МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени И.Т. ТРУБИЛИНА»

Юридический факультет
Криминалистики

КубГАУ
Кубанский государственный аграрный университет
Документ подписан простой электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 2a0000098add596f008935c40900020000098a
Владелец: Куемжиева Светлана Александровна
Действителен от 23-05-2021 до 22-05-2026

УТВЕРЖДЕНО
Декан
Куемжиева С.А.
Протокол от 19.05.2025 № 5

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ И ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Уровень высшего образования: магистратура

Направление подготовки: 40.04.01 Юриспруденция

Направленность (профиль)подготовки: Теория и практика расследования преступлений

Квалификация (степень) выпускника: магистр

Формы обучения: очная, очно-заочная

Год набора (приема на обучение): 2025

Срок получения образования: Очная форма обучения – 2 года
Очно-заочная форма обучения – 3 года

Объем: в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

2025

Разработчики:
Доцент, кафедра криминалистики Агеев Н.В.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлени ю подготовки 40.04.01 Юриспруденция, утвержденного приказом Минобрнауки от 25.11.2020 № 1451, с учетом трудовых функций профессиональных стандартов: "Специалист в сфере предупреждения коррупционных правонарушений", утвержден приказом Минтруда России от 08.08.2022 № 472н; "Следователь-криминалист", утвержден приказом Минтруда России от 23.03.2015 № 183н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Земельного, трудового и экологического права	Председатель методической комиссии/совета	Сапфирова А.А.	Согласовано	21.04.2025, № 6
2	Криминалистики	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Меретуков Г.М.	Согласовано	30.04.2025, № 13
3	Юридический факультет	Руководитель образовательной программы	Зеленский В.Д.	Согласовано	30.04.2025, № 13

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - является формирование комплекса знаний, умений и навыков, необходимых для осуществления защиты и исследования компьютерной информации при производстве расследования и раскрытия преступлений.

Задачи изучения дисциплины:

- - формирование способности применять нормативные правовые акты при расследовании преступлений, реализовывать нормы материального и процессуального права в профессиональной деятельности, отражать ход и результаты профессиональной деятельности в процессуальной документации. .

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-П6 Способен квалифицированно применять нормативные правовые акты при расследовании преступлений, реализовывать нормы материального и процессуального права в профессиональной деятельности, отражать ход и результаты профессиональной деятельности в процессуальной документации.

ПК-П6.1 Квалифицированно реализует нормы материального и процессуального права в процессиональной деятельности

Знать:

ПК-П6.1/Зн1 Знает как квалифицированно реализовать нормы материального и процессуального права в профессиональной деятельности.

ПК-П6.1/Зн2 Знает как валифицированно реализовать нормы материального и процессуального права в процессиональной деятельности

ПК-П6.1/Зн3 Знает как квалифицированно реализовывать нормы материального и процессуального права в сфере интеллектуальной деятельности

ПК-П6.1/Зн4

Уметь:

ПК-П6.1/Ум1 Умеет квалифицированно реализовать нормы материального и процессуального права в профессиональной деятельности.

ПК-П6.1/Ум2 Квалифицированно реализовывать нормы материального и процессуального права в сфере интеллектуальной деятельности

Владеть:

ПК-П6.1/Нв1 Владеет навыками квалифицированно реализовать нормы материального и процессуального права в профессиональной деятельности.

ПК-П6.1/Нв2 Владеет навыками квалифицированного разъяснения материального и процессуального права, в сфере интеллектуальной деятельности

ПК-П6.2 Квалифицированно отражает ход и результаты профессиональной деятельности в процессуальной документации

Знать:

ПК-П6.2/Зн1 Знает как квалифицированно отражать ход и результаты профессиональной деятельности в процессуальной документации.

ПК-П6.2/Зн2 Умеет квалифицированно отражать ход и результаты профессиональной деятельности в процессуальной документации.

ПК-П6.2/Зн3 Знает как квалифицированно отражать ход и результаты профессиональной деятельности в процессуальной документации, в сфере интеллектуальной деятельности

Уметь:

ПК-П6.2/Ум1 Умеет квалифицированно отражать ход и результаты профессиональной деятельности в процессуальной документации.

ПК-П6.2/Ум2 Умеет квалифицированно отражать ход и результаты профессиональной деятельности в процессуальной документации, в сфере интеллектуальной деятельности

Владеть:

ПК-П6.2/Нв1 Владеет навыками квалифицированно отражать ход и результаты профессиональной деятельности в процессуальной документации.

ПК-П6.2/Нв2 Владеет навыками квалифицированно отражать ход и результаты профессиональной деятельности в процессуальной документации, в сфере интеллектуальной деятельности

ПК-П6.3 Применяет теоретические и практические знания при квалификации преступлений

Знать:

ПК-П6.3/Зн1 Знает как применять теоретические и практические знания при квалификации преступлений

ПК-П6.3/Зн2 Знает как прмененять теоретические и практические знания при квалификации преступлений, связанных с интеллектуальной деятельностью

Уметь:

ПК-П6.3/Ум1 Умеет применять теоретические и практические знания при квалификации преступлений

ПК-П6.3/Ум2 Умеет прмененять теоретические и практические знания при квалификации преступлений, связанных с интеллектуальной деятельностью

Владеть:

ПК-П6.3/Нв1 Владеет навыками применения теоретических и практических знаний при квалификации преступлений

ПК-П6.3/Нв2 Владаеет навыками прменения теоретических и практических знаний при квалификации преступлений, связанных с интеллектуальной деятельностью

ПК-П6.4 Владеет профессиональными знаниями, связанными с вопросами уголовной ответственности и наказания.

Знать:

ПК-П6.4/Зн1 Владеет профессиональными знаниями, связанными с вопросами уголовной ответственности и наказания.

ПК-П6.4/Зн2 Владеет профессиональными знаниями, связанными с вопросами уголовной ответственности и наказания, в сфере интеллектуальной деятельности

Уметь:

ПК-П6.4/Ум1 Владеет профессиональными знаниями и умениями, связанными с вопросами уголовной ответственности и наказания.

ПК-П6.4/Ум2 Владеет профессиональными умениями, связанными с вопросами уголовной ответственности и наказания, в сфере интеллектуальной деятельности

Владеть:

ПК-П6.4/Нв1 Имеет навык применения профессиональных знаний, связанных с вопросами уголовной ответственности и наказания.

ПК-П6.4/Нв2 Владеет профессиональными навыками, связанными с вопросами уголовной ответственности и наказания, в сфере интеллектуальной деятельности

ПК-П6.5 Использует информативно-коммуникационные технологии в выявлении, раскрытии, расследовании и предупреждении преступлений.

Знать:

ПК-П6.5/Зн1 Знает и использует информационно-коммуникационные технологии в выявлении, раскрытии, расследовании и предупреждении преступлений.

ПК-П6.5/Зн2 Знает как использовать информативно-коммуникационные технологии в выявлении, раскрытии, расследовании и предупреждении преступлений, связанных с интеллектуальной деятельностью

Уметь:

ПК-П6.5/Ум1 Умеет использовать информационно-коммуникационные технологии в выявлении, раскрытии, расследовании и предупреждении преступлений.

