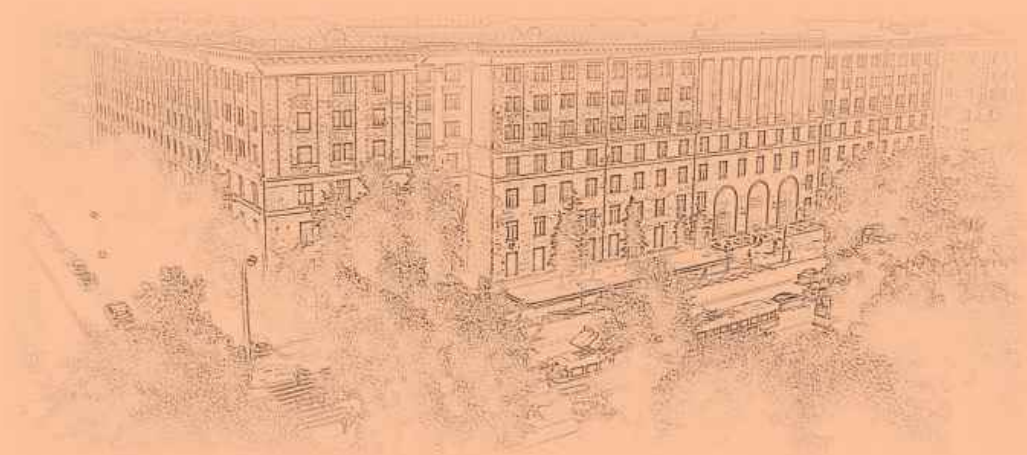


**АКАДЕМИЯ УПРАВЛЕНИЯ МВД РОССИИ**

Ю. Е. Салеева, Ю. В. Гаврилин

**КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ  
ГОСУДАРСТВЕННОЙ  
НАУЧНО-ТЕХНИЧЕСКОЙ ПОЛИТИКИ  
В СФЕРЕ КРИМИНАЛИСТИЧЕСКОГО  
ОБЕСПЕЧЕНИЯ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ  
И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ**

*Монография*



**Москва  
2025**

Академия управления МВД России

Ю. Е. Салеева, Ю. В. Гаврилин

**КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ  
ГОСУДАРСТВЕННОЙ  
НАУЧНО-ТЕХНИЧЕСКОЙ ПОЛИТИКИ  
В СФЕРЕ КРИМИНАЛИСТИЧЕСКОГО  
ОБЕСПЕЧЕНИЯ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ  
И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ**

*Монография*

Москва  
2025

УДК 343.98  
ББК 67.52  
С 16

*Одобрено редакционно-издательским советом  
Академии управления МВД России*

**Рецензенты:** *Суров О. А.*, кандидат юридических наук, доцент (Сибирский юридический институт МВД России); *Новикова Л. В.*, кандидат юридических наук, доцент (Рязанский филиал Московского университета МВД России имени В. Я. Кикотя).

С 16

**Салеева, Юлия Евгеньевна.**

Концептуальные основы государственной научно-технической политики в сфере криминалистического обеспечения выявления, раскрытия и расследования преступлений : монография / Ю. Е. Салеева, Ю. В. Гаврилин. – Москва : Академия управления МВД России, 2025. – 116 с.

ISBN 978-5-908091-14-5

В представленной монографии проведен анализ путей совершенствования методической и нормативной базы, обеспечивающей эффективное применение отдельных видов технико-криминалистических средств для решения экспертных и следственных задач, что подчеркивает высокую актуальность и прикладную ценность полученных результатов

Монография ориентирована на слушателей Академии управления МВД России, обучающихся по направлению подготовки 38.04.04 Государственное и муниципальное управление; по дисциплине «Организация противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»; по дополнительной профессиональной программе повышения квалификации начальников (заместителей начальников) подразделений по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, начальников территориальных органов МВД России на региональном уровне, сотрудников органов внутренних дел, состоящих в кадровом резерве на замещение указанных должностей; по программе подготовки научных и научно-педагогических кадров в адъюнктуре по научной специальности «5.1.4 Уголовно-правовые науки».

УДК 343.98  
ББК 67.52

ISBN 978-5-908091-14-5

© Салеева Ю. Е., Гаврилин Ю. В., 2025  
© Академия управления МВД России, 2025

## ОГЛАВЛЕНИЕ

<b>Введение</b> .....	5
<b>1. Предпосылки формирования, понятие и задачи научно-технической политики в сфере криминалистического обеспечения выявления, раскрытия и расследования преступлений</b> .....	8
<b>2. Предмет и структура научно-технической политики в сфере криминалистического обеспечения выявления, раскрытия и расследования преступлений</b> .....	36
<b>3. Основные направления научно-технической политики в сфере криминалистического обеспечения производства следственных действий и организации расследования</b> .....	59
<b>Заключение</b> .....	106
<b>Список использованных источников</b> .....	108

## СПИСОК СОКРАЩЕНИЙ

**БАС** – беспилотные авиационные системы

**ГК РФ** – Гражданский кодекс Российской Федерации

**ГНТП КО** – государственная научно-техническая политика в сфере криминалистического обеспечения выявления, раскрытия и расследования преступлений

**ДИТСиЗИ** – департамент информационных технологий, связи и защиты информации МВД России

**ИИ** – искусственный интеллект

**ИТТ** – информационно-телекоммуникационные технологии

**НИОКР** – научно-исследовательские и опытно-конструкторские работы

**НИР** – научно-исследовательские работы

**НТД** – научно-техническая деятельность

**ОКР** – опытно-конструкторские работы

**ОМП** – осмотр места происшествий

**ОРМ** – оперативно-розыскные мероприятия

**ПО** – программное обеспечение

**ТКС** – технико-криминалистические средства

**УК РФ** – Уголовный кодекс Российской Федерации

**УПК РФ** – Уголовно-процессуальный кодекс Российской Федерации

**ФКУ НПО «СТиС»** МВД России – Научно-производственное объединение “Специальная техника и связь”

**ЦВ** – цифровая валюта

**ЦИАДИС-МВД** – централизованная интегрированная автоматизированная дактилоскопическая информационная система МВД России

**ЦФА** – цифровые финансовые активы

**ЭКП** – экспертно-криминалистическое подразделение

## ВВЕДЕНИЕ

В условиях развития информационного общества большое значение приобретает научно-техническая политика, направленная на повышение эффективности правоохранительной деятельности, включая вопросы предупреждения, выявления, раскрытия и расследования преступлений. Представляя собой совокупность основополагающих идей, определяющих векторы научно-технического обеспечения вышеназванной деятельности, она призвана определить приоритетные направления разработки и внедрения перспективных технологий, включая технологии на основе искусственного интеллекта, биоинженерии, беспилотных авиационных систем и др.

В условиях сложной криминогенной обстановки, активизации деятельности организованных преступных формирований, приобретающей транснациональный характер, постоянного роста технического, научного и финансового потенциала преступной среды перед МВД России ставится задача выработки и реализации адекватных мер противодействия преступности, повышения эффективности правоохранительной деятельности.

Важным направлением совершенствования борьбы с преступностью является научно-техническое обеспечение деятельности подразделений органов внутренних дел, которые непосредственно реализуют возложенные на них полномочия в сфере уголовно-процессуальной, оперативно-розыскной и экспертно-криминалистической деятельности. В процессе реализации каждого из обозначенных направлений, в условиях развития научно-технического прогресса особое значение приобретает использование специальных знаний в области науки, техники, искусства или ремесла, осуществляемое в различных формах, совокупность которых образует криминалистическое обеспечение предупреждения, выявления, раскрытия и расследования преступлений.

Развитие технического оснащения органов предварительного следствия, дознания и экспертно-криминалистических подразделений направлено на реализацию целей и задач, определенных основными направлениями деятельности полиции в соответствии с Федеральным законом от 7 февраля 2011 г. № 3-ФЗ «О полиции». Среди иных наиболее значимых нормативно-правовых актов, регламентирующих криминалистическое обеспечение деятельности органов внутренних дел, следует отметить Уголовно-процессуальный кодекс Российской Федерации, Федеральные законы от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности», от 23 августа 1996 г. № 127-ФЗ «О науке и государ-

ственной научно-технической политике», а также ряд ведомственных актов МВД России и других органов, уполномоченных на осуществление экспертно-криминалистической деятельности.

Помимо вопросов совершенствования существующих и разработки новых технологий, используемых при производстве судебных экспертиз, актуальными остаются вопросы развития научно-технического обеспечения осмотра места происшествия, ресурсного и кадрового обеспечения, а также обеспечения достоверности результатов экспертно-криминалистической деятельности.

Несмотря на то, что вопросы повышения эффективности правоохранительной деятельности в сфере уголовного судопроизводства традиционно находятся в центре внимания научной общественности не одно десятилетие, они рассматриваются преимущественно фрагментарно, дискретно, поскольку направлены на отдельные (частные) вопросы выявления, раскрытия и расследования преступлений.

Сказанное обретает особую актуальность на фоне ставших уже очевидными тенденций цифровой трансформации современной преступности<sup>1</sup>. Ситуацию усугубляют складывающиеся геополитические процессы, прямым следствием которых является то, что обеспечение подготовки, совершения и сокрытия преступлений в отношении наших граждан и организаций является элементом государственной политики ряда недружественных стран. Эти тенденции сложились довольно давно и неоднократно являлись предметом анализа значительного числа научно-практических конференций, а также монографических и иных научных изданий.

Несмотря на это, сегодня органы расследования преступлений по-прежнему испытывают острый недостаток в научно обоснованных методических рекомендациях по противодействию этим новым вызовам, особенно в сферах противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий, незаконного оборота наркотиков, преступлений экстремистской направленности и террористического характера, а также при решении иных приоритетных вопросов.

В этих условиях особое значение приобретает криминалистическая наука, которая реализует специальные юридические познания, максимально приближенные к практике борьбы с преступностью.

---

<sup>1</sup> *Гаврилин Ю. В., Салеева Ю. Е.* О концепции государственной научной и научно-технической политики в области криминалистического обеспечения борьбы с преступностью // Труды Академии управления МВД России. 2023. № 4 (68). С. 80–87 ; *Гаврилин Ю. В.* О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практ. пособие. М., 2021. С. 6.

Прошло время, когда научные рекомендации строились исключительно на обобщении правоприменительной практики и выявлении передового опыта, когда наука шла вслед за практикой. Как представляется, сегодня задача науки должна состоять в том, чтобы она опережала практику, прогнозировала практические ситуации, выдавала действенные рекомендации, показывала верные направления разрешения практических, правовых, криминалистических и организационных вопросов.

Приходится констатировать, что современный этап развития криминалистических знаний характеризуется недостаточным уровнем вовлечения передовых цифровых технологий, систем обработки больших объемов данных, машинного обучения и искусственного интеллекта, нейротехнологий, систем распределенного реестра, технологий дополненной реальности, семантических технологий обработки естественного языка, распознавания речи, интеллектуальных систем поддержки принятия решений. Сказанное ставит под угрозу обеспечение национальной безопасности страны вследствие наметившегося технологического отставания органов правопорядка от криминальной среды, не имеющей ресурсных и организационных ограничений<sup>1</sup>.

Совокупность приведенных обстоятельств требует выработки единой государственной научно-технической политики в области криминалистического обеспечения выявления, раскрытия и расследования преступлений, поскольку в условиях отсутствия системы основных идей стратегического характера данная деятельность не может в полной мере удовлетворять потребности общества в защите от противоправных посягательств.

Использованные при подготовке монографии нормативно-правовые акты приведены в редакции, действовавшей на момент подготовки издания. Действительность ссылок на публикации в Интернет-изданиях, а также иные электронные ресурсы подтверждена на даты обращения к ним. Приведенный в монографии иллюстративный материал заимствован из открытых источников. В начале издания приведен список использованных сокращений.

---

<sup>1</sup> Гаверилин Ю. В., Салеева Ю. Е. Указ. соч. С. 80–87.

# **1. ПРЕДПОСЫЛКИ ФОРМИРОВАНИЯ, ПОНЯТИЕ И ЗАДАЧИ НАУЧНО-ТЕХНИЧЕСКОЙ ПОЛИТИКИ В СФЕРЕ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ**

Современный этап развития российского общества и государства характеризуется активной интеграцией цифровых технологий во все сферы жизнедеятельности, что открывает новые возможности для развития экономики, государственного управления, гуманитарной сферы, обеспечения общественной безопасности и национальной обороны страны.

Формирование информационного общества, отвечающего национальным интересам и способного обеспечить технологический суверенитет<sup>1</sup>, выступает в качестве приоритетного направления государственной политики, что в условиях санкционного давления со стороны недружественных стран приобретает особую актуальность.

Приоритеты государственной политики Российской Федерации в области развития информационного общества<sup>2</sup> определены: указами Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года», от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы», от 28 февраля 2024 г. № 145 «О Стратегии научно-технологического развития Российской Федерации», от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» и др.

Обеспечение национальных интересов при развитии информационного общества осуществляется путем:

- а) формирования информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений;
- б) развития информационной и коммуникационной инфраструктуры Российской Федерации;

---

<sup>1</sup> О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации от 15 мая 2017 г. № 20. Ст. 2901.

<sup>2</sup> Об утверждении государственной программы Российской Федерации «Информационное общество» : постановление Правительства Рос. Федерации от 15 апр. 2014 г. № 313 // Собр. законодательства Рос. Федерации от 5 мая 2014 г. № 18 (Ч. II). Ст. 2159.

в) создания и применения российских информационных и коммуникационных технологий, обеспечения их конкурентоспособности на международном уровне;

г) формирования новой технологической основы для развития экономики и социальной сферы;

д) обеспечения национальных интересов в области цифровой экономики<sup>1</sup>.

Таким образом, создание единого информационно-телекоммуникационного пространства является основой для социально-экономического роста государства. Оно предполагает развитие государственных цифровых сервисов, поддержку отечественных IT-разработок, направленных на интенсификацию процесса импортозамещения. Цифровые сервисы интенсивно внедряются в повседневную деятельность органов государственной власти Российской Федерации, обеспечивая коммуникацию с бизнесом и гражданами.

В целях решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере Правительством Российской Федерации сформирована национальная программа «Цифровая экономика Российской Федерации»<sup>2</sup>, которая призвана способствовать совершенствованию и развитию информационной инфраструктуры<sup>3</sup>; подготовке кадров для цифровой экономики<sup>4</sup>; обеспечению безопасности цифровых данных<sup>5</sup>

---

<sup>1</sup> Организация противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : учеб. : в 2-х ч. / Ю.В. Гаврилин, Т.В. Пинкевич, Н.Э. Мартыненко [и др.] ; под общ. ред. Ю.В. Гаврилина. М., 2024. Ч. 1. С. 21

<sup>2</sup> Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» [Электронный ресурс] : утв. президиумом Совета при Президенте Рос. Федерации по стратегическому развитию и национальным проектам : протокол от 4 июня 2019 г. № 7 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

<sup>3</sup> Паспорт федерального проекта «Информационная инфраструктура» [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

<sup>4</sup> Паспорт федерального проекта «Кадры для цифровой экономики» [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

<sup>5</sup> Паспорт федерального проекта «Информационная безопасность» [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

и технологической независимости государства; стимулированию исследований и ускорению технологического развития российских компаний; обеспечению их конкурентоспособности<sup>1</sup>; а также созданию соответствующей правовой основы<sup>2</sup>.

В числе приоритетов, закрепленных в Доктрине информационной безопасности Российской Федерации<sup>3</sup>, обозначена защита данных, борьба с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий, противодействие фактам дезинформации общества и др. О необходимости баланса между открытостью информации и защитой информационного суверенитета государства говорится и в юридическом сообществе<sup>4</sup>.

Несмотря на очевидные и неоспоримые преимущества, которые несет цифровизация общественных отношений и экономической жизни, обеспечивая цивилизационный прогресс, невозможно отрицать и сопряженные с ней глобальные угрозы и риски, которые требуют пристального внимания и адекватных мер противодействия.

К числу наиболее значимых с точки зрения общественной безопасности рисков следует отнести:

1. Широкие возможности манипуляции массовым сознанием путем распространения недостоверной социально-значимой информации в социальных сетях, информационных каналах и иных сервисах сети Интернет, которая приводит к подрыву доверия к государственным институтам и созданию социальной напряженности. Цифровая среда способствует формированию неких «эхо-пузырей», в рамках которых происходит искаженное восприятие информации, основанное на взглядах только одной социальной группы. Они представляют собой замкнутые коммуникативные простран-

---

<sup>1</sup> Паспорт федерального проекта «Цифровые технологии» [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

<sup>2</sup> Паспорт федерального проекта «Нормативное регулирование цифровой среды» [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

<sup>3</sup> Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Рос. Федерации от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации от 12 дек. 2016 г. № 50. Ст. 7074.

<sup>4</sup> *Меньшиков П.В.* Эволюция государственной информационной политики в России // Международные коммуникации : электрон. журн. 2017. № 4. URL: <https://intcom-mgimo.ru/2017/2017-04/state-information-policy-of-russia> (дата обращения: 15.02.2025).

ства, образованные посредством объединения людей со сходными взглядами. При этом субъекты с отличными взглядами намеренно не допускаются в эти пространства, они умышленно дискредитируются и выставляются в порочном свете<sup>1</sup>. Это усиливает социальную поляризацию и снижает способность к диалогу и компромиссу. Широкое распространение получил «кибер-буллинг»<sup>2</sup> и совершение преступлений сексуального характера в отношении несовершеннолетних. Формирование цифровой зависимости негативным образом сказывается как на физическом, так и на психическом здоровье человека.

2. Нарушение неприкосновенности частной жизни, персональных данных и иной конфиденциальной информации за счет эксплуатации программных уязвимостей в цифровых базах данных.

3. Изменение структуры рынка труда и риск безработицы вследствие сокращения рабочих мест для неквалифицированных трудовых ресурсов (водители, продавцы, кассиры и др.) за счет монополизации розничных рынков цифровыми платформами, внедрения беспилотных транспортных систем, дистанционных образовательных технологий и пр.

Особую категорию рисков, связанных с цифровой трансформацией общественных отношений и широкого внедрения цифровых технологий, представляет явление, получившее название «цифровая трансформация преступности». Она представляет собой комплекс изменений как в механизме совершения «традиционных» преступлений, возникших в «доцифровую» эпоху, так и в возникновении новых видов преступлений, непосредственно связанных с развитием ИТТ и использованием технических средств сбора, обработки, хранения компьютерной информации и ее передачи по линиям связи<sup>3</sup>.

Прежде всего, такая трансформация проявляется в росте числа преступлений, совершаемых с использованием ИТТ, что создает угрозу не только для отдельных граждан, но и для критически важной инфраструктуры государства. Так, в период с 2019 по 2024 гг. количество подобных преступлений увеличилось более чем на 260 %

---

<sup>1</sup> *Бажанов В. А.* Особенности познавательных механизмов в информационную эпоху: «эхо-пузыри» и «эхо-камеры» // *Философский журнал.* 2022. Т. 15. № 4. С. 152–164. URL: <https://pj.iphras.ru/article/view/8231/3847> (дата обращения: 14.03.2025).

<sup>2</sup> *Ищук Я. Г., Пипкевич Т. В., Смольянинов Е. С.* Цифровая криминология : учеб. пособие. М., 2021. 244 с.

<sup>3</sup> *Гаврилин Ю. В.* О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практ. пособие. М., 2021. С. 6.

(с 294 тыс. до 765,4 тыс.)<sup>1</sup>. Неуклонно растет число кибератак на экономическую инфраструктуру, банки, энергетические сети, транспортные коммуникации и пр. Так, по данным «Лаборатории Касперского», в первом квартале 2022 г. выявлено в 4 раза больше киберинцидентов, чем за аналогичный период 2021 г.<sup>2</sup> Сегодня можно констатировать, что кибератаки приобретают новые формы<sup>3</sup>, носящие характер информационных войн, ведущихся при активной государственной поддержке со стороны недружественных стран.

Для цифровой трансформации преступности как основного фактора, определяющего изменения в ее структуре и динамике, характерны следующие тенденции:

*Первая тенденция.* Появление дистанционных (бесконтактных) способов совершения преступлений, при которых взаимодействие субъектов преступления с потерпевшими, а также между собой осуществляется опосредованно, по каналам связи и через сети передачи данных, включая (но не ограничиваясь) социальные сети, электронную почту, сервисы мгновенных сообщений, онлайн-продаж и пр.

Показательно, что данная тенденция проявляется при анализе преступлений, связанных с незаконным сбытом наркотических средств и психотропных веществ, переместившихся на торговые площадки в теневые сегменты сети Интернет, заменив способ «из рук в руки». Электронные площадки принимают оплату в цифровой валюте, обеспечивая анонимность сделок. Информация о местонахождении тайника с приобретаемым веществом («закладки») передается покупателю дистанционно, исключая его непосредственный контакт с продавцом.

Именно этот способ, предоставляющий широкие возможности дистанционно и анонимно координировать незаконные операции, в том числе из-за рубежа, в настоящее время используется для анонимной продажи объектов, ограниченных в обороте или вовсе изъятых из гражданского оборота.

---

<sup>1</sup> Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // МВД РФ : сайт. URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 25.02.2025).

<sup>2</sup> «Лаборатория Касперского»: количество киберинцидентов в российских компаниях увеличилось в 4 раза // Kaspersky : сайт. URL: <https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-kolichestvo-kiberincidentov-v-rossijskih-kompaniyah-uvlechilos-v-4-raza> (дата обращения 11.05.2025).

<sup>3</sup> *Меньшиков П.В.* Эволюция государственной информационной политики в России // Международные коммуникации : электрон. журн. 2017. № 4 : сайт. URL: <https://intcom-mgimo.ru/2017/2017-04/state-information-policy-of-russia> (дата обращения: 15.02.2025).

Широкую распространенность получили преступления, совершаемые с использованием социальной инженерии, которая основана на эксплуатации психологических особенностей потерпевших, а не технических уязвимостей. Преступниками применяются информационно-психологические манипуляции и обман в целях получения конфиденциальной информации, побуждения к выполнению определенных действий, которые могут привести к утечке данных, финансовым потерям или иным негативным последствиям. Расширение спектра платежных систем, программных и технических средств побуждают к совершенствованию методов и приемов использования социальной инженерии.

Особенностью дистанционных способов совершения преступлений является возможность их совершения из любой точки мира, отдаленной от места наступления общественно опасных последствий; использование инфраструктуры Интернет-провайдеров, операторов мобильной связи, а также анонимных IP-адресов и сервисов анонимизации VPN/TOR. Несомненно, приведенные обстоятельства влияют на возможность и сроки получения информации, имеющей доказательственное значение.

*Вторая тенденция.* Использование цифровых технологий анонимизации личности в цифровом пространстве, которые обеспечивают сокрытие подлинных данных о личности пользователя сети Интернет и направлены на воспрепятствование установлению лица, совершающего те или иные действия в виртуальном пространстве, включая противоправные действия<sup>1</sup>.

К числу наиболее распространенных технологий анонимизации относится использование VPN-сервисов (Virtual Private Network), прокси-серверов и анонимных Интернет-браузеров. Широкая распространенность VPN-сервисов (платных и бесплатных) объясняется простотой их использования и широкой доступностью. Обозначенные сервисы шифруют интернет-трафик, подменяют IP-адрес пользователя, тем самым затрудняя его идентификацию.

Прокси-серверы выступают посредниками между веб-сайтом и пользователем и позволяют скрыть месторасположение и идентификатор устройства, позволяя получать доступ к информационным ресурсам, который ограничен в соответствии с требованиями российского законодательства (например, к торговым площадкам в даркнет и пр.).

---

<sup>1</sup> Гаверилин Ю.В. Указ. соч. С.12.

Использование анонимных платежных систем и цифровой валюты помогает преступникам скрывать финансовые следы от их противоправной деятельности.

Обеспечению анонимизации в цифровом пространстве служат также технологии обфускации и стеганографии, которые используются для сокрытия вредоносного кода или информации в других данных. Обфускация затрудняет анализ вредоносного программного обеспечения, а стеганография позволяет скрыть информацию, встраивая ее в изображения, видео и аудиофайлы.

Совершению преступлений с использованием ИТТ способствует развитый криминальный рынок услуг по продаже идентификационных модулей средств мобильной связи (сим-карт), зарегистрированных на «фирмы-однодневки», без проведения обязательной в таких случаях процедуры идентификации абонента. Многочисленные объявления о продаже таких модулей содержатся в неиндексируемом сегменте сети Интернет (Даркнет), где также осуществляется анонимная вербовка соучастников для осуществления наиболее рискованных элементов механизма преступления: размещение запрещенных веществ в тайниках («кладмены»), снятие наличных денежных средств в банкоматах («дроперы») и др.<sup>1</sup>

*Третья тенденция.* Использование цифровых валют и цифровых финансовых активов в криминальных взаиморасчетах. Сокрытие следов финансовых операций все чаще осуществляется посредством виртуальных валют, оборот которых не подконтролен для уполномоченных государственных органов, что препятствует реализации механизмов противодействия легализации (отмыванию) доходов, полученных противоправным путем.

Базовым нормативным правовым актом, определяющим понятие цифровых финансовых активов и цифровых валют является Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Федеральный закон № 259-ФЗ), которым регулируются отношения, возникающие при выпуске, учете и обращении цифровых финансовых активов, особенности деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператора обмена цифровых финансовых активов. В отношении цифровой валюты урегулированы лишь отдельные правоотношения, возникающие при ее обращении на территории Российской Федерации, и сформулировано ее понятие.

---

<sup>1</sup> Гаерлин Ю.В. Указ. соч. С.13.

Цифровыми финансовыми активами признаются цифровые права, включающие: денежные требования; возможность осуществлять права по эмиссионным ценным бумагам; права участия в капитале непубличного акционерного общества; право требовать передачи эмиссионных ценных бумаг, которое предусмотрено решением о выпуске ЦФА.

Указанным законом в гражданское законодательство внесено понятие «цифровые права» (ст. 141.1 ГК РФ), а также внесены изменения в ст. 128 ГК РФ, где наряду с вещами, безналичными денежными средствами, бездокументарными ценными бумагами и безналичными денежными средствами цифровые права отнесены к объектам гражданских прав<sup>1</sup>. Их статус определен в ГК РФ в качестве отдельных видов имущества и четко обозначено, что цифровые права не относятся к безналичным деньгам, а значит, не могут быть использованы при расчетах.

Выпуск, учет и обращение ЦФА возможны только путем добавления записей в информационную систему на основе распределенного реестра, таким образом, переход прав на них осуществляется исключительно в цифровой среде<sup>2</sup>. Иными словами, распоряжение ЦФА совершается только посредством цифровой транзакции, о чем должна быть сделана цифровая запись, зафиксированная в реестре. Права и обязанности сторон по отчуждению цифрового права определяются в смарт-контракте, под которым понимается договор в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределенном реестре цифровых записей в строго определенной им последовательности и при наступлении определенных им обстоятельств.

В соответствии с п. 3 ст. 1 Федерального закона № 259-ФЗ цифровая валюта – это совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за

---

<sup>1</sup> Гражданский кодекс Российской Федерации (ч. 1): Федер. закон от 30 нояб. 1994 г. № 51-ФЗ // Собр. законодательства Рос. Федерации. 1994. № 32. Ст. 3301.

<sup>2</sup> Мурадян С.В. Цифровые активы: правовое регулирование и оценка рисков // Журнал цифровых технологий и права. 2023. № 1. URL: <https://doi.org/10.21202/jdtl.2023.5> (дата обращения: 13.02.2025).

исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.

Основные признаки ЦВ:

1. Представляет собой цифровой код, который сам по себе не имеет имущественного содержания и может выступать лишь средством фиксации какого-либо имущественного права.

2. Обладание ЦВ подлежит фиксации в информационной системе.

3. Выполняет функцию средства платежа или инвестицией для нерезидентов Российской Федерации.

4. Не относится к денежной единице и иным валютным ценностям, в том числе иностранным, и в законодательных актах<sup>1</sup> квалифицируется как имущество.

В зависимости от наличия или отсутствия имущественного обеспечения ЦВ принято классифицировать как необеспеченные и обеспеченные (стейблкойны).

Необеспеченные цифровые валюты (например, биткойн как наиболее распространенная в мире цифровая валюта и альткойны<sup>2</sup>) характеризуются отсутствием обеспечения, не могут быть погашены у эмитента.

Стейблкойны обеспечены иными активами, и/или при их выпуске используется специальная система, ограничивающая волатильность их курса. Они могут применяться в целях платежей или представлять собой аналог фонда денежного рынка или иного имущественного комплекса.

Относительно анонимности цифровых валют следует отметить следующее. Анализ Федерального закона № 259-ФЗ позволяет сделать вывод об отсутствии указанного свойства у ЦВ в силу того, что оператор информационной системы обязан вносить в нее и хранить сведения о пользователе. Данное требование призвано воспрепятствовать использованию ЦВ в коррупционных преступлениях, финансировании терроризма и иной противоправной деятельности.

---

<sup>1</sup> Ст. 3 Федер. закона от 7 авг. 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Собр. законодательства Рос. Федерации. 2001 (ч. 1). Ст. 3418 ; ст. 8 Федер. закона от 25 дек. 2008 г. № 273-ФЗ «О противодействии коррупции» // Собр. законодательства Рос. Федерации. 2008. № 52 (ч. 1). Ст. 6228.

<sup>2</sup> Данное название получили все цифровые валюты, являющиеся альтернативой биткойну.

Говоря о технологической основе цифровых валют, следует отметить, что ее могут составлять не только технология блокчейн, но иные технологии, не сводящиеся к технологии распределенного реестра.

Организация выпуска и (или) выпуск, а также организация обращения ЦВ в Российской Федерации регулируются в соответствии с федеральными законами, которые на момент подготовки настоящей работы еще не приняты. В частности, в настоящее время осуществляется разработка соответствующих проектов федеральных законов, предусматривающих регулирование вопросов, связанных с выпуском и оборотом цифровых валют. Согласно ч. 8 ст. 14 Федерального закона от 31 июля 2020 г. № 259-ФЗ запрещается предложение неограниченному кругу лиц ЦВ, а также товаров (работ, услуг) в целях организации обращения и (или) обращения цифровой валюты.

Правительством в Госдуму внесен проект федерального закона о внесении изменений в ст. 104.1 УК РФ и УПК РФ, разработанный в целях снижения рисков, связанных с оборотом и использованием цифровой валюты в преступной деятельности.

Законопроектом цифровая валюта признается имуществом для целей УК РФ и УПК РФ.

Также предусматривается дополнение УПК РФ ст. 164.2, регламентирующей действия следователя (дознателя) в тех случаях, когда в ходе предварительного расследования выявляется цифровая валюта, подлежащая изъятию и признанию вещественным доказательством. Информация о наличии цифровой валюты или материальный носитель с такой валютой (кодами доступа к ней), в том числе полученной преступным путем, может обнаружиться, например, при производстве обыска. В целях недопущения сокрытия цифровой валюты следователь (дознатель) наделяется полномочиями по ее изъятию. При этом предусматривается возможность выбора следующих мер в зависимости от ситуации и конкретного вида цифровой валюты: 1) изъятие материального носителя, содержащего цифровую валюту или коды доступа к ней; 2) перевод ее на адрес-идентификатор, позволяющий обеспечить ее сохранность. Возможно осуществление обеих указанных мер. Изъятие осуществляется с участием специалиста, который определяет в том числе выбор необходимых мер для обеспечения сохранности с учетом особенностей цифровой валюты.

Так, при получении доступа к «горячему» или «холодному» кошельку, на котором хранится цифровая валюта, органами расследования с участием специалиста может быть осуществлено ее изъятие путем перевода на адрес-идентификатор, обеспечивающий ее сохранность. При отсутствии такого доступа возможно изъятие материального носителя, на котором хранятся цифровая валюта либо коды доступа к ней,

в целях недопущения операций с цифровой валютой со стороны владельца либо третьих лиц.

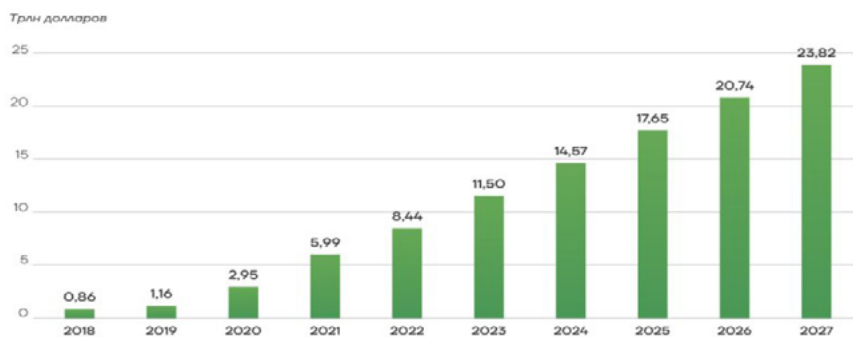
Указанные действия могут быть произведены в целях последующего наложения ареста на цифровую валюту. В отношении изъятой в ходе обыска цифровой валюты судом решается вопрос о ее аресте согласно проектируемым положениям ч. 71 и 72 ст. 115 УПК РФ.

Применение цифровых валют при осуществлении криминальных взаиморасчетов одновременно с маскировкой реальных IP-адресов существенно затрудняет использование в процессе доказывания информации о финансовых операциях и о лицах, их совершающих. Поэтому ЦВ становится основным средством расчетов в сфере наркобизнеса, а также оборота иных запрещенных объектов.

Одновременно следует отметить рост числа мошенничеств под видом продажи цифровой валюты. Кроме того, ЦВ употребляется при совершении должностных преступлений, выступая в качестве предмета взяточничества.

*Четвертая тенденция.* Рост масштабов межрегиональной и трансграничной преступности, использование при совершении преступлений сетевой инфраструктуры, расположенной за пределами Российской Федерации, что наиболее ярко проявляется при совершении дистанционных мошенничеств с использованием «социальной инженерии» (рис. 1).

Прогноз ежегодного ущерба от киберпреступлений в мире



Источник: Statista Market Insights

Рис. 1. По оценкам Statista's Market Insights, глобальный ущерб от киберпреступности в ближайшие четыре года удвоится 1.

<sup>1</sup> Институт изучения мировых рынков : сайт.: URL: <https://worldmarketstudies.ru/article/userb-ot-kiberprestuplenij-vyrastet-na-tret-za-sleduusie-4-goda/> (дата обращения: 12.02.2025).

Приведенные данные свидетельствуют о том, что в эпоху цифровизации трансграничная преступность достигает глобальных масштабов.

Масштабы трансграничной преступности в Российской Федерации иллюстрируются следующим примером: 8 апреля 2024 г. ФСБ задержала создателей узла связи в России для работы мошенников из Украины. За два года своей деятельности данная преступная группа похитила более 7 млрд руб. у российских граждан<sup>1</sup>.

Ранее нами подчеркивались широкие возможности свободного использования серверных мощностей и информационных ресурсов, расположенных в иностранных юрисдикциях, что существенным образом препятствует установлению лиц, совершивших преступления, и выяснению обстоятельств расследуемого события, подрывая базовый принцип неотвратимости наказания. Так, серверы почтовых ящиков @google.com, @yahoo.com, @aol.com и ряда других находятся на территории США. Там же располагаются хостинг-провайдеры крупнейших ресурсов, таких как Facebook, iCloud, Instagram, Skure и др. Даже при наличии на территории Российской Федерации официального представительства иностранной компании, располагающего сведениями о ее российских пользователях, возможности получения информации о них весьма ограничены<sup>2</sup>.

Помимо этого, геополитическая ситуация, складывающаяся в современном мире, также осложняет взаимодействие правоохранительных органов в борьбе с трансграничными преступлениями, в том числе совершаемыми с использованием информационно-телекоммуникационных технологий. Недружественные Российской Федерации страны превращаются фактически в преступные анклав, представляющие угрозу не только для нашего государства, но и всего мирового сообщества.

*Пятая тенденция.* Характеризуется предоставлением противоправных услуг, связанных с арендой ботнетов (сети устройств, инфицированных вредоносным ПО) в целях фишинговых и спам-рассылок, DDoS-атак, кражи данных, а также атак на корпорации с использованием криптолокеров (программ-шифровальщиков). Кроме того, происходит активизация преступной деятельности по коммерциализации услуг по несанкционированному доступу к конфиденциальной информации (частной переписке в мессендже-

---

<sup>1</sup> ФСБ задержала пять человек по делу об «украинских call-центрах» и 7 млрд // РБК : сайт. URL: <https://www.rbc.ru/politics/08/04/2024/661399849a7947d8c59e6e4> (дата обращения: 20.02.2025).

<sup>2</sup> Гаверилин Ю. В. Указ. соч. С. 13.

рах и социальных сетях), которая открыто рекламируется в отдельных информационных каналах популярного мессенджера Telegram, профессиональных форумах и иных информационных ресурсах. Ransomware стало глобальной угрозой, превратившись в сложную подпольную индустрию с Ransomware-as-a-Service (RaaS), сайтами утечки и брокерами первоначального доступа. В 2024 г. российская компания Group-IB выявила 39 рекламных объявлений RaaS и 44-процентный рост партнерских предложений. На выделенные сайты утечки было совершено 5 066 атак, что на 10 % больше, чем в 2023 г.<sup>1</sup>

*Шестая тенденция.* Использование технологий искусственного интеллекта в противоправной деятельности.

ИИ – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека<sup>2</sup>.

В противоправной деятельности получили распространение большие языковые модели (LLM), которые обладают способностью создавать тысячи версий вредоносного JavaScript-кода, который не распознается антивирусным программным обеспечением. Эксперты Palo Alto Networks Unit 42 показали, что ИИ генерирует более 10 000 вариантов, обходя защиту в 88 % случаев<sup>3</sup>.

К числу иных направлений противоправного использования ИИ-технологий относится массовая рассылка спам-писем и сообщений с адаптивностью к конкретным получателям, обход систем безопасности, поиск уязвимостей в системах безопасности, а также глобальное распространение Deepfakes (синтез изображения и голоса в противоправных целях).

*Приведенные тенденции цифровой трансформации преступности непосредственно сказываются на содержании уголовно-процессуальной, экспертно-криминалистической и оперативно-розыскной деятельности правоохранительных органов Российской Федерации.*

---

<sup>1</sup> Отчет о тенденциях преступности в сфере высоких технологий Group-IB в 2025 году // Group-IB : сайт. URL: <https://www.group-ib.com/ru/landing/high-tech-crime-trends-2025/> (дата обращения: 13.03.2025).

<sup>2</sup> пп. «а» п. 5 Национальной стратегии развития искусственного интеллекта на период до 2030 года : утв. Указом Президента Рос. Федерации от 10 окт. 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собр. законодательства Рос. Федерации. 2019. № 41. Ст. 5700.

<sup>3</sup> Никифорова А. ИИ научился создавать тысячи вирусов: их не видят антивирусы // Хайтек : сайт. URL: <https://hightech.fm/2024/12/26/ai-can-malware> (дата обращения: 13.03.2025).

В частности, на фоне снижения общего количества тяжких и особо тяжких насильственных и имущественных общеуголовных преступлений<sup>1</sup>, по которым чаще всего применяются экспертно-криминалистические методы и средства, и с учетом роста числа преступлений, совершенных с использованием ИТТ, а также противоправных деяний, связанных с незаконным оборотом наркотических средств, осуществленных дистанционным (бесконтактным) способом, на протяжении ряда лет фиксируется сокращение числа осмотров мест происшествий, проведенных с участием специалистов экспертно-криминалистических подразделений, а также снижение числа назначенных традиционных криминалистических экспертиз. Более подробное представление относительно обозначенной тенденции дает следующая таблица:

**Количество осмотров мест происшествий, экспертиз  
и оперативно-розыскных мероприятий с участием специалистов**

	2019	2020	2021	2022	2023	2024
<b>Количество ОМП</b>	988728	884395	817601	741646	560156	445966
<b>Назначено экспертиз</b>	1276114	1238461	1193572	1134894	991809	851873
<b>Участие в ОРМ</b>	2751533	2383421	2458142	2427577	2412937	2330592

На этом фоне возрастают потребности органов предварительного расследования в проведении исследований специальных видов. С 2015 г. в практику внедрены шесть новых видов экспертиз (лесотехническая, товароведческая, психофизиологическая, три вида строительно-технических). В 2021–2023 гг. суммарно рост числа специальных экспертиз и исследований составил 2,5 %. Наибольшая динамика отмечена по направлениям биологических (+35,3 %), взрывотехнических (+19,5 %), радиотехнических (+67,9 %) и товароведческих (+57,0 %) исследований. Как следствие, количество назначаемых экспертиз специальных видов в общем объеме зарегистрированных материалов практически сравнялось с числом выполненных традиционных экспертиз (с 2015 г. удельный вес назначаемых экспертных исследований специальных видов возрос с 33 до 48 %).

<sup>1</sup> Преступления, предусмотренные ст. 105–107, 111, 131, ч. 2, 3, 4 ст. 158 (связанные с проникновением в жилище, помещение либо иное хранилище, а также хищением транспортных средств), ч. 2 ст. 161, ч. 3 ст. 162, ст. 166 УК РФ.

В этих условиях региональные экспертно-криминалистические подразделения зачастую функционируют с превышением нормативной нагрузки<sup>1</sup> по наиболее востребованным направлениям. Так, в 2023 г. нагрузка по автотехническим экспертизам превышена в 1,3 раза; компьютерным – в 1,8 раза; лингвистическим – в 2,4 раза; исследованиям ДНК – в 4,3 раза; наркотических средств – в 1,9 раза.

Дальнейшее расширение круга лиц, подлежащих государственной геномной регистрации<sup>2</sup>, а также прогнозируемая работа по геномной регистрации мигрантов и военнослужащих потребуют дальнейшего укрепления и технического обеспечения соответствующих экспертных подразделений. При этом следует учитывать, что для выполнения таких работ в абсолютном большинстве случаев необходимо дорогостоящее аналитическое оборудование и соответствующие условия его размещения. Расходы на их обеспечение на районном уровне<sup>3</sup>, как правило, несоизмеримы с объемами экспертных исследований, выполняемых в интересах конкретного территориального органа МВД России.

При таких обстоятельствах для решения вопросов оптимального перераспределения нагрузки, консолидации материально-технических средств и кадровых ресурсов требуется комплексный подход к совершенствованию научно-технической политики в сфере криминалистического обеспечения<sup>4</sup>.

Заметим, что комплексное решение вопросов повышения эффективности деятельности в сфере уголовного судопроизводства возможно лишь в рамках реализации единой уголовной политики государства как совокупности правовых идей стратегического характера в области борьбы с преступностью<sup>5</sup>.

---

<sup>1</sup> Согласно приказу МВД России от 30 мая 2003 г. № 366 «О вопросах организации деятельности экспертно-криминалистических центров органов внутренних дел».

<sup>2</sup> В соответствии с Федер. законом от 3 дек. 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации».

<sup>3</sup> Затраты на подготовку лабораторных помещений, приобретение дорогостоящего аналитического оборудования, закупку расходных материалов, проведение техобслуживания, метрологических поверок, обучение сотрудников и т. п.

<sup>4</sup> *Гаврилин Ю. В., Салеева Ю. Е.* О концепции государственной научной и научно-технической политики в области криминалистического обеспечения борьбы с преступностью // Труды Академии управления МВД России. 2023. № 4 (68). С. 80–87; *Гаврилин Ю. В., Салеева Ю. Е.* Развитие учения о криминалистической регистрации в условиях цифровой трансформации преступности // Труды Академии управления МВД России. 2023. № 2 (66). С. 99–105.

<sup>5</sup> Уголовная политика Российской Федерации : учеб. : в 2-х ч. / под ред. Л. И. Беляевой. М., 2018. Ч. 1. С. 32–34.

К числу основных элементов уголовной политики, как правило, относят профилактическую политику; уголовно-правовую политику; уголовно-процессуальную политику; уголовно-исполнительную политику. В научной литературе представлено обоснованное мнение относительно существования оперативно-розыскной политики, а также научно-технической политики в сфере криминалистического обеспечения выявления, раскрытия и расследования преступлений (криминалистической политики)<sup>1</sup>. При этом надо заметить, что термин «криминалистическая политика» до настоящего времени еще в полной мере не прижился в языке криминалистики.

Вместе с тем в Российской Федерации сформирована нормативно-правовая база государственной научно-технической политики, основу которой составляет Федеральный закон от 23 августа 1996 г. № 127-ФЗ «О науке и государственной научно-технической политике». Последняя представляет собой часть социально-экономической политики, выражающая отношение государства к научной и научно-технической деятельности, определяющая цели, направления и формы деятельности государственных органов в данной области в целях развития и эффективного использования научно-технического потенциала, увеличения его вклада в развитие экономики, повышения эффективности и конкурентоспособности производства, укрепления обороноспособности, интеграции науки и образования<sup>2</sup>.

Приведенные нормативно-правовые акты формируют основания для разработки государственной научно-технической политики в сфере криминалистического обеспечения выявления, раскрытия и расследования преступлений. Она призвана определять векторы развития криминалистического обеспечения, задавать его целевые ориентиры, предоставлять необходимые ресурсы и кадры.

---

<sup>1</sup> *Гаврилин, Ю. В.* О концепции государственной научно-технической политики в области криминалистического обеспечения уголовно-процессуальной деятельности // Криминалистика в международном измерении : материалы Всеросс. науч.-практ. конф. с междунар. участием. Москва, 21 апреля 2023 г. С. 92–97 ; *Гаврилин Ю. В.* О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности (криминалистической политики) // Труды Академии управления МВД России. 2022. № 2 (62). С. 96–102 ; *Гаврилин Ю. В., Салеева Ю. Е.* О концепции государственной научной и научно-технической политики в области криминалистического обеспечения борьбы с преступностью // Труды Академии управления МВД России. 2023. № 4 (68). С. 80–87.

<sup>2</sup> О науке и государственной научно-технической политике : Федер. закон от 23 авг. 1996 г. № 127-ФЗ. Ст. 2, 11 // Доступ из СПС «КонсультантПлюс» (дата обращения: 11.02.2025).

Для формирования ГНТП КО важно учитывать следующие факторы<sup>1</sup>:

1. Криминалистическое обеспечение выявления, раскрытия и расследования преступлений нуждается в научном обосновании на основе совокупности идей стратегического характера, направленных на обеспечение допустимости доказательств, научной обоснованности используемых при их получении методов и средств, обеспечение рационального использования ресурсов, реализация которых возможна в рамках единой уголовной политики государства.

2. Эффективность криминалистического обеспечения достигается целенаправленной деятельностью уполномоченных государственных органов и иных организаций, направленной на создание надлежащей ресурсной базы, развитие кадрового потенциала и совершенствование методических основ борьбы с преступностью.

3. Решение задачи обеспечения безопасности личности, общества и государства от противоправных посягательств носит комплексный характер и наряду с материально-правовыми и процессуальными средствами достигается за счет использования научно-технических методов и средств и иных достижений криминалистической науки.

С учетом того, что ГНТП КО является направлением уголовной политики, ей присущи такие характерные черты, как публично-правовой и государственно-властный характер, реализация в сфере уголовно-правовых и уголовно-процессуальных правоотношений, а также высокая общественная значимость и социальная ценность ее результатов.

Основываясь на базовом определении уголовной политики, приведенном выше, с учетом единства целеполагания и особенностей предмета, методов и средств ГНТП КО предлагаем понимать под ней *выражение отношения государства к деятельности по предупреждению, выявлению, раскрытию и расследованию преступлений, определяющее направления развития научно-технических, тактических и организационно-управленческих средств решения задач уголовного судопроизводства.*

**Значение** ГНТП КО состоит в том, что она определяет основные направления развития методов и средств криминалистического обеспечения предупреждения, выявления, раскрытия и расследова-

---

<sup>1</sup> *Гаврилин Ю. В.* О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности (криминалистической политики) // Труды Академии управления МВД России. 2022. № 2 (62). С. 96–102.

ния преступлений, призвана повышать эффективность правоохранительной деятельности, направлена на создание условий для применения на практике криминалистических рекомендаций<sup>1</sup>.

В целом, ГНТП КО как особое направление уголовной политики характеризуется комплексностью и системностью, которые проявляются в том, что образующие ее правовые, ресурсные, научно-технические и организационно-тактические компоненты взаимно влияют друг на друга и в своей совокупности обеспечивают достижение единой цели, направленной на повышение эффективности предупреждения, выявления, раскрытия и расследования преступлений.

**Исходя из приведенного выше назначения ГНТП КО, к числу ее задач следует отнести<sup>2</sup>:**

– обеспечение достоверности результатов применения криминалистических методов и средств, включая научную обоснованность методического обеспечения судебно-экспертных исследований, его соответствие современному уровню развития науки и техники, точность проводимых измерений, неизменность получаемых на его основе результатов, а также проведение научной экспертизы и валидации результатов научно-исследовательской деятельности в области криминалистики и судебной экспертологии;

– повышение уровня компетентности субъектов применения криминалистических методов и средств, совершенствование подготовки кадров в области криминалистики и судебной экспертологии;

– разработка новых и совершенствование существующих методов обнаружения, фиксации, изъятия и исследования следов преступления и вещественных доказательств с учетом современных вызовов, включая совершенствование механизма внедрения в практику передового опыта, разработку критериев оценки эффективности его применения, обеспечение грантовой поддержки научных исследований по приоритетным направлениям и импортозамещение производства криминалистической техники, в том числе лабораторного оборудования и расходных материалов.

---

<sup>1</sup> *Гаврилин Ю. В., Салеева Ю. Е.* О концепции государственной научной и научно-технической политики в области криминалистического обеспечения борьбы с преступностью // Труды Академии управления МВД России. 2023. № 4 (68). С. 80–87; *Гаврилин Ю. В.* О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практ. пособие. М., 2021. 71 с.

<sup>2</sup> *Гаврилин Ю. В.* О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности (криминалистической политики) // Труды Академии управления МВД России. 2022. № 2 (62). С. 96–102.

С учетом приведенных задач **система** ГНТП КО включает в себя научно-технический, организационно-управленческий и кадровый компоненты, содержание которых более подробно будет рассмотрено во втором параграфе настоящей работы<sup>1</sup>.

**Субъектами** ГНТП КО являются государственные органы и должностные лица, образовательные организации, коммерческие и некоммерческие организации негосударственного сектора экономики, а также индивидуальные предприниматели<sup>2</sup>.

Категорию государственных органов и должностных лиц целесообразно дифференцировать на субъектов выработки и субъектов реализации НТП КО. К числу первых относятся:

– государственные органы и должностные лица общей компетенции (Президент Российской Федерации, Совет Федерации, Государственная Дума Российской Федерации, Правительство Российской Федерации, высшие должностные лица субъектов Российской Федерации и высшие исполнительные органы государственной власти субъектов Российской Федерации);

– государственные органы специальной компетенции в сфере правоохранительной деятельности (МВД России, Следственный комитет Российской Федерации, ФСБ России, МЧС России [в части государственного противопожарного надзора], Федеральная служба войск национальной гвардии [в части участия в обеспечении общественного порядка и общественной безопасности, борьбе с терроризмом и экстремизмом], Минобороны России [в части обеспечения укрепления правопорядка и воинской дисциплины в Вооруженных Силах, участия в обеспечении законности в Вооруженных Силах, а также осуществления в пределах своей компетенции противодействия преступности], государственные органы субъектов Российской Федерации, уполномоченные на взаимодействие с территориальными органами федеральных органов исполнительной власти в правоохранительной сфере);

– государственные органы в сфере управления экономикой, финансами и производственной сферой (Министерство финансов Российской Федерации, Министерство экономического развития Российской Федерации, Министерство промышленности

---

<sup>1</sup> Там же. С. 96–102.

