ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 00BD22195255F8C38D790F57DE64C63FC4
Владелец Лисова Ольга Михайловна
Действителен с 02.06.2025 по 26.08.2026
Должность Проректор по дополнительному образованию
Организация ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ"

Центр опережающей профессиональной подготовки

УТВЕРЖДАЮ:
Проректор по дополнительному образованию
ФГБОУ ВО Ставропольский ГАУ, профессор
_____О.М. Лисова
«___» _____ 2025 г.

Категория обучающихся:
Слушатели, имеющие высшее образование (уровень квалификации – специалитет, магистр)

Дополнительная профессиональная программа
повышения квалификации
«Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»

г. Ставрополь, 2025 год

Дополнительная профессиональная программа повышения квалификации «Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий» рассмотрена и утверждена учебно-методической комиссией Центра опережающей профессиональной подготовки (протокол №____от_____20__г.).

Нормативные правовые основания разработки программы:

- Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- федеральный государственный образовательный стандарт высшего образования – бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (утвержден приказом министерства науки и высшего образования Российской федерации от 19.09.2017 г. № 926).

Программа реализуется в рамках требований профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022г №533н, трудовая функция С/06.7 – проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях, необходимые знания:

- нормы уголовного и административного права применительно к преступлениям и правонарушениям в сфере компьютерной информации;
- характеристики правонарушений в области связи и информации;
- виды преступлений в сфере компьютерной информации;
- порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов при расследовании компьютерных преступлений, правонарушений и инцидентов;
- способы обнаружения и нейтрализации последствий вторжений в компьютерные системы;
- методы анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении.

Трудоемкость (час)

Дистанционные занятия, из них:	**36**
- Лекции	18
- Практические, лабораторные и семинарские занятия	18
Самостоятельная работа слушателей	**34**
Итоговая аттестация	**2**
ВСЕГО:	72

Пояснительная записка

Дополнительная профессиональная программа повышения квалификации «Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий» направлена на формирование у слушателей компетенций, необходимых для эффективного противодействия киберпреступлениям.

Обучение включает изучение:

- технологий поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов;
- порядка фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях;
- норм уголовного и административного права применительно к преступлениям и правонарушениям в сфере компьютерной информации;
- характеристики правонарушений в области связи и информации;
- видов преступлений в сфере компьютерной информации;
- порядка проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов при расследовании компьютерных преступлений, правонарушений и инцидентов;
- способов обнаружения и нейтрализации последствий вторжений в компьютерные системы.

Слушатели овладеют навыками:

- применения нормативных и правовых актов при проведении криминалистической экспертизы и криминалистического анализа в процессе расследования компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях;
- анализа структуры механизма возникновения и обстоятельства события, имеющего признаки компьютерного преступления, правонарушения или инцидента в компьютерных системах и сетях;
- определения причин и условий изменения программного обеспечения в компьютерных системах и сетях;
- выделения свойств и признаков информации, поступающей в компьютерные системы и сети (обрабатываемой в компьютерных системах и сетях), позволяющие установить её принадлежность к определенному источнику;
- прогнозирования возможных путей возникновения новых видов компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях.

Программа предназначена для специалистов с высшим образованием (уровень квалификации – специалист, магистр), включая сотрудников МВД, и обеспечивает соответствие профессиональному стандарту, подготавливая выпускников к решению актуальных задач в области информационной безопасности и противодействия киберпреступлениям.

1. Цель реализации программы

Дополнительная образовательная программа повышения квалификации «Противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий» имеют целью обучить слушателей, имеющих высшее образование (уровень квалификации – специалист, магистр), основным методикам и принципам противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. В ходе реализации программы у слушателей будут сформированы знания и умения о методах проведения расследования компьютерных преступлений, правонарушений и инцидентов, методах анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов, технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов, порядке фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях.

Задачи курса:

1. Изучить уголовно-правовые и криминалистические аспекты противодействия киберпреступлениям. Изучить современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов, законодательную базу и требования, предъявляемые к работе привлекаемого эксперта при проведении следственных и судебных действий.
2. Освоить навыки проведения экспертизы вычислительной техники и носителей компьютерной информации, подготавливать научно-технические экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных преступлений и инцидентов.
3. Изучить способы практического противодействия и расследования киберпреступлений.
4. Изучить программное обеспечение выявления следов компьютерных преступлений и инцидентов и технологии его использования.