ПК-П6.5/Ум2 Умеет использовать информативно-коммуникационные технологии в выявлении, раскрытии, расследовании и предупреждении преступлений, связанных с интеллектуальной деятельностью

Владеть:

ПК-П6.5/Нв1 Владеет навыками использования информационно-коммуникационных технологий в выявлении, раскрытии, расследовании и предупреждении преступлений.

ПК-П6.5/Нв2 Владеет навыками использования информативно-коммуникационные технологии в выявлении, раскрытии, расследовании и предупреждении преступлений, связанных с интеллектуальной деятельностью

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Криминалистическое обеспечение защиты и исследования компьютерной информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): Очная форма обучения - 3, Очно-заочная форма обучения - 4.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Очная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Зачет (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Третий семестр	72	2	19	1		4	14	53	Зачет
Всего	72	2	19	1		4	14	53	

Очно-заочная форма обучения

Период	доемкость сы)	доемкость ЗЕТ)	ая работа всего)	ая контактная (часы)	(часы)	ые занятия сы)	кие занятия сы)	ьная работа сы)	ая аттестация сы)

обучения	Общая тру (ча	Общая тру (ЗЕ	Контактн (часы,	Внеаудиторна работа	Зачет	Лекционны (ча	Практическ (ча	Самостоятел (ча	Промежуточн (ча
Четвертый семестр	72	2	15	1	4	4	6	57	Зачет (4) Контрольная работа
Всего	72	2	15	1	4	4	6	57	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Очная форма обучения

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Криминалистические методы защиты и исследования компьютерной информации в раскрытии преступлений в сфере IT	**71**		**4**	**14**	**53**	ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 1.1. Компьютерные преступления.	16		2	3	11	
Тема 1.2. Следственные действия при расследовании преступлений в информационной сфере.	16		2	3	11	
Тема 1.3. Криминалистическая значимость данных в реестре.	14			3	11	
Тема 1.4. Анализ следов воздействия на информацию в операционной системе Windows при решении задачи поиска по контексту.	13			3	10	
Тема 1.5. Журналы операционной системы Windows, их криминалистическая значимость.	12			2	10	
Раздел 2. Вид контроля	**1**	**1**				ПК-П6.1 ПК-П6.2 ПК-П6.3

Тема 2.1. Зачет.	1	1				ПК-П6.3 ПК-П6.4 ПК-П6.5
Итого	**72**	**1**	**4**	**14**	**53**	

Очно-заочная форма обучения

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Криминалистические методы защиты и исследования компьютерной информации в раскрытии преступлений в сфере IT	**67**		**4**	**6**	**57**	ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 1.1. Компьютерные преступления.	16			2	14	
Тема 1.2. Следственные действия при расследовании преступлений в информационной сфере.	17		2	1	14	
Тема 1.3. Криминалистическая значимость данных в реестре.	8		2	1	5	
Тема 1.4. Анализ следов воздействия на информацию в операционной системе Windows при решении задачи поиска по контексту.	6			1	5	
Тема 1.5. Журналы операционной системы Windows, их криминалистическая значимость.	20			1	19	
Раздел 2. Вид контроля	**1**	**1**				ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 2.1. Зачет.	1	1				
Итого	**68**	**1**	**4**	**6**	**57**	

5.2. Содержание разделов, тем дисциплин

Раздел 1. Криминалистические методы защиты и исследования компьютерной информации в раскрытии преступлений в сфере IT
(Заочная: Лекционные занятия - 2ч.; Практические занятия - 6ч.; Самостоятельная работа - 59ч.; Очная: Лекционные занятия - 4ч.; Практические занятия - 14ч.; Самостоятельная работа - 53ч.; Очно-заочная: Лекционные занятия - 4ч.; Практические занятия - 6ч.; Самостоятельная работа - 57ч.)

Тема 1.1. Компьютерные преступления.
(Заочная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 12ч.; Очная: Лекционные занятия - 2ч.; Практические занятия - 3ч.; Самостоятельная работа - 11ч.; Очно-заочная: Практические занятия - 2ч.; Самостоятельная работа - 14ч.)

Понятие компьютерной информации. Компьютерные преступления. Понятие компьютерного преступления. Борьба с преступлениями в сфере высоких технологий. Уголовный кодекс РФ о преступлениях в сфере компьютерной информации

Тема 1.2. Следственные действия при расследовании преступлений в информационной сфере.
(Очная: Лекционные занятия - 2ч.; Практические занятия - 3ч.; Самостоятельная работа - 11ч.; Очно-заочная: Лекционные занятия - 2ч.; Практические занятия - 1ч.; Самостоятельная работа - 14ч.; Заочная: Практические занятия - 1ч.; Самостоятельная работа - 12ч.)

Особенности осмотра и выемки средств компьютерной техники и носителей информации. Под-готовка к осмотру компьютер-ных средств. Предварительная ориентировка перед обыском или осмотром компьютерной техники. Исследование носите-лей и хранящейся информации. Исследование программного обеспечения. Исследование файлов и компьютерных доку-ментов. Исследование и экспер-тиза по компьютерной аппара-туре и информации. Исследова-ние, анализ и восстановление компьютерных данных. Виды хранящейся компьютерной ин-формации. Исследование аппа-ратных средств. Идентификация компьютеров и данных. Сред-ства диагностики и идентифика-ции компьютеров.

Тема 1.3. Криминалистическая значимость данных в реестре.
(Очно-заочная: Лекционные занятия - 2ч.; Практические занятия - 1ч.; Самостоятельная работа - 5ч.; Заочная: Практические занятия - 1ч.; Самостоятельная работа - 12ч.; Очная: Практические занятия - 3ч.; Самостоятельная работа - 11ч.)

Структура реестра: понятие куста, ветви, ключа, значения ключа. Типы данных. Логиче-ская организация данных в рее-стре. Изменения содержимого реестра при изменении аппарат-ной конфигурации компьютера, установке программного обес-печения, операциях с файлами. Программное обеспечение для работы с данными в реестре: виды программного обеспече-ния, его функциональные воз-можности и особенности приме-нения при производстве компь-ютерной экспертизы.

Тема 1.4. Анализ следов воздействия на информацию в операционной системе Windows при решении задачи поиска по контексту.
(Заочная: Практические занятия - 1ч.; Самостоятельная работа - 12ч.; Очная: Практические занятия - 3ч.; Самостоятельная работа - 10ч.; Очно-заочная: Практические занятия - 1ч.; Самостоятельная работа - 5ч.)

Моделирование и анализ иско-мой информации при решении задачи поиска по контексту. Стандартные и специальные средства кодирования информа-ции для оптимизации ее хране-ния или предотвращения не-санкционированного доступа. Инструментальные средства по-лучения доступа к информации и ее поиска по контексту.

Тема 1.5. Журналы операционной системы Windows, их криминалистическая значимость.
(Заочная: Практические занятия - 1ч.; Самостоятельная работа - 11ч.; Очная: Практические занятия - 2ч.; Самостоятельная работа - 10ч.; Очно-заочная: Практические занятия - 1ч.; Самостоятельная работа - 19ч.)

