



Организация по безопасности и
сотрудничеству в Европе

ИСПОЛЬЗОВАНИЕ НОВЫХ И РАЗВИВАЮЩИХСЯ ТЕХНОЛОГИЙ **В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ**

ИТОГОВЫЙ ДОКЛАД ПО РЕЗУЛЬТАТАМ
ЭКСПЕРТНОГО КРУГЛОГО СТОЛА,
СОСТОЯВШЕГОСЯ НА МЕРОПРИЯТИИ ПО
ВОПРОСАМ БЕЗОПАСНОСТИ И
ПОЛИЦЕЙСКОЙ ДЕЯТЕЛЬНОСТИ,
ВЕЛИКОБРИТАНИЯ (11-12 МАРТА 2025 Г.)

Отказ от ответственности: В настоящем документе обобщены материалы круглого стола, проведенного в соответствии с «правилом Четэм-хауса». Представленные здесь взгляды, мнения и выводы отражают обобщение обсуждений за круглыми столами и не обязательно отражают официальную позицию Организации по безопасности и сотрудничеству в Европе (ОБСЕ) и/или ее государств-участников. Цель настоящего документа — передать суть дискуссии без указания конкретных участников или их принадлежности к тем или иным организациям. ОБСЕ не поддерживает и не проверяет достоверность отдельных утверждений, высказанных в ходе круглого стола. Читателям следует рассматривать данный документ как отражение многообразия точек зрения, озвученных в ходе мