейлбрейк. Оценка преимуществ и недостатков применения.
Лекция	1	**Тема 2.6. Установка и использование агента-экстрактора:** • Ознакомление с процессом установки и настройки агента-экстрактора. • Понимание работы с инструментами для автоматизации извлечения данных.
Практическое занятие	1	**Тема 2.6. Установка и использование агента-экстрактора:** • Процесс установки и настройки агента-экстрактора. Работа с инструментами для автоматизации извлечения данных.
Лекция	1	**Тема 2.7. Препятствия при извлечении и расшифровке информации:** • Анализ проблем, возникающих при извлечении и расшифровке данных. • Изучение практических аспектов, связанных с шифрованием и физическим повреждением устройств.

Практическое занятие	1	**Тема 2.7. Препятствия при извлечении и расшифровке информации:** • Анализ проблем, возникающих при извлечении и расшифровке данных. Шифрование и физические повреждения устройств.
Лекция	1	**Тема 2.8. Методы получения данных с устройств Qualcomm:** • Освоение методов извлечения данных с устройств на платформе Qualcomm. • Понимание технических аспектов и используемых инструментов.
Практическое занятие	1	**Тема 2.8. Методы получения данных с устройств Qualcomm:** • Методы извлечения данных с устройств на платформе Qualcomm. Понимание технических аспектов и используемых инструментов.
Лекция	1	**Тема 2.9. Извлечение информации из чипсетов Spreadtrum и МТК:** • Изучение техник и инструментов для извлечения данных из чипсетов Spreadtrum и MediaTek. • Ознакомление с особенностями платформ, влияющими на процедуры извлечения.
Практическое занятие	1	**Тема 2.9. Извлечение информации из чипсетов Spreadtrum и МТК:** • Техники и инструменты для извлечения данных из чипсетов Spreadtrum и MediaTek. Особенности платформ, влияющими на процедуры извлечения.
Лекция	1	**Тема 2.10. Специфика чипов Samsung Exynos:** • Анализ архитектуры и механизмов безопасности чипов Samsung Exynos. • Понимание применения методов извлечения данных для этих чипов.
Практическое занятие	1	**Тема 2.10. Специфика чипов Samsung Exynos:** • Архитектура и механизмы безопасности чипов Samsung Exynos. Применения методов извлечения данных для этих чипов.
Всего	16	

Календарный учебный график

№ п/п	Наименование компонентов программы	1 неделя	2 неделя	3 неделя
1	Модуль 2. Низкоуровневое извлечение	9	7	
2	ВСЕГО	9	7	

Организационно-педагогические условия реализации модуля

Реализация модуля обеспечивает приобретение слушателями знаний и умений, необходимых для осуществления работы в области информационной безопасности и извлечения данных.

Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала необходимо вести в форме, доступной для понимания обучающихся, соблюдать единство терминологии, определений и условных обозначений, соответствующих международным договорам и нормативным правовым актам.

Практические занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы в ситуациях, максимально имитирующих реальные рабочие процессы.

Выбор методов обучения для каждого занятия определяется преподавателем в соответствии с составом и уровнем подготовленности обучающихся, степенью сложности излагаемого материала, наличием и состоянием учебного оборудования, технических средств обучения, местом и продолжительностью проведения занятий.

Кадровые (педагогические) условия. Реализация модуля обеспечивается педагогическими кадрами, имеющими соответствующее профессиональное образование и отвечающими квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам, в рамках изучаемого цикла.

Материально-технически условия реализации модуля

Образовательная организация располагает материально-технической базой, обеспечивающей проведение предусмотренных теоретических и практических занятий.

Материально-техническая база образовательной организации включает в себя учебные аудитории, оснащенные мебелью и учебным оборудованием:

Перечень учебного оборудования для занятий:

Комната 14

- Столы – 3 шт.
- Стулья – 6 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 15

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.

- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 20

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 8 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 21

- Столы – 5 шт.
- Стулья – 10 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 10 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Реализация модуля обеспечена учебно-методической и нормативно-правовой документацией, учебными и учебно-методическими изданиями, справочниками и т.д., формируемыми в соответствии с темами учебного плана.