Журнал системы, журнал при-ложений и журнал безопасно-сти: их назначение, структура, криминалистическая значи-мость. Журнал программы «Проводник», его назначение, структура, криминалистическая значимость. Журнал сведений о системе, формируемый инстру-ментарием Windows Management Instrumentation (WMI), его на-значение, структура, кримина-листическая значимость. Иные журналы операционной системы Windows, их структура, крими¬налистическая значимость. Про¬граммное обеспечение для ра¬боты с журналами операцион¬ной системы Windows: виды программного обеспечения, его функциональные возможности и особенности применения при производстве компьютерной экспертизы

Раздел 2. Вид контроля
(Заочная: Внеаудиторная контактная работа - 1ч.; Очная: Внеаудиторная контактная работа - 1ч.; Очно-заочная: Внеаудиторная контактная работа - 1ч.)

Тема 2.1. Зачет.
(Заочная: Внеаудиторная контактная работа - 1ч.; Очная: Внеаудиторная контактная работа - 1ч.; Очно-заочная: Внеаудиторная контактная работа - 1ч.)
Зачет

6. Оценочные материалы текущего контроля

Раздел 1. Криминалистические методы защиты и исследования компьютерной информации в раскрытии преступлений в сфере IT

Форма контроля/оценочное средство: Задача

Вопросы/Задания:

1. Установите соответствие между видами компьютерных преступлений и их характеристиками:

Преступление
1. Неправомерный доступ к информации (ст. 272 УК РФ)
2. Создание вредоносных программ (ст. 273 УК РФ)
3. Нарушение правил эксплуатации ЭВМ (ст. 274 УК РФ)

Характеристика
A. Уничтожение, блокирование, модификация данных, приводящая к нарушению работы системы
B. Разработка и распространение программ, предназначенных для повреждения данных
C. Несоблюдение требований защиты информации, повлекшее ущерб

2. Установите последовательность действий при изъятии электронных носителей информации:
1. Фиксация состояния устройства (фото-, видеосъемка).
2. Отключение устройства от сети.
3. Изъятие с составлением протокола.
4. Упаковка и опечатывание.
5. Проверка на наличие вредоносного ПО.

3. Какие данные из реестра Windows могут иметь криминалистическую значимость? Приведите примеры.
В реестре Windows хранятся ключи, которые могут указывать на действия пользователя:

- UserAssist – история запуска программ;
- RecentDocs – список последних открытых файлов;
- USBSTOR – информация о подключенных USB-устройствах;
- Run, RunOnce – автозагрузка программ.

Эти данные помогают установить, какие приложения использовались, какие файлы открывались, а также факты подключения внешних носителей.

Подходит ли вышесказанное к заданному вопросу? Если нет, то укажите свой вариант ответа. Если да, то укажите "Да, подходит"

4. Какой нормативный акт регулирует порядок изъятия электронных доказательств?

A) Уголовно-процессуальный кодекс РФ
B) Федеральный закон "О персональных данных"
C) Закон "Об информации, информационных технологиях и о защите информации"

5. Какие журналы Windows могут использоваться при расследовании киберпреступлений? (Выберите 3 варианта)

A) Журнал событий (Event Viewer)
B) Журнал браузера
C) Журнал установки программ
D) Журнал печати

6. Какие процессуальные ошибки могут привести к недопустимости электронных доказательств в суде?

1. Нарушение порядка изъятия (отсутствие понятых, неправильная упаковка).
2. Отсутствие протокола или его некорректное оформление.
3. Незаконное получение данных (без санкции суда).
4. Непроведение экспертизы для подтверждения подлинности данных.

Подходит ли вышесказанное к заданному вопросу? Если нет, то укажите свой вариант ответа. Если да, то укажите "Да, подходит"

7. Установите соответствие между следственными действиями и их целями

Действие
1. Обыск
2. Выемка
3. Наложение ареста на данные
4. Истребование информации

Цель
A. Получение данных с серверов провайдера
B. Обнаружение и изъятие электронных устройств
C. Запрет на удаление или изменение информации
D. Получение данных без изъятия носителей

8. Какой закон регулирует вопросы защиты персональных данных в РФ?

A) Федеральный закон "О связи"
B) Федеральный закон "О персональных данных" (№ 152-ФЗ)
C) Уголовный кодекс РФ (ст. 137)

9. Установите порядок действий при анализе журналов Windows Event Viewer:

1. Определение временного периода, подлежащего изучению.
2. Фильтрация событий по ключевым кодам (например, 4624 — успешный вход).
3. Экспорт логов для дальнейшего исследования.
4. Проверка системных и пользовательских событий на аномалии.

10. Какие следы в операционной системе Windows могут указывать на несанкционированный доступ?

- Неизвестные учетные записи в разделе Локальные пользователи и группы.
- Подозрительные процессы в диспетчере задач (например, mimikatz.exe).

• Изменения в реестре (например, новые записи в HKLM\Software\Microsoft\Windows\CurrentVersion\Run).
• Логи неудачных попыток входа (коды 4625, 4771 в Event Viewer).

Подходит ли вышесказанное к заданному вопросу? Если нет, то укажите свой вариант ответа. Если да, то укажите "Да, подходит"

11. Какие методы используются для криминалистического анализа жесткого диска? (Выберите 3 варианта)

A) Создание посекторной копии (образ диска).
B) Восстановление удаленных файлов через MFT.
C) Изменение атрибутов файлов для сокрытия данных.
D) Анализ метаданных (даты создания, изменения).

12. Соотнесите виды цифровых доказательств с их источниками:

Доказательство
1. Логи сетевого трафика
2. Дампы оперативной памяти
3. Кеш браузера

Источник
A. Файрволы, IDS/IPS
B. Программы типа FTK Imager, Belkasoft
C. Папки AppData, Local Settings

13. Как отразить в процессуальной документации изъятие облачных данных?

1. Указать юридическое основание (ст. 186.1 УПК РФ — истребование электронных данных).
2. Зафиксировать запрос к провайдеру (например, через роскомнадзор).
3. Приложить метаданные (даты доступа, IP-адреса).
4. Оформить протокол с участием специалиста в области IT.

Подходит ли вышесказанное к заданному вопросу? Если нет, то укажите свой вариант ответа. Если да, то укажите "Да, подходит"

14. Установите порядок расследования DDoS-атаки

1. Фиксация логов сетевого оборудования.
2. Идентификация IP-адресов ботнета.
3. Проверка уязвимостей на атакованном сервере.
4. Направление запроса провайдеру для блокировки трафика.

15. Какой кодекс регулирует порядок назначения компьютерно-технической экспертизы?

A) Гражданский процессуальный кодекс РФ
B) Уголовно-процессуальный кодекс РФ
C) КоАП РФ

16. Прочитайте задание и установите соответствие между видами компьютерных преступлений и статьями УК РФ

Вид преступления
1. Неправомерный доступ к компьютерной информации
2. Создание, использование и распространение вредоносных программ
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации
4. Компьютерный шпионаж

Статья УК РФ
A. Ст. 272
B. Ст. 273
C. Ст. 274

D. Ст. 283.1

17. Прочитайте задание и установите правильную последовательность действий при осмотре места происшествия с изъятием компьютерной техники

1. Фиксация общего вида места происшествия (фото, видео).
2. Проверка включенных устройств на предмет активных процессов.
3. Отключение устройств от сети (при необходимости).
4. Изъятие устройств с составлением протокола.
5. Упаковка и опечатывание изъятых устройств.

18. Какие данные из файла подкачки (pagefile.sys) могут быть полезны при расследовании киберпреступлений?