<sup>2</sup> *Гаврилин Ю. В., Салеева Ю. Е.* О концепции государственной научной и научно-технической политики в области криминалистического обеспечения борьбы с преступностью // Труды Академии управления МВД России. 2023. № 4 (68). С. 80–87; *Гаврилин Ю. В.* О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практ. пособие. М, 2021. 71 с.

и торговли Российской Федерации, финансовые органы субъектов Российской Федерации);

– государственные органы, осуществляющие контрольно-надзорную деятельность (Счетная палата Российской Федерации, контрольно-счетные органы субъектов Российской Федерации, контрольно-ревизионные подразделения государственных органов специальной компетенции в сфере правоохранительной деятельности).

К числу субъектов реализации ГНТП КО относятся:

– участники судопроизводства со стороны обвинения (руководители следственных органов, следователи, начальники органов дознания, руководители подразделений дознания, дознаватели, органы и должностные лица, обладающие административно-юрисдикционными полномочиями);

– иные участники уголовного судопроизводства (эксперты, специалисты, руководители государственных судебно-экспертных учреждений);

– организации (независимо от организационно-правовых форм и ведомственной принадлежности) и индивидуальные предприниматели – разработчики, производители и поставщики научно-технических средств по заказам на поставки товаров, выполнение работ и оказание услуг для государственных нужд в сфере обеспечения правопорядка и общественной безопасности, защиты от противоправных посягательств;

– образовательные и научные организации, осуществляющие выполнение научно-исследовательских и опытно-конструкторских работ, а также подготовку кадров в рассматриваемой области.

**Правовую основу** реализации ГНТП КО составляют положения Конституции Российской Федерации, Уголовно-процессуального кодекса Российской Федерации, Федеральных законов от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», от 7 февраля 2011 г. № 3-ФЗ «О полиции», а также ряда ведомственных актов МВД России и иных государственных органов.

К числу конституционных положений, имеющих ключевое значение для ГНТП КО, относятся ст. 2, 19, 21–25, 27, 46–53, определяющие основы конституционно-правового статуса человека и гражданина. В основе этого статуса находится признание человека, его прав и свобод высшей ценностью, провозглашение обязанностью государства признание, соблюдение и защиту прав и свобод человека и гражданина. Кроме того, это принципы равенства всех перед законом и судом; недопустимости пыток, насилия, другого жестокого или унижающего человеческое достоинство обращения; свободы

и личной неприкосновенности; неприкосновенности частной жизни; защиты личной и семейной тайны, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; неприкосновенности жилища; свободы передвижения; судебной защиты прав и свобод; презумпции невиновности; недопустимости доказательств, полученных с нарушением федерального закона; защиты прав потерпевших и др.

Уголовно-процессуальная регламентация порядка применения криминалистической техники на досудебных стадиях уголовного судопроизводства включает в себя:

ч. 2 ст. 82 УПК РФ, согласно которой вещественные доказательства в виде предметов, которые в силу громоздкости или иных причин не могут храниться при уголовном деле, фотографируются или снимаются на видео- или кинолентку;

ч. 6 ст. 164 УПК РФ, устанавливающую, что при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступления и вещественных доказательств. Перед началом следственного действия следователь предупреждает лиц, участвующих в следственном действии, о применении технических средств;

ч. 3 ст. 164.1 УПК РФ, согласно которой следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронных носителях. В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты.

В соответствии с ч. 5 ст. 166 УПК РФ в протоколе должны быть указаны также технические средства, примененные при производстве следственного действия, условия и порядок их использования, объекты, к которым эти средства были применены, и полученные результаты. В протоколе должно быть отмечено, что лица, участвующие в следственном действии, были заранее предупреждены о применении технических средств.

Из содержания ч. 1.1. ст. 170 УПК РФ следует, что если при производстве следственного действия понятые не участвуют, то применение технических средств фиксации хода и результатов следственного действия является обязательным. Если в ходе следственного действия применение технических средств невозможно, то следователь делает в протоколе соответствующую запись.

Согласно ч. 3 указанной статьи в труднодоступной местности, при отсутствии надлежащих средств сообщения, а также в случаях,

если производство следственного действия связано с опасностью для жизни и здоровья людей, следственные действия могут производиться без участия понятых, о чем в протоколе следственного действия делается соответствующая запись. При этом применяются технические средства фиксации его хода и результатов. Если их применение невозможно, то следователь делает в протоколе соответствующую запись.

В соответствии с требованиями ч. 2 ст. 178 УПК РФ непознанные трупы подлежат фотографированию, дактилоскопированию и обязательной государственной геномной регистрации.

Часть 5 ст. 179 УПК РФ устанавливает, что если освидетельствование лица сопровождается его обнажением, то фотографирование, видеозапись и киносъемка проводятся с его согласия.

Наконец, согласно ч. 3 ст. 180 УПК РФ в протоколах должно быть указано, в какое время, при какой погоде и каком освещении производились осмотр или освидетельствование, какие технические средства были применены и какие получены результаты, какие предметы изъяты и опечатаны.

Правовые основы экспертно-криминалистической и судебно-экспертной деятельности заложены в ст. 57, 58 УПК РФ, закрепляющих правовой статус эксперта и специалиста, ст. 80 УПК РФ, относящей к числу доказательств заключение и показания эксперта и специалиста, ч. 1 ст. 144 УПК РФ, согласно которой при проверке сообщения о преступлении дознаватель, орган дознания, следователь, руководитель следственного органа вправе назначать судебную экспертизу, принимать участие в ее производстве и получать заключение эксперта в разумный срок; ст. 195–207 УПК РФ, регламентирующих порядок назначения и производства судебной экспертизы.

Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» определяет ее задачи и принципы, регламентирует обязанности и права эксперта и руководителя государственного судебно-экспертного учреждения, а также особенности производства судебной экспертизы в данном учреждении.

Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» устанавливает, что она в своей деятельности обязана использовать достижения науки и техники, информационные системы, технические средства (ст. 11).

Регламентация порядка осуществления экспертно-криминалистической деятельности в системе Министерства внутренних дел Российской Федерации обеспечивается приказами МВД России

от 11 января 2009 г. № 7 «Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России»; от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации»; от 10 февраля 2006 г. № 70 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации»; от 28 декабря 2018 г. № 896 «Вопросы материально-технического обеспечения деятельности экспертно-криминалистических подразделений системы МВД России»; от 29 декабря 2012 г. № 1157 «Об утверждении норм положенности специальной техники для отдельных подразделений центрального аппарата МВД России и средств связи, вычислительной, электронной организационной и специальной техники для территориальных органов МВД России».

Ведомственными правовыми актами Следственного комитета Российской Федерации<sup>1</sup>, Министерства юстиции Российской Федерации<sup>2</sup>, МЧС России<sup>3</sup>, Минздрава России<sup>4</sup> регламентирована экспертная деятельность в системе данных государственных органов.

**Механизм реализации ГНТП КО в системе МВД России.** Использование в своей деятельности достижений науки и техники, включая информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру, является одновременно правом и обязанностью органов внутренних дел. В ст. 11 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» закреплена ее обязанность по применению электрон-

---

<sup>1</sup> Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации» на право самостоятельного производства судебных экспертиз : приказ Следственного комитета Рос. Федерации от 24 июля 2020 г. № 77 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

<sup>2</sup> Об утверждении Инструкции по организации производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Министерства юстиции Российской Федерации : приказ Минюста России от 28 дек. 2023 г. № 404 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

<sup>3</sup> Об утверждении Инструкции по организации и производству судебных экспертиз в судебно-экспертных учреждениях и экспертных подразделениях федеральной противопожарной службы : приказ МЧС России от 19 авг. 2015 г. № 640 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

<sup>4</sup> Об утверждении Порядка проведения судебно-медицинской экспертизы : приказ Минздрава России от 25 сент. 2023 г. № 491н // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025) ; Об утверждении Порядка проведения судебно-психиатрической экспертизы : приказ Минздрава России от 12 янв. 2017 г. № 3н // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

ных форм приема и регистрации документов, уведомления о ходе предоставления государственных услуг, взаимодействия с другими правоохранительными органами, государственными и муниципальными органами, общественными объединениями и организациями. Кроме того, полиция использует технические средства, включая аппаратуру для аудио-, фото- и видеофиксации, при документировании обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе в общественных местах, а также для фиксации действий сотрудников полиции, выполняющих возложенные на них обязанности.

Приведенная норма возлагает на МВД России обязанность по обеспечению возможности использования полицией информационно-телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных<sup>1</sup>.

В соответствии с п/п 92, 93 Положения о Министерстве внутренних дел Российской Федерации<sup>2</sup> оно обеспечивает внедрение в деятельность органов внутренних дел достижений науки, техники и положительного опыта, а также развитие систем связи и автоматизированного управления в системе МВД России; осуществляет информационно-правовое обеспечение деятельности органов внутренних дел, в том числе ведение баз данных правовой информации в сфере внутренних дел.

Согласно пп. 14 п. 14 Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации<sup>3</sup> последний в целях осуществления своих полномочий имеет право использовать достижения в области науки и техники, современные технологии и информационные системы. Аналогичные полномочия отражены в пп. 8 п. 11 Типового положения о территориальном органе Министерства внутренних дел Российской Федерации на районном уровне<sup>4</sup>.

Использование новых технологий в деятельности органов внутренних дел по выявлению, раскрытию и расследованию преступлений должно строиться на комплексе принципов, обеспечивающих защиту гарантированных Конституцией и действующим законо-

---

<sup>1</sup> Комментарий к Федеральному закону «О полиции» (постатейный) / Ю.Е. Аврутин [и др.]. М., 2015. 551 с.

<sup>2</sup> Утв. Указом Президента Российской Федерации от 21 дек. 2016 г. № 699.

<sup>3</sup> Утв. Указом Президента Российской Федерации от 21 дек. 2016 г. № 699.

<sup>4</sup> Утв. приказом МВД России от 5 июня 2017 г. № 355.

дательством прав и законных интересов граждан и организаций, а именно<sup>1</sup>:

– недопустимость чрезмерного вмешательства со стороны государственных органов в частную жизнь;

– достоверность получаемых с использованием технологий ИИ доказательств;

– баланс между частными и публичными интересами, состоящими в защите от противоправных посягательств на охраняемые законом общественные отношения;

– доверие общества к правоохранительной системе в целом и органам внутренних дел в частности;

– законность, состоящая в надлежащей правовой регламентации оснований и порядка использования интеллектуальных средств поиска и изъятия доказательственной информации в цифровом пространстве;

– недопустимость произвольного ограничения прав и законных интересов юридических и физических лиц, а также установления ответственности за нарушение соответствующих правовых предписаний;

– подконтрольность, состоящая в том, что использование интеллектуальных средств, направленных на предупреждение, выявление, раскрытие и расследование преступлений, должно носить управляемый характер; действия должностных лиц, получающих результаты использования интеллектуальных средств, должны быть подотчетны и прозрачны для контрольно-надзорных органов;

– достоверность, состоящая в том, что результаты применения интеллектуальных средств и систем должны быть объяснимыми и понятными для их потребителей, включая источник происхождения исходных данных и алгоритмы их обработки;

– конфиденциальность, обеспечивающая возможность использования результатов применения интеллектуальных систем только уполномоченными лицами, а также защиту полученных сведений от неправомерного доступа к ним;

– технологическое опережение, направленное на недопустимость отставания правоохранительных органов от современного уровня развития информационно-телекоммуникационных технологий и искусственного интеллекта, осуществление постоянного мониторинга технологических достижений и оценки рисков их про-

---

<sup>1</sup> *Гаврилин Ю.В.* Цифровая трансформация уголовно-процессуальной деятельности в контексте государственной научно-технической политики // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности : сб. науч. статей по материалам междунар. науч.-практ. конф. Москва, 26 мая 2023 г. М., 2023. Ч. 2. С. 40–46.

тивоправного использования с целью выработки научно обоснованных рекомендаций по выявлению, раскрытию и расследованию преступлений, совершенных с их использованием.

Научная и научно-техническая деятельность в системе МВД России осуществляется в соответствии с приказом МВД России от 28 апреля 2023 г. № 260 «Об организации научной и научно-технической деятельности в системе МВД России», которым определены ее цели, задачи и принципы, представлен понятийный аппарат, а также утверждено Положение об организации научно-технической деятельности в системе Министерства внутренних дел Российской Федерации.

Участниками научно технической деятельности в системе МВД России являются<sup>1</sup>: научно-технический совет МВД России, научно-практические секции подразделений МВД России, главный конструктор ИСОД МВД России, государственные заказчики НИОКР (ФКУ НПО «СТиС» МВД России, подразделения, учреждения, организации, определенные в соответствии с приказом МВД России), заказывающие подразделения (подразделения центрального аппарата МВД России; ФКУ «ГИАЦ МВД России»; ЭКЦ МВД России, ФКУ «ЦКО МВД России»; территориальные органы МВД России на окружном, межрегиональном и региональном уровне)<sup>2</sup>; исполнители (сторонние организации, подразделения МВД России, авторские коллективы или отдельные сотрудники [работники] МВД России)<sup>3</sup>.

Основные этапы разработки научно-технической продукции включают в себя:

- выявление подразделением МВД России проблемы, требующей научно-технического разрешения, разработки нового, модернизации или совершенствования существующего изделия. При этом заказчик научно-технической продукции<sup>4</sup> осуществляет выявление и анализ проблемы, рассматривает проблему на заседании своей научно-практической секции, формирует заявку на выполнение научно-исследовательских и/или опытно-конструкторских работ<sup>5</sup>;
- подготовка заказывающим подразделением заявки на выполнение НИР или ОКР;
- организация планирования НТД;

---

<sup>1</sup> п. 2 Положения о НТД.

<sup>2</sup> пп. 2.5 Положения о НТД.

<sup>3</sup> пп. 2.6 Положения о НТД.

<sup>4</sup> п. 6 Положения о НТД.

<sup>5</sup> Приложение № 2 к Положению о НТД.

- подготовка, согласование и утверждение технического задания на НИР или ОКР;
- проведение конкурсных процедур на размещение заказа на выполнение НИОКР;
- организация сопровождения работ, включая создание рабочих группы с участием представителей заказывающего подразделения и головного исполнителя; формирование плана работ; осуществление контроля выполнения работ исполнителем НИР или ОКР в соответствии с контрактом; проведение экспертизы материалов по результатам этапов; создание комиссии по приемке НИР или ОКР; испытания и приемка результатов НИР или ОКР.

По завершении работ и приемки результатов производится:

- передача созданных результатов (нематериальных активов и основных фондов) заказывающему подразделению;
- регистрация и учет результатов интеллектуальной деятельности;
- организация использования научно-технической продукции, созданной в результате выполнения НИР или ОКР, в оперативно-служебной деятельности подразделений МВД России (внедрение).

Ввод в эксплуатацию результатов НИР и ОКР, а также их принятие на вооружение (снабжение) обеспечивается в соответствии с ведомственными нормативными правовыми актами. ФКУ НПО «СТиС» МВД России осуществляет разработку нормативного (нормативного правового) акта о принятии научно-технической продукции на вооружение и снабжение органов внутренних дел Российской Федерации. Координацию деятельности по внедрению научно-технической продукции в системе МВД России осуществляет ФКУ НПО «СТиС» МВД России<sup>1</sup>.

В целях активного развития, рационального и эффективного использования научно-технического потенциала криминалистического обеспечения, увеличения вклада науки и техники в развитие криминалистической деятельности, повышения эффективности и конкурентоспособности криминалистической техники, защиты информационных ресурсов, укрепления безопасности личности, общества и государства, интеграции науки и образования в криминалистической сфере, а также достижения иных целей ГНТП КО перспективными направлениями являются: разработка и принятие технического регламента таможенного союза «Криминалистическая техника», установление обязательной сертификации средств криминалистической техники (действующее законодательство предусматривает только поверки средств измерений), а также разработка

---

<sup>1</sup> п. 10 Приложения № 5 к Положению о НТД.

единой концепции научно-технической политики в сфере экспертно-криминалистической деятельности в качестве документа стратегического планирования<sup>1</sup>.

Основными показателями эффективности ГНТП КО являются: повышение производительности труда личного состава; экономическая эффективность использования достижений науки и техники для решения задач уголовно-процессуальной, оперативно-розыскной и экспертно-криминалистической деятельности; удовлетворенность личного состава качеством научно-технического обеспечения деятельности.

Подготовка распорядительных документов в рамках реализации ГНТП КО осуществляется на основе прогнозов развития научно-технического потенциала и динамики изменений в сферах предполагаемого применения конкретных научно-технических средств и технологий.

---

<sup>1</sup> *Гаврилин Ю. В.* О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности (криминалистической политики) // Труды Академии управления МВД России. 2022. № 2 (62). С. 96–102.

## **2. ПРЕДМЕТ И СТРУКТУРА НАУЧНО-ТЕХНИЧЕСКОЙ ПОЛИТИКИ В СФЕРЕ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ**

Как указано выше, ГНТП КО имеет своим назначением повышение эффективности уголовно-процессуальной, оперативно-розыскной и экспертно-криминалистической деятельности на основе использования криминалистических методов и средств. Соответственно, предметом ГНТП КО, на который она направлена и сфокусирована, является особый вид правоохранительной деятельности, реализуемый названными выше методами и средствами, который в литературе получил название криминалистического обеспечения выявления, раскрытия и расследования преступлений. При этом ГНТП КО определяет векторы развития криминалистического обеспечения, задает ему целевые ориентиры, обеспечивает его необходимыми ресурсами и кадрами.

Впервые определение понятия криминалистического обеспечения сформулировал В. Г. Коломацкий, понимая под ним «систему внедрения в практическую деятельность должностных лиц, подразделений, служб и органов внутренних дел криминалистических знаний, воплощенных в умение работников использовать научные, методические и тактические рекомендации, технико-криминалистические средства и технологии их применения в целях предотвращения, раскрытия и расследования преступлений»<sup>1</sup>.

Впоследствии подход, в основе которого лежит представление о криминалистическом обеспечении как о системе знаний и сформированных на их основе навыков и умений их использования, был поддержан значительным количеством авторов, включая Р. С. Белкина<sup>2</sup>, В. А. Жбанкова, А. М. Нуждина и др.

Несколько иной подход к рассматриваемому понятию демонстрируют в своих работах З. И. Кирсанов, Е. С. Романова, Р. Г. Аксенов, С. Р. Акимов и А. В. Шмонин, считающие, что сутью кримина-

---

<sup>1</sup> Коломацкий В. Г. Криминалистическое обеспечение деятельности органов внутренних дел по расследованию преступлений // Криминалистика: история, общая и частные теории : учеб. : в 3-х т. / под ред. Р. С. Белкина, В. Г. Коломацкого, И. М. Лузина. М., 1995. Т. 1. С. 62.

<sup>2</sup> Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования : учеб. / под ред. Т. В. Аверьяновой, Р. С. Белкина. М., 1997. 398 с.

листического обеспечения является система криминалистических рекомендаций и средств обучения их эффективному применению.

Третий подход, яркими представителями которого являются А. Ф. Волынский, В. А. Волынский, В. Ю. Сокол, состоит в понимании криминалистического обеспечения расследования преступлений как деятельности по формированию условий постоянной готовности к эффективному использованию криминалистических рекомендаций.

С определенной степенью условности первый подход можно назвать компетентностным, второй – дидактическим, а третий – деятельностным.

Все приведенные подходы объединяет то, что в основе криминалистического обеспечения расследования преступлений лежат криминалистические знания (рекомендации). Различия проявляются в объеме анализируемого понятия.

Исходя из того, что само понятие «обеспечение» означает вооружение кого-либо определенными ресурсами, средствами и технологиями, позволяющими эффективно, качественно осуществить действие, операцию, деятельность<sup>1</sup>, становится очевидным назначение рассматриваемой категории – повышение эффективности деятельности по выявлению, раскрытию, расследованию и предупреждению преступлений, т. е. основных сфер применения криминалистических знаний.

Действительно, сами по себе криминалистические знания, даже облеченные в форму рекомендаций, еще не способны оказывать непосредственное влияние на правоохранительную деятельность. Эти знания должны быть доведены до правоприменителей, постоянно поддерживаться в актуальном состоянии с учетом развития возможностей криминалистической техники, передового отечественного и зарубежного опыта борьбы с преступностью, трансформации способов совершения отдельных видов преступлений, а также быть реально применимыми с учетом существующих правовых и ресурсных ограничений.

Принимая во внимание сказанное, *под криминалистическим обеспечением следует понимать систему мероприятий научно-технического и организационно-управленческого характера, направленную на формирование технического, тактического и организационно-методического инструментария субъектов правоохранительной*

---

<sup>1</sup> Ожегов С. И. Толковый словарь русского языка. М., 2010. С. 350.

деятельности в целях эффективного решения задач уголовного судопроизводства<sup>1</sup>.

На основании вышеизложенного можно выделить несколько компонентов в структуре криминалистического обеспечения расследования преступлений.

Р. С. Белкин называл в числе таких компонентов знания, образование и технику<sup>2</sup>.

А. Ф. Волынский обозначает два уровня криминалистического обеспечения: содержательный (создание условий постоянной готовности уполномоченных субъектов к применению криминалистических знаний) и деятельностный (практическая реализация таких знаний)<sup>3</sup>. Сходного подхода придерживается и В. Ю. Сокол, выделяя научно-дидактический и исполнительный уровни криминалистического обеспечения<sup>4</sup>.

В содержании криминалистического обеспечения следует выделить два уровня:

1) криминалистическое обеспечение расследования в целом включает в себя алгоритмы действий и раскрывает содержание деятельности его участников на стадии проверки сообщения о преступлении, на первоначальном, последующем и заключительном этапах расследования в зависимости от складывающейся следственной ситуации;

2) криминалистическое обеспечение производства отдельных следственных действий раскрывает содержание деятельности их участников на каждом этапе их проведения, вырабатывает комплекс тактических приемов их производства, содержит рекомендации по использованию средств криминалистической техники для обнаружения, фиксации и изъятия доказательственной информации.

Исходя из того, что в основе криминалистического обеспечения расследования преступлений лежат научные знания, сформированные в предметной области науки криминалистики, с учетом

---

<sup>1</sup> Гаерилин Ю. В. О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности (криминалистической политики) // Труды Академии управления МВД России. 2022. № 2 (62). С. 96–102.

<sup>2</sup> Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования : учеб. / под ред. А. В. Аверьяновой, Р. С. Белкина. М., 1997. С. 64–69.

<sup>3</sup> Криминалистика : учеб. / под ред. А. Ф. Волынского, В. П. Лаврова. М., 2008. С. 52–56.

<sup>4</sup> Сокол В. Ю. Тактико-криминалистическое обеспечение раскрытия и расследования преступлений (Методологические и организационные аспекты) : дис. ... канд. юрид. наук. М., 1998. С. 57.

общепринятых взглядов на систему криминалистики, в содержании рассматриваемого объекта ГНТП КО целесообразно выделить теоретико-методологическое, технико-криминалистическое, тактико-криминалистическое и методико-криминалистическое обеспечение.

Рассмотрим содержание названных разделов более подробно.

*Теоретико-методологические основы* криминалистического обеспечения представляют собой систему научных положений о его понятии, содержании, значении. На основе результатов анализа преступности и практики выявления, раскрытия и расследования преступлений осуществляется обоснование потребности правоохранительных органов в научно обоснованных рекомендациях по разрешению тактических задач с учетом развития технологий, зарубежного опыта и анализа научных разработок.

Теоретико-методологические основы криминалистического обеспечения представляют собой основные идеи, теоретические концепции, принципы, наиболее общие категории, понятия, определения и термины в сфере криминалистики, а также методы их познания.

Кроме того, в данном разделе содержится научно-теоретический фундамент криминалистической деятельности в виде системы частных теорий и учений: о криминалистической идентификации и диагностике, о механизме преступления, признаках, пространственных связях и временных отношениях, о навыках, фиксации доказательственной информации, противодействии расследованию и его преодолению, о криминалистическом прогнозировании и др.

Частные криминалистические теории представляют теоретическую основу разработки и применения средств и методов расследования и предотвращения преступлений. Они могут относиться к одному, двум, трем или всем разделам науки криминалистики и соответствует основным направлениям теоретической деятельности, потребность в которой испытывает практика борьбы с преступностью.

Система частных криминалистических теорий и учений динамична и развивается с учетом потребности практики в ответах на вызовы и угрозы текущей криминальной ситуации. Однако образующие ее элементы неоднородны по своему объему и степени научной разработанности.

С учетом синтетической природы криминалистической науки, которая представляет собой сплав естественно-научных знаний и правовых принципов, рассматриваемый элемент криминалистического обеспечения определяет основные подходы к разработке и применению криминалистических методов и средств. Это положение

имеет под собой философско-правовой фундамент. Например, в основе криминалистической идентификации лежит теория отражения, в рамках которой материальные следы преступления, включая материально-фиксированные отображения, биологические следы, цифровые данные рассматриваются с позиции отражения взаимодействия объектов в связи и по поводу свершившегося события – преступления. Принцип системности также обуславливает применение комплексного подхода к расследованию преступления, где криминалистические методы и средства выступают неотъемлемым элементом и интегрируются в общую схему доказывания (например, использование криминалистической техники специалистом при фиксации следов на месте происшествия (3D-сканирование, спектральный анализ). При этом требуется соблюдение правовых гарантий участников уголовного судопроизводства, определенных уголовно-процессуальным законодательством.

Теоретико-методологические основы криминалистического обеспечения представляют собой базис для разработки технико-криминалистических методов и средств, включая такие современные направления, как: использование спектрального анализа, ультрафиолетового и инфракрасного излучения (спектрометры для идентификации состава наркотических средств, микрочастиц; УФ-лампы для обнаружения биологических следов и т. д.); хроматография (портативные наркотестеры); генетика, секвенирование ДНК (ПЦР-амплификаторы, автоматические секвенаторы); большие данные, машинное обучение (программы для блокчейн-анализа, алгоритмы распознавания лиц) и пр. Эти и другие технико-криминалистические методы и средства более подробно будут представлены ниже.