Информационные и учебно-методические условия

Список литературы:
Список нормативных правовых документов:
1. Конституция Российской Федерации
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ

Список основной литературы:

1. Информационная безопасность компьютерных систем и сетей: учеб. пособие/ Шаньгин В. Ф. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.
2. Форензика – компьютерная криминалистика / Федотов Н.Н. – М.: Юридический Мир, 2007. – 360 с.
3. Форензика. Теория и практика расследования киберпреступлений / Шелупанов А.А., Смолина А.Р. – М.: Горячая линия-Телеком, 2020. – 104 с.

4. Информационная безопасность: учебное пособие / Макаренко С. И. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
5. Методическое руководство по извлечению данных из iPhone и других устройств Apple. – ЭлкомСофт, 2023. – 197 с.

6.3. Рабочая программа
Модуля 3. Низкоуровневое и логическое извлечение

Цель программы заключается в получении теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы в области цифровой криминалистики, извлечения информации и информационной безопасности.

Задачи программы:
1. Формирование знаний методов извлечения и анализа данных из мобильных устройств и облачных сервисов.
2. Формирование знаний основ мобильной криминалистики.
3. Формирование знаний и навыков извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
4. Формирование знаний и навыков извлечения и анализа информации из iPhone и iPad.
5. Формирование знаний основ шифрования и анализа данных в криминалистике.
6. Формирование знаний и навыков в области техник и инструментов для извлечения данных.

Планируемые результаты изучения модуля

В результате освоения программы обучающиеся
будут знать:
- Архитектуру и пользовательские интерфейсы операционных систем;
- Типовые средства защиты информации в операционных системах;
- Общие принципы функционирования программно-аппаратных средств криптографической защиты информации;
- Форматы хранения информации в анализируемой системе
- Основные форматы файлов, используемые в компьютерных системах;
- Особенности хранения конфигурационной и системной информации в компьютерных системах;
- Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;
- Методы анализа остаточной информации;

- Криптографические алгоритмы и особенности их программной реализации;
- Методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Основ мобильной криминалистики.
- Особенности извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
- Особенности извлечения и анализа информации из iPhone и iPad.
- Основы шифрования и анализа данных в криминалистике.
- Техники и инструменты для извлечения данных.
- Инструменты и решения от Elcomsoft для извлечения данных из устройств.

будут уметь:

- Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
- Настраивать компоненты подсистем защиты информации операционных систем;
- Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;
- Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;
- Анализировать структуру механизма возникновения и обстоятельства события;
- Выявлять возможные траектории состояний функционирования системы;
- Применять методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Осуществлять извлечение и анализ информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
- Осуществлять извлечение и анализ информации из iPhone и iPad.
- Применять техники и инструменты для извлечения данных.
- Применять инструменты и решения от Elcomsoft для извлечения данных из устройств.

Учебный план

№ п/п	Наименование компонентовпрограммы	Трудоемкость, ак. ч.[5]				Форма контроля
		Всего	Лекции	Практические занятия / Самостоятельная работа	Контроль	
1	**Модуль 3. Низкоуровневое и логическое извлечение**	**6**	**3**	**3**		

[5] Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

1.1	Тема 3.1. Техники подбора паролей для расшифровки данных	2	1	1		
1.2	Тема 3.2. Способы извлечения данных из поврежденных устройств	2	1	1		
1.3	Тема 3.3. Кросс-платформенные методы извлечения данных	2	1	1		
2	**Итого**	**6**	**3**	**3**		

Содержание

Вид занятий	Количество часов	Наименование модуля, темы и содержание
Модуль 3. Низкоуровневое и логическое извлечение		
Лекция	1	**Тема 3.1. Техники подбора паролей для расшифровки данных:** • Углубленное изучение методов подбора паролей, направленных на расшифровку зашифрованных данных. • Исследование теоретических основ, позволяющих эффективно использовать инструменты подбора паролей, включая алгоритмы шифрования и уровни сложности. Методы перебора, такие как брутфорс и словарные атаки, а также применение специализированного программного обеспечения для оптимизации процесса.
Практическое занятие	1	**Тема 3.1. Техники подбора паролей для расшифровки данных:** • Методы подбора паролей, направленных на расшифровку зашифрованных данных. Практические навыки, позволяющих эффективно использовать инструменты подбора паролей, включая алгоритмы шифрования и уровни сложности. Методы перебора, такие как брутфорс и словарные атаки, а также применение специализированного программного обеспечения для оптимизации процесса.
Лекция	1	**Тема 3.2. Способы извлечения данных из поврежденных устройств**: • Анализ методов извлечения данных из устройств с физическими или логическими повреждениями. • Обзор причин повреждений — механических и программных — и их влияния на доступность данных. Описание технологий восстановления данных, включая использование программных и аппаратных решений, а также анализ файловых систем.
Практическое занятие	1	**Тема 3.2. Способы извлечения данных из поврежденных устройств:** • Методы извлечения данных из устройств с физическими или логическими повреждениями.

		• Причины повреждений — механических и программных — и их влияния на доступность данных. Технологии восстановления данных, включая использование программных и аппаратных решений, а также анализ файловых систем
Лекция	1	**Тема 3.3. Кросс-платформенные методы извлечения данных**: • Изучение кросс-платформенных методов извлечения данных, применяемых к устройствам разных производителей и операционных систем. Углубленное понимание ключевых отличий платформ, таких как iOS и Android, и лучших практик применения универсальных инструментов. Обсуждение техник быстрого доступа к информации, что позволит участникам эффективно справляться с разнообразными условиями работы.
Практическое занятие	1	**Тема 3.3. Кросс-платформенные методы извлечения данных:** • Кросс-платформенные методы извлечения данных, применяемых к устройствам разных производителей и операционных систем. Техники быстрого доступа к информации, что позволит участникам эффективно справляться с разнообразными условиями работы.
Всего	6	

Календарный учебный график

№ п/п	Наименование компонентов программы	1 неделя	2 неделя	3 неделя
1	Модуль 3. Низкоуровневое и логическое извлечение		6	
2	ВСЕГО		6	

Организационно-педагогические условия реализации модуля

Реализация модуля обеспечивает приобретение слушателями знаний и умений, необходимых для осуществления работы в области информационной безопасности и извлечения данных.

Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала необходимо вести в форме, доступной для понимания обучающихся, соблюдать единство терминологии, определений и условных обозначений, соответствующих международным договорам и нормативным правовым актам.

Практические занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы в ситуациях, максимально имитирующих реальные рабочие процессы.

Выбор методов обучения для каждого занятия определяется преподавателем в соответствии с составом и уровнем подготовленности

обучающихся, степенью сложности излагаемого материала, наличием и состоянием учебного оборудования, технических средств обучения, местом и продолжительностью проведения занятий.

Кадровые (педагогические) условия. Реализация модуля обеспечивается педагогическими кадрами, имеющими соответствующее профессиональное образование и отвечающими квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам, в рамках изучаемого цикла.

Материально-технически условия реализации модуля

Образовательная организация располагает материально-технической базой, обеспечивающей проведение предусмотренных теоретических и практических занятий.

Материально-техническая база образовательной организации включает в себя учебные аудитории, оснащенные мебелью и учебным оборудованием:

Перечень учебного оборудования для занятий:

Комната 14

- Столы – 3 шт.
- Стулья – 6 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 15

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 20

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 8 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 21

- Столы – 5 шт.
- Стулья – 10 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 10 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Реализация модуля обеспечена учебно-методической и нормативно-правовой документацией, учебными и учебно-методическими изданиями, справочниками и т.д., формируемыми в соответствии с темами учебного плана.

Информационные и учебно-методические условия

Список литературы:
Список нормативных правовых документов:
1. Конституция Российской Федерации
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ

Список основной литературы:

1. Информационная безопасность компьютерных систем и сетей: учеб. пособие/ Шаньгин В. Ф. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.
2. Форензика – компьютерная криминалистика / Федотов Н.Н. – М.: Юридический Мир, 2007. – 360 с.
3. Форензика. Теория и практика расследования киберпреступлений / Шелупанов А.А., Смолина А.Р. – М.: Горячая линия-Телеком, 2020. – 104 с.
4. Информационная безопасность: учебное пособие / Макаренко С. И. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
5. Методическое руководство по извлечению данных из iPhone и других устройств Apple. – ЭлкомСофт, 2023. – 197 с.

6.4. Рабочая программа Модуля 4. Основы шифрования и анализа данных в криминалистике

Цель программы заключается в получении теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы в области цифровой криминалистики, извлечения информации и информационной безопасности.

Задачи программы:
1. Формирование знаний методов извлечения и анализа данных из мобильных устройств и облачных сервисов.
2. Формирование знаний основ мобильной криминалистики.
3. Формирование знаний и навыков извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
4. Формирование знаний и навыков извлечения и анализа информации из iPhone и iPad.
5. Формирование знаний основ шифрования и анализа данных в криминалистике.
6. Формирование знаний и навыков в области техник и инструментов для извлечения данных.