Файл подкачки (pagefile.sys) может содержать:

- Фрагменты оперативной памяти, включая пароли, ключи шифрования.
- Данные о работавших приложениях и процессах.
- Следы вредоносного ПО, которое использовало подкачку для своей работы.
- Фрагменты сетевых пакетов или незашифрованных сообщений.

Для анализа требуется создание дампа памяти и использование специализированного ПО (например, Volatility).

Подходит ли вышесказанное к заданному вопросу? Если нет, то укажите свой вариант ответа. Если да, то укажите "Да, подходит"

19. Какой нормативный акт регламентирует порядок проведения судебной компьютерно-технической экспертизы?

A) Федеральный закон "О государственной судебно-экспертной деятельности"
B) Уголовно-процессуальный кодекс РФ
C) Федеральный закон "Об информации, информационных технологиях и о защите информации"

20. Какие методы используются для идентификации пользователя, работавшего за компьютером? (Выберите 3 варианта)

A) Анализ журналов событий Windows (Event Viewer).
B) Проверка истории браузера.
C) Изучение MAC-адреса сетевой карты.
D) Анализ содержимого файла SAM.

21. Какие процессуальные особенности необходимо учитывать при назначении и проведении экспертизы электронных доказательств?

1. Обоснование необходимости экспертизы в постановлении (ст. 195 УПК РФ).
2. Правильная формулировка вопросов эксперту (например: "Имеются ли следы удаления файлов?").
3. Обеспечение целостности доказательств (передача данных на защищенных носителях).
4. Участие специалиста при изъятии и исследовании цифровых данных.
5. Соблюдение сроков (не более 30 дней, ст. 199 УПК РФ).

Подходит ли вышесказанное к заданному вопросу? Если нет, то укажите свой вариант ответа. Если да, то укажите "Да, подходит"

22. Установите соответствие между типами киберпреступлений и методами их расследования

Тип преступления
1. Фишинг
2. Распространение вредоносного ПО
3. Несанкционированный доступ к серверам
4. Утечка данных

Метод расследования
A. Анализ почтовых заголовков (headers)

B. Исследование дампов памяти
C. Анализ журналов аутентификации
D. Мониторинг Darknet

23. Установите порядок действий при расследовании инцидента с шифровальщиком (ransomware)

1. Изоляция зараженных систем от сети.
2. Сбор образцов вредоносного ПО.
3. Анализ логов на предмет точки входа.
4. Расшифровка данных (при наличии возможности).
5. Установление способа распространения вируса.

24. Опишите алгоритм проверки компьютера на наличие следов использования анонимайзеров (VPN, Tor)

1. Анализ установленных программ (наличие Tor Browser, VPN-клиентов).
2. Проверка сетевых подключений (нестандартные порты, IP-адреса узлов выхода Tor).
3. Изучение истории браузера (доступ к доменам .onion).
4. Поиск конфигурационных файлов (например, torrc).
5. Анализ логов брандмауэра на предмет подключений к известным VPN-серверам.

Подходит ли вышесказанное к заданному вопросу? Если нет, то укажите свой вариант ответа. Если да, то укажите "Да, подходит"

25. Установите соответствие между видами цифровых следов и их источниками

Цифровой след
1. Метаданные файлов
2. Журналы событий
3. Дампы оперативной памяти
4. История браузера

Источник
A. Свойства файла (дата создания, изменения)
B. Event Viewer
C. FTK Imager, Belkasoft RAM Capturer
D. Папки AppData, Local Settings

26. Установите порядок действий при расследовании утечки данных через облачное хранилище

1. Фиксация времени и обстоятельств утечки.
2. Анализ логов доступа к облачному аккаунту.
3. Истребование данных у провайдера облачного сервиса.
4. Проверка устройств, с которых осуществлялся доступ.
5. Установление круга лиц, имевших доступ к данным.

27. Какие криминалистически значимые данные можно извлечь из файла hiberfil.sys в Windows?

Файл гибернации (hiberfil.sys) содержит:
- Дамп оперативной памяти на момент перевода системы в режим гибернации.
- Незашифрованные пароли и ключи сеансов.
- Следы работавших приложений и процессов.
- Сетевые подключения и активные сеансы.

Для анализа требуются инструменты типа Volatility или Magnet RAM Capture.

Подходит ли вышесказанное к заданному вопросу? Если нет, то укажите свой вариант ответа. Если да, то укажите "Да, подходит"

28. Какой нормативный акт регулирует порядок изъятия электронной почты в рамках уголовного дела?

А) Федеральный закон "О связи"

B) Ст. 186.1 УПК РФ (истребование электронных сообщений)
C) Закон "Об оперативно-розыскной деятельности"

29. Какие данные из журналов Windows могут свидетельствовать о попытке подбора пароля? (Выберите 2 варианта)

A) Код события 4625 (неудачный вход).
B) Множественные события 4771 (ошибка аутентификации Kerberos).
C) Код события 7036 (остановка службы).
D) События 1102 (очистка журнала событий).

30. Установите порядок действий при расследовании инцидента с компрометацией учетных записей

1. Фиксация времени несанкционированного доступа.
2. Анализ логов аутентификации (Active Directory, серверы RADIUS).
3. Проверка устройств, с которых выполнялся вход.
4. Идентификация точки входа (фишинг, брутфорс).
5. Назначение экспертизы для анализа вредоносного ПО (при наличии).

Раздел 2. Вид контроля

Форма контроля/оценочное средство:

Вопросы/Задания:

.

7. Оценочные материалы промежуточной аттестации

Очная форма обучения, Третий семестр, Зачет
Контролируемые ИДК: ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Вопросы/Задания:

1. Понятие компьютерной информации.

2. Компьютерные преступления.

3. Понятие компьютерного преступления.

4. Борьба с преступлениями в сфере высоких технологий.

5. Уголовный кодекс РФ о преступлениях в сфере компьютерной информации.

6. Особенности осмотра и выемки средств компьютерной техники и носителей информации.

7. Подготовка к осмотру компьютерных средств.

8. Предварительная ориентировка перед обыском или осмотром компьютерной техники.

9. Исследование носителей и хранящейся информации.

10. Исследование программного обеспечения.

11. Исследование файлов и компьютерных документов.

12. Исследование и экспертиза компьютерной аппаратуры и информации.

13. Исследование, анализ и восстановление компьютерных данных.

14. Виды хранящейся компьютерной информации.

15. Исследование аппаратных средств.

16. Идентификация компьютеров и данных.

17. Средства диагностики и идентификации компьютеров.

18. Структура реестра: понятие куста, ветви, ключа, значения ключа.

19. Типы данных.

20. Логическая организация данных в реестре.

21. Изменения содержимого реестра при изменении аппаратной конфигурации компьютера, установке программного обеспечения, операциях с файлами.

22. Программное обеспечение для работы с данными в реестре: виды, функциональные возможности и особенности применения при компьютерной экспертизе.

23. Моделирование и анализ искомой информации при решении задачи поиска по контексту.

24. Стандартные и специальные средства кодирования информации для оптимизации хранения или предотвращения несанкционированного доступа.

25. Инструментальные средства получения доступа к информации и её поиска по контексту.

26. Журнал системы, журнал приложений и журнал безопасности: назначение, структура, криминалистическая значимость.

27. Журнал программы «Проводник»: назначение, структура, криминалистическая значимость.