*Технико-криминалистическое обеспечение* представляет собой вид правоохранительной деятельности, предполагающий использование специальных знаний в целях предупреждения, выявления, раскрытия и расследования преступлений<sup>1</sup>.

Специальные знания в современном мире – довольно широкая сфера, постоянно пополняемая новой информацией, в связи с этим именно они помогают органам предварительного расследо-

---

<sup>1</sup> Гаврилин Ю. В., Салеева Ю. Е., Марушко А. В. О научных подходах к понятию и содержанию технико-криминалистического обеспечения раскрытия и расследования преступлений // Криминалистика, уголовный процесс и судебная экспертиология в XXI веке: векторы развития (к 70-летию кафедры управления органами расследования преступлений Академии управления МВД России), 66-е ежегодные криминалистические чтения : сб. науч. статей по материалам междунар. науч.-практ. конф. Москва, 25 апреля 2025 г. М., 2025. Ч. 2. С. 66–77.

вания осуществлять оперативно-служебные функции с наибольшей эффективностью. Они представляют собой систему теоретических положений и практических навыков в области конкретной науки либо техники, искусства или ремесла, приобретаемых путем специальной подготовки или профессионального опыта и необходимых для решения вопросов, возникающих в процессе уголовного судопроизводства<sup>1</sup>.

Технико-криминалистическое обеспечение включает в себя несколько относительно самостоятельных видов криминалистической деятельности, к которым относятся:

- судебно-экспертная деятельность;
- применение технических средств и специальных знаний в уголовно-процессуальной деятельности;
- применение технических средств и специальных знаний в оперативно-розыскной деятельности;
- осуществление криминалистической регистрации;
- экспертно-криминалистическая деятельность по предупреждению преступлений и реализации избирательных прав.

Рассмотрим названные виды криминалистической деятельности более подробно.

*Судебно-экспертная деятельность* состоит в организации и производстве судебной экспертизы. Последняя представляет собой предусмотренное законодательством Российской Федерации о судопроизводстве процессуальное действие, включающее в себя проведение исследований и дачу заключения экспертом по вопросам, требующим специальных знаний в области науки, техники, искусства или ремесла. Она способствует раскрытию практически каждого второго преступления, совершаемого в Российской Федерации.

В зависимости от ведомственной принадлежности судебно-экспертная деятельность подразделяется на государственную и негосударственную. Правовую основу государственной судебно-экспертной деятельности составляют нормы УПК РФ (ст. 195–207 и др.), положения Федерального закона от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», а также ведомственные нормативно-правовые акты.

В настоящее время в экспертно-криминалистических подразделениях органов внутренних дел осуществляется производство 52 видов судебных экспертиз, их номенклатура постоянно рас-

---

<sup>1</sup> *Россинская Е.Р.* Специальные познания и современные проблемы их использования в судопроизводстве // Журнал российского права. 2001. № 5. С. 32.

ширяется<sup>1</sup>. Основные изменения перечня родов (видов) судебных экспертиз связаны с возрастающей потребностью органов предварительного расследования и дознания в использовании специальных знаний в новых областях. За последнее десятилетие появились радиотехническая, строительно-техническая, товароведческая и психофизиологическая экспертизы, а также исследование стоимости строительства, финансируемого с привлечением бюджетных средств и исследования автомобильных дорог, автодорожных мостов и тоннелей, аэродромов, специальных сооружений.

В 2023 г. названный перечень дополнен лесотехнической экспертизой. При ее проведении устанавливается породный состав и жизненное состояние деревьев, определяется объем и давность проведенных вырубок, а также рассчитывается ущерб, причиненный уничтожением или повреждением деревьев. Сегодня в сфере нормативного регулирования судебно-экспертной деятельности в целом существует ряд дискуссионных моментов, а именно:

- отсутствие нормативно закрепленных критериев оценки компетентности негосударственных экспертов;
- различия в ведомственных подходах классификации судебных экспертиз<sup>2</sup> и, как следствие, методическом обеспечении разрешения однотипных экспертных задач;

---

<sup>1</sup> Инструкция по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации : приложение № 1 к Приказу МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации».

<sup>2</sup> Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России [Электронный ресурс] : приказ Минюста России от 20 апр. 2023 г. № 72 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.02.2025) ; Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации (вместе с «Инструкцией по организации формирования, ведения и использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации», «Правилами ведения экспертно-криминалистических учетов в органах внутренних дел Российской Федерации») [Электронный ресурс] : приказ МВД России от 10 февр. 2006 г. № 70 // Доступ из СТРАС «Юрист» (дата обращения: 10.02.2025) ; Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации» на право самостоятельного производства судебных экспертиз [Электронный ресурс] : приказ СК России от 24 июля 2020 г. № 77 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.02.2025).

– научная обоснованность отдельных методов экспертных исследований<sup>1</sup> и др.

Совокупность данных обстоятельств негативно сказывается на качестве экспертиз, создает предпосылки для назначения повторных и дополнительных экспертиз, приводит к нарушению разумных сроков судопроизводства, выходу за пределы компетенции эксперта и иным процессуальным нарушениям.

На разрешение обозначенных проблемных вопросов нацелены ожидаемые изменения законодательства о судебно-экспертной деятельности<sup>2</sup>. Разработка подготовленного ко второму чтению в Государственной Думе проекта федерального закона о судебно-экспертной деятельности обусловлена тем, что действующий Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности» уже не соответствует развитию регламентируемого им вида деятельности, в первую очередь, в контексте регламентации оснований и порядка привлечения негосударственных экспертных организаций и индивидуальных предпринимателей к производству экспертиз. Законопроектом предусматриваются требования к проверке (апробации, испытаниям), внедрению (стандартизации, сертификации, валидации) экспертных методик; введение единого реестра судебных экспертов и экспертных организаций; регламентация порядка исключения из реестра.

В зависимости от отраслевой принадлежности используемых специальных знаний выделяют следующие классы судебных экспертиз: криминалистические, медицинские и психиатрические, инженерно-технические, инженерно-транспортные, инженерно-технологические, экономические, экологические, сельскохозяйственные, искусствоведческие и биологические.

*Применение технических средств и специальных знаний в уголовно-процессуальной деятельности* осуществляется в следующих формах: участие специалиста при производстве следственных действий (ст. 58, 168 УПК РФ); заключение специалиста (ч. 3 ст. 80 УПК РФ); показания специалиста (ч. 4 ст. 80 УПК РФ); производство

---

<sup>1</sup> Обзор кассационной практики судебной коллегии по уголовным делам Верховного Суда Российской Федерации за второе полугодие 2012 года : утв. Президиумом Верховного Суда Рос. Федерации 3 апр. 2013 г. // Доступ из СПС «Консультант-Плюс» (дата обращения: 10.04.2025) ; Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 21 авг. 2019 г. № 5-АПУ19-59 // Доступ из СПС «Консультант-Плюс» (дата обращения: 10.04.2025).

<sup>2</sup> О судебно-экспертной деятельности в Российской Федерации : проект федер. закона // Система обеспечения законодательной деятельности Государственной Думы Федерального собрания Российской Федерации : сайт. URL: <https://sozd.duma.gov.ru/bill/306504-6> (дата обращения: 09.02.2025).

исследований документов, предметов, трупов (ч. 1 ст. 144 УПК РФ); производство ревизий и документальных проверок (ч.1 ст. 144 УПК РФ).

Участие специалиста при производстве следственных действий включает в себя оказание содействия в обнаружении, фиксации, изъятии, упаковке и хранении вещественных доказательств, содействие в правильном отражении в протоколе криминалистически значимой информации, обмен информацией, консультации, содействие в получении образцов для сравнительного исследования, помощь в производстве следственных действий и исследовании следов на месте происшествия, участие в выдвижении версий и совместном планировании расследования. Перед началом следственного действия, в котором участвует специалист, следователь удостоверяется в его компетентности, выясняет его отношение к подозреваемому, обвиняемому и потерпевшему, разъясняет специалисту его права и ответственность.

Так, в ходе осмотра места происшествия применяется широкий спектр технико-криминалистических методов и средств (УФ-осветители, использование беспилотных воздушных судов, 3D-сканеры), что минимизирует риск утраты криминалистически значимой информации.

Актуальным направлением совершенствования ТКС является разработка и внедрение методов и средств цифровой криминалистики, направленных на обнаружение, фиксацию и изъятие доказательственной информации на электронных носителях. Более подробно названные методы и средства будут рассмотрены ниже.

Заключение специалиста – это представленное в письменном виде суждение по вопросам, поставленным перед ним сторонами. Применяется тогда, когда не требуется производство исследования объекта. В этом состоит основное отличие заключения специалиста от заключения эксперта.

Показания специалиста – это сведения, сообщенные им на допросе об обстоятельствах, требующих специальных познаний, а также разъяснение своего мнения.

Производство исследований представляет собой предварительное изучение объектов, еще не имеющих статуса вещественных доказательств, но могущих стать таковыми при наступлении определенных процессуальных условий. Предварительное исследование может проводиться сотрудником, имеющим право самостоятельного производства судебных экспертиз по экспертной специальности, соответствующей характеру выполняемого исследования. При проведении предварительного исследования применяются только те методы, которые не вызывают изменения вида и свойств объектов

исследования и не исключают возможности, в случае необходимости, последующего производства судебной экспертизы. Если проведение предварительного исследования невозможно без изменения свойств объекта, оно выполняется только после письменного согласования с инициатором исследования. Результаты предварительного исследования оформляются справкой.

Под ревизией понимается система контрольных действий по документальной и фактической проверке обоснованности совершенных организацией хозяйственных и финансовых операций в ревизуемом периоде или результатов ее финансово-хозяйственной деятельности<sup>1</sup>.

Под документальной проверкой понимается контрольное действие по определенному кругу вопросов, участку или эпизоду финансово-хозяйственной деятельности ревизуемой организации, включая проверку документов с целью решения вопроса о достаточности или документальной возможности проведения намечаемой ревизии (проверки).

К числу перспективных технологий, способных повысить эффективность производства отдельных следственных действий, относятся машинное зрение, дополненная реальность, 3D-моделирование и др. Эти и другие перспективные технологии будут подробно описаны ниже. В частности, совместными исследованиями Академии управления МВД России и ЭКЦ МВД России раскрыт потенциал использования технологий оптического и лазерного 3D-сканирования в процессе фиксации следов на месте происшествия в виде высокоточной трехмерной цифровой модели, позволяющей произвести все необходимые измерения. Экспериментально доказано, что с помощью 3D-технологий можно успешно решать экспертные задачи по фиксации обстановки места происшествия (в том числе взаимного расположения транспортных средств на месте дорожно-транспортного происшествия, определения типа и мощности взрывного устройства и т. д.)<sup>2</sup>.

В настоящее время в условиях проведения специальной военной операции активно используются беспилотные авиационные системы, оснащенные цифровой фото- и видеотехникой, что повышает точность при проведении измерений, значительно сокращает продолжительность осмотра, а также позволяет осуществлять осмотр больших площадей, труднодоступных и опасных участков

---

<sup>1</sup> Курс уголовного процесса / под ред. Л. В. Головки. 2-е изд., испр. М., 2017. 1280 с.

<sup>2</sup> Севастьянов П. В. Цифровые технологии фиксации невербальной доказательственной информации : дис. ... канд. юрид. наук. М., 2024. С. 46.

местности и помещений (например, в сгоревших зданиях [сооружениях] и на прилегающей территории).

*Участие специалистов в оперативно-розыскной деятельности* осуществляется в формах и при наличии оснований, установленных Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». В соответствии с Наставлением по организации экспертно-криминалистической деятельности в системе МВД России участие специалистов при осуществлении оперативно-розыскной деятельности осуществляется путем:

- участия в проведении исследований предметов (веществ) и документов в целях выявления преступлений;
- оказания помощи в установлении (отождествлении) личности неопознанных трупов;
- изготовления субъективных портретов;
- изготовления розыскных таблиц, содержащих криминалистически значимую информацию о лицах, предметах, орудиях преступлений;
- участия в обследовании помещений, зданий, сооружений, участков местности и транспортных средств;
- применения фотосъемки, видео- и аудиозаписи, иных экспертно-криминалистических средств при проведении оперативно-розыскных мероприятий;
- оказания помощи в отборе образцов для сравнительного исследования.

Использование методов поиска информации в открытых источниках в рамках наведения справок широко используется для решения задач установления владельцев криптовалютных кошельков<sup>1</sup>, осуществления интеллектуального поиска информации в сети Интернет, а также решения иных поисковых и аналитических задач, возникающих в процессе выявления, раскрытия и расследования преступлений, совершенных с использованием ИТТ.

Перспективным направлением технико-криминалистического обеспечения оперативно-розыскной деятельности видится участие специалистов при получении компьютерной информации с использованием метода логирования, который предполагает осуществление определенного взаимодействия с представляющим интерес интернет-пользователем, в ходе которого ему предлагается запустить на своем устройстве файл или пройти по гиперссылке. Запу-

---

<sup>1</sup> Гаурилин Ю. В., Бедеров И. С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4 (60). С. 101–108.

скающиеся при этом специальные алгоритмы сбора пользовательских данных позволяют получить цифровой профиль устройства, необходимый для решения идентификационных задач, возникающих в процессе расследования<sup>1</sup>.

Зарождение криминалистики как науки и ее активное развитие во второй половине XIX – первой четверти XX века непосредственно связано с методологией решения отдельных практических задач, относящихся к предметной области *криминалистической регистрации* – разделу криминалистической техники, посвященному изучению закономерностей собирания, систематизации, хранения и использования криминалистически значимой информации в целях наиболее полного, своевременного и всестороннего обеспечения раскрытия, расследования и предупреждения преступлений. В разные годы вопросам криминалистической регистрации посвящали свои работы А.И. Винберг, Р.С. Белкин, В.Я. Дорохов, В.Я. Колдин, З.И. Кирсанов, Н.С. Полевой, В.А. Образцов, Л.Г. Эджубов и другие видные ученые, труды которых оказали определяющее воздействие на развитие криминалистической науки в целом. Однако, несмотря на значительное количество научных и учебных изданий по данной проблематике, круг вопросов, требующих своего научного разрешения в рассматриваемой области научных знаний, если и сократился, то весьма незначительно.

Ведение экспертно-криминалистических учетов предполагает деятельность по систематизации и размещению в информационных системах (базах данных) экспертно-криминалистической информации об объектах учета, позволяющей осуществлять ее использование в целях решения задач уголовно-процессуальной и оперативно-розыскной деятельности.

Так, по-прежнему не разрешен вопрос о процессуальном значении регистрационной информации, научно-технологических основах дактилоскопической регистрации, создании научно обоснованной классификации способов совершения преступлений, правовом положении справочно-вспомогательных учетов и порядке их формирования, межведомственном информационном обмене.

На современном этапе развития криминалистической науки развитие учения о криминалистической регистрации обусловлено

---

<sup>1</sup> Гаерлин Ю.В. Научные основы технико-криминалистического обеспечения оперативно-розыскной деятельности органов внутренних дел по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий // Развитие научных идей профессора Р.С. Белкина в условиях современных вызовов (к 100-летию со дня рождения) : сб. науч. статей по материалам междунар. науч.-практ. конф. : в 2-х ч. М., 2022. С. 62–71.

изменениями объектов учета, системы регистрации, способов ведения учетов, внедрением новых видов автоматизированных информационно-поисковых систем, совершенствованием технологии получения информации (из различных источников), необходимой для принятия субъектами расследования процессуальных, тактических, организационных решений<sup>1</sup>.

Ранее нами поднимался вопрос о формировании криминалистического учета цифровых следов преступления и справочно-вспомогательного учета цифровых профилей личности и (или) электронных устройств<sup>2</sup>. Если приведенные цифровые следы находятся в непосредственной причинно-следственной связи с событием преступления, они являются актуальной криминалистически значимой информацией и могут быть объектами криминалистической регистрации.

Вместе с тем система криминалистической регистрации достаточно консервативна. Действующий с 2006 г. приказ МВД России, регламентирующий вопросы организации формирования, ведения и использования экспертно-криминалистических учетов органов внутренних дел<sup>3</sup>, специализированного учета цифровых следов не предусматривает.

При этом решением коллегии МВД России от 1 ноября 2019 г. № 3 км отмечалась необходимость систематизации в рамках единой базы данных «Дистанционное мошенничество» информации о зарегистрированных ИТ-преступлениях, а также создания автоматизированных систем мониторинга сети Интернет, в частности, информационных систем поиска по метаданным<sup>4</sup>.

---

<sup>1</sup> *Гаврилин Ю. В.* Основные направления развития криминалистических знаний в условиях информационного общества // Криминалистика в условиях информационного общества : сб. статей междунар. науч.-практ. конф. (59-е ежегодные криминалистические чтения). М., 2018. С. 65–73.

<sup>2</sup> *Гаврилин Ю. В., Салеева Ю. Е.* Развитие учения о криминалистической регистрации в условиях цифровой трансформации преступности // Труды Академии управления МВД России. 2023. № 2 (66). С. 99–105.

<sup>3</sup> Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации (вместе с «Инструкцией по организации формирования, ведения и использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации», «Правилами ведения экспертно-криминалистических учетов в органах внутренних дел Российской Федерации») [Электронный ресурс] : приказ МВД России от 10 февр. 2006 г. № 70 // Доступ из СТРАС «Юрист» (дата обращения: 10.02.2025).

<sup>4</sup> Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км [Электронный ресурс] : приказ МВД России от 25 нояб. 2019 г. № 878 // Доступ из СТРАС «Юрист» (дата обращения: 10.02.2025).

Следует заметить, что в подсистему «Дистанционное мошенничество»<sup>1</sup> подлежит внесению такая информация, как абонентский номер заявителя, абонентский номер подозреваемого, номер банковской карты заявителя, номер расчетного счета заявителя, номер банковской карты подозреваемого, номер расчетного счета подозреваемого, способ совершения преступления, что представляет собой далеко не полный перечень цифровых следов, позволяющих установить лицо, совершившее преступление, а также факт совершения одним лицом нескольких эпизодов преступления. Сказанное открывает широкие возможности для совершенствования информационного обеспечения расследования преступлений, совершенных с использованием ИТТ.

Правовое регулирование криминалистической регистрации получило свое развитие в части, касающейся осуществления государственной геномной регистрации, формы и основания которой установлены Федеральным законом от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации».

Государственная геномная регистрация – это деятельность, осуществляемая уполномоченными государственными органами и учреждениями по получению, учету, хранению, использованию, передаче и уничтожению биологического материала и обработке геномной информации. Биологическим материалом являются содержащие геномную информацию ткани и выделения человека или тела (останков) умершего человека. Геномная информация представляет собой персональные данные, включающие кодированную информацию об определенных фрагментах дезоксирибонуклеиновой кислоты физического лица или неопознанного трупа, не характеризующих их физиологические особенности.

В Российской Федерации проводятся добровольная государственная геномная регистрация и обязательная государственная геномная регистрация. До 2023 г. обязательной государственной геномной регистрации подлежали лица, осужденные и отбывающие наказание в виде лишения свободы за совершение тяжких или особо тяжких преступлений, а также всех категорий преступлений против половой неприкосновенности и половой свободы личности; неустановленные лица, биологический материал которых изъят в ходе производства следственных действий; неопознанные трупы.

---

<sup>1</sup> Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф» [Электронный ресурс]: приказ МВД России от 29 дек. 2020 г. № 925 // Доступ из СТРАС «Юрист» (дата обращения: 12.02.2025).

Федеральный закон от 6 февраля 2023 г. № 8-ФЗ «О внесении изменений в Федеральный закон «О государственной геномной регистрации в Российской Федерации» и отдельные законодательные акты Российской Федерации» расширил перечень лиц, подлежащих обязательной государственной геномной регистрации, за счет лиц, осужденных и отбывающих наказание за совершение преступлений в виде лишения свободы, подозреваемых и обвиняемых в совершении преступлений, а также подвергнутых административному аресту<sup>1</sup>.

В целях нормативного правового регулирования механизмов опознания лиц, пропавших без вести, в том числе в ходе специальной военной операции, принят Федеральный закон от 14 февраля 2024 г. № 16-ФЗ «О внесении изменений в Федеральный закон «О государственной геномной регистрации в Российской Федерации», предусматривающий расширение перечня лиц, подлежащих обязательной государственной геномной регистрации, за счет близких родственников пропавшего. Его положениями также закреплено определение категории близких родственников, установлен перечень органов, осуществляющих получение их биологического материала и их геномной информации, закреплены сроки хранения и основания уничтожения полученной геномной информации<sup>2</sup>.

Приведенные изменения в законодательстве о геномной регистрации повлекли кратный рост наполнения федеральной базы геномной информации. Так, за 2024 г. сформирована четверть общего объема информационного массива обязательных учетных категорий, тогда как на формирование оставшейся части потребовалось 15 лет. Добровольная государственная геномная регистрация граждан Российской Федерации, а также иностранных граждан и лиц без гражданства, проживающих или временно пребывающих на территории Российской Федерации, проводится на основании их письменного заявления и на платной основе.

---

<sup>1</sup> С учетом положения Федер. закона принято постановление Правительства Рос. Федерации от 24 июня 2023 г. № 1027 «О некоторых вопросах реализации Федерального закона «О государственной геномной регистрации в Российской Федерации», которым утверждено Положение о проведении государственной геномной регистрации, определяющее порядок проведения обязательной и добровольной государственной геномной регистрации, а также порядок взимания платы за проведение добровольной государственной геномной регистрации.

<sup>2</sup> Для реализации положений указанного Федер. закона издано постановление Правительства Рос. Федерации от 11 апр. 2024 г. № 455 «О внесении изменений в постановление Правительства Российской Федерации от 24 июня 2023 г. № 1027», устанавливающее порядок проведения обязательной государственной геномной регистрации близких родственников лица, пропавшего без вести.

Правовую основу государственной дактилоскопической регистрации составляет Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации». Последняя представляет собой деятельность, осуществляемую уполномоченными органами исполнительной власти и федеральными государственными учреждениями по получению, учету, хранению, классификации и выдаче дактилоскопической информации, установлению или подтверждению личности человека. Дактилоскопической информацией являются биометрические персональные данные об особенностях строения папиллярных узоров пальцев и (или) ладоней рук человека, позволяющие установить его личность.

Дактилоскопическая информация, полученная в результате проведения государственной дактилоскопической регистрации, используется для розыска пропавших без вести лиц; установления личности по отпечаткам пальцев (ладоней) рук неопознанного трупа; установления личности лиц, не способных по состоянию здоровья или возрасту сообщить данные о себе либо не имеющих документов, удостоверяющих личность; подтверждения личности; предупреждения, раскрытия и расследования преступлений, а также предупреждения и выявления административных правонарушений.

Обязательной государственной дактилоскопической регистрации подлежат: военнослужащие и граждане, призываемые на военную службу; граждане, проходящие службу в органах внутренних дел и иных правоохранительных органах; спасатели; члены экипажей воздушных судов; лица, не способные по состоянию здоровья или возрасту сообщить данные о своей личности, если установить указанные данные иным способом невозможно; подозреваемые и обвиняемые в совершении преступления, осужденные за совершение преступления, подвергнутые административному аресту; совершившие административное правонарушение, если установить их личность иным способом невозможно; иностранные граждане, подлежащие выдворению (депортации) за пределы территории Российской Федерации, и некоторые другие категории лиц.

Обязательной государственной дактилоскопической регистрации подлежат все неопознанные трупы.

Еще одним важным направлением совершенствования криминалистической регистрации является дальнейшее развитие федеральной и региональных пулегильзотек в части формирования электронной базы изображений контрольных пуль и гильз гражданского и служебного огнестрельного оружия с нарезным стволом.

*Экспертно-криминалистическая деятельность по предупреждению преступлений* осуществляется в формах разработки и утверждения криминалистических требований к оружию и патронам, а также проведения исследований и экспертной оценки степени защищенности бланков ценных бумаг.

Криминалистические требования к оружию представляют собой комплекс технических характеристик и конструктивных особенностей оружия, необходимых для определения его видовой принадлежности и возможности последующей идентификации. Они призваны обеспечить исключение возможности переделки списанного, пневматического, сигнального и газового оружия, а также огнестрельного оружия ограниченного поражения, поступающего в оборот, в огнестрельное оружие, пригодное для стрельбы.

В 2024 г. вступили в силу изменения, предусмотренные федеральными законами в сфере оборота оружия в Российской Федерации. Федеральным законом от 8 августа 2024 г. № 250-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» установлен запрет на производство гражданского и служебного огнестрельного длинноствольного оружия с использованием основных частей огнестрельного короткоствольного оружия и (или) ранее произведенного огнестрельного оружия, имеющего возможность ведения огня очередями.

*Экспертно-криминалистическая деятельность при реализации избирательных прав* гражданами Российской Федерации осуществляется в соответствии с законодательством о выборах и референдумах и включает в себя участие специалистов по запросам избирательных комиссий в деятельности рабочих групп по проверке соблюдения порядка сбора подписей, оформления подписных листов, достоверности сведений об избирателях или участниках референдума, содержащихся в подписных листах, и их подписей.

*Тактико-криминалистическое обеспечение* расследования преступлений представляет собой систему научных положений и основанных на них рекомендаций по организации и планированию производства предварительного расследования, определению линии поведения его участников, по разработке тактических приемов производства следственных и иных процессуальных действий.

Содержание тактико-криминалистического обеспечения составляют вопросы выдвижения и проверки следственных версий, планирования расследования, организации взаимодействия участников расследования, использования помощи общественности, тактических приемов производства следственных действий.

Технико-криминалистическое и тактико-криминалистическое обеспечение находятся в тесной взаимосвязи. Если первая из обозначенных составляющих криминалистического обеспечения включает технический инструментарий субъектов уголовно-процессуальной, оперативно-розыскной и экспертно-криминалистической деятельности, то вторая составляющая отвечает за порядок его использования. Так, ТКС широко применимы для воссоздания условий произошедшего события и реконструкции обстановки при проведении следственного эксперимента, а также решения иных тактических задач.