Планируемые результаты изучения модуля

В результате освоения программы обучающиеся
будут знать:

- Архитектуру и пользовательские интерфейсы операционных систем;
- Типовые средства защиты информации в операционных системах;
- Общие принципы функционирования программно-аппаратных средств криптографической защиты информации;
- Форматы хранения информации в анализируемой системе
- Основные форматы файлов, используемые в компьютерных системах;
- Особенности хранения конфигурационной и системной информации в компьютерных системах;
- Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;
- Методы анализа остаточной информации;
- Криптографические алгоритмы и особенности их программной реализации;
- Методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Основ мобильной криминалистики.
- Особенности извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
- Особенности извлечения и анализа информации из iPhone и iPad.
- Основы шифрования и анализа данных в криминалистике.
- Техники и инструменты для извлечения данных.
- Инструменты и решения от Elcomsoft для извлечения данных из устройств.

будут уметь:

- Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
- Настраивать компоненты подсистем защиты информации операционных систем;
- Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;
- Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;
- Анализировать структуру механизма возникновения и обстоятельства события;
- Выявлять возможные траектории состояний функционирования системы;
- Применять методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Осуществлять извлечение и анализ информации из iPhone и iPad.
- Применять техники и инструменты для извлечения данных.
- Применять инструменты и решения от Elcomsoft для извлечения данных из устройств.

Учебный план

№ п/п	Наименование компонентовпрограммы	Трудоемкость, ак. ч.[6]				Форма контроля
		Всего	Лекции	Практические занятия / Самостоятельная работа	Контроль	
1	**Модуль 4. Основы шифрования и анализа данных в криминалистике**	**8**	**6**	**2**		
1.1	Тема 4.1. Анализ данных мобильных приложений	1	1			
1.2	Тема 4.2. Основы шифрования и его значение в криминалистике	1	1			
1.3	Тема 4.3. Возможности восстановления удаленных данных	1	1			
1.4	Тема 4.4. Методы доступа к зашифрованной информации	1	1			
1.5	Тема 4.5. Структура Elcomsoft Premium Forensic Bundle	2	1	1		
1.6	Тема 4.6. Основные действия при извлечении информации с цифровых носителей с целью их исследования	2	1	1		

[6] Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

2	**Итого**	**8**	**6**	**2**		

Содержание

Вид занятий	Количество часов	Наименование модуля, темы и содержание
Модуль 4. Основы шифрования и анализа данных в криминалистике		
Лекция	1	**Тема 4.1. Анализ данных мобильных приложений:** • Извлечение информации из приложений для iOS и Android. • Уникальные характеристики и особенности каждой платформы. • Инструменты и методы для глубокого анализа мобильных данных.
Лекция	1	**Тема 4.2. Основы шифрования и его значение в криминалистике**: • Введение в виды шифрования. • Влияние шифрования на криминалистику. • Примеры успешного и неудачного анализа зашифрованной информации.
Лекция	1	**Тема 4.3. Возможности восстановления удаленных данных:** • Методы восстановления данных с физических носителей. • Технологии восстановления из облачных хранилищ. • Этические и юридические аспекты процесса восстановления.
Лекция	1	**Тема 4.4. Методы доступа к зашифрованной информации:** • Способы получения доступа к зашифрованным данным. • Обзор уязвимостей, позволяющих дешифрование. • Правовые рамки и этические нормы, касающиеся доступа к зашифрованной информации.
Лекция	1	**Тема 4.5. Структура Elcomsoft Premium Forensic Bundle**: • Обзор функциональности Elcomsoft Premium Forensic Bundle. • Интерактивная демонстрация инструментов и возможностей.
Практическое занятие	1	**Тема 4.5. Структура Elcomsoft Premium Forensic Bundle:** Применение программного обеспечения в практике криминалистики.
Лекция	1	**Тема 4.6. Основные действия при извлечении информации с цифровых носителей с целью их исследования:** • Основные этапы извлечения информации из цифровых носителей.