28. Журнал сведений о системе (Windows Management Instrumentation, WMI): назначение, структура, криминалистическая значимость.

29. Иные журналы операционной системы Windows: структура, криминалистическая значимость.

30. Программное обеспечение для работы с журналами ОС Windows: виды, функциональные возможности и применение в компьютерной экспертизе.

31. Криминалистическая характеристика киберпреступлений: особенности и классификация.

32. Современные тенденции развития компьютерных преступлений.

33. Правовые основы изъятия электронных доказательств в РФ.

34. Особенности процессуального оформления результатов компьютерно-технической экспертизы.

35. Методы противодействия фальсификации цифровых доказательств.

36. Роль криптографии в защите компьютерной информации.

37. Принципы работы с зашифрованными носителями информации.

38. Особенности расследования преступлений в darknet.

39. Юридическая сила электронных доказательств в суде.

40. Международное сотрудничество в борьбе с киберпреступлениями.

41. Алгоритм изъятия жесткого диска с соблюдением процессуальных норм.

42. Методика обнаружения удаленных файлов на носителе.

43. Порядок работы с виртуальными машинами при расследовании.

44. Тактика изъятия данных с мобильных устройств.

45. Особенности анализа сетевого трафика при расследовании.

46. Методы выявления следов использования анонимайзеров.

47. Технология восстановления переписки из мессенджеров.

48. Анализ метаданных файлов как источник доказательств.

49. Методика выявления признаков несанкционированного доступа к системе.

50. Особенности работы с облачными хранилищами при расследовании.

51. Анализ журналов событий для установления времени совершения преступления.

52. Методы выявления следов использования вредоносного ПО.

53. Криминалистический анализ истории браузера.

54. Исследование cookie-файлов и кэша приложений.

55. Методика установления личности пользователя по цифровым следам.

56. Анализ временных меток файловой системы.

57. Выявление признаков подделки цифровых документов.

58. Методы обнаружения скрытых разделов на носителях.

59. Анализ данных биометрии в компьютерных системах.

60. Перспективные направления развития компьютерно-технической экспертизы.

Очно-заочная форма обучения, Четвертый семестр, Зачет
Контролируемые ИДК: ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Вопросы/Задания:

1. Понятие компьютерной информации.

2. Компьютерные преступления.

3. Понятие компьютерного преступления.

4. Борьба с преступлениями в сфере высоких технологий.

5. Уголовный кодекс РФ о преступлениях в сфере компьютерной информации.

6. Особенности осмотра и выемки средств компьютерной техники и носителей информации.

7. Подготовка к осмотру компьютерных средств.

8. Предварительная ориентировка перед обыском или осмотром компьютерной техники.

9. Исследование носителей и хранящейся информации.

10. Исследование программного обеспечения.

11. Исследование файлов и компьютерных документов.

12. Исследование и экспертиза компьютерной аппаратуры и информации.

13. Исследование, анализ и восстановление компьютерных данных.

14. Виды хранящейся компьютерной информации.

15. Исследование аппаратных средств.

16. Идентификация компьютеров и данных.

17. Средства диагностики и идентификации компьютеров.

18. Структура реестра: понятие куста, ветви, ключа, значения ключа.

19. Типы данных.

20. Логическая организация данных в реестре.

21. Изменения содержимого реестра при изменении аппаратной конфигурации компьютера, установке программного обеспечения, операциях с файлами.

22. Программное обеспечение для работы с данными в реестре: виды, функциональные возможности и особенности применения при компьютерной экспертизе.

23. Моделирование и анализ искомой информации при решении задачи поиска по контексту.

24. Стандартные и специальные средства кодирования информации для оптимизации хранения или предотвращения несанкционированного доступа.

25. Инструментальные средства получения доступа к информации и её поиска по контексту.

26. Журнал системы, журнал приложений и журнал безопасности: назначение, структура, криминалистическая значимость.

27. Журнал программы «Проводник»: назначение, структура, криминалистическая значимость.

28. Журнал сведений о системе (Windows Management Instrumentation, WMI): назначение, структура, криминалистическая значимость.

29. Иные журналы операционной системы Windows: структура, криминалистическая значимость.

30. Программное обеспечение для работы с журналами ОС Windows: виды, функциональные возможности и применение в компьютерной экспертизе.

31. Криминалистическая характеристика киберпреступлений: особенности и классификация.

32. Современные тенденции развития компьютерных преступлений.

33. Правовые основы изъятия электронных доказательств в РФ.

34. Особенности процессуального оформления результатов компьютерно-технической экспертизы.

35. Методы противодействия фальсификации цифровых доказательств.

36. Роль криптографии в защите компьютерной информации.

37. Принципы работы с зашифрованными носителями информации.

38. Особенности расследования преступлений в darknet.

39. Юридическая сила электронных доказательств в суде.

40. Международное сотрудничество в борьбе с киберпреступлениями.

41. Алгоритм изъятия жесткого диска с соблюдением процессуальных норм.

42. Методика обнаружения удаленных файлов на носителе.

43. Порядок работы с виртуальными машинами при расследовании.

44. Тактика изъятия данных с мобильных устройств.

45. Особенности анализа сетевого трафика при расследовании.

46. Методы выявления следов использования анонимайзеров.

47. Технология восстановления переписки из мессенджеров.

48. Анализ метаданных файлов как источник доказательств.

49. Методика выявления признаков несанкционированного доступа к системе.

50. Особенности работы с облачными хранилищами при расследовании.

51. Анализ журналов событий для установления времени совершения преступления.

52. Методы выявления следов использования вредоносного ПО.

53. Криминалистический анализ истории браузера.

54. Исследование cookie-файлов и кэша приложений.

55. Методика установления личности пользователя по цифровым следам.

56. Анализ временных меток файловой системы.

57. Выявление признаков подделки цифровых документов.

58. Методы обнаружения скрытых разделов на носителях.

59. Анализ данных биометрии в компьютерных системах.

60. Перспективные направления развития компьютерно-технической экспертизы.

Очно-заочная форма обучения, Четвертый семестр, Контрольная работа
Контролируемые ИДК: ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Вопросы/Задания:

1. Составьте пошаговый алгоритм изъятия жесткого диска с соблюдением процессуальных норм

2. Разработайте методику документальной фиксации состояния компьютерной техники при осмотре места происшествия

3. Составьте перечень необходимого оборудования для проведения выемки компьютерной техники

4. Опишите методику поиска и анализа удаленных файлов на носителе

5. Разработайте алгоритм исследования метаданных файлов для установления авторства документа

6. Составьте план анализа истории браузера для установления действий пользователя

7. Опишите технологию восстановления данных после форматирования диска

8. Разработайте методику восстановления переписки из популярных мессенджеров

9. Составьте перечень программных средств для восстановления удаленных фотографий

10. Опишите методику анализа журналов событий Windows для установления времени совершения действий

11. Разработайте алгоритм исследования реестра Windows на предмет следов вредоносного ПО

12. Составьте план анализа временных меток файловой системы

13. Опишите методику анализа сетевого трафика для выявления несанкционированного доступа

14. Разработайте алгоритм исследования кэша DNS

15. Составьте перечень признаков использования анонимайзеров и VPN

16. Опишите методику изъятия данных с Android-устройства

17. Разработайте алгоритм исследования резервных копий iPhone

18. Составьте перечень артефактов, которые могут быть извлечены из мобильного приложения

19. Опишите методику работы с зашифрованными контейнерами

20. Разработайте алгоритм выявления признаков использования стеганографии

21. Составьте перечень методов обхода базовой защиты файлов

22. Опишите методику выявления следов работы кейлоггера

23. Разработайте алгоритм анализа подозрительного исполняемого файла

24. Составьте перечень признаков заражения системы ransomware

25. На основании предоставленного образа диска составьте хронологию действий пользователя

26. По предоставленным журналам событий восстановите последовательность действий злоумышленника

27. На основании анализа сетевого трафика выявите факт утечки данных

28. Составьте образец постановления о назначении компьютерно-технической экспертизы

29. Разработайте форму акта изъятия электронных носителей информации

30. Составьте перечень типовых вопросов для эксперта при исследовании компьютерной техники

Заочная форма обучения, Третий семестр, Зачет
Контролируемые ИДК: ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Вопросы/Задания:

1. Понятие компьютерной информации.