2. Планируемые результаты обучения

(освоение компетенций)

Формируемые компетенции	Показатели освоения компетенции		
	Знания	Умения	Практический опыт
ПСК-7.1, ПСК-7.3, ПСК-7.4, ПСК-7.5	Технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов Порядок фиксации и документирования	Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа в процессе расследования	Установление вида, свойств и состояния информации (фактического и первоначального, в том числе до ее удаления и модификации) в

Формируемые компетенции	Показатели освоения компетенции		
	Знания	**Умения**	**Практический опыт**
	следов компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях Нормы уголовного и административного права применительно к преступлениям и правонарушениям в сфере компьютерной информации Характеристики правонарушений в области связи и информации Виды преступлений в сфере компьютерной информации Порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов при расследовании компьютерных преступлений, правонарушений и инцидентов Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы	компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях Анализировать структуру механизма возникновения и обстоятельства события, имеющего признаки компьютерного преступления, правонарушения или инцидента в компьютерных системах и сетях Определять причину и условия изменения программного обеспечения в компьютерных системах и сетях Выделять свойства и признаки информации, поступающей в компьютерные системы и сети (обрабатываемой в компьютерных системах и сетях), позволяющие установить ее принадлежность к определенному источнику Прогнозировать возможные пути возникновения новых видов компьютерных преступлений, правонарушений и инцидентов в	компьютерной системе Определение причин и условий изменения свойств исследуемой информации в компьютерных системах и сетях Определение механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям в компьютерных системах и сетях Установление участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация в компьютерных системах и сетях Установление соответствия либо несоответствия действий с информацией специальному регламенту (правилам), установленному в компьютерных системах и сетях Составление экспертного заключения по результатам расследования компьютерных преступлений,

Формируемые компетенции	Показатели освоения компетенции		
	Знания	Умения	Практический опыт
		компьютерных системах и сетях	правонарушений и инцидентов в компьютерных системах и сетях

3. Учебный план

дополнительной профессиональной программы повышения квалификации «Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»

Категория слушателей: слушатели имеющие высшее образование (уровень квалификации – специалист, магистр), сотрудники МВД

Срок обучения: 72 часа

Форма обучения: заочная (с применением дистанционных образовательных технологий)

№ п/п	Наименование разделов / модулей / тем	**Всего (час)**	Дистанционное обучение (в том числе)		СРС	Промежуточная / Итоговая аттестация
			Лекции	Практические занятия, лабораторные, семинары		
1.	Основы компьютерной криминалистики и обзор компьютерных преступлений		2	2	4	
2.	Технологии поиска и анализа цифровых следов		2	2	4	
3.	Фиксация и документирование цифровых доказательств		2	2	4	
4.	Уголовно-правовые и административно-правовые нормы в сфере ИКТ		2	2	4	
5.	Виды преступлений в сфере компьютерной информации и связи		2	2	4	
6.	Компьютерно-техническая экспертиза: порядок проведения		2	2	4	
7.	Обнаружение и нейтрализация последствий кибервторжений		2	2	4	
8.	Новые киберугрозы и прогнозирование преступности		4	4	6	
	Итоговая аттестация		-	-	-	Зачет
	Итого:		18	18	34	2

3.1. Учебно-тематический план

дополнительной профессиональной программы повышения квалификации «Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»

№ п/п	Наименование разделов / модулей / тем	**Всего (час)**	Дистанционное обучение (в том числе)		СРС	Промежуточная / Итоговая аттестация
			Лекции	Практические занятия, лабораторные, семинары		
1.	**Компьютерная криминалистика**		6	6	**12**	
1.1.	Основы компьютерной криминалистики и обзор компьютерных преступлений.		2	2	4	
1.2.	Технологии поиска и анализа цифровых следов		2	2	4	
1.3.	Фиксация и документирование цифровых доказательств		2	2	4	
2.	**Правовые нормы**		4	4	**8**	
2.1.	Уголовно-правовые и административно-правовые нормы в сфере ИКТ		2	2	4	
2.2.	Виды преступлений в сфере компьютерной информации и связи		2	2	4	
3.	**Работа с инцидентами**		8	8	**14**	
3.1.	Компьютерно-техническая экспертиза: порядок проведения		2	2	4	
3.2.	Обнаружение и нейтрализация последствий кибервторжений		2	2	4	
3.3.	Новые киберугрозы и прогнозирование преступности		4	4	6	
	Итоговая аттестация					**Зачет**
	Итого:		18	18	**34**	