Таким образом, эффективность тактико-криминалистического обеспечения находится в прямой зависимости от технической оснащенности правоохранительных органов.

*Методико-криминалистическое обеспечение* представляет собой систему научных положений и разрабатываемых на их основе рекомендаций по организации и осуществлению предварительного расследования и предотвращению отдельных видов преступлений.

Основное его содержание составляют частные криминалистические методики – комплексы рекомендаций типизированного вида по решению типовых тактических задач, возникающих в процессе расследования отдельных видов преступлений.

Структурно любая частная криминалистическая методика включает в себя криминалистическую характеристику преступления, особенности тактики проверки сообщения о преступлении, подлежащие доказыванию обстоятельства преступления, типичные исходные следственные ситуации и основные направления для их разрешения, особенности тактики отдельных следственных действий, особенности организации взаимодействия с другими участниками расследования, использования помощи общественности, а также выявления и устранения причин и условий, способствующих совершению преступления.

Рассматривая криминалистическое обеспечение в качестве предмета ГНТП КО отметим особое значение технико-криминалистического обеспечения, которое выступает комплексной организационно-функциональной системой, направленной на собирание и исследование криминалистически значимой информации и использующей при этом возможности технико-криминалистических методов и средств. Тактические приемы производства следственных и иных процессуальных действий, методические алгоритмы, используемые в рамках предупреждения, выявления, раскрытия и расследования преступлений неразрывно связаны с применением технико-криминалистических средств. Подчеркнем при этом

взаимосвязь теоретико-методологического, технико-криминалистического, тактико-криминалистического и методико-криминалистического видов обеспечения, образующих единую систему, в которой теория задает направление, тактика реализует замысел, методика стандартизирует процессы, опираясь при этом на технические решения (инновации) и образуя синергию элементов криминалистического обеспечения.

В завершение рассмотрения вопросов криминалистического обеспечения расследования преступлений как предмета ГНТП КО следует обозначить некоторые **тенденции** его развития:

В области теоретико-методологического обеспечения следует отметить интеграцию достижений смежных областей знания, прежде всего, цифровых технологий, технологий больших данных, биологии, психологии. Универсальный закон непрерывного развития научного знания диктует дальнейшее познание закономерностей, входящих в предмет криминалистики в контексте частных криминалистических теорий, число которых пополнилось за счет общих положений цифровой криминалистики – комплекса методов и средств собирания и исследования доказательств на электронных носителях информации и их использования в процессе доказывания.

В области технико-криминалистического обеспечения происходит дальнейшее развитие технологий криминалистической идентификации (по ДНК, запаху, биометрической информации и цифровым следам). Развиваются технологии выявления, фиксации и изъятия «традиционных» трасологических следов: предметов, веществ, отображений, в том числе за счет использования методов 3D-моделирования. Технологии обработки больших данных дают существенный импульс развитию средств криминалистической регистрации и информационно-аналитического обеспечения.

Тактико-криминалистическое обеспечение развивается в направлении совершенствования приемов работы с цифровыми доказательствами и технологий планирования расследования за счет внедрения методов проектного управления. Важное значение имеет разработка тактических основ использования полиграфа, а также совершенствование тактики возмещения ущерба, взаимодействия участников расследования и криминалистической профилактики.

Тенденциями методико-криминалистического обеспечения являются переработка частных криминалистических методик, построенных без учета использования цифровых следов преступления, а также разработка частных криминалистических методик по новым составам преступлений.

Обращаясь к вопросам **структуры** ГНТП КО, важно учитывать, что ее структурно-логические элементы могут дифференцироваться в зависимости от выбранных критериев для их классификации. Авторский подход в этом вопросе заключается в применении многомерной классификационной модели, основанной на гетерогенных параметрах систематизации. Это позволит более полно и всесторонне исследовать рассматриваемую сферу правоохранительной деятельности.

*По виду правоохранительной деятельности*, в котором находят свое применение ТКС, возможно выделить в качестве элементов научно-технической политики криминалистическое обеспечение уголовно-процессуальной, оперативно-розыскной и экспертно-криминалистической деятельности.

*По своему содержанию* структура НТП КО включает в себя научно-технический, организационно-управленческий и кадровый компоненты. Рассмотрим их более подробно.

**Научно-технический компонент** основан на положениях науки криминалистики как системе знаний о закономерностях, входящих в ее предмет. Центральное место в его содержании занимают вопросы, связанные с определением назначения, функциональными возможностями, эксплуатационными особенностями соответствующих средств криминалистической техники с учетом влияния цифровой трансформации преступности на механизм следообразования.

Развитие инновационных технологий в правоохранительной сфере невозможно без привлечения научных знаний в криминалистику, а также учета вышеназванных тенденций развития ее структурных элементов. Криминалистика сама по себе является интегративной наукой, сочетающей в себе большое количество разноплановых знаний. С учетом высокой скорости преобразований жизнедеятельности общества и отдельных лиц под воздействием цифровизации, представляется необходимым переосмыслить понятие и содержание криминалистического обеспечения как предмета ГНТП КО.

Особое значение в формировании государственной политики и определении мер государственной поддержки технологического развития экономики имеет выделение совокупности областей, играющих ключевую роль и непосредственно обеспечивающих воспроизводственный процесс в технологическом развитии. Определяющую роль в технологическом развитии на современном этапе играет фундаментальная и прикладная наука. В последние 20–30 лет наука стала рассматриваться в качестве одной из ведущих производительных сил и инструментов обеспечения технологического и социаль-

но-экономического прогресса. Результаты исследований и разработок приводят к созданию новых технологий. Технологии лежат в основе создания и производства инновационной продукции.

Следовательно, выстраивается непрерывная цепь: наука – технологии – инновации. Развитые страны активно работают над созданием механизмов государственной поддержки, направленных на ускоренное преобразование научных идей в технологии, а технологий – в продукты на рынке, востребованные национальной и глобальной экономикой.

Сегодня появляется все больше исследований, направленных на изучение и обоснование положений криминалистической техники, проводится большое количество научно-исследовательских работ, посвященных этим вопросам. Государство, принимая нормативно-правовые акты в сфере научно-технической политики и научно-технологического развития, старается создавать механизмы, которые будут способствовать устранению технического отставания.

Не вызывает сомнений то, что теоретические рекомендации криминалистики и, в частности, криминалистической техники адресованы следственной, судебной и экспертной практике и от того, насколько они обоснованы и современны, зависит уровень решения практическими работниками поставленных задач технико-криминалистическими средствами и методами.

Цифровая трансформация механизма большинства преступлений требует совершенствования технических средств, предназначенных для обнаружения, фиксации и изъятия орудий, следов преступления, других вещественных доказательств в различных средах. В свою очередь, развитие средств криминалистической техники, их усложнение и расширение функциональных возможностей требует разработки рекомендаций по практическому ее использованию, включая криминалистические технологии решения конкретных тактических и экспертных задач, возникающих в процессе расследования отдельных видов преступлений.

Рассматриваемый компонент включает в себя также вопросы формирования, ведения и использования федеральных и ведомственных банков криминалистической и иной информации о лицах, предметах и фактах, а также информационно-аналитического обеспечения процесса расследования и деятельности органов предварительного следствия.

**Организационно-правовой компонент ГНТП КО** характеризует правовые основания применения средств криминалистической техники, особенности ресурсного обеспечения криминалистической деятельности, а также особенности построения организационно-

правовых форм соответствующих подразделений правоохранительных органов, призванных на практике применять криминалистические рекомендации и технологии, включая вопросы взаимодействия.

Организационные основы обозначенной деятельности в императивном порядке диктуют субъектам управления организовывать свою работу, как и работу подчиненного личного состава, основываясь на принципах упорядоченности и согласованности взаимодействия. Рассогласованность действий может привести к негативному результату.

Организационная составляющая криминалистического обеспечения правоохранительной деятельности – это процесс упорядочения деятельности по раскрытию и расследованию преступлений. Он характеризуется многоуровневой системой организации соответствующих служб, аппаратов, учреждений и подразделений.

Первым компонентом этой системы выступает управленческий, правовой (за основу берем общегосударственный и межведомственный) уровень, на котором формируется и создается система правоохранительных органов, в которых субъекты управления обладают компетенцией по общему руководству интересующей нас сферой. Второй компонент, неразрывно связанный с управленческой организационной ступенью, – это внутриведомственный уровень, характеризующийся созданием и организацией деятельности служб и подразделений, имеющих в своем функционале задачи, направленные на выявление, раскрытие и расследование преступлений. Третий же уровень является предметно-деятельностным, т. е. связанным с организацией деятельности объектов управления, включая определение и обоснование необходимости потребностей этих объектов.

Наконец, **кадровый компонент ГНП КО** включает в себя особенности подготовки высококвалифицированных специалистов, обладающих компетенциями в области криминалистического обеспечения и представлениями о перспективах его развития.

Происходящие процессы цифровизации экспертно-криминалистической деятельности и технологического перевооружения экспертной службы внесли свои коррективы в организацию криминалистического обеспечения и подготовку экспертных кадров.

Вопросы подготовки кадров относятся к числу приоритетных направлений деятельности МВД России. В решении коллегии МВД России от 30 мая 2023 г. № 2 отмечается, что ведомственная система подготовки кадров, выстроенная в соответствии с требованиями, предъявляемыми к профессиональной подготовленности личного состава органов внутренних дел, и с учетом возможностей,

обусловленных их предельной штатной численностью, продолжает поступательно развиваться, реагирует на новые вызовы и угрозы<sup>1</sup>.

Вместе с тем качественные изменения в структуре и характере преступности, с которыми столкнулась правоохранительная система России, требуют новых подходов в вопросах профессиональной подготовки личного состава органов внутренних дел, в том числе к выполнению задач в особых условиях.

В этих условиях особое значение приобретает тесное сотрудничество практики и науки, прежде всего, криминалистики, направленное на прогнозирование практических ситуаций, формирование рекомендаций по их разрешению, определение путей разрешения практических, правовых, технических, тактических, организационных и методических вопросов.

Не менее важной задачей представляется активная интеграция современных технологичных решений в экспертно-криминалистическую деятельность. Для этого необходимо формировать навыки их применения, в том числе в рамках освоения образовательных программ, реализуемых в ведомственных вузах.

Отдельно следует остановиться на вопросе подготовки экспертных кадров для новых территорий в составе Российской Федерации. В условиях специальной военной операции требуется увеличение числа экспертов, имеющих право самостоятельного производства взрывотехнической экспертизы, а также завершение укомплектования ЭКП в новых субъектах Российской Федерации специалистами иных востребованных экспертных специальностей. В решении этой важной государственной задачи роль образовательных организаций МВД России невозможно переоценить.

В завершение рассмотрения вопросов, образующих содержание научно-технической политики в сфере криминалистического обеспечения выявления, раскрытия и расследования преступлений, следует подчеркнуть, что понимание закономерностей ее формирования обеспечивает реализацию комплексного подхода в процессе подготовки руководящего состава для органов внутренних дел.

---

<sup>1</sup> Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 30 мая 2023 г. № 2км [Электронный ресурс] : приказ МВД России от 3 июля 2023 г. № 480 // Доступ из СТРАС «Юрист» (дата обращения: 13.02.2025).

### 3. ОСНОВНЫЕ НАПРАВЛЕНИЯ НАУЧНО-ТЕХНИЧЕСКОЙ ПОЛИТИКИ В СФЕРЕ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ И ОРГАНИЗАЦИИ РАССЛЕДОВАНИЯ

Формирование ГНТП КО неразрывно связано с научно-техническим прогрессом и развитием криминалистики как отрасли знания, использующей достижения науки и техники для борьбы с преступностью. К числу основных направлений научно-технической политики в сфере криминалистического обеспечения производства следственных действий и организации расследования следует отнести следующие:

- формирование номенклатуры ТКС, предназначенных для обнаружения, фиксации и изъятия следов преступлений при производстве следственных действий;

- развитие технологий криминалистической регистрации, расширение перечня объектов криминалистического учета и поддержки принятия решений в условиях информационной неопределенности.

Рассмотрим указанные направления более подробно.

Криминалистические средства обнаружения, фиксации и изъятия следов преступлений на месте происшествия различаются в зависимости от видов следов, под которыми понимаются любые изменения окружающей среды, находящиеся в причинно-следственной связи с событием преступления.

Номенклатура ТКС данной категории включает в себя:

#### **1. Средства обнаружения материальных следов преступлений**

**Средства освещения** – это источники (приборы) искусственного освещения, применяемые при недостаточности естественного света. Создают рассеянное, направленное, косопадающее, моно- и полихроматическое, а также другие виды освещения.

В качестве источников белого рассеянного или направленного света могут использоваться как бытовые фонарики, так и специальные фонари для осмотра места происшествия, дающие мощный ровный световой луч, ширина и интенсивность которого регулируется в зависимости от условий осмотра – от обширного ближнего света до узконаправленного дальнего. Изготавливаются в пылевлагозащищенном корпусе, оснащаются аккумуляторными источниками питания.

Для производства осмотра места происшествия в темное время суток могут применяться специальные световые башни с бензогенератором, обеспечивающие освещение участка местности в радиусе до 20 м (рис. 2).

К специальным средствам освещения относятся источники ультрафиолетового света, позволяющие благодаря вызываемой ими люминесценции выявлять наслоения веществ, совпадающих по цвету с поверхностью, а также следы биологического и органического происхождения.

Для решения вопросов, связанных с установлением признаков подделки документов (паспортов, водительских удостоверений, паспортов транспортных средств и иных документов со специальной УФ-защитой) используются источники ультрафиолетового света. За счет различной интенсивности люминесценции при освещении отдельных участков документа, вызывающего сомнения в подлинности, источники ультрафиолетового света позволяют также выявить признаки частичной подделки документов: подчистки, травления, смывания, дописки, дорисовки, переклейки фотокарточек и т. п. Ультрафиолетовый осветитель (рис. 3.) позволяет обнаруживать также невидимые и слабовидимые следы биологического происхождения (крови, спермы, пота и др.), химических веществ (нефтепродуктов, клея и пр.), которые под действием ультрафиолетовых лучей люминесцируют либо отличаются по оттенку от фона поверхности, на которой они находятся.

Ультрафиолетовые осветители изготавливаются как в корпусах бытовых фонарей, так и в специальных корпусах, обеспечивающих щелевой поток света.

Высокоэффективным средством поиска биологических выделений, следов крови, семенной жидкости, фрагментов костей и зубов на месте происшествия для проведения дальнейшего анализа ДНК являются источники криминалистического света («ИКС 450» [рис. 4.], МИКС, «Projectina SL-450» и др). В отличие от ультрафиолетовых осветителей источники криминалистического света позволяют изменять длину световой волны в различных диапазонах спектра (белый свет, УФ 365, 415, 450, 470, 505, 530 нм). Кроме того, они используются как источники щелевого света для обнаружения следов, проявляющихся при косопадающем освещении (пальцы рук, отпечатки подошв на полу и т. д.). Успешно применяются при работе со специальными химическими веществами в процессе оперативно-розыскных мероприятий и для экспресс-проверки документов в комплексе со специальными регистрирующими устройствами для исследования следов выстрела, документов, поиска и обнаружения следов крови, а также для выявления следов пальцев рук с помощью флуоресцентных дактилоскопических порошков. Приборы обладают регулируемой мощностью излучения, наличием белой подсветки. Комплекуются штативом, очками-светофильтрами для оператора, а также светофильтрами для фотокамеры, ударопрочным влагозащищенным кейсом.



*Рис. 2.* Световая башня «Свеча» с бензогенератором



*Рис. 3.* Ультрафиолетовый осветитель



*Рис. 4.* Источник криминалистического света ИКС-450

В условиях отсутствия дневного света и полной темноты могут применяться приборы ночного видения (ночные визиры).

В экспертной практике хорошо зарекомендовали себя источники света с мультиспектральным диапазоном (ультрафиолетовые и инфракрасные осветители с изменяемой длиной волны и монохроматические источники света различных зон спектра). Так, положительные результаты демонстрирует УФ-осветитель МИКС-450 с длиной волны 450 нм (синий, производитель: конструкторское бюро специального приборостроения, г. Москва). Применение данного прибора позволяет не только экономно использовать дорогостоящие расходные материалы, но и сокращает время осмотра места происшествия и вещественных доказательств при производстве биологических экспертиз. Обнаружение большинства следов с помощью данного прибора может быть осуществлено в затемненном помещении либо в темное время суток. Прибор компактен и удобен в эксплуатации (вес – 1,5 кг). Мобильный источник экспертного света серии МИКС-К обладает более высокими заявленными техническими характеристиками, в связи с чем имеет более широкую область применения.

Перспектива развития источников криминалистического света видится в разработке интегрированных устройств, объединяющих возможности осмотра в условиях изменяемой длины световой волны, выявления температурных аномалий, построения 3D-моделей и проверки объектов по криминалистическим учетам. Такой прибор, выполненный в мобильном исполнении, с возможностью проводной и (или) беспроводной передачи полученных данных для их анализа и проверки позволит повысить качество работы по обнаружению и фиксации материальных следов и иной криминалистически значимой информации.

**Средства увеличения** предназначены для расширения возможностей зрения человека. В ходе осмотра места происшествия применяются криминалистические лупы (в том числе складные и с подсветкой). Современные оптические лупы могут комплектоваться дополнительной линзой для детального изучения или работы с мелкими объектами, что позволяет повысить кратность увеличения с 2–3 до 6–10. Как правило, они входят в стандартную комплектацию унифицированных следственных чемоданов. В настоящее время на смену оптическим лупам приходят электронные, передающие видеоизображение на экран ноутбука. Подобные лупы имеют регулируемую кратность увеличения и различные виды подсветки: верхняя белая, косопадующая, боковая с двух направлений, ультрафиолетовая.

**Средства измерения** предназначены для фиксации размерных характеристик объекта осмотра в целом, отдельных следов и предметов, определения расстояний между объектами, а также выполнения «привязки» места происшествия к постоянным ориентирам. Для измерения значительных расстояний используются рулетки и лазерные измерители расстояний (дальномеры). Современные дальномеры способны производить вычисления площади прямоугольных и треугольных участков, объемов, размеров помещений, измерения углов наклона, а также значительных по протяженности расстояний до 100 м. При этом точность измерений составляет +/- 1 мм.

Для измерения размерных характеристик отдельных следов и объектов малого размера используются линейка и штангенциркуль. Для определения реальных размеров объектов, запечатлеваемых на фотоизображении, применяются масштабные линейки с контрастными (черно-белыми) делениями. Они используются для фиксации размерных величин отдельно взятых, как правило, небольших по объему и площади объектов.

При производстве осмотра места происшествия по делам о дорожно-транспортных происшествиях применяются измерители глубины протектора шин, которые помогают определить степень износа покрышек (шин), а также могут быть использованы для измерения износа автомобильных колодок.

**Средства обнаружения невидимых и слабовидимых следов пальцев рук, используемые в ходе осмотра места происшествия,** основаны на свойствах адгезии (прилипания) мелкодисперсных порошков с потожировым веществом, химической реакции, а также люминисценции в ультрафиолетовых лучах.

Наиболее распространенным приемом выявления следов пальцев рук на месте происшествия является обработка поверхности, с которой, вероятно, соприкасался субъект преступления, дактилоскопическим порошком. Порошки различаются по цвету (светлые и темные, применяемые, соответственно, на темных и светлых поверхностях) и магнитным свойствам (магнитные и немагнитные, применяемые, соответственно, на металлических и немаetalлических поверхностях). Обработка поверхностей дактилоскопическими порошками производится с помощью мягкой кисти (флейц-кисть, стекловолоконная кисть «Марабу») или магнитной кисти.

Химические средства выявления следов пальцев рук включают в себя нингидриновые планшеты, предназначенные для проведения обработки пористых поверхностей на предмет выявления мало-видимых потожировых следов пальцев рук с применением спрея

нингидрина, а также комплекты для йодного дактилоскопирования, позволяющие производить обработку поверхностей парами йода.

Для обнаружения следов пальцев рук на мокрых поверхностях используются специальные аэрозоли, представляющие собой раствор для обнаружения отпечатков пальцев на мокрой, светлой и темной, непористой вертикальной поверхности. Аэрозоль равномерно распыляется по поверхности, на которой предполагается найти следы пальцев. Через несколько секунд следы проявляются. После высыхания их можно отделить и сохранить обычным образом.

Визуальные способы выявления маловидимых следов пальцев рук основаны на использовании источников направленного, рассеянного, косопadaющего света и ультрафиолетового освещения, рассмотренных выше.

**Поисковая техника** применяется для обнаружения различных объектов, поиск которых затруднен в силу их малых размерных характеристик, умышленных действий заинтересованных в их сокрытии лиц или отсутствия точных сведений об их местонахождении. Принцип действия поисковой техники зависит от физических характеристик искомого объекта: магнитных свойств четных металлов (металлоискатели [рис. 5], магнитные искатели – подъемники), выделяемых объектами поиска специфических газообразных веществ (газоанализаторы), создаваемых объектами поиска шумов и вибраций (акустические анализаторы, стетоскопы), зрительного образа находящегося за непрозрачной преградой объекта (эндоскопы), различной температуры объектов поиска и окружающей среды (тепловизоры, инфракрасные обнаружители), различной плотности объектов поиска (щупы, рентгеновские досмотровые установки [рис. 6]) и т. д.



*Рис. 5. Metalлоискатель Кондор 7252*



*Рис. 6.* Портативный ИК-Фурье спектрометр Agilent 4300 ExoScan

Для выявления электронных устройств независимо от того, включены они или нет, либо находятся в режиме ожидания, применяются нелинейные локаторы (детекторы нелинейных переходов [рис. 7]).



*Рис. 7.* Профессиональный нелинейный локатор (детектор нелинейных переходов NR-900EMS)

Для обнаружения зарядов взрывчатых веществ в негерметичных объемах и выявления их следов на поверхности обследуемых объектов используется портативный обнаружитель (детектор) паров взрывчатых веществ (рис. 8). Обнаружение осуществляется путем отбора проб воздуха с поверхности или из внутреннего объема обследуемых объектов и их анализа на содержание характерных компонентов паров взрывчатых веществ.



*Рис. 8.* Портативный обнаружитель (детектор) паров взрывчатых веществ «Пилот-М»

Для обнаружения различных объектов, в том числе неметаллических, в различных средах (грунт, песок, вода) применяются георадары (рис. 9). Для поиска металлических предметов в диэлектрических (сухой силиконовый песок, дерево и т. п.) и слабопроводящих средах (грунт, кирпичные стены и т. п.) используются металлоискатели (рис. 5, 10). Особой разновидностью металлоискателя является пинпоинтер – узконаправленное устройство, предназначенное для локализации отдельных металлических объектов (рис. 11).



*Рис. 9.* Георадар «Око-3»



*Рис. 10.* Переносной индукционный миноискатель ИМП-2

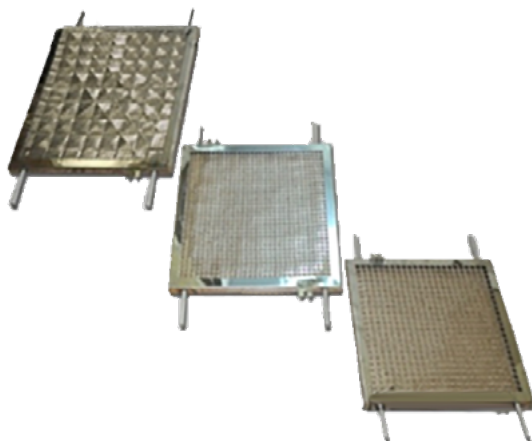


*Рис. 11.* Металлоискатель (пинпоинтер)  
«Сфинкс 02»

Для поиска объектов (металлических осколков, пуль и гильз) в полевых и городских условиях используются магнитные грабли (рис. 12). Для поиска металлических объектов в водоемах, их подъема, поиска и сбора крупных и мелких предметов из ферромагнитных сплавов (металлических осколков, пуль и гильз) в полевых условиях применяется магнитный маятниковый плуг. В целях поиска вещественных доказательств на местах взрывов применяется комплект сит, предназначенных для просеивания грунта (рис. 13, 14).



*Рис. 12. Магнитные грабли «Ёж»*



*Рис. 13. Комплект сит*



*Рис. 14.* Магнитный маятниковый пflug «Скат»

Для изъятия микрочастиц и следов, оставленных на коврах, покрывалах, скатертях, полах, подоконниках и других поверхностях используются приборы, основанные на применении электростатического метода (рис. 15). Суть последнего состоит в том, что объект с пылевыми следами помещается между двумя плоскими электродами, на которые подается высокое напряжение. Под действием электрического поля частицы пыли переносятся на основной электрод, откуда в последствии копируются на дактопленку.



*Рис. 15.* Прибор для изъятия пылевых следов «Следокоп»

**Средства фиксации** включают в себя фотоаппаратуру, диктофоны, видеоаппаратуру, применяемые для запечатления обстановки на месте происшествия и ее визуализации, а также различных следов и объектов, имеющих значение для дела.



Рис. 16. Полупрофессиональная цифровая фотокамера Canon EOS 600D

**Фотографические средства фиксации** хода и результатов осмотра места происшествия представлены в основном цифровыми устройствами, в основе принципа действия которых лежит фотоэлектрическое преобразование изображения в цифровой сигнал, происходящее в светочувствительной матрице.