2. Компьютерные преступления.

3. Понятие компьютерного преступления.

4. Борьба с преступлениями в сфере высоких технологий.

5. Уголовный кодекс РФ о преступлениях в сфере компьютерной информации.

6. Особенности осмотра и выемки средств компьютерной техники и носителей информации.

7. Подготовка к осмотру компьютерных средств.

8. Предварительная ориентировка перед обыском или осмотром компьютерной техники.

9. Исследование носителей и хранящейся информации.

10. Исследование программного обеспечения.

11. Исследование файлов и компьютерных документов.

12. Исследование и экспертиза компьютерной аппаратуры и информации.

13. Исследование, анализ и восстановление компьютерных данных.

14. Виды хранящейся компьютерной информации.

15. Исследование аппаратных средств.

16. Идентификация компьютеров и данных.

17. Средства диагностики и идентификации компьютеров.

18. Структура реестра: понятие куста, ветви, ключа, значения ключа.

19. Типы данных.

20. Логическая организация данных в реестре.

21. Изменения содержимого реестра при изменении аппаратной конфигурации компьютера, установке программного обеспечения, операциях с файлами.

22. Программное обеспечение для работы с данными в реестре: виды, функциональные возможности и особенности применения при компьютерной экспертизе.

23. Моделирование и анализ искомой информации при решении задачи поиска по контексту.

24. Стандартные и специальные средства кодирования информации для оптимизации хранения или предотвращения несанкционированного доступа.

25. Инструментальные средства получения доступа к информации и её поиска по контексту.

26. Журнал системы, журнал приложений и журнал безопасности: назначение, структура, криминалистическая значимость.

27. Журнал программы «Проводник»: назначение, структура, криминалистическая значимость.

28. Журнал сведений о системе (Windows Management Instrumentation, WMI): назначение, структура, криминалистическая значимость.

29. Иные журналы операционной системы Windows: структура, криминалистическая значимость.

30. Программное обеспечение для работы с журналами ОС Windows: виды, функциональные возможности и применение в компьютерной экспертизе.

31. Криминалистическая характеристика киберпреступлений: особенности и классификация.

32. Современные тенденции развития компьютерных преступлений.

33. Правовые основы изъятия электронных доказательств в РФ.

34. Особенности процессуального оформления результатов компьютерно-технической экспертизы.

35. Методы противодействия фальсификации цифровых доказательств.

36. Роль криптографии в защите компьютерной информации.

37. Принципы работы с зашифрованными носителями информации.

38. Особенности расследования преступлений в darknet.

39. Юридическая сила электронных доказательств в суде.

40. Международное сотрудничество в борьбе с киберпреступлениями.

41. Алгоритм изъятия жесткого диска с соблюдением процессуальных норм.

42. Методика обнаружения удаленных файлов на носителе.

43. Порядок работы с виртуальными машинами при расследовании.

44. Тактика изъятия данных с мобильных устройств.

45. Особенности анализа сетевого трафика при расследовании.

46. Методы выявления следов использования анонимайзеров.

47. Технология восстановления переписки из мессенджеров.

48. Анализ метаданных файлов как источник доказательств.

49. Методика выявления признаков несанкционированного доступа к системе.

50. Особенности работы с облачными хранилищами при расследовании.

51. Анализ журналов событий для установления времени совершения преступления.

52. Методы выявления следов использования вредоносного ПО.

53. Криминалистический анализ истории браузера.

54. Исследование cookie-файлов и кэша приложений.

55. Методика установления личности пользователя по цифровым следам.

56. Анализ временных меток файловой системы.

57. Выявление признаков подделки цифровых документов.

58. Методы обнаружения скрытых разделов на носителях.

59. Анализ данных биометрии в компьютерных системах.

60. Перспективные направления развития компьютерно-технической экспертизы.

Заочная форма обучения, Третий семестр, Контрольная работа
Контролируемые ИДК: ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Вопросы/Задания:

1. Составьте пошаговый алгоритм изъятия жесткого диска с соблюдением процессуальных норм

2. Разработайте методику документальной фиксации состояния компьютерной техники при осмотре места происшествия

3. Составьте перечень необходимого оборудования для проведения выемки компьютерной техники

4. Опишите методику поиска и анализа удаленных файлов на носителе

5. Разработайте алгоритм исследования метаданных файлов для установления авторства документа

6. Составьте план анализа истории браузера для установления действий пользователя

7. Опишите технологию восстановления данных после форматирования диска

8. Разработайте методику восстановления переписки из популярных мессенджеров

9. Составьте перечень программных средств для восстановления удаленных фотографий

10. Опишите методику анализа журналов событий Windows для установления времени совершения действий

11. Разработайте алгоритм исследования реестра Windows на предмет следов вредоносного ПО

12. Составьте план анализа временных меток файловой системы

13. Опишите методику анализа сетевого трафика для выявления несанкционированного доступа

14. Разработайте алгоритм исследования кэша DNS

15. Составьте перечень признаков использования анонимайзеров и VPN

16. Опишите методику изъятия данных с Android-устройства

17. Разработайте алгоритм исследования резервных копий iPhone

18. Составьте перечень артефактов, которые могут быть извлечены из мобильного приложения

19. Опишите методику работы с зашифрованными контейнерами

20. Разработайте алгоритм выявления признаков использования стеганографии

21. Составьте перечень методов обхода базовой защиты файлов

22. Опишите методику выявления следов работы кейлоггера

23. Разработайте алгоритм анализа подозрительного исполняемого файла

24. Составьте перечень признаков заражения системы ransomware

25. На основании предоставленного образа диска составьте хронологию действий пользователя

26. По предоставленным журналам событий восстановите последовательность действий злоумышленника

27. На основании анализа сетевого трафика выявите факт утечки данных

28. Составьте образец постановления о назначении компьютерно-технической экспертизы

29. Разработайте форму акта изъятия электронных носителей информации

30. Составьте перечень типовых вопросов для эксперта при исследовании компьютерной техники

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. ГРИЦАЕВ С. И. Криминалистическое обеспечение защиты и исследования компьютерной информации: метод. указания / ГРИЦАЕВ С. И.. - Краснодар: КубГАУ, 2025. - 45 с. - Текст: непосредственный.