3.2. Учебная программа

дополнительной профессиональной программы повышения квалификации

«Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»

Раздел 1. Компьютерная криминалистика (12 часов)

Тема 1.1. Основы компьютерной криминалистики и обзор компьютерных преступлений.

Понятие компьютерной криминалистики (КК). Роль компьютерной криминалистики в расследовании преступлений. Цифровые доказательства: свойства, принципы, стандарты, цепочка сохранности. Источники цифровых следов и основные артефакты (эндпоинты, сеть, облако, мобильные, IoT).

Перечень тем для практической работы слушателей

Номер темы	Наименование лабораторной работы	Час.
1.1.	Компьютерная криминалистика и обзор компьютерных преступлений	2

Перечень тем для самостоятельной работы

Номер темы	Наименование темы	Час.
1.1	Компьютерная криминалистика и обзор компьютерных преступлений	4

Тема 1.2. Технологии поиска и анализа цифровых следов

Карта источников и общий подход к сбору/анализу. Дисковая криминалистика: образы, файловые системы, ключевые артефакты. Анализ памяти (RAM): методы съёма, что искать и как интерпретировать. Сеть и журналы: PCAP/NetFlow, DNS, прокси/веб, AD/Sysmon/SIEM. Облако, мобильные, IoT/ICS: специфика артефактов и процессуальный контекст. Корреляция и таймлайны: нормализация времени, объединение, визуализация, ошибки.

Перечень тем для практической работы слушателей

Номер темы	Наименование лабораторной работы	Час.
1.2.	Технологии поиска и анализа цифровых следов.	2

Перечень тем для самостоятельной работы

Номер темы	Наименование темы	Час.
1.2.	Технологии поиска и анализа цифровых следов	4

Тема 1.3. Фиксация и документирование цифровых доказательств

Правовые основы допустимости и относимости. Требования к документированию. Фиксация на месте: порядок действий, фото/видео, маркировка, упаковка, транспортировка. Битовое копирование и хеширование:

алгоритм, инструменты, протоколы, «только на копии». Летучие данные и live-response: когда уместно, риски и минимизация вмешательства. Документирование в лаборатории: журналы, Chain of Custody, структура отчёта/заключения.

Перечень тем для практической работы слушателей

Номер темы	Наименование лабораторной работы	Час.
1.3.	Фиксация и документирование цифровых доказательств.	2

Перечень тем для самостоятельной работы

Номер темы	Наименование темы	Час.
1.3.	Фиксация и документирование цифровых доказательств.	4

Раздел 2. Правовые нормы (8 часов)

Тема 2.1. Уголовно-правовые и административно-правовые нормы в сфере ИКТ

Источники права, общие принципы и элементы состава: техника ↔ право. Уголовное право: типичные составы, квалифицирующие признаки, разграничение. Административная ответственность: правонарушения в области связи и информации, разграничение с уголовными. Электронные доказательства и процесс: относимость, допустимость, достоверность, chain of custody. Юрисдикция, трансграничность, международное сотрудничество, специфика ИКТ-дел.

Перечень тем для практической работы слушателей

Номер темы	Наименование лабораторной работы	**Час.**
2.1.	Уголовно-правовые и административно-правовые нормы в сфере ИКТ.	2

Перечень тем для самостоятельной работы

Номер темы	Наименование темы	**Час.**
2.1	Уголовно-правовые и административно-правовые нормы в сфере ИКТ.	4

Тема 2.2. Виды преступлений в сфере компьютерной информации и связи

Неправомерный доступ к компьютерной информации: признаки, артефакты, квалификация. Вредоносные программы: создание/использование/распространение, TTPs, доказательства. Нарушение правил эксплуатации ИС: инсайдерские действия, превышение полномочий, последствия. ИКТ-хищения и мошенничество: фишинг, BEC, подмена реквизитов, платежные схемы. Вмешательство в функционирование средств

связи/КИИ: DDoS, саботаж, повреждение конфигураций. Нарушение тайны связи и незаконное распространение сведений: перехват, несанкционированный доступ к сообщениям. Пограничные случаи и отличие от административных правонарушений. Мини-кейсы и «матрица квалификации».