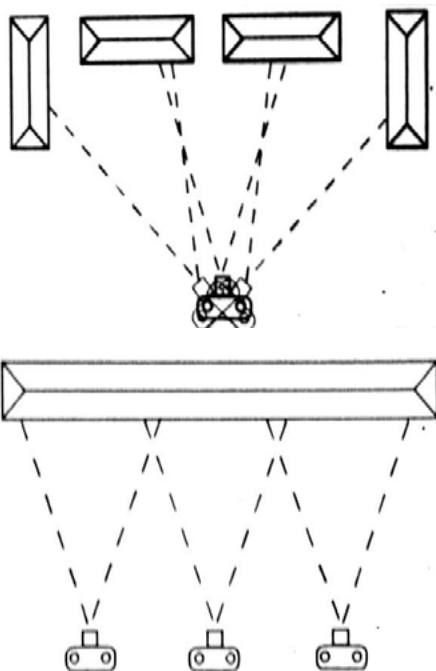


Рис. 17. Схемы кругового и линейного панорамирования

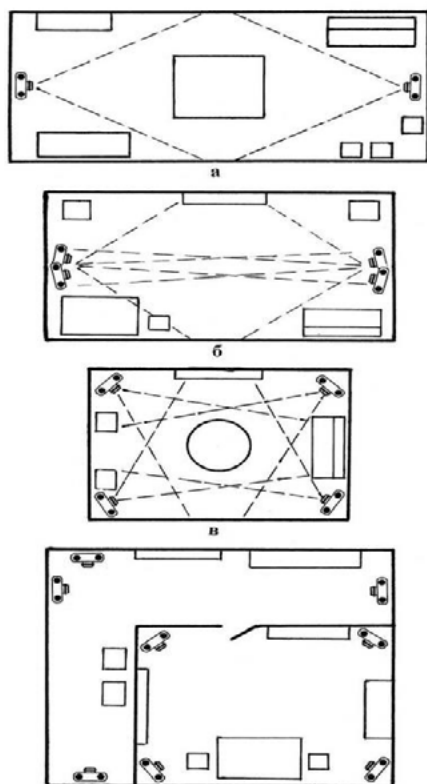


Рис. 18. Обзорная съемка помещения

Стандартный комплект для цифровой фотосъемки на месте происшествия включает в себя: фотоаппарат цифровой с разрешающей способностью не менее 20 млн пикселей и восьмикратным оптическим зумом (функцией приближения и удаления объектов [рис. 16]); флеш-карта для фотоаппарата емкостью не менее 16 Гб; устройство записи на CD-диски с фотоаппарата без использования компьютера; сменные аккумуляторы для фотокамеры и устройства записи на CD-диски; зарядное устройство; фотоштатив; внешняя фотовспышка. Положительные отзывы получают кольцевые фотовспышки, позволяющие избавиться от ненужных теней и хорошо себя зарекомендовавшие при производстве макросъемки. В их конструкцию вмонтированы светодиоды низкой температуры свечения в форме кольца. Основные приемы фотосъемки на месте происшествия представлены на рис. 17, 18.

Одним из передовых средств фотофиксации является цифровая камера круговой съемки, дающая панорамное фотоизображение высокого разрешения с углом 360° (рис. 19). Этот метод позволяет наиболее полно запечатлеть все существенные обстоятельства, порядок производства следственного действия, обеспечивая точность отображения материальной обстановки в целом и отдельных ее элементов, а также предоставляет возможность детального изучения места происшествия. Как правило, конструкция таких камер предполагает наличие нескольких объективов, синхронно фиксирующих окружающую обстановку относительно точки съемки. Единый видеофайл создается либо при последующей обработке результатов фиксации с помощью специализированного программного обеспечения, либо процессором используемой видеокамеры параллельно с видеозаписью<sup>1</sup>.



Рис. 19. Камера круговой съемки Ricoh Theta

<sup>1</sup> *Севастьянов П.В.* Цифровые технологии фиксации невербальной доказательственной информации : дис. ... канд. юрид. наук. М., 2024. С. 79

**Средства изготовления объемных копий следов** включают в себя средства для изготовления их гипсовых копий (смесь гипса и воды), применяемые для фиксации объемных следов обуви и босых ног, а также протекторов шин. Для изъятия следов орудий взлома и инструментов применяются силиконовые пасты.

**Средства 3D-моделирования** предназначены для проведения фиксации обстановки места происшествия, сбора необходимых материалов и информации для дальнейшего исследования. Сегодня 3D-технологии широко применяются в медицине, промышленности.

В основе этой технологии заложено формирование геометрии объекта через массивы точек и линий, образующих пересекающиеся плоскости. Полученные при сканировании координаты сохраняются в виде параметрических моделей, обрабатываемых специализированным программным обеспечением. Большинство современных 3D-сканеров способны определять расстояние до объекта и его форму, а также преобразовывать полученные данные в цифровое трехмерное изображение (рис. 20, 21).

3D-сканирование возможно эффективно применять при осмотре места происшествия для воспроизводства с высокой точностью обстановки на обследуемом участке местности. Данная технология позволяет решить ряд задач: анализ трасологических следов, определение траектории пули, оценка параметров взрывных устройств, реконструкция ДТП и т. д.

Эти методы превосходят традиционные подходы по детализации и точности данных, позволяют производить осмотр места происшествия в кратчайшие сроки с получением изображений и видеоряда обстановки места происшествия с различных ракурсов и высокой детализацией объектов. При помощи специализированного программного обеспечения выстраивается точная 3D-модель объекта осмотра с последующим применением для метрологически корректных измерений, проверок, составления проекций и моделирования различных ситуаций. В комплект входит квадрокоптер, фотокамера, специализированное программное обеспечение для проведения измерений и обработки получаемых изображений, а также рабочая станция для построения 3D-моделей<sup>1</sup>.

Положительный опыт использования технологий 3D-сканирования и 3D-моделирования при фиксации обстановки на месте происшествия

---

<sup>1</sup> *Севастьянов П. В.* Там же. С. 116.

имеется в полиции Австралии, Великобритании, США, Израиля и еще ряда государств<sup>1</sup>.

Процесс 3D-моделирования заключается в математическом координатном представлении объекта фиксации в трех измерениях с помощью специальных технических средств и программного обеспечения.

К основным видам 3D-моделирования относятся: каркасное, поверхностное, твердотельное, гибридное. Основные технологии 3D-сканирования: фотограмметрия, сканирование с использованием структурированного света, лазерное триангуляционное сканирование, сканирование на основе лазерных импульсов, контактное сканирование с использованием датчика<sup>2</sup>.

Технология 3D-сканирования применима для фиксации доказательственной информации и создания объемных цифровых моделей реальных объектов. Она применима в ситуациях, когда традиционные криминалистические средства и методы не достаточно эффективны. Так, фотосъемка предметов и объемных следов не всегда позволяет зафиксировать ряд криминалистически значимых признаков на двухмерном изображении, что ограничивает возможности проведения по ним сравнительного исследования. Трехмерные же цифровые модели наблюдаемых объектов устраняют указанный недостаток.

Несмотря на то, что 3D-сканеры обеспечивают возможность передачи цвета, текстуры поверхности и иных особенностей объектов, могут применяться в труднодоступных местах и достаточно просты в использовании, существуют определенные ограничения возможности их применения, в частности:

- отдельные модели сканеров не способны распознавать прозрачные или черно-белые объекты (обработка объектов специальными матирующими спреями или красящими составами может исказить точность передачи идентификационных признаков в исследуемых следах);
- объекты сложной структуры не всегда корректно отображаются в построенной 3D-модели;
- для работы со сканером и программным обеспечением требуется специальная подготовка операторов.

---

<sup>1</sup> *Еремченко В.И.* Анализ зарубежного опыта использования 3D-сканеров на месте происшествия и перспективы их внедрения в деятельности полиции России // Вестник Краснодарского университета МВД России. 2021. № 1 (51). С. 49–52.

<sup>2</sup> *Севастьянов П.В.* Указ. соч. С.100–101.



*Рис. 20.* Стационарный 3D-сканер «VT Mini»



*Рис. 21.* Портативный 3D-сканер «VT Laser»

В ЭКЦ МВД России проведены эксперименты, в ходе которых осуществлялось сканирование объемных следов при помощи 3D-сканеров различных типов: с использованием технологии

структурированного света и лазерного триангуляционного сканирования с последующим исследованием полученных цифровых моделей следов с точки зрения запечатления в них комплекса идентификационных признаков, индивидуализирующих следообразующие объекты. Результаты проведенных экспериментов позволяют прийти к следующим выводам<sup>1</sup>:

1. Полученные надлежащим образом полигональные модели объемных следов пригодны для идентификации следообразующих объектов и могут быть использованы в качестве объектов криминалистических экспертиз и исследований.

В них детально зафиксированы форма, размеры, расположение и взаиморасположение рельефа следообразующего объекта, а также особенности его внешнего строения (микрорельефа). При этом исследование общих и частных признаков следообразующих объектов, зафиксированных в 3D-моделях следов, возможно в трех плоскостях с применением методов измерения, сопоставления и наложения (самих моделей, а также их профилограмм (сечений плоскостей)).

2. Ключевым параметром для получения моделей, пригодных для идентификационных исследований, является оптимальное разрешение при их сборке:

2.1. Портативные сканеры с разрешением выше 0,2 мм, работа которых основана на принципе структурированного света (например, 3D-сканер «Calibry Mini»), могут использоваться для фиксации полноразмерных объемных трасологических следов, таких как следы подошв обуви, шин транспортных средств, некоторых видов статических следов орудий и инструментов и других следов (объектов).

2.2. Портативные 3D-сканеры с разрешением ниже 0,2 мм вне зависимости от принципа работы непригодны для фиксации небольших по размеру объемных статических и статико-динамических трасологических следов, а также объемных следов папиллярного узора рук.

2.3. Стационарные 3D-сканеры с разрешением выше 0,05 мм, работа которых основана на принципе структурированного света (на примере 3D-сканера «VT Mini»), могут использоваться для фиксации незначительных по размеру объемных статических и стати-

---

<sup>1</sup> Севастьянов П. В., Гаврилин Ю. В. Совершенствование методов и средств фиксации доказательственной информации на основе цифровых технологий // Вестник МВД России. 2025. №1. С. 63–69.

ко-динамических трасологических следов, а также объемных следов папиллярного узора рук.

Таким образом, применение 3D-сканирующих устройств может существенно оптимизировать процесс изъятия объемных следов, улучшить качество фиксации криминалистически значимой следовой информации, облегчить процессы ее хранения, передачи и последующего исследования, что в свою очередь позволит повысить результативность судебных экспертиз<sup>1</sup>.

Существенным преимуществом таких технических решений является возможность хранения, передачи и использования результатов сканирования в электронном виде. В дальнейшем этот потенциал можно использовать для создания автоматической информационной системы хранения 3D-моделей, что позволит оптимизировать процесс ведения учетов объемных следов и сохранять больше криминалистически значимой информации о них, чем это возможно с использованием традиционных средств фиксации. Это еще раз подчеркивает востребованность цифровой формы фиксации доказательственной информации, рассмотренной в настоящем исследовании.

Полученные результаты являются отправной точкой в процессе совершенствования технической и методической базы фиксации доказательственной информации цифровыми устройствами нового поколения при производстве экспертиз, исследований и осмотров мест происшествий. Перспектива изучения данного направления видится в дальнейшем раскрытии функциональных возможностей 3D-сканирующих устройств, которые находятся на стадии апробации, в оценке результатов использования описанных средств фиксации и их применения в целях сохранения и последующего исследования криминалистически значимой информации для установления истины по уголовным делам<sup>2</sup>.

К иным преимуществам подобной технологии относятся:

– быстрота изготовления модели (создание детализированных моделей, процесс сканирования, например, лазерного сканера Leica BLK360 (рис. 22) занимает около 30 сек., оператор может наблюдать и контролировать эту процедуру непосредственно в программе Recap Mobile Professional<sup>3</sup>;

---

<sup>1</sup> Севастьянов П. В. Указ. соч. С. 109.

<sup>2</sup> Там же. С. 109.

<sup>3</sup> Официальный сайт производителя «Leica Geosystems». URL: <https://leica-geosystems.com/ru/products/laser-scanners/scanners/blk360g1> (дата обращения: 11.04.2025).



*Рис. 22. Лазерный сканер Leica BLK360*



*Рис. 23. Портативный 3D-сканер Scantech AXE-B17*

- неразрушающий метод фиксации (технология не требует физического контакта с объектами, сохраняя целостность доказательств [следы обуви на снегу, отпечатки пальцев на неровной поверхности]);
- независимость от условий внешней среды (лазерные устройства способны работать в полной темноте, фиксируя дета-

ли на открытой местности или в помещениях без окон; лазерные 3D-сканеры практически не подвержены колебаниям условий окружающей среды, так как используют источники когерентного света);

- компактность (габариты портативного 3D-сканера Scantech AXE-B17 190x98x289 мм [рис. 23]);

- надежность (устройства устойчивы к вибрациям, перепадам температур и электромагнитным помехам);

- точность измерений (большинство 3D-сканеров, имеющих на рынке, обеспечивают погрешность менее 1 мм, что позволяет анализировать микроследы — царапины на металле, деформации пуль или следы инструментов при взломе).

**Беспилотные авиационные системы** с целевыми полезными нагрузками могут быть использованы для осмотра места происшествия, включая фото- и видеофиксацию материальной обстановки (в том числе в различных зонах спектра), 3D-моделирование, поиск следов и иной криминалистически значимой информации.

Применение БАС позволяет фиксировать обстановку места происшествия в режиме реального времени, обеспечивать безопасность участникам осмотра, передавать информацию в режиме реального времени на планшетный компьютер или иное цифровое устройство специалиста. При этом их применение не ограничивается осмотром места происшествия – есть положительные примеры их результативного использования в рамках оперативно-розыскной деятельности, охраны общественного порядка, раскрытия преступлений «по горячим следам», преследовании скрывающегося преступника.

Кроме того, в процессе экспертно-криминалистической деятельности БАС позволяют осуществлять:

- радиоэлектронную разведку (аэро-, видео- и аэрофотосъемку) воздушных, надводных и наземных объектов, целей и территорий, мониторинг оперативной обстановки;

- поиск, обнаружение, распознавание и сопровождение (отслеживание перемещения) интересующих физических лиц и транспортных средств на участках местности;

- контроль с воздуха за проведением митингов, демонстраций, шествий и пикетирований, а также культурно-зрелищных, спортивных и других мероприятий, связанных с массовым скоплением людей;

- координацию действий следственно-оперативных групп и сотрудников подразделений ОВД, находящихся на земле;

- связь, передачу и ретрансляцию команд и оперативно значимой информации;
- постановку помех для подавления средств связи правонарушителей при проведении специальных операций;
- трансляцию громкоговорящих голосовых сообщений (оповещение населения).

Для осмотра места происшествия целесообразно использовать БАС коптерного типа специального назначения – профессионального сегмента, поскольку их функции, возможности и качество изготовления на порядок выше любительской категории<sup>1</sup>.

Еще одна сфера применения подобных устройств связана с возможностью их предварительного направления на место происшествия до выезда следственной группы, что позволит уточнить характер произошедшего события, уточнить состав следственной группы, зафиксировать обстановку на месте происшествия, принять иные необходимые организационные решения.

Основными требованиями к БАС, используемым в криминалистическом обеспечении, являются<sup>2</sup>:

- возможность круглосуточного применения;
- повышенная помехоустойчивость от неблагоприятных внешних условий (атмосферные явления, метеорологические условия, электромагнитные излучения и др.);
- низкая радиолокационная, радиотехническая, магнитная, акустическая, тепловая, оптическая и визуальная заметность;
- оснащение БАС средствами дистанционного распознавания и предупреждения столкновений в воздухе с пилотируемыми воздушными судами, обеспечивающими безопасное выполнение совместных полетов;
- использование защищенных, высокоскоростных, помехоустойчивых каналов управления и передачи данных;
- обеспечение полной информационно-технической совместимости с системами связи и информации, принятыми на снабжение МВД России;
- унификация модулей полезной нагрузки с возможностью их замены, ремонта и модернизации в ходе эксплуатации;

---

<sup>1</sup> Использование цифровых технологий в технико-криминалистическом обеспечении осмотров мест происшествий: практические рекомендации / П. В. Севастьянов [и др.]. М., 2022. С. 12.

<sup>2</sup> Кубасов И. А., Сушков В. И. О концептуальном подходе к развитию и применению беспилотных авиационных систем специального назначения // Вестник Воронежского института ФСИН России. 2023. № 4. С. 86–95.

- возможность одновременного применения и управления требуемым количеством БАС с одной станции дистанционного управления;
- автоматический (автоматизированный) взлет (старт) и посадка (возвращение в район посадки) БАС на стартово-посадочные (посадочные) площадки;
- возможность рационального сочетания автоматического (программного) и автоматизированного (с участием внешнего пилота) управления БАС и его целевой нагрузки;
- возможность изменения маршрута и профиля полета БАС;
- оснащение сертифицированным по требованиям безопасности информации базовым и специальным программным обеспечением;
- мобильность и транспортабельность;
- максимально возможная унификация процессов обслуживания комплексов и систем, а также обучения экипажей БАС;
- наличие программно-аппаратных средств, обеспечивающих тренажерную подготовку внешних пилотов без реального использования БАС;
- приоритетное использование комплектующих, материалов, компонентов полезной нагрузки и элементной базы отечественного производства, при необходимости использование импортных комплектующих с возможностью их последующей замены на аналогичные российского производства;
- возможность защиты оперативно-служебной (специальной) и телеметрической информации, циркулирующей в БАС, обеспечение имитозащиты радиоканала управления БАС криптографическими средствами, сертифицированными в установленном порядке по соответствующему классу.

Интерес в рамках исследования представляет квадрокоптер «Геоскан 401» (Россия) – это профессиональный аэрофотосъемочный комплекс с вертикальным взлетом и посадкой, разработанный российской компанией «Геоскан» (рис. 24). Комплекс может находиться в воздухе до 60 мин., развивая скорость до 50 км/ч. За вылет производится фотосъемка до 2,1 км<sup>2</sup>. Поддерживает различные полезные нагрузки до 2,5 кг, включая мультиспектральные камеры, лазерные сканеры и магнитометры<sup>1</sup>.

---

<sup>1</sup> Официальный сайт производителя «ГеоСпектр». URL: <https://www.geo-spektr.ru/bespilotnye-letatelnye-apparaty/kvadrokoptery/geoscan/geoskan-401-geodeziya.html> (дата обращения: 11.04.2025).



*Рис. 24. Квадрокоптер «Геоскан 401» (Россия)*



*Рис. 25. Квадрокоптер DJI Mavic Pro*

Можно рассматривать и более бюджетный вариант БАС – DJI Mavic Pro (Китай) – компактный складной квадрокоптер, оснащенный 4К-камерой с 3-осевым стабилизатором, GPS-модулем, системой избегания препятствий и временем полета до 27 мин (рис. 25)<sup>1</sup>. Обладает высокой автономностью, качеством камер и системами стабилизации, имеется возможность установки тепловизоров, динамиков и другого оборудования, что делает подобные дроны универ-

---

<sup>1</sup> Официальный сайт производителя «DJI». URL: <https://www.dji.com/ru/mavic/info?ysclid=masoxlnjqz307837520> (дата обращения: 11.04.2025).

сальными. При этом уже появляются и более новые модели, например DJI Mavic 2 Enterprise Advanced с тепловизорами.

Относительно перспектив широкого внедрения БАС в оперативно-служебную деятельность МВД России следует отметить следующее. В связи с преобразованием внутренних войск МВД России в Федеральную службу войск национальной гвардии Российской Федерации и в соответствии с Указом Президента Российской Федерации от 5 апреля 2016 г. № 157 «Вопросы Федеральной службы войск национальной гвардии Российской Федерации» авиационные отряды специального назначения МВД России, являвшиеся эксплуатантами беспилотной авиационной техники, были включены в структуру Федеральной службы войск национальной гвардии Российской Федерации.

Организация и проведение совместных действий МВД России и Федеральной службы войск национальной гвардии показали, что для решения внезапно возникающих задач, требующих незамедлительного реагирования сотрудников полиции, МВД России должно располагать собственными силами и средствами для авиационного обеспечения оперативно-служебной деятельности. С этой целью в последние годы был проведен ряд мероприятий нормативно-правовой, организационно-штатной, технической и кадровой направленности.

В соответствии с приказом МВД России от 22 октября 2021 г. № 770 на департамент информационных технологий, связи и защиты информации МВД России возложены полномочия по обеспечению и осуществлению в пределах своей компетенции функции по выработке и реализации государственной политики, нормативному правовому регулированию в области организации применения и эксплуатации робототехнических комплексов и беспилотных воздушных судов.

## **2. Средства обнаружения, фиксации и изъятия цифровых следов преступления**

В условиях цифровой трансформации преступности, проявляющейся в изменениях механизма совершения преступлений, предусматривающих использование информационно-телекоммуникационных технологий при их подготовке, совершении или сокрытии, определяющее значение приобретает развитие криминалистических методов и средств обнаружения, фиксации и изъятия цифровых следов преступления. Последние представляют собой результаты преобразования компьютерной информации в форме уничтожения, копирования, блокирования или модификации, а также соответствующие им изменения физических характеристик ее носителя,

причинно связанные с событием преступления. Они позволяют установить лицо, совершившее преступление, идентифицировать орудия его совершения, а также иные значимые обстоятельства.

Цифровые следы материальны по своей природе, возникают на электронных носителях информации, а механизм их образования определяется технологией записи информации. Их можно обнаружить посредством преобразования с использованием аппаратно-программного обеспечения.

К цифровым следам относятся признаки, идентифицирующие компьютерную информацию: имя файла, его размер и формат, свойства (дата и время создания, автор и другие метаданные), переписка пользователей посредством отправления электронной почты и сервисов мгновенного обмена сообщениями, фото- и видеоизображения, биллинговая информация (данные о входящих и исходящих вызовах и сообщениях, их продолжительность, привязка к базовым станциям сотовой связи), данные геолокации (маршрутов движения), контакты, IMEI-номера<sup>1</sup> и MAC-адреса<sup>2</sup> устройств, IP-адреса<sup>3</sup>, телефонные номера и др.

К числу цифровых следов, позволяющих установить личность отправителя электронного сообщения, относятся: никнейм (сетевой псевдоним пользователя), адрес электронной почты и номер телефона, привязанный к нему при регистрации, фотография или аватар (изображение, графический объект), рекламные идентификаторы, геолокационная информация, данные о соединении и устройстве пользователя, платежные реквизиты, публичные переписки и участие в сообществах, иные связанные веб-узлы и уникальные идентификаторы<sup>4</sup>.

Криминалистические средства работы с цифровыми следами преступления включают в себя:

---

<sup>1</sup> IMEI (от англ. International Mobile Equipment Identity – международный идентификатор мобильного оборудования) – это уникальный 15-значный идентификационный номер мобильного устройства, который позволяет идентифицировать его в сети оператора.

<sup>2</sup> MAC-адрес (от англ. Media Access Control – управление доступом к среде) – идентификатор, присваиваемый производителем каждой единице сетевого адаптера соответствующего устройства (ноутбука, нетбука, планшетного ПК, смартфона).

<sup>3</sup> IP-адрес (от англ. Internet Protocol Address) – уникальный сетевой адрес компьютера (сервера), построенный на основе протокола адресации IP в виде четырех десятичных чисел значением от 0 до 255, разделенных точками.

<sup>4</sup> Гаверилин Ю. В., Салеева Ю. Е. Развитие учения о криминалистической регистрации в условиях цифровой трансформации преступности // Труды Академии управления МВД России. 2023. № 2 (66). С. 99–105.

**Средства поиска информации на электронных носителях**, обладающей определенными характеристиками, с использованием методов: логического извлечения (копирования) данных, физического извлечения данных, извлечения данных из интегральной схемы памяти, обхода парольной защиты, извлечения и анализа метаданных<sup>1</sup>. Кроме того, современные средства извлечения данных из цифровых устройств позволяют выполнять и логические операции по анализу данных. Так, аппаратно-программный комплекс «Мобильный криминалист» (рис. 26) дает возможность извлекать данные из большинства моделей мобильных устройств, импортировать резервные копии устройств, получать данные из облачных хранилищ, загружать и анализировать информацию о соединениях абонентов (абонентских устройств), извлекать контакты, сообщения, звонки, файловую систему, местоположения и удаленную информацию, находить общие места пребывания нескольких лиц и строить маршруты их передвижения на карте, выявлять общие связи между несколькими устройствами и устанавливать круг общения пользователя, анализировать контент по ключевым словам, регулярным выражениям посредством фильтров для быстрого поиска информации.



Рис. 26. АПК «Мобильный Криминалист»

<sup>1</sup> Гаверилин Ю.В. Развитие методов цифровой криминалистики: пределы допустимости // Уголовный процесс и криминалистика: теория, практика, дидактика : сб. материалов VII Всеросс. науч.-практ. конф. Рязань, 16 декабря 2021 г. Рязань, 2022. С. 69–75.



Для восстановления данных с мобильных устройств используются аппаратно-программные комплексы PC-3000 Mobile, а также Elcomsoft Mobile Forensic Bundle, предназначенные для извлечения данных из мобильных устройств методами физического, логического и «облачного» анализа.

Для восстановления паролей сегодня применяются:

Elcomsoft Distributed Password Recovery – восстанавливает пароли к архивам и зашифрованным файлам, ускоряя доступ к критической информации.

Elcomsoft Premium Forensic Bundle / Elcomsoft Desktop Forensic Bundle – используются для снятия парольной защиты и мобильной криминалистики.

Для извлечения данных из персональных компьютеров, ноутбуков и серверов на операционных системах Windows, macOS, GNU/Linux, внешних подключенных дисков, физических образов E01, RAW (DD/BIN/IMG), DMG, ISO, логических образов L01, AD1, архивов ZIP, 7Z, RAR, TAR и образов виртуальных жестких дисков виртуальных машин VDI, VHD, VMDK с файловыми системами NTFS, FAT, EXFAT, EXT2, EXT3, EXT4, HFS, HFS+, APFS используется СПО – Мобильный Криминалист Десктоп, – которое поддерживает работу с образами дисков и виртуальными машинами, упрощая анализ данных без риска их повреждения.

**Средства поиска информации в сетевом пространстве**, основанные на методах парсинга<sup>1</sup>, логгирования, анализа связей цифровых идентификаторов лица (аккаунт в социальных сетях, электронная почта, номер телефона, никнейм, фотография, IP-адрес, цифровой профиль устройства и т. п.), эвристического метода, кластерного анализа, анализа графов<sup>2</sup>.