2. ГРИЦАЕВ С. И. Криминалистическое обеспечение защиты и исследования компьютерной информации: учеб. пособие / ГРИЦАЕВ С. И., Шевель Д. В.. - Краснодар: КубГАУ, 2022. - 80 с. - 978-5-907597-10-5. - Текст: электронный. // : [сайт]. - URL: https://edu.kubsau.ru/mod/resource/view.php?id=12047 (дата обращения: 15.10.2025). - Режим доступа: по подписке

Дополнительная литература

1. Мистров, Л.Е. Информационные технологии в юридической деятельности: Microsoft Office 2010: Учебное пособие / Л.Е. Мистров, А.В. Мишин. - Москва: Российский государственный университет правосудия, 2016. - 232 с. - 978-5-93916-503-7. - Текст: электронный // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.com/cover/1191/1191410.jpg (дата обращения: 08.09.2025). - Режим доступа: по подписке

2. Информационные технологии в юридической деятельности: учебное пособие / составители: И. П. Хвостова, А. А. Плетухина. - Информационные технологии в юридической деятельности - Ставрополь: Северо-Кавказский федеральный университет, 2015. - 222 с. - 2227-8397. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/63091.html (дата обращения: 08.10.2025). - Режим доступа: по подписке

3. ПОМАЗАНОВ В.В. Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности: учеб. пособие / ПОМАЗАНОВ В.В.. - Краснодар: КубГАУ, 2021. - 101 с. - 978-5-907474-90-1. - Текст: непосредственный.

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. https://www.consultant.ru/ - КонсультантПлюс
2. https://sudact.ru/ - Судебные и нормативные акты РФ

Ресурсы «Интернет»

1. www.мвд.рф - Официальный сайт МВД России
2. http://www.pravo.gov.ru/ips/ - Официальный интернет-портал правовой информации
3. https://www.kublse.ru - Официальный сайт ФБУ «Краснодарская лаборатория судебной экспертизы Министерства юстиции Российской Федерации»
4. https://www.kublse.ru - Официальный сайт ФБУ «Краснодарская лаборатория судебной экспертизы Министерства юстиции Российской Федерации»
5. https://www.rsl.ru/ - ФГБУ «Российская государственная библиотека»
6. http://www.pravo.gov.ru/ips/ - Официальный интернет-портал правовой информации

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине позволяют:
– обеспечить взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет»;
– фиксировать ход образовательного процесса, результатов промежуточной аттестации по дисциплине и результатов освоения образовательной программы;
– организовать процесс образования путем визуализации изучаемой информации посредством использования презентаций, учебных фильмов;
– контролировать результаты обучения на основе компьютерного тестирования.
Перечень лицензионного программного обеспечения:
1 Microsoft Windows - операционная система.
2 Microsoft Office (включает Word, Excel, Power Point) - пакет офисных приложений.
Перечень профессиональных баз данных и информационных справочных систем:
1 Гарант - правовая, https://www.garant.ru/
2 Консультант - правовая, https://www.consultant.ru/
3 Научная электронная библиотека eLibrary - универсальная, https://elibrary.ru/
Доступ к сети Интернет, доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Университет располагает на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы бакалавриата, специлитета, магистратуры по Блоку 1 "Дисциплины (модули)" и Блоку 3 "Государственная итоговая аттестация" в соответствии с учебным планом.
Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне его. Условия для функционирования электронной информационно-образовательной среды могут быть созданы с использованием ресурсов иных организаций.

Лаборатория
032зоо
Коммплект оборудывания для дактилоскопирования (базовая Комплектация напольный вариант - 2 шт.
033зоо
Брошюратор (в комплекте с электродрелью) - 0 шт.
комплект для безкраскового изъятия оттисков обуви - 0 шт.
Комплект для изъятия биоматериалов КИБС-14 - 0 шт.
Комплект для работы с микрообъектами - 0 шт.
комплект криминал. №6 (УФ и ИК излучатели) - 0 шт.
Комплект магнитных систем "Поиск" - 0 шт.
Комплект медико-криминалистический УК-01М - 0 шт.
комплект пожарно-технический - 0 шт.
комплект сотрудника ДПС в чемодане - 0 шт.
Комплект эксперта-криминалиста "Кремний" - 0 шт.
Магнитные грабли "Ёж" - 0 шт.
металлоискатель - 0 шт.
микроскоп МБС-10 - 0 шт.
микроскоп цифровой 25-200 крат - 0 шт.
Микроскоп цифровой DigiMicro LCD - 0 шт.
прибор отбора запаха - 0 шт.
прибор ПОС-Т для обнаружения и изъятия пылевых следов обуви и микрочастиц на ковровых покрытиях и т.д. - 0 шт.
сумка для работы с объемн. следами - 0 шт.
сумка-фотокомплект цифр. - 0 шт.
универсальный просмотровый детектор - 0 шт.
Унифицированный дактилоскопический набор "Дакто" (в полиэстеровой сумке) - 0 шт.
Унифицированный комплект криминалиста УК-01 (с фотокамерой) - 0 шт.
чемодан криминалиста - 0 шт.
чемодан спец. для работы на месте происшествия - 0 шт.
чемодан эксперта-криминалиста - 0 шт.
034зоо
Брошюратор (в комплекте с электродрелью) - 0 шт.
Комплект "Автоэксперт-Т" КАТ-04 - 0 шт.
Комплект для изъятия биоматериалов КИБС-14 - 0 шт.
Комплект для работы с микрообъектами - 0 шт.
Комплект для работы со следами пальцев рук - 0 шт.
Комплект магнитных систем "Поиск" - 0 шт.
Комплект медико-криминалистический УК-01М - 0 шт.
Комплект оборудования для дактилоскопирования (базовая комплектация): напольный вариант - 0 шт.
Комплект эксперта-криминалиста "Кремний" - 0 шт.
микроскоп МБС-10 - 0 шт.

Микроскоп цифровой DigiMicro LCD - 0 шт.
Парта - 10 шт.
прибор отбора запаха - 0 шт.
следствен.сумка работ.прокурат - 0 шт.
универсальный просмотровый детектор - 0 шт.
Унифицированный комплект криминалиста УК-01 (с фотокамерой) - 0 шт.
чемодан спец. для работы на месте происшествия - 0 шт.
чемодан эксперта-криминалиста - 0 шт.

035зоо
манекен Федя - 0 шт.
стул - 6 шт.
холодильник "Саратов" - 0 шт.
Шкаф книжный - 3 шт.

Лекционный зал
415гл
кафедра - 0 шт.
стол 2 местный - 1 шт.

Учебная аудитория
437гл
сплит-система BEKO - 0 шт.

026а зоо
Парта - 16 шт.
телевизор SONY - 0 шт.

Компьютерный класс
025а зоо
Компьютер персональный Lenovo ThinkCentre 4GbDDR4 128 GB SSD+монитор Dell - 0 шт.
стол компьютерный - 10 шт.

9. Методические указания по освоению дисциплины (модуля)

Учебная работа по направлению подготовки осуществляется в форме контактной работы с преподавателем, самостоятельной работы обучающегося, текущей и промежуточной аттестаций, иных формах, предлагаемых университетом. Учебный материал дисциплины структурирован и его изучение производится в тематической последовательности. Содержание методических указаний должно соответствовать требованиям Федерального государственного образовательного стандарта и учебных программ по дисциплине. Самостоятельная работа студентов может быть выполнена с помощью материалов, размещенных на портале поддержки Moodl.