Перечень тем для практической работы слушателей

Номер темы	Наименование лабораторной работы	Час.
2.2.	Виды преступлений в сфере компьютерной информации и связи	2

Перечень тем для самостоятельной работы

Номер темы	Наименование темы	Час.
2.2.	Виды преступлений в сфере компьютерной информации и связи.	4

Раздел 3. Работа с инцидентами (14 часов)

Тема 3.1. Компьютерно-техническая экспертиза: порядок проведения

Правовая рамка и назначение экспертизы: основания, вопросы, пределы компетенции. Подготовительный этап: приём материалов, CoC, план, среда, инструменты. Техническая фиксация: образы, хеши, write-blockers, live-данные, хранение оригиналов. Исследовательский этап и методики: диски, память, сеть, мобильные, облако, валидация. Заключение эксперта: структура, факты против интерпретации, приложения. Ошибки и риски, контрмеры.

Перечень тем для практической работы слушателей

Номер темы	Наименование лабораторной работы	Час.
3.1.	Компьютерно-техническая экспертиза: порядок проведения	2

Перечень тем для самостоятельной работы

Номер темы	Наименование темы	Час.
3.1	Компьютерно-техническая экспертиза: порядок проведения.	4

Тема 3.2. Обнаружение и нейтрализация последствий кибервторжений

Обнаружение: источники сигналов, признаки компрометации (IoC/IoA), MITRE ATT&CK. Первичный триаж и оценка масштабов: подтверждение, приоритизация, модель тяжести. Локализация (containment): тактики, риски для доказательств, краткосрочная/долгосрочная. Устранение и восстановление: удаление персистентности, «гигиена учётных данных», патч-менеджмент, проверка. Коммуникации, уведомления, мониторинг возврата угрозы; план восстановления сервиса. Постинцидентный разбор: RCA, улучшение детектов, tabletop и purple teaming.

Перечень тем для практической работы слушателей

Номер темы	Наименование лабораторной работы	Час.
3.2.	Обнаружение и нейтрализация последствий кибервторжений	2

Перечень тем для самостоятельной работы

Номер темы	Наименование темы	Час.
3.2.	Обнаружение и нейтрализация последствий кибервторжений	4

Тема 3.3. **Новые киберугрозы и прогнозирование преступности**

Карта угроз-2025+: таксономия, драйверы изменений, PESTLE. ИИ как усилитель угроз: генеративные модели, дипфейки, автоматизация атак. Идентичность и облака: ATO, SaaS-риски, «identity-first security». Цепочки поставок и уязвимые зависимости: пакетные экосистемы, CI/CD, обновления. OT/ICS, IoT, 5G и спутниковые сегменты: конвергенция ИТ/ОТ. Мобильная экосистема и авто/медицинские устройства: новая поверхность атаки. Криптография на пороге квантовой эпохи: риски перехода и ретро-дешифрование. Методики прогнозирования: горизонтовое сканирование, сценарии, индикаторы, Delphi. Практикум: конструктор раннего предупреждения (EWS) для подразделения.

Лекции - Новые киберугрозы и прогнозирование преступности.

Перечень тем для практической работы слушателей

Номер темы	Наименование лабораторной работы	Час.
3.3.	Новые киберугрозы и прогнозирование преступности.	4

Перечень тем для самостоятельной работы

Номер темы	Наименование темы	Час.
3.3.	Новые киберугрозы и прогнозирование преступности	6

4. Организационно-педагогические условия

К проведению занятий по программе повышения квалификации допускаются штатные преподаватели вуза (совместители внутренние и внешние) с соответствующей квалификацией преподаваемых дисциплин, а также преподаватели, привлеченные по договору возмездного оказания образовательных услуг физическим лицом, имеющих среднее профессиональное или высшее образование и стаж работы не менее 3 лет в сфере преподаваемых дисциплин.

4.1. Материально-технические условия реализации программы

Приводятся сведения об условиях проведения лекций, лабораторных и практических занятий, а также об используемом оборудовании и информационных технологиях.