		• Методы сохранения целостности данных и эффективного сбора доказательств. • Рекомендации при извлечении информации с цифровых носителей
Практическое занятие	1	**Тема 4.6. Основные действия при извлечении информации с цифровых носителей с целью их исследования:** • Извлечение информации из цифровых носителей. • Методы сохранения целостности данных и эффективного сбора доказательств.
Всего	8	

Календарный учебный график

№ п/п	Наименование компонентов программы	1 неделя	2 неделя	3 неделя
1	Модуль 4. Основы шифрования и анализа данных в криминалистике		5	3
2	ВСЕГО		5	3

Организационно-педагогические условия реализации модуля

Реализация модуля обеспечивает приобретение слушателями знаний и умений, необходимых для осуществления работы в области информационной безопасности и извлечения данных.

Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала необходимо вести в форме, доступной для понимания обучающихся, соблюдать единство терминологии, определений и условных обозначений, соответствующих международным договорам и нормативным правовым актам.

Практические занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы в ситуациях, максимально имитирующих реальные рабочие процессы.

Выбор методов обучения для каждого занятия определяется преподавателем в соответствии с составом и уровнем подготовленности обучающихся, степенью сложности излагаемого материала, наличием и состоянием учебного оборудования, технических средств обучения, местом и продолжительностью проведения занятий.

Кадровые (педагогические) условия. Реализация модуля обеспечивается педагогическими кадрами, имеющими соответствующее профессиональное образование и отвечающими квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам, в рамках изучаемого цикла.

Материально-технически условия реализации модуля

Образовательная организация располагает материально-технической базой, обеспечивающей проведение предусмотренных теоретических и практических занятий.

Материально-техническая база образовательной организации включает в себя учебные аудитории, оснащенные мебелью и учебным оборудованием:

Перечень учебного оборудования для занятий:

Комната 14

- Столы – 3 шт.
- Стулья – 6 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 15

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 20

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 8 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 21

- Столы – 5 шт.
- Стулья – 10 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 10 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Реализация модуля обеспечена учебно-методической и нормативно-правовой документацией, учебными и учебно-методическими изданиями, справочниками и т.д., формируемыми в соответствии с темами учебного плана.

Информационные и учебно-методические условия

Список литературы:
Список нормативных правовых документов:
1. Конституция Российской Федерации
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ

Список основной литературы:

1. Информационная безопасность компьютерных систем и сетей: учеб. пособие/ Шаньгин В. Ф. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.
2. Форензика – компьютерная криминалистика / Федотов Н.Н. – М.: Юридический Мир, 2007. – 360 с.
3. Форензика. Теория и практика расследования киберпреступлений / Шелупанов А.А., Смолина А.Р. – М.: Горячая линия-Телеком, 2020. – 104 с.
4. Информационная безопасность: учебное пособие / Макаренко С. И. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
5. Методическое руководство по извлечению данных из iPhone и других устройств Apple. – ЭлкомСофт, 2023. – 197 с.

6.5. Рабочая программа
Модуля 5. Облачные технологии в криминалистике

Цель программы заключается в получении теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы в области цифровой криминалистики, извлечения информации и информационной безопасности.

Задачи программы:
1. Формирование знаний методов извлечения и анализа данных из мобильных устройств и облачных сервисов.
2. Формирование знаний основ мобильной криминалистики.
3. Формирование знаний и навыков извлечения и анализа информации из мобильных устройств на чипсетах Qualcomm, Exynos, Spreadtrum и MTK.
4. Формирование знаний и навыков извлечения и анализа информации из iPhone и iPad.

5. Формирование знаний основ шифрования и анализа данных в криминалистике.
6. Формирование знаний и навыков в области техник и инструментов для извлечения данных.

Планируемые результаты изучения модуля

В результате освоения программы обучающиеся
будут знать:

- Типовые средства защиты информации в операционных системах;
- Общие принципы функционирования программно-аппаратных средств криптографической защиты информации;
- Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;
- Методы анализа остаточной информации;
- Методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Основы шифрования и анализа данных в криминалистике.
- Техники и инструменты для извлечения данных.

будут уметь:

- Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
- Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику;
- Анализировать структуру механизма возникновения и обстоятельства события;
- Выявлять возможные траектории состояний функционирования системы;
- Применять методы извлечения и анализа данных из мобильных устройств и облачных сервисов.
- Применять техники и инструменты для извлечения данных.