Для анализа приведенных выше данных может применяться специализированное программное обеспечение «Аналитический Центр Криминалист», позволяющее одному или нескольким пользователям в любой момент одновременно анализировать большие объемы данных из полной базы загруженных извлечений, хранящихся на сервере.

---

<sup>1</sup> Парсинг представляет собой метод собирания и систематизации компьютерной информации, размещенной на определенных Интернет-страницах, с помощью специальных программ, автоматизирующих процесс ее синтаксического анализа и структурирования.

<sup>2</sup> Гаверилин Ю.В. Развитие методов цифровой криминалистики: пределы допустимости // Уголовный процесс и криминалистика: теория, практика, дидактика : сб. материалов VII Всеросс. науч.-практ. конф. Рязань, 16 декабря 2021 г. Рязань, 2022. С. 69–75.

Определение местоположения цифровых устройств, оснащенных модулями Wi-Fi, в том числе замаскированных и скрытых преградами<sup>1</sup>, позволяет технология Wi-Peep.

К иным группам технических средств для работы с доказательственной цифровой информацией относятся:

- средства поиска следов определенных манипуляций с компьютерной информацией в процессе ее создания, обработки, изменения, копирования, уничтожения на основе методов анализа резервных копий, журналов операций (log-файлов), списка последних запускаемых программ и последних файлов, к которым обращается пользователь, данных файла подкачки оперативной памяти, информации о пути к исполняемым приложениям и пр.;

- средства определения свойств и функциональных возможностей программного обеспечения на основе методов реверс-инжиниринга, исследования исходных текстов программного обеспечения (включая статический и динамический анализ), исследования загрузочных модулей (исполняемых кодов) и анализа графов;

- средства определения свойств и функциональных возможностей информационных систем и их периферийных устройств, а также установления определенных обстоятельств, имеющих значение для дела, путем изучения записей о различных действиях пользователя исследуемого персонального компьютера за определенный период времени;

- средства построения хронологической последовательности событий в информационной системе и выявления периодов активности пользователя;

- средства криминалистического копирования информации, обеспечивающие неизменность исходной информации и создание ее байтовой копии на другом электронном носителе.

Говоря о допустимости применения вышеназванных средств, следует отметить следующее. Согласно ст. 75 УПК РФ доказательства, полученные с нарушением порядка, установленного уголовно-процессуальным законом, являются недопустимыми. Более подробно свойство допустимости доказательств раскрывается в постановлении Пленума Верховного Суда Российской Федерации от 31 октября 1995 г. № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении

---

<sup>1</sup> Wi-Peep: особенности беспроводного подглядывания // Kaspersky : сайт. URL: <https://www.kaspersky.ru/blog/wi-peep-wireless-localization/34417/?ysclid=m9751slzb2187534028> (дата обращения: 06.04.2025).

правосудия»<sup>1</sup>, в соответствии с которым доказательства должны признаваться полученными с нарушением закона, если:

- 1) субъект собирания доказательств не имеет полномочий на проведение процессуального действия по их собиранию;
- 2) источник сведений о фактах (источник доказательства) не указан в законе;
- 3) способ собирания, закрепления и проверки сведений о фактах не предусмотрен законом;
- 4) порядок собирания, закрепления и проверки сведений о фактах должен соответствовать закону<sup>2</sup>.

Очевидно, современные технологии открывают значительный простор для всевозможных манипуляций с такой информацией, что может создавать предпосылки для признания ее недопустимым доказательством<sup>3</sup>. С учетом сказанного, специальными критериями оценки допустимости доказательственной информации, полученной в результате применения выше-названных методов, следует считать<sup>4</sup>:

*Аутентичность информации* как возможность достоверного установления источника ее происхождения, создавшего ее лица или процесса, порядка (процедур) ее создания. Проверимость источника происхождения доказательственной информации обеспечивается максимальной детализацией при описании порядка ее обнаружения и изъятия в протоколе следственного действия, с указанием вида использованного специального программного обеспечения, приложением составленных с его помощью формализованных отчетов, фиксацией содержимого экрана на различных этапах следственного действия, метаданных копируемых файлов (сопутствующей технологической информации), индивидуальных характеристик изымаемых электронных носителей и способов их упаковки.

*Достоверность информации*, т. е. ее соответствие реально происходящим явлениям, событиям и процессам. Обеспечивается механизмом (технологией) создания информации, соответствием

---

<sup>1</sup> Бюллетень Верховного Суда Российской Федерации. 1996. № 2.

<sup>2</sup> Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учеб. пособие / А. А. Балашова [и др.] ; под ред. Ю. В. Гаврилина, А. В. Победкина. М., 2021. С. 103–104.

<sup>3</sup> *Гаврилин Ю. В., Победкин А. В.* Модернизация уголовно-процессуальной формы в условиях информационного общества // Труды Академии управления МВД России. 2019. № 3 (51). С. 28.

<sup>4</sup> Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании. С. 110–116.

ему метаданных файла, научности методов восстановления уничтоженных и поврежденных данных, а также данных, доступ к которым ограничен посредством применения методов криптографической защиты.

*Целостность информации*, т. е. отсутствие изменений в ее составе, содержании и свойствах, что обеспечивается использованием средств криминалистического копирования информации (дубликаторов), обеспечивающих побайтовый перенос данных с одного электронного носителя на другой без модификации данных оригинала; использованием электронных носителей, не допускающих перезапись информации; эффективными средствами подтверждения целостности информации являются криптографическая защита изымаемой информации, а также использование электронной подписи должностного лица, проводящего следственное действие.

К перспективным технологиям работы со следовой и иной криминалистически значимой информацией на месте происшествия можно отнести следующие:

*Технология дополненной реальности и машинного зрения*, обеспечивающая совмещение материальных и цифровых объектов, а также наложение виртуальных изображений на картину реального события<sup>1</sup>. Применительно к задачам осмотра места происшествия эта технология способна в режиме реального времени предоставлять специалисту необходимые справочно-вспомогательные сведения об объектах осмотра, в частности, их точное наименование, конструктивное устройство, предназначение, технические характеристики, особенности управления и эксплуатации, технологии изготовления и сведения о производителе (рис. 28). Технология может быть реализована в виде аппаратно-программного комплекса, включающего в свой состав очки со встроенными видеокамерами, планшетный компьютер для вывода справочных данных и модуль беспроводной передачи данных для проверки объекта осмотра по криминалистическим учетам. В процессе работы на экран планшетного компьютера выводится справочная информация, помогающая специалисту на месте происшествия получить информационную поддержку.

---

<sup>1</sup> Маркин В.В. AR- и VR-технологии в современном обществе // Научный аспект. 2024. Т. 11. № 5. С. 1436–1440.



Рис. 28. Смарт-очки дополненной реальности «Xloong»

Повышению функциональных возможностей устройств на основе приведенных технологий может способствовать их интеграция со средствами 3D-сканирования. Положительные результаты проведенных опытов по проверке возможности использования подобной технологии в экспертно-криминалистической деятельности описаны в диссертационных исследованиях<sup>1</sup>.

Кроме того, технология машинного зрения может способствовать автоматизации формирования описательной части протокола осмотра места происшествия на основе распознавания объектов и их описания.

Заметим, что технологии преобразования устной речи в письменный текст успешно применяются в судах и органах расследования в ряде государств уже не одно десятилетие. Они способны повысить эффективность производства следственных действий, связанных с получением вербальной доказательственной информации (допросы, очные ставки). Вместе с тем в отдельных государствах внедрение цифровых технологий в уголовно-процессуальную деятельность связано, в первую очередь, с оцифровкой докумен-

---

<sup>1</sup> *Севастьянов П.В.* Цифровые технологии фиксации невербальной доказательственной информации : дис. ... канд. юрид. наук. М., 2024. С. 99–123.

тов на бумажных носителях, что фактически приводит к дополнительной нагрузке на следователей, а не к оптимизации их работы и избавлению от канцелярских функций. Подобная псевдоцифровизация создает лишь иллюзию цифровой трансформации правоохранительной деятельности, поскольку при этом остаются неизменными базовые принципы бумажного документооборота. Совершенствование технологии составления процессуальных документов возможно за счет внедрения программ распознавания устной речи и формирования текстового описания по фото- и видеоизображению<sup>1</sup>.

В целях проведения экспресс-анализов химического состава веществ, обнаруженных на месте происшествия, может использоваться технология **мобильной ускоренной хроматографии**, позволяющая оперативно идентифицировать наиболее распространенные контролируемые вещества<sup>2</sup>.



Рис. 29. Спектрометр microRAMAN

---

<sup>1</sup> Гаврилин Ю.В. Цифровая трансформация уголовно-процессуальной деятельности в контексте государственной научно-технической политики // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности : сб. науч. статей по материалам междунар. науч.-практ. конф. Москва, 26 мая 2023 г. М., 2023. Ч. 2. С. 40–46.

<sup>2</sup> Лисовская С. Б., Виноградова Н. И. Применение методов хроматографического разделения в судебной практике // Вестник Московского университета МВД России. 2018. № 4. С. 23–25.

В последние годы масс-спектрометрия (рис. 29) с ионизацией в окружающей среде, такая как прямой анализ в режиме реального времени (DART-MS), стала мощным инструментом правоохранительных органов США, позволяющим быстро проверять изъятые наркотики практически без подготовки образцов. Эти методы позволяют исключить этап хроматографического разделения и в течение нескольких секунд получать почти полный химический профиль жидкостей, порошков и других твердых веществ. Низкие пределы обнаружения (субнанограмм) и высокие уровни повторяемости были достигнуты для новых лекарственных средств, таких как аналоги фентанила, синтетические каннабиноиды и замещенные фенилэтиламины. Такие методы, как DART-MS, использовались для обнаружения новых структур синтетических психоактивных веществ, которые в противном случае было бы трудно идентифицировать с помощью традиционных методов, таких как ГХ-МС и жидкостная хроматографическая масс-спектрометрия (LC-MS)<sup>1</sup>.

Исследование следов биологического происхождения с последующей проверкой по криминалистическим учетам возможно посредством технологии **мобильного секвенирования**, позволяющей получать необходимую для идентификации геномную информацию в автономном режиме и проводить все стадии исследования ДНК на месте происшествия (рис. 30).



Рис. 30. Секвенатор MinIon

<sup>1</sup> Цвисти М., Сиско Э., Лурье И. Разработка и валидация метода экспресс-ГХ-МС для скрининга изъятых наркотиков // Sciencedirect : сайт. URL: <https://www.sciencedirect.com/science/article/abs/pii/S2468170923000152> (дата обращения: 10.05.2025).

**Мобильные робототехнические комплексы** позволяют под управлением оператора производить осмотр в труднодоступных и опасных местах, а также сбор и экспресс-анализ следов, образцов и иных объектов. Такой комплекс представляет собой управляемую самоходную платформу с манипуляторами, видеокамерами, источниками света и средствами для отбора образцов химических веществ во время осмотра мест происшествий, связанных с использованием потенциально опасных для жизни и здоровья эксперта веществ.

Развитие методов и средств криминалистической регистрации связано с возможностями использования технологий на основе *искусственного интеллекта*, учетом цифровых следов и биометрической информации.

На основании публикаций в открытых источниках о направлениях научно-исследовательских и опытно-конструкторских работ в области использования ИИ в правоохранительной сфере ранее нами выделялись следующие задачи, эффективность решения которых может быть повышена за счет применения технологий ИИ<sup>1</sup>:

– выявление признаков синтеза речи и изображений («дипфейков»);

– распознавание объектов при проведении идентификационных исследований (компьютерное зрение);

– анализ материалов уголовного дела, выдвижение следственных версий и определение алгоритмов действий следователя;

– моделирование событий преступления на основе его следов и выявление признаков серийности преступлений;

– раннее предупреждение совершения преступлений на основе прогнозирования будущих криминальных событий, включая распознавание признаков противоправных действий при проведении финансовых транзакций и заключении хозяйственных договоров;

– контентный и семантический анализ текстов для оценки психологического состояния их автора, а также скрытых смыслов, заложенных в сообщениях и др.

В деятельности экспертно-криминалистических подразделений России и зарубежных стран находят свое применение следующие технологии, основанные на использовании искусственного интеллекта:

---

<sup>1</sup> Гаприлин Ю. В., Бородина А. А. Обеспечение достоверности результатов применения технологий на основе искусственного интеллекта в экспертно-криминалистической деятельности // Судебная экспертиза. 2024. № 2 (78). С. 52–61.

*Интеллектуальный анализ данных.* Эта технология позволяет обрабатывать большие массивы структурированных и неструктурированных данных для выявления скрытых закономерностей. Так, например, полиция США применяет программу от израильской компании Zencity. Система анализирует публичные записи и комментарии в социальных сетях, определяя, о чем говорят пользователи, и составляет отчет на основе этих данных. Из-за большого объема предсказывать отдельные преступления сложно, но разработчики утверждают, что программа помогает полиции отслеживать общественные настроения и предотвращать протесты, массовые беспорядки<sup>1</sup>.

*Компьютерное зрение.* Используется для распознавания объектов, лиц и действий на видео. В России примером может выступать использование технологии компьютерного зрения для предупреждения правонарушений и розыска преступников по изображениям лиц (аппаратно-программный комплекс «Безопасный город»).

*Анализ фото-, видеоизображений и аудиосообщений, модифицированных с применением нейросетевых технологий.* К числу основных функций систем видеоаналитики можно отнести следующие: классификация объекта; идентификация (распознавание) объекта; распознавание действий; сегментация фона; трекинг; подсчет объектов и др.

Еще одной перспективной задачей видеоаналитики видится улучшение визуального восприятия и выделение объектов на цифровых изображениях. Решение этой задачи возможно путем математической обработки цифровых изображений в целях улучшения визуального восприятия объектов, распознавания и выделения среди других объектов. В частности, цифровая обработка фотоизображения лица человека с учетом возможных возрастных изменений (старения) имеет потенциал в решении задач идентификации личности гражданина на основе распознавания физиологических особенностей и особых примет.

Перспективными направлениями использования ИИ при расследовании преступлений считаем также разработку средств анализа фото-, видеоизображений и аудиосообщений, модифицированных с применением нейросетевых технологий. Назначением подобных средств является определение вероятности внесения

---

<sup>1</sup> Ваганова Д. Робокоп и детекторы выстрелов: технологии будущего на службе полиции // РБК : сайт. URL: <https://trends.rbc.ru/trends/industry/61e145ed9a794785b12743b9?from=copy> (дата обращения: 10.05.2025).

модификаций в аудио- или видеоконтент с использованием нейросетевых аналитических технологий<sup>1</sup>.

*Контентный и семантический анализ.* Программы анализируют тексты в соцсетях, мессенджерах и электронных письмах для выявления угроз различного типа. На российском рынке представлена разработка ИСП РАН Texterra, представляющая собой платформу для анализа русскоязычных текстов. Она способна адаптироваться к сленгу и выявлять неявные упоминания объектов. ПО такого рода возможно использовать для анализа социальных медиа<sup>2</sup>.

*Системы поддержки принятия решений и автоматизация процессов.* Эти инструменты предоставляют рекомендации на основе анализа данных. Понятно, что технологии ИИ не могут подменять процесс экспертного исследования, а способны лишь обеспечить поддержку принятия решений, автоматизируя определенные операции, выполняемые в процессе производства экспертизы.

Разработка инструментов для поддержки принятия решений на основе технического анализа цифровых изображений направлена на выявление идентификационных признаков фото- и видеозаписывающих устройств для принятия решений при производстве экспертных исследований. При этом производится поиск и систематизация групповых признаков фото-, видеозаписывающих устройств, выделение индивидуализирующих следов и особенностей конкретных устройств при техническом анализе цифровых изображений (в том числе из фото- и видеоконтента мессенджеров и социальных сетей).

На примере почерковедческой экспертизы можно констатировать, что внедрение программных продуктов на основе нейросетей позволяет существенно улучшить качество и полноту заключений эксперта, создать условия для всестороннего и более точного анализа, выстроить структуру исследования в соответствии с имеющимися методиками, предоставить доступ к постоянно обновляющейся методической литературе для проведения исследований самых разнообразных объектов; позволит создать многофункциональный и адаптивный инструмент, способный учитывать большое количество разнообразных факторов, подстраиваться под текущую экспертную ситуацию для оформления заключений эксперта-почерковеда и иллюстрационных таблиц к ним. Это может обеспечить высокую эффективность и определенную стандартизацию процесса

---

<sup>1</sup> Гаверилин Ю. В., Бородин А. А. Указ. соч. С. 52–61.

<sup>2</sup> Texterra: базовый семантический анализатор // ИСП РАН : сайт. URL: <https://www.ispras.ru/technologies/texterra/> (дата обращения: 10.05.2025).

составления заключения эксперта, даст возможность в автоматизированном режиме быстро и качественно изготавливать иллюстрационные таблицы с соблюдением всех криминалистических правил, повысит качество и надежность выводов эксперта-почерковеда.

Главным управлением криминалистики Следственного комитета Российской Федерации была разработана специализированная нейросетевая программа Crimeserieslinkage, позволяющая строить поисковый портрет серийного преступника, выявлять в массиве нераскрытых деяний те, которые носят серийный характер и совершены одним и тем же субъектом, устанавливать наиболее вероятного подозреваемого из числа лиц, учтенных в базе данных об уже привлеченных к уголовной ответственности преступниках. При этом программой анализируется такая информация, как расстояние от места жительства преступника до места преступления, возраст совершившего деяние лица, наличие у него судимости и психического заболевания, а также факт использования автотранспорта и наличия связи с потерпевшим до реализации преступного замысла<sup>1</sup>.

Основным препятствием активного внедрения технологий ИИ видится некоторое противоречие между сущностными свойствами данных технологий и базовыми принципами уголовно-процессуальной и экспертно-криминалистической деятельности.

Нейросетевые технологии, направленные на имитацию мыслительных процессов человека на основе самообучения, не обеспечивают в должной мере воспроизводимость полученных результатов в силу отсутствия заранее определенного алгоритма принятия решений. В этой связи технологии ИИ не могут подменять процесс экспертного исследования, а способны лишь обеспечить поддержку принятия решений, автоматизируя определенные операции, выполняемые в процессе производства экспертизы. Они могут рассматриваться как дополнительные методы, которые объективизируют полученные результаты при условии, что они соответствуют экспертным методикам, обеспечивают достоверность выводов и воспроизводимость полученных результатов.

Так, внедрение программных продуктов на основе нейросетевых технологий в методику производства почерковедческой экспертизы может существенно улучшить качество и полноту заключений эксперта, создать условия для всестороннего и более точного

---

<sup>1</sup> Бардаченко А. Н., Евстропов Д. А. Использование технологии для установления обстоятельств применения огнестрельного оружия на месте происшествия // Актуальные проблемы криминалистики и судебной экспертизы : сб. материалов междунар. науч.-практ. конф., посвященной 105-летию Экспертно-криминалистической службы МВД России. Иркутск, 6–7 июня 2024 г. Иркутск, 2024. С. 91–95.

анализа, выстроить структуру исследования в соответствии с имеющимися методиками, предоставить доступ к постоянно обновляющейся методической литературе для проведения исследований самых разнообразных объектов; позволит создать многофункциональный и адаптивный инструмент, способный учитывать большое количество разнообразных факторов, подстраиваться под текущую экспертную ситуацию для оформления заключений эксперта-почерковеда и иллюстрационных таблиц к ним. Все эти преимущества должны обеспечить высокую эффективность и определенную стандартизацию процесса составления заключения эксперта, позволят в автоматизированном режиме быстро и качественно изготавливать иллюстрационные таблицы с соблюдением всех криминалистических правил, повысят качество и надежность выводов эксперта-почерковеда.

В связи с вышесказанным на передний план выходят вопросы оценки качества систем ИИ на стадиях их разработки, создания и эксплуатации в целях подтверждения необходимого уровня их соответствия установленным требованиям. Наличие грамотно выстроенной системы оценки качества обеспечивает доверие к системам ИИ на физическом уровне при условии выполнения требований к обеспечению надежности, безопасности и функциональности<sup>1</sup>.

Для получения достоверных результатов оценки качества систем искусственного интеллекта целесообразно, чтобы установленные показатели обладали следующими характерными свойствами, определяющими точность проводимых измерений согласно ГОСТ Р ИСО 5725-1:

1) достоверность – влияние случайных ошибок на результат измерения незначительно или может быть учтено в процессе анализа, т. е. не может повлиять на результат измерения;

2) воспроизводимость – повторное измерение показателя для той же системы с использованием той же самой шкалы ранжирования и оценки, входных данных и условий проведения тестирования различными специалистами по оценке качества должно привести к тем же самым результатам в пределах соответствующей погрешности;

3) повторяемость (также сходимостью результатов измерений) – близость друг к другу результатов измерений одной и той же величины, выполненных повторно одними и теми же средствами, одним

---

<sup>1</sup> Гаверилин Ю. В., Бородин А. А. Указ. соч. С. 52–61.

и тем же методом в одинаковых условиях и с одинаковой тщательностью.

Для оценки функциональных возможностей систем искусственного интеллекта применяется следующий набор функциональных субхарактеристик:

- полнота, используемая для оценки степени покрытия совокупностью функций исследуемой системы всех определенных задач и целей пользователя в условиях отсутствия предвзятости (необъективности);

- корректность (правильность), используемая для оценки обеспечения точности результатов, а также частоты встречаемости ошибок и недопустимых отклонений;

- пригодность, используемая для оценки степени функционального упрощения выполнения определенных задач и достижения целей;

- способность к самообучению, используемая для оценки уровня владения системы умением автоматически извлекать знания из накопленного опыта и применять их для улучшения качества решения поставленных задач.

Говоря о достоверности результатов применения систем ИИ, необходимо обратить внимание на еще одно важное обстоятельство – достоверность исходных данных. Остается открытым вопрос о том, насколько полные, достоверные и качественные данные с места совершения преступления будут предложены на рассмотрение ИИ. Если предположить, что изначальные данные будут содержать ошибку или неточность, то высока вероятность того, что ИИ воспримет их неправильно и сделает неточные или ошибочные выводы.

Таким образом, обеспечение доверия к системам ИИ в процессе выявления, раскрытия, расследования и предупреждения преступлений должно строиться на основе национальных стандартов, регламентирующих как общие, так и отраслевые требования к качеству систем ИИ и методам их испытаний.

К числу перспективных **объектов криминалистической регистрации** могут относиться цифровые профили лиц и устройств.

Цифровой профиль личности как совокупность цифровых записей, содержащихся в различных информационных системах<sup>1</sup>,

---

<sup>1</sup> О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах (вместе с «Положением о проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах») [Электронный ресурс] :

основан на информационных ресурсах МВД России, ФНС России, Банка России, ФССП России, Социального фонда России и включает в себя массив данных о лице, образующийся при оказании государственных услуг и осуществлении контрольно-надзорной деятельности. В него могут входить данные миграционного учета, сведения о судимости, доменах, удостоверяющих личность, участии в управлении юридическими лицами, исполнительных производств, судебных актах, зарегистрированном недвижимом имуществе, социальных выплатах, документах об образовании и пр. К дополнительным сведениям о лице может относиться информация из открытых источников, включая социальные сети и иные интернет-сервисы: фото- и видеоизображения, круг контактов, личный идентификатор. Организаторы распространения информации в сети Интернет располагают сведениями о дате и времени регистрации пользователя, указанной им при этом информации, использованном IP-адресе, номере телефона, адресе электронной почты и др.<sup>1</sup> Кроме того, цифровой профиль может формироваться с учетом сведений, содержащихся в Единой системе идентификации и аутентификации<sup>2</sup>.

Электронные профили цифровых устройств могут формироваться на основе особенностей настроек браузера и операционной системы, технических характеристик устройства, а также поведенческих стереотипов его владельца.

Совершение операций с **цифровыми валютами** сопровождается возникновением следующего комплекса следовой информации: дата и время приобретения, продажи, обмена, перевода цифровой валюты, адреса криптовалютных кошельков отправителя и получателя, используемая обменная площадка (биржа)<sup>3</sup>.

---

постановление Правительства Рос. Федерации от 3 июня 2019 г. № 710 // Доступ из СПС «КонсультантПлюс» (дата обращения: 11.05.2025).

<sup>1</sup> См. ст. 10.1 Федер. закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. I). Ст. 3448.

<sup>2</sup> О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [Электронный ресурс] : постановление Правительства Рос. Федерации от 28 нояб. 2011 г. № 977 // Доступ из СПС «КонсультантПлюс» (дата обращения: 11.05.2025).

<sup>3</sup> *Гаверилин Ю. В., Бедеров И. С.* Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учеб. пособие. М., 2022. С. 11.

Указанные цифровые следы, находясь в причинно-следственной связи с событием преступления и являясь криминалистически значимой информацией, могут относиться к объектам криминалистической регистрации.

Одним из направлений развития учения о криминалистической регистрации в условиях цифровой трансформации преступности видится совершенствование способов учета на основе внедрения цифровых технологий. В этой связи весьма перспективным видится внедрение технологий комплексной обработки видео- и фотоинформации и внедрения систем технического зрения с применением:

- алгоритмов геометрического совмещения изображений в режиме реального времени;
- способов совместной визуализации анализируемых и сравниваемых изображений, обеспечивающих максимально полную информацию о состоянии следов, а также об особенностях микрорельефа отдельных трасс каждого отдельного следа;
- алгоритмов автоидентификации следообразующих объектов по их следам, а именно: совмещения координат местоположения, геометрических и пространственных характеристик, углов позиционирования трасс, рельефной следовой картины.

С использованием вышеперечисленных программных технологий решается и не менее важная задача, являющаяся неотъемлемым элементом надежного и результативного алгоритма автоидентификации, – устранение субъективности человеческого фактора при разметке и кодировании следов вручную. Использование алгоритмов сопоставления проверяемого объекта и изображения следа на следовоспринимающей поверхности способно повысить качество трасологических исследований.

Решение подобной задачи требует комплексной проработки правовых, технических и организационных вопросов в рамках единой государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности.