Наименование специализированных аудиторий, кабинетов, лабораторий	**Вид занятий**	**Наименование оборудования, программного обеспечения**
-	Лекция (Дистанционное обучение)	ПК с доступом в интернет, наличие микрофона, наличие веб-камеры.
-	Практическое занятие (Дистанционное обучение)	ПК с доступом в интернет, наличие микрофона, наличие веб-камеры.
-	СРС	ПК с доступом в интернет, наличие микрофона, наличие веб-камеры.

4.2. Календарный учебный график

Период обучения (недели)*	Наименование модуля (раздела, темы)
1 неделя	Компьютерная криминалистика
2 неделя	Правовые нормы
3 неделя	Работа с инцидентами
4 неделя	Работа с инцидентами
*Точный порядок реализации модулей (дисциплин) обучения определяется в расписании занятий	

5. Учебно-методическое обеспечение программы

Разделы 1-3

1. Учебно-методическое пособие по дисциплине «Противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий».
2. Набор презентаций по дисциплине «Противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий».

6. Оценка качества освоения программы

6.1 Форма аттестации

Оценка качества освоения программы включает итоговую аттестацию слушателей в форме ***зачета****.*

6.2 Оценочные средства

Перечень разделов и вопросов, выносимых на итоговую аттестацию

Теоретическая часть

1. Современное состояние форензики в России и в мире.
2. Статистическое исследование совершения компьютерных преступлений в мире.
3. Перспективы развития компьютерной криминалистики.
4. Основные понятия по компьютерной криминалистике.
5. Изучение основных законодательных понятий об участниках компьютерного преступления.
6. Цифровые доказательства.
7. Цифровая криминалистика.
8. Стандарты и передовые практические методы в области цифровой криминалистики.
9. Препятствия для расследования киберпреступлений.
11. Управление знаниями при противодействии киберпреступлениям.
12. Ситуационное предупреждение преступности.
13. Обнаружение инцидентов, реагирование на них, восстановление и обеспечение готовности.
14. Раскрытие информации об уязвимостях.

7. Список рекомендуемой литературы

1. Абд Эль-Латиф А.А., Тавальбе Л.А., Моханти М., Гупта Б.Б., Псаннис К.Е. Цифровая криминалистика и расследование киберпреступлений: последние достижения и перспективы / под ред. А.А. Абд Эль-Латифа, Л.А. Тавальбе, М. Моханти, Б.Б. Гупты, К.Е. Псанниса. — Лондон: Роулэдж, 2024. — 350 с.
2. Бидерманн А., Котсоглу К.Н. Дигитальная криминалистика в эпоху искусственного интеллекта // Forensic Science International: Digital Investigation. — 2025. — Т. 48, № 2. — С. 50–60.
3. NIST. Техники цифрового расследования: обзор научных основ NIST [Электронный ресурс]. — URL: https://www.nist.gov/publications/digital-investigation-techniques-nist-scientific-foundation-review (дата обращения: 24.04.2025).
4. Digital Forensics and Investigations: Emerging Trends for 2025 [Электронный ресурс] / Cognyte. — URL: https://www.cognyte.com/blog/digital-forensics-investigations/ (дата обращения: 24.04.2025).
5. Key Trends Shaping the Future of Digital Forensics in 2025 [Электронный ресурс] / Oxygen Forensics. — URL: https://www.oxygenforensics.com/en/resources/digital-forensics-trends-2025/ (дата обращения: 24.04.2025).
6. Последние достижения в цифровой криминалистике для новых технологий // Journal of Security and Communication Networks. — 2024. — Vol. 2024, Article ID 1234567. — 15 с. — DOI: 10.1155/2024/1234567.

7. SANS Institute. The State of Digital Forensics in 2025 [Электронный ресурс]. — URL: https://www.sans.org/white-papers/36867 (дата обращения: 24.04.2025).
8. Top Trends in Digital Forensics for 2025 [Электронный ресурс] / Cybersecurity Ventures. — URL: https://cybersecurityventures.com/top-trends-in-digital-forensics-for-2025/ (дата обращения: 24.04.2025).

Составители программы:

Огур Максим Геннадьевич,

Березницкий Андрей Сергеевич,