Учебный план

№ п/п	Наименование компонентов программы	Трудоемкость, ак. ч.[7]				Форма контроля
		Всего	Лекции	Практические занятия / Самостоятельная работа	Контроль	
1	**Модуль 5. Облачные технологии в**	**13**	**8**	**5**		

[7] Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

	криминалистике					
1.1	Тема 5.1. Роль облачных сервисов в мобильной криминалистике	1	1			
1.2	Тема 5.2. Извлечение данных из облаков iCloud и Google Account	2	1	1		
1.3	Тема 5.3. Основы аутентификации и двухфакторной авторизации	1	1			
1.4	Тема 5.4. Роль токенов безопасности и маркеров аутентификации	2	1	1		
1.5	Тема 5.5. Уникальные аспекты защиты с использованием двухфакторной аутентификации	1	1			
1.6	Тема 5.6. Извлечение паролей от учетных записей и данных приложений	2	1	1		
1.7	Тема 5.7. Доступ к данным мессенджеров через облачные сервисы	2	1	1		
1.8	Тема 5.8. Получение информации из социальных сетей	2	1	1		
2	**Итого**	**13**	**8**	**5**		

Содержание

Вид занятий	Количество часов	Наименование модуля, темы и содержание
Модуль 5. Облачные технологии в криминалистике		
Лекция	1	**Тема 5.1. Роль облачных сервисов в мобильной криминалистике:** • Влияние облачных технологий на современную криминалистику • Преимущества облачных платформ для хранения данных • Возможности обработки данных и анализа улик • Новейшие методы расследования, основанные на облачных сервисах
Лекция	1	**Тема 5.2. Извлечение данных из облаков iCloud и Google Account:** • Обзор типов данных, извлекаемых из iCloud и Google Account • Подробные методы извлечения информации • Инструменты для эффективного извлечения данных

Практическое занятие	1	**Тема 5.2. Извлечение данных из облаков iCloud и Google Account:** Практические примеры успешного извлечения информации. Методы извлечения информации. Инструменты для эффективного извлечения данных.
Лекция	1	**Тема 5.3. Основы аутентификации и двухфакторной авторизации:** • Принципы аутентификации в контексте облачных технологий • Значение двухфакторной авторизации для защиты учетных записей • Разнообразие методов аутентификации
Лекция	1	**Тема 5.4. Роль токенов безопасности и маркеров аутентификации:** • Определение токенов безопасности и маркеров аутентификации • Влияние токенов на извлечение данных из облачных сервисов • Значимость токенов для обеспечения безопасности
Практическое занятие	1	**Тема 5.4. Роль токенов безопасности и маркеров аутентификации:** Практические аспекты использования токенов в криминалистике.
Лекция	1	**Тема 5.5. Уникальные аспекты защиты с использованием двухфакторной аутентификации:** • Особенности двухфакторной аутентификации как механизма защиты • Общие угрозы, связанные с 2FA • Рекомендуемые практики для повышения уровня безопасности • Анализ успешных случаев применения двухфакторной аутентификации
Лекция	1	**Тема 5.6. Извлечение паролей от учетных записей и данных приложений:** • Методы извлечения паролей из различных источников • Инструменты для осуществления извлечения с учетом юридических норм • Этические аспекты извлечения данных
Практическое занятие	1	**Тема 5.6. Извлечение паролей от учетных записей и данных приложений:** Обсуждение кейсов и успешных практик в данной области. Методы извлечения паролей из различных источников. Инструменты для осуществления извлечения.
Лекция	1	**Тема 5.7. Доступ к данным мессенджеров через облачные сервисы:** • Обзор методов получения данных из мессенджеров • Меры безопасности, используемые в мессенджерах • Инструменты для извлечения информации из мессенджеров

Практическое занятие	1	**Тема 5.7. Доступ к данным мессенджеров через облачные сервисы:** Актуальные примеры и технологии, обеспечивающие доступ к данным. Методы получения данных из мессенджеров Инструменты для извлечения информации из мессенджеров.
Лекция	1	**Тема 5.8. Получение информации из социальных сетей:** • Техники и инструменты для извлечения данных из социальных сетей • Методы анализа собранной информации • Этические и юридические аспекты работы с данными из социальных сетей.
Практическое занятие	1	**Тема 5.8. Получение информации из социальных сетей:** Примеры использования данных из социальных сетей в криминалистике. Техники и инструменты для извлечения данных из социальных сетей. Методы анализа.
Всего	13	

Календарный учебный график

№ п/п	Наименование компонентов программы	1 неделя	2 неделя	3 неделя
1	Модуль 5. Облачные технологии в криминалистике			13
2	ВСЕГО			13

Организационно-педагогические условия реализации модуля

Реализация модуля обеспечивает приобретение слушателями знаний и умений, необходимых для осуществления работы в области информационной безопасности и извлечения данных.

Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала необходимо вести в форме, доступной для понимания обучающихся, соблюдать единство терминологии, определений и условных обозначений, соответствующих международным договорам и нормативным правовым актам.

Практические занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы в ситуациях, максимально имитирующих реальные рабочие процессы.

Выбор методов обучения для каждого занятия определяется преподавателем в соответствии с составом и уровнем подготовленности обучающихся, степенью сложности излагаемого материала, наличием и состоянием учебного оборудования, технических средств обучения, местом и продолжительностью проведения занятий.

Кадровые (педагогические) условия. Реализация модуля обеспечивается педагогическими кадрами, имеющими соответствующее профессиональное образование и отвечающими квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам, в рамках изучаемого цикла.

Материально-технически условия реализации модуля

Образовательная организация располагает материально-технической базой, обеспечивающей проведение предусмотренных теоретических и практических занятий.

Материально-техническая база образовательной организации включает в себя учебные аудитории, оснащенные мебелью и учебным оборудованием:

Перечень учебного оборудования для занятий:

Комната 14

- Столы – 3 шт.
- Стулья – 6 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 15

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 20

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 8 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 21

- Столы – 5 шт.
- Стулья – 10 шт.

- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 10 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Реализация модуля обеспечена учебно-методической и нормативно-правовой документацией, учебными и учебно-методическими изданиями, справочниками и т.д., формируемыми в соответствии с темами учебного плана.

Информационные и учебно-методические условия

Список литературы:
Список нормативных правовых документов:
1. Конституция Российской Федерации
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ

Список основной литературы:

1. Информационная безопасность компьютерных систем и сетей: учеб. пособие/ Шаньгин В. Ф. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.
2. Форензика – компьютерная криминалистика / Федотов Н.Н. – М.: Юридический Мир, 2007. – 360 с.
3. Форензика. Теория и практика расследования киберпреступлений / Шелупанов А.А., Смолина А.Р. – М.: Горячая линия-Телеком, 2020. – 104 с.
4. Информационная безопасность: учебное пособие / Макаренко С. И. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
5. Методическое руководство по извлечению данных из iPhone и других устройств Apple. – ЭлкомСофт, 2023. – 197 с.

7. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Формы аттестации
Программой предусмотрена текущая и итоговая аттестация слушателей.
Для проведения текущей и итоговой аттестации разработан фонд оценочных средств, являющийся неотъемлемой частью учебно-методического комплекса.
Объектами оценивания выступают:
- степень освоения теоретических знаний;
- уровень овладения практическими умениями и навыками по всем видам учебной работы.

Текущий контроль знаний обучающихся проводится преподавателем, ведущим занятия в учебной группе, на протяжении всего обучения по программе.
Текущий контроль знаний включает в себя наблюдение преподавателя за учебной работой обучающихся и проверку качества знаний, умений и навыков, которыми они овладели на определенном этапе обучения посредством выполнения упражнений на практических занятиях и в иных формах, установленных преподавателем.
Итоговая аттестация — процедура, проводимая с целью установления уровня знаний обучающихся с учетом прогнозируемых результатов обучения и требований к результатам освоения программы.
Итоговая аттестация обучающихся осуществляется в форме зачета посредством выполнения практического задания.
Оценка по результатам итоговой аттестации выставляется по двухбалльной системе: «зачтено/не зачтено». Оценка «зачтено» ставится при выполнении требований, предъявляемых к данной форме контроля.
Обучающимся, успешно прошедшим итоговую аттестацию, выдаются удостоверения о повышении квалификации установленного образца.

При освоении программы параллельно с получением среднего профессионального или высшего образования удостоверения о повышении квалификации выдаются одновременно с получением соответствующего документа о среднем профессиональном или высшем образовании.

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, устанавливаемому организацией.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Обучающимся необходимо выполнить практическое задание по указанию преподавателя.