Сегодня правоохранительными органами используются:

### **1. Трасологические системы:**

**1.1. Автоматизированная трасологическая идентификационно-поисковая система «СЛЕД-12»**, которая позволяет:

- проводить множественные настройки фильтрации следов;
- ведение различных журналов;
- выводить графические изображения на монитор, печать журнала, списков, справок, статистической информации.

**1.2. Экспертная система следов протекторов шин**, которая обладает следующими возможностями:

- проведение поиска типа «след-след», «оттиск-след», «след-оттиск», «поиск в найденном»;
- проведение многообразных выборок, сортировка, удаление и редактирование записей;
- формирование журнала шин и следов шин.

**1.3. Экспертная система следов орудий взлома**, которая обеспечивает:

- ввод и хранение в базе данных изображений следов орудий взлома и сопроводительной информации;
- поиск по векторному и словесному описанию;
- автоматизированную аналитическую систему генерации отчетов.

**2. Баллистические системы**, обеспечивающие:

- хранение информационных данных учета и цифровых изображений пуль и гильз;
- доступ пользователей к хранящимся на сервере информационным данным учета и цифровым изображениям пуль и гильз;
- ведение информационного учета пуль и гильз;
- сканирование пуль и гильз;
- кодирование пуль и гильз;
- сравнительное исследование цифровых изображений пуль и гильз.

В основу построения автоматизированных информационных баллистических систем положена технология автоматизации дактилоскопических экспертиз и учетов, в том числе дактилоскопической идентификации.

Применяемые в настоящее время автоматизированные информационные баллистические системы обладают следующими возможностями:

- автоматическое определение граней нарезов, следов бойка, патронного упора;
- работа со следами нарезного и травматического оружия;
- поддержка сканирующих устройства;
- проведение сравнительных исследований 3D-изображений в режиме геодезической расцветки;
- одновременное исследование нескольких изображений объектов;
- формирование текстового отчета с изображениями;
- адаптация под наиболее распространенные операционные системы и др.<sup>1</sup>

---

<sup>1</sup> Возможности применения цифровых технологий при производстве баллистических экспертиз и ведения баллистических учетов : аналитический обзор с предложени-

Современные баллистические информационные системы обладают способностью автоматически размечать криминалистически значимые следы на пулях и гильзах, что значительно ускоряет процесс идентификации. Кроме того, мультипользовательский поиск позволяет использовать сетевые информационные ресурсы для сокращения времени идентификации<sup>1</sup>.

С целью определения возможностей использования нейросетевых технологий для решения диагностических и классификационных задач в ходе предварительного исследования следов и объектов на месте происшествия авторским коллективом на кафедре трасологии и баллистики УНК ЭКД Волгоградской академии МВД России совместно с ООО «Сбер Бизнес Софт» был реализован пилотный проект по созданию прототипа модели ИИ, устанавливающей на основании фотографий боковой и донной поверхности гильзы наименование патрона, частью которого она являлась, и определяющей перечень моделей огнестрельного оружия, для стрельбы из которого этот патрон предназначен.

Сотрудники Волгоградской академии МВД России осуществили экспериментальный отстрел различных образцов огнестрельного оружия. Объекты предоставлялись также из Экспертно-криминалистического центра ГУ МВД России по Волгоградской области, Управления Федеральной службы войск национальной гвардии Российской Федерации по Волгоградской области, с полигона войсковой части 33180 Министерства обороны Российской Федерации. Особую ценность имеют гильзы патронов иностранного производства, предоставленные МВД по Донецкой Народной Республике из зоны проведения специальной военной операции. В результате массив объектов составили гильзы подавляющего большинства используемых в настоящее время пистолетных, револьверных, промежуточных и винтовочных патронов стрелкового нарезного огнестрельного оружия отечественного и иностранного производства. При этом варьировались средства фиксации (зеркальный цифровой фотоаппарат, беззеркальный цифровой фотоаппарат, камера сотового телефона) и условия съемки (вид освещения [естественное, искусственное, вспышка фотоаппарата/сотового телефона], угол съемки и т. д.). Всего было получено более 10 тыс. фотографий<sup>2</sup>.

---

ями (п. 35 Плана научного обеспечения деятельности органов внутренних дел Российской Федерации на 2024 год; заявка ГУ МВД России по г. Санкт-Петербургу и Ленинградской области от 29.09.2023 №2/1-1428) / В. Ю. Владимиров [и др.]. С. 38–39.

<sup>1</sup> Там же. С. 24–25.

<sup>2</sup> Бардаченко А. Н., Евстропов Д. А. Указ. соч. С. 91–95.

Для создания модели ИИ программисты «Сбер Бизнес Софт» использовали сверточную нейронную сеть (ConvNet/CNN) с архитектурой ResNet152 и алгоритмом обучения методом обратного распространения ошибки (Backpropagation). При разработке модели использовалось разделение фотографий на обучение/валидацию – 80/20 со стратификацией.

После создания и обучения на кафедру трасологии и баллистики учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской академии МВД России для проведения валидации была предоставлена версия прототипа модели ИИ.

Оценка точности работы прототипа модели осуществлялась путем подсчета результатов ее работы на группе фотографий гильз, которые не использовались для ее обучения. Всего было осуществлено более 10 000 тестовых запросов. В результате проверки работы итоговой версии прототипа модели ИИ, определяющей наименование патрона по фотографиям гильзы, точность составила порядка 65–70%.

Наиболее часто наблюдались ошибки при определении патронов с одинаковой (цилиндрической) формой гильзы, но незначительно различающихся по длине гильзы (например, патроны 9x17 мм, 9x18 мм, 9x19 мм).

В настоящее время для формирования и ведения **дактилоскопических учетов** в органах внутренних дел Российской Федерации используется централизованная интегрированная автоматизированная дактилоскопическая информационная система МВД России. В 2023 г. сотрудниками экспертно-криминалистических подразделений с применением ЦИАДИС-МВД установлены лица, возможно, причастные к совершению более чем 39,9 тыс. преступлений.

В данной системе внедряется программное обеспечение нового поколения, в котором реализованы технологии ИИ. Результаты его апробации, проведенной ранее в отдельных территориальных органах МВД России, и начало эксплуатации в МВД по Республике Крым, ГУ МВД России по Ростовской и Воронежской областям и УМВД России по Ямало-Ненецкому автономному округу свидетельствуют о существенном повышении результативности проверок по дактилоскопическим учетам и одновременном снижении временных затрат на их проведение. Результаты применения названных технологий обеспечивают формирование рекомендательных списков проверяемых объектов, окончательное решение об идентификации которых принимается непосредственно экспертом, проводящим исследование, в строгом соответствии с принятыми методиками.

Алгоритмы нейросети «обучены» на реальных дактилоскопических массивах, на предмет сходства сравниваются оригиналы дактилоскопических изображений, а не их математические модели. Новый алгоритм существенно расширяет возможности АДИС «Папилон» при поиске малоинформативных следов рук, имеющих одновременно шрамированные и «смазанные» участки, с наложением папиллярных узоров, загрязнением папиллярных линий, отсутствием интегральных признаков (дельта, центров); следов ладоней, имеющих частные признаки на участках с большим количеством складок-морщин (в тенарах и подпальцевых зонах). Применение «Папилон-Нейро» позволяет существенно сократить трудозатраты операторов, а также получить совпадения, ранее не попадавшие в рекомендательные списки.

Учитывая изложенное, рассматривается возможность распространения технологий ИИ во всех территориальных органах МВД России, а также его внедрения в другие виды экспертно-криминалистических учетов.

## ЗАКЛЮЧЕНИЕ

Государственная научно-техническая политика в области криминалистического обеспечения предупреждения, выявления, раскрытия и расследования преступлений представляет собой выражение отношения государства к деятельности в названной сфере. Она определяет направления развития научно-технических средств, необходимых для решения задач уголовного судопроизводства, а также правовые и организационно-управленческие механизмы ее реализации.

Основной предпосылкой для ее формирования является потребность в совершенствовании использования специальных знаний в процессе уголовно-процессуальной, оперативно-розыскной и экспертно-криминалистической деятельности в условиях новых вызовов. Требуют дальнейшего развития вопросы деанонимизации личности в цифровом пространстве, что является комплексной задачей, разрешаемой правовыми, научно-техническими и организационными средствами.

Налицо острая потребность в повышении качества и конкурентоспособности производства отечественной криминалистической и иной специальной техники: если ранее при проведении компьютерных экспертиз в ЭКП ОВД использовалось не имеющее российских аналогов оборудование зарубежных производителей (особенно при исследовании мобильных устройств), то сегодня в результате незаконных, так называемых «санкций» со стороны ряда недружественных стран возможность их надлежащей эксплуатации зачастую утрачена. Например, не поддерживаются лицензии АПК UFED компании Cellebrite (Израиль). И здесь важно не просто уйти от зависимости от одних иностранных производителей, попав в зависимость к другим. Важно развивать и поддерживать отечественных производителей и разработчиков высокотехнологичных средств криминалистической техники. Необходимо широкое использование механизмов государственно-частного партнерства для вовлечения финансовых и бизнес-структур, IT-компаний в решение задач ОВД, связанных с разработкой и внедрением новейших технологий, для привлечения к этой работе высококлассных специалистов.

Наконец, существует настоятельная потребность в создании надлежащей ресурсной базы, развитии кадрового потенциала и совершенствовании методических основ использования современных высокотехнологичных методов и средств борьбы с преступностью, что также является одной из предпосылок разработки и принятия ГНТП КО.

Исходя из приоритетов научно-технологического развития Российской Федерации, с учетом специфики правоохранительной деятельности, можно выделить следующие основные направления ГНТП КО: внедрение технологий 3D-моделирования, распознавания и синтеза речи, а также ее преобразования в машиночитаемый формат, анализа данных, основанного на алгоритмах машинного обучения, распознавания образов, изображений, объектов (компьютерное зрение); развитие интеллектуальных систем поддержки принятия решений и имитации человеческих действий для целей их автоматизации, беспилотных авиационных систем, оснащенных многофункциональными полезными нагрузками; совершенствование технологий криминалистической регистрации на основе алгоритмов геометрического совмещения изображений в режиме реального времени, совместной визуализации анализируемых и сравниваемых изображений, цифровых технологий совмещения координат местоположения, геометрических и пространственных характеристик, углов позиционирования трасс, рельефной следовой картины.

С использованием перечисленных технологий решается и не менее важная задача, являющаяся неотъемлемым элементом надежного и результативного алгоритма идентификации, – устранение субъективности человеческого фактора при разметке и кодировании следов вручную. Использование алгоритмов сопоставления проверяемого объекта и изображения следа на следовоспринимающей поверхности способно повысить качество трасологических исследований.

Отдельным направлением ГНТП КО является развитие методов и средств цифровой криминалистики, направленных на исследование информации в цифровой форме.

Приведенные выводы и рекомендации могут быть положены в основу соответствующей государственной программы Российской Федерации в сфере борьбы с преступностью.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

## НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. : с изм., одобренными в ходе общерос. голосования 1 июля 2020 г. // Собр. законодательства Рос. Федерации. – 2014. – № 31. – Ст. 4398.

Гражданский кодекс Российской Федерации (Ч. I) : Федер. закон от 30 нояб. 1994 г // Собр. законодательства Рос. Федерации. – 1994 г. – № 32 – Ст. 3301.

О науке и государственной научно-технической политике : Федер. закон от 23 авг. 1996 г. № 127-ФЗ // Собр. законодательства Рос. Федерации. – 1996. – № 35. – Ст. 4137.

О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федер. закон от 7 августа 2001 г. № 115-ФЗ // Собр. законодательства Рос. Федерации. – 2001. – № 33 (Ч. I). – Ст. 3418.

Об информации, информационных технологиях и о защите информации : Федер. закон от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31 (Ч. I). – Ст. 3448.

О государственной геномной регистрации в Российской Федерации : Федер. закон от 3 дек. 2008 г. № 242-ФЗ // Собр. законодательства Рос. Федерации. – 2008. – № 49. – Ст. 5740.

О противодействии коррупции : Федер. закон от 25 дек. 2008 г. № 273-ФЗ // Собр. законодательства Рос. Федерации. – 2008. – № 52 (Ч. I). – Ст. 6228.

О внесении изменений в Федеральный закон «О государственной геномной регистрации в Российской Федерации» и отдельные законодательные акты Российской Федерации» [Электронный ресурс] : Федер. закон от 6 февр. 2023 г. № 8-ФЗ // Официальный интернет-портал правовой информации (дата обращения: 15.04.2025).

Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Рос. Федерации от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50. – Ст. 7074.

Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации

по субъекту Российской Федерации : Указ Президента Рос. Федерации от 21 дек. 2016 г. № 699 // Собр. законодательства Рос. Федерации. – 2016. – № 52 (Ч. V). – Ст. 7614.

О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. – 2017. – № 20. – Ст. 2901.

О развитии искусственного интеллекта в Российской Федерации : Указ Президента Рос. Федерации от 10 окт. 2019 г. № 490 // Собр. законодательства Рос. Федерации. – 2019. – № 41. – Ст. 5700.

О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» : постановление Правительства Рос. Федерации от 28 нояб. 2011 г. № 977 // Собр. законодательства Рос. Федерации. – 2011. – № 49 (Ч. V). – Ст. 7284.

Об утверждении государственной программы Российской Федерации «Информационное общество» : постановление Правительства Рос. Федерации от 15 апр. 2014 г. № 313 // Собр. законодательства Рос. Федерации – 2014 г. – № 18 (Ч. II). – Ст. 2159.

О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах (вместе с «Положением о проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» : постановление Правительства Рос. Федерации от 3 июня 2019 г. № 710 // Собр. законодательства Рос. Федерации. – 2019. – № 23. – Ст. 2963.

О некоторых вопросах реализации Федерального закона «О государственной геномной регистрации в Российской Федерации» : постановление Правительства Рос. Федерации от 24 июня 2023 г. № 1027 // Собр. законодательства Рос. Федерации. – 2023. – № 27. – Ст. 5004.

О внесении изменений в постановление Правительства Российской Федерации от 24 июня 2023 г. № 1027 : постановление Правительства Рос. Федерации от 11 апр. 2024 г. № 455 // Собр. законодательства Рос. Федерации. – 2024. – № 16. – Ст. 2240.

О вопросах организации деятельности экспертно-криминалистических центров органов внутренних дел : приказ МВД России от 30 мая 2003 г. № 366 // Доступ из СТРАС «Юрист» (дата обращения: 13.03.2025).

Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел

Российской Федерации : приказ МВД России от 29 июня 2005 г. № 511 // Доступ из СТРАС «Юрист» (дата обращения: 13.04.2025).

Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации (вместе с «Инструкцией по организации формирования, ведения и использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации», «Правилами ведения экспертно-криминалистических учетов в органах внутренних дел Российской Федерации») : приказ МВД России от 10 февр. 2006 г. № 70 // Доступ из СТРАС «Юрист» (дата обращения: 10.02.2025).

Об утверждении Типового положения о территориальном органе Министерства внутренних дел Российской Федерации на районном уровне : приказ МВД России от 5 июня 2017 г. № 355 // Доступ из СТРАС «Юрист» (дата обращения: 10.02.2025).

Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км : приказ МВД России от 25 нояб. 2019 г. № 878 // Доступ из СТРАС «Юрист» (дата обращения: 10.02.2025).

Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф» : приказ МВД России от 29 дек. 2020 г. № 925 // Доступ из СТРАС «Юрист» (дата обращения: 12.02.2025).

Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 30 мая 2023 г. № 2 км : приказ МВД России от 3 июля 2023 г. № 480 // Доступ из СТРАС «Юрист» (дата обращения: 13.02.2025).

Об утверждении Инструкции по организации и производству судебных экспертиз в судебно-экспертных учреждениях и экспертных подразделениях федеральной противопожарной службы : приказ МЧС России от 19 авг. 2015 г. № 640 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России : приказ Минюста России от 20 апр. 2023 г. № 72 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.02.2025).

Об утверждении Инструкции по организации производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Министерства юстиции Российской Федерации : приказ

Минюста России от 28 дек. 2023 г. № 404 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации» на право самостоятельного производства судебных экспертиз : приказ Следственного комитета Рос. Федерации от 24 июля 2020 г. № 77 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

О судебно-экспертной деятельности в Российской Федерации : проект федер. закона // Система обеспечения законодательной деятельности Государственной Думы Федерального собрания Российской Федерации : сайт. URL: <https://sozd.duma.gov.ru/bill/306504-6> (дата обращения: 09.02.2025).

Бюллетень Верховного Суда Российской Федерации. 1996. № 2.

Паспорт федерального проекта «Информационная безопасность» [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Паспорт федерального проекта «Информационная инфраструктура» [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Паспорт федерального проекта «Кадры для цифровой экономики» [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Паспорт федерального проекта «Нормативное регулирование цифровой среды [Электронный ресурс] : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Паспорт федерального проекта «Цифровые технологии» [Электронный ресурс] : утв. президиумом Правительственной комиссии

по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности : протокол от 28 мая 2019 г. № 9 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» [Электронный ресурс] : утв. президиумом Совета при Президенте Рос. Федерации по стратегическому развитию и национальным проектам : протокол от 04 июня 2019 г. № 7 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.05.2025).

Обзор кассационной практики судебной коллегии по уголовным делам Верховного Суда Российской Федерации за второе полугодие 2012 года : утв. Президиумом Верховного Суда Рос. Федерации 3 апр. 2013 г. // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.04.2025);

Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 21 авг. 2019 г. № 5-АПУ19-59 // Доступ из СПС «КонсультантПлюс» (дата обращения: 10.04.2025).

## **ДИССЕРТАЦИОННЫЕ ИССЛЕДОВАНИЯ**

*Севастьянов, П.В.* Цифровые технологии фиксации невербальной доказательственной информации : дис. ... канд. юрид. наук. – Москва, 2024. – 194 с.

*Сокол, В.Ю.* Тактико-криминалистическое обеспечение раскрытия и расследования преступлений (Методологические и организационные аспекты) : дис. ... канд. юрид. наук. – Москва, 1998. – 188 с.

## **НАУЧНАЯ ЛИТЕРАТУРА**

*Бажанов, В.А.* Особенности познавательных механизмов в информационную эпоху: «эхо-пузыри» и «эхо-камеры» // Философский журнал. – 2022. – Т. 15. – № 4. – С. 152–164.

*Бардаченко, А.Н.* Использование технологии для установления обстоятельств применения огнестрельного оружия на месте происшествия / А.Н. Бардаченко, Д.А. Евстропов // Актуальные проблемы

криминалистики и судебной экспертизы : сб. материалов междунар. науч.-практ. конф., посвященной 105-летию Экспертно-криминалистической службы МВД России, Иркутск, 6–7 июня 2024 г. – Иркутск : Восточно-Сибирский институт МВД России, 2024. – С. 91–95.

Возможности применения цифровых технологий при производстве баллистических экспертиз и ведении баллистических учетов : аналитический обзор с предложениями (п. 35 Плана научного обеспечения деятельности органов внутренних дел Российской Федерации на 2024 год; заявка ГУ МВД России по г. Санкт-Петербургу и Ленинградской области от 29.09.2023 №2/1-1428) / В. Ю. Владимиров, А. М. Кустов, Г. З. Гаспарян [и др.]. 175 с.

*Гаврилин, Ю. В.* Модернизация уголовно-процессуальной формы в условиях информационного общества / Ю. В. Гаврилин, А. В. Победкин // Труды Академии управления МВД России. – 2019. – № 3 (51). – С. 27–38.

*Гаврилин, Ю. В.* Научные основы технико-криминалистического обеспечения оперативно-розыскной деятельности органов внутренних дел по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий / Ю. В. Гаврилин, А. Г. Парадников // Развитие научных идей профессора Р. С. Белкина в условиях современных вызовов (к 100-летию со дня рождения) : сб. науч. статей по материалам междунар. науч.-практ. конф. : в 2-х ч. – Москва : Академия управления МВД России, 2022. – С. 62–71.

*Гаврилин, Ю. В.* Обеспечение достоверности результатов применения технологий на основе искусственного интеллекта в экспертно-криминалистической деятельности / Ю. В. Гаврилин, А. А. Бородина // Судебная экспертиза. – 2024. – № 2 (78). – С. 52–61.

*Гаврилин, Ю. В.* О концепции государственной научной и научно-технической политики в области криминалистического обеспечения борьбы с преступностью / Ю. В. Гаврилин, Ю. Е. Салеева // Труды Академии управления МВД России. – 2023. – № 4 (68). – С. 80–87.

*Гаврилин, Ю. В.* О научных подходах к понятию и содержанию технико-криминалистического обеспечения раскрытия и расследования преступлений / Ю. В. Гаврилин, Ю. Е. Салеева, А. В. Марушко // Криминалистика, уголовный процесс и судебная экспертология в XXI веке: векторы развития (к 70-летию кафедры управления органами расследования преступлений Академии управления МВД России) ; 66-е ежегодные криминалистические чтения : сб. науч. статей по материалам междунар. науч.-практ. конф. Москва, 25 апреля 2025 г. – Москва : Академия управления МВД России, 2025. – Ч. 2. – С. 66–77.

*Гаврилин, Ю. В.* О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : науч.-практ. пособие. – Москва : Академия управления МВД России, 2021. – 71 с.

*Гаврилин, Ю. В.* О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности (криминалистической политики) // Труды Академии управления МВД России. – 2022. – № 2 (62). – С. 96–102.

*Гаврилин, Ю. В.* Основные направления развития криминалистических знаний в условиях информационного общества // Криминалистика в условиях информационного общества (59-е ежегодные криминалистические чтения) : сб. статей междунар. науч.-практ. конф. – Москва : Академия управления МВД России, 2018. – С. 65–73.

Уголовная политика Российской Федерации : учеб. : в 2-х ч. / под ред. Л. И. Беляевой. – Москва : Академия управления МВД России, 2018. – Ч. 1. – 184 с.

## **ЭЛЕКТРОННЫЕ РЕСУРСЫ:**

*Ваганова, Д.* Робокоп и детекторы выстрелов: технологии будущего на службе полиции // РБК : сайт. URL: <https://trends.rbc.ru/trends/industry/61e145ed9a794785b12743b9?from=copy> (дата обращения: 10.05.2025).

«Лаборатория Касперского»: количество киберинцидентов в российских компаниях увеличилось в 4 раза // Kaspersky : сайт. URL: <https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-kolichestvo-kiberincidentov-v-rossijskih-kompaniyah-uvlechilos-v-4-raza> (дата обращения: 11.05.2025).

Институт изучения мировых рынков : сайт. URL: <https://worldmarketstudies.ru/article/userb-ot-kiberprestuplenij-vyrastet-natret-za-sleduusie-4-goda/> (дата обращения: 12.02.2025).

Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // МВД России : сайт. URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 25.02.2025).

*Меньшиков, П. В.* Эволюция государственной информационной политики в России // Журнал «Международные коммуникации» : сайт. URL: <https://intcom-mgimo.ru/2017/2017-04/state-information-policy-of-russia> (дата обращения: 15.02.2025).

*Мурадян, С. В.* Цифровые активы: правовое регулирование и оценка рисков // Journal of Digital Technologies and Law : сайт. URL: <https://doi.org/10.21202/jdtl.2023.5> (дата обращения: 13.02.2025).

*Никифорова, А.* ИИ научился создавать тысячи вирусов: их не видят антивирусы // ХАЙТЕК : сайт. URL: <https://hightech.fm/2024/12/26/ai-can-malware> (дата обращения: 13.03.2025).

Отчет о тенденциях преступности в сфере высоких технологий Group-IB в 2025 год // Group-IB : сайт. URL: <https://www.group-ib.com/ru/landing/high-tech-crime-trends-2025/> (дата обращения: 13.03.2025).

Официальный сайт производителя «ГеоСпектр». URL: <https://www.geo-spektr.ru/bespilotnye-letatelnye-apparaty/kvadrokoptery/geoscan/geoskan-401-geodeziya.html> (дата обращения: 11.04.2025).

Официальный сайт производителя «DJI». URL: <https://www.dji.com/ru/mavic/info?ysclid=macoxlnjqz307837520> (дата обращения: 11.04.2025).

Официальный сайт производителя «Leica Geosystems». URL: <https://leica-geosystems.com/ru/products/laser-scanners/scanners/blk360g1> (дата обращения: 11.04.2025)

ФСБ задержала пять человек по делу об «украинских call-центрах» и 7 млрд // РБК : сайт. URL: <https://www.rbc.ru/politics/08/04/2024/661399849a7947d8c59ee6e4> (дата обращения: 20.02.2025).

*Цвести М., Сиско Э., Лурье И.* Разработка и валидация метода экспресс-ГХ-МС для скрининга изъятых наркотиков // Sciencedirect : сайт. URL: <https://www.sciencedirect.com/science/article/abs/pii/S2468170923000152> (дата обращения: 10.05.2025).

Texterra: базовый семантический анализатор // ИСП РАН : сайт. URL: <https://www.ispras.ru/technologies/texterra/> (дата обращения: 10.05.2025).

Wi-Реер: особенности беспроводного подглядывания // Kaspersky : сайт. URL: <https://www.kaspersky.ru/blog/wi-peepr-wireless-localization/34417/?ysclid=m9751slzb2187534028> (дата обращения: 06.04.2025).

*Научное издание*

**Салеева Юлия Евгеньевна,  
Гаврилин Юрий Викторович**

**КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ  
ГОСУДАРСТВЕННОЙ  
НАУЧНО-ТЕХНИЧЕСКОЙ ПОЛИТИКИ  
В СФЕРЕ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ  
ВЫЯВЛЕНИЯ, РАСКРЫТИЯ  
И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ**

*Монография*

*Редактор Е. Л. Дробкова  
Верстка С. Х. Аминова*

Подписано в печать 25.11.2025. Формат 60×84 <sup>1</sup>/<sub>16</sub>.  
Усл. печ. л. 6,74. Уч.-изд. л. 5,74. Тираж 39 экз. Заказ 60у

Академия управления МВД России.  
125171, Москва, ул. Зои и Александря Космодемьянских, д. 8

ISBN 978-5-908091-14-5



9 785908 091145 >