Методические указания по формам работы

Лекционные занятия

Передача значительного объема систематизированной информации в устной форме достаточно большой аудитории. Дает возможность экономно и систематично излагать учебный материал. Обучающиеся изучают лекционный материал, размещенный на портале поддержки обучения Moodl.

Практические занятия

Форма организации обучения, проводимая под руководством преподавателя и служащая для

детализации, анализа, расширения, углубления, закрепления, применения (или выполнения разнообразных практических работ, упражнений) и контроля усвоения полученной на лекциях учебной информации. Практические занятия проводятся с использованием учебно-методических изданий, размещенных на образовательном портале университета.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

Для инвалидов и лиц с ОВЗ может изменяться объём дисциплины (модуля) в часах, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося (при этом не увеличивается количество зачётных единиц, выделенных на освоение дисциплины).

Фонды оценочных средств адаптируются к ограничениям здоровья и восприятия информации обучающимися.

Основные формы представления оценочных средств – в печатной форме или в форме электронного документа.

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением зрения:

– устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;

– с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.;

– при возможности письменная проверка с использованием рельефно-точечной системы Брайля, увеличенного шрифта, использование специальных технических средств (тифлотехнических средств): контрольные, графические работы, тестирование, домашние задания, эссе, отчеты и др.

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением слуха:

– письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;

– с использованием компьютера: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.;

– при возможности устная проверка с использованием специальных технических средств (аудиосредств, средств коммуникации, звукоусиливающей аппаратуры и др.): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением опорно-двигательного аппарата:

– письменная проверка с использованием специальных технических средств (альтернативных средств ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;

– устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;

– с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы предпочтительнее обучающимся, ограниченным в передвижении и др.

Адаптация процедуры проведения промежуточной аттестации для инвалидов и лиц с ОВЗ.

В ходе проведения промежуточной аттестации предусмотрено:

– предъявление обучающимся печатных и (или) электронных материалов в формах, адаптированных к ограничениям их здоровья;

– возможность пользоваться индивидуальными устройствами и средствами, позволяющими адаптировать материалы, осуществлять приём и передачу информации с учетом их индивидуальных особенностей;

– увеличение продолжительности проведения аттестации;

– возможность присутствия ассистента и оказания им необходимой помощи (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем).
Формы промежуточной аттестации для инвалидов и лиц с ОВЗ должны учитывать индивидуальные и психофизические особенности обучающегося/обучающихся по АОПОП ВО (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями зрения:
– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить плоскопечатную информацию в аудиальную или тактильную форму;
– возможность использовать индивидуальные устройства и средства, позволяющие адаптировать материалы, осуществлять приём и передачу информации с учетом индивидуальных особенностей и состояния здоровья студента;
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– использование чёткого и увеличенного по размеру шрифта и графических объектов в мультимедийных презентациях;
– использование инструментов «лупа», «прожектор» при работе с интерактивной доской;
– озвучивание визуальной информации, представленной обучающимся в ходе занятий;
– обеспечение раздаточным материалом, дублирующим информацию, выводимую на экран;
– наличие подписей и описания у всех используемых в процессе обучения рисунков и иных графических объектов, что даёт возможность перевести письменный текст в аудиальный;
– обеспечение особого речевого режима преподавания: лекции читаются громко, разборчиво, отчётливо, с паузами между смысловыми блоками информации, обеспечивается интонирование, повторение, акцентирование, профилактика рассеивания внимания;
– минимизация внешнего шума и обеспечение спокойной аудиальной обстановки;
– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, на ноутбуке, в виде пометок в заранее подготовленном тексте);
– увеличение доли методов социальной стимуляции (обращение внимания, апелляция к ограничениям по времени, контактные виды работ, групповые задания и др.) на практических и лабораторных занятиях;
– минимизирование заданий, требующих активного использования зрительной памяти и зрительного внимания;
– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы.
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями опорно-двигательного аппарата (маломобильные студенты, студенты, имеющие трудности передвижения и патологию верхних конечностей):
– возможность использовать специальное программное обеспечение и специальное оборудование и позволяющее компенсировать двигательное нарушение (коляски, ходунки, трости и др.);
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– применение дополнительных средств активизации процессов запоминания и повторения;
– опора на определенные и точные понятия;
– использование для иллюстрации конкретных примеров;
– применение вопросов для мониторинга понимания;
– разделение изучаемого материала на небольшие логические блоки;
– увеличение доли конкретного материала и соблюдение принципа от простого к сложному при объяснении материала;
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– увеличение доли методов социальной стимуляции (обращение внимания, аппеляция к ограничениям по времени, контактные виды работ, групповые задания др.);

– обеспечение беспрепятственного доступа в помещения, а также пребывания них;
– наличие возможности использовать индивидуальные устройства и средства, позволяющие обеспечить реализацию эргономических принципов и комфортное пребывание на месте в течение всего периода учёбы (подставки, специальные подушки и др.).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями слуха (глухие, слабослышащие, позднооглохшие):
– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить аудиальную форму лекции в плоскопечатную информацию;
– наличие возможности использовать индивидуальные звукоусиливающие устройства и сурдотехнические средства, позволяющие осуществлять приём и передачу информации; осуществлять взаимообратный перевод текстовых и аудиофайлов (блокнот для речевого ввода), а также запись и воспроизведение зрительной информации;
– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;
– наличие наглядного сопровождения изучаемого материала (структурно-логические схемы, таблицы, графики, концентрирующие и обобщающие информацию, опорные конспекты, раздаточный материал);
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;
– особый речевой режим работы (отказ от длинных фраз и сложных предложений, хорошая артикуляция; четкость изложения, отсутствие лишних слов; повторение фраз без изменения слов и порядка их следования; обеспечение зрительного контакта во время говорения и чуть более медленного темпа речи, использование естественных жестов и мимики);
– чёткое соблюдение алгоритма занятия и заданий для самостоятельной работы (называние темы, постановка цели, сообщение и запись плана, выделение основных понятий и методов их изучения, указание видов деятельности студентов и способов проверки усвоения материала, словарная работа);
– соблюдение требований к предъявляемым учебным текстам (разбивка текста на час¬ти; выделение опорных смысловых пунктов; использование наглядных средств);
– минимизация внешних шумов;
– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;
– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с прочими видами нарушений (ДЦП с нарушениями речи, заболевания эндокринной, центральной нервной и сердечно-сосудистой систем, онкологические заболевания):
– наличие возможности использовать индивидуальные устройства и средства, позволяющие осуществлять приём и передачу информации;
– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;
– наличие наглядного сопровождения изучаемого материала;
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;
– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;
– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего);
– предоставление образовательного контента в текстовом электронном формате;
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном

образовательном портале;
– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, в виде пометок в заранее подготовленном тексте);
– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы;
– стимулирование выработки у студентов навыков самоорганизации и самоконтроля;
– наличие пауз для отдыха и смены видов деятельности по ходу занятия.

10. Методические рекомендации по освоению дисциплины (модуля)

Дисциплина "Криминалистическое обеспечение защиты и исследования компьютерной информации" ведется в соответствии с учебным планом и расписанием занятий по неделям. Темы проведения занятий определяются тематическим планом рабочей программы дисциплины.