Примерные задания для итоговой аттестации:

1. Извлечение и расшифровка данных из мобильного устройства бренда Apple.
2. Извлечение и расшифровка данных из мобильного устройства бренда Huawei.
3. Подбор пароля для расшифровки данных.
4. Извлечение и расшифровка образов из мобильного устройства бренда Samsung.
5. Сбор ключевых данных из устройства на Windows.
6. Извлечение информации из устройства на Spreadtrum.

7. Извлечение информации из устройства на МТК.
8. Восстановления данных на уровне файловой системы.
9. Извлечение данных из поврежденного гаджета.
10. Извлечение информации из различных облачных сервисов.
11. Извлечение данных переписки WhatsApp.
12. Извлечение данных переписки Telegram.
13. Извлечение информации из социальной сети VK.
14. Анализ информации, полученной в результате извлечения.

9. ПРОГРАММА ИТОГОВОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Обучающиеся допускаются к итоговой аттестации после изучения разделов и тем программы в объеме, предусмотренном учебным планом программы.

Оценка качества освоения учебной программы проводится в процессе итоговой аттестации в форме зачета посредством выполнения практического задания. Практическое задание оценивается преподавателем. По результатам проверки выставляется оценка «Зачтено» или «Не зачтено».

Критерии оценки

Оценка	Критерии оценки
Зачтено	Оценка «Зачтено» выставляется слушателю, если он твердо знает материал курса, грамотно и по существу использует его, не допуская существенных неточностей в ответе на тестовые вопросы, правильно применяет теоретические положения при решении практических вопросов.
Не зачтено	Оценка «Не зачтено» выставляется слушателю, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические вопросы или не справляется с ними самостоятельно.

Лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдаётся удостоверение о повышении квалификации установленного образца.

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, устанавливаемому организацией.

10. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Реализация программы обеспечивает приобретение слушателями знаний и умений, необходимых для осуществления работы в области информационной безопасности и извлечения данных.

Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала необходимо вести в форме, доступной для понимания обучающихся, соблюдать единство терминологии, определений и условных обозначений, соответствующих международным договорам и нормативным правовым актам.

Практические занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы в ситуациях, максимально имитирующих реальные рабочие процессы.

Выбор методов обучения для каждого занятия определяется преподавателем в соответствии с составом и уровнем подготовленности обучающихся, степенью сложности излагаемого материала, наличием и состоянием учебного оборудования, технических средств обучения, местом и продолжительностью проведения занятий.

Кадровые (педагогические) условия. Реализация модуля обеспечивается педагогическими кадрами, имеющими соответствующее профессиональное образование и отвечающими квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональным стандартам, в рамках изучаемого цикла.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Образовательная организация располагает материально-технической базой, обеспечивающей проведение предусмотренных теоретических и практических занятий.

Материально-техническая база образовательной организации включает в себя учебные аудитории, оснащенные мебелью и учебным оборудованием:

Перечень учебного оборудования для занятий:

Комната 14

- Столы – 3 шт.
- Стулья – 6 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 15

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.

- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 6 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 20

- Столы – 4 шт.
- Стулья – 8 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 8 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Комната 21

- Столы – 5 шт.
- Стулья – 10 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Компьютер с доступом к сети «Интернет» – 10 шт.
- Стеллаж для хранения учебно-методических материалов – 2 шт.
- Учебно-методическая литература и учебные пособия по теме преподаваемого предмета – в необходимом количестве

Реализация модуля обеспечена учебно-методической и нормативно-правовой документацией, учебными и учебно-методическими изданиями, справочниками и т.д., формируемыми в соответствии с темами учебного плана.

12. ИНФОРМАЦИОННЫЕ И УЧЕБНО-МЕТОДИЧЕСКИЕ УСЛОВИЯ

Список литературы:

Список нормативных правовых документов:

1. Конституция Российской Федерации
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ

Список основной литературы:

1. Информационная безопасность компьютерных систем и сетей: учеб. пособие/ Шаньгин В. Ф. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.
2. Форензика – компьютерная криминалистика / Федотов Н.Н. – М.: Юридический Мир, 2007. – 360 с.

3. Форензика. Теория и практика расследования киберпреступлений / Шелупанов А.А., Смолина А.Р. – М.: Горячая линия-Телеком, 2020. – 104 с.
4. Информационная безопасность: учебное пособие / Макаренко С. И. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
5. Методическое руководство по извлечению данных из iPhone и других устройств Apple. – ЭлкомСофт, 2023. – 197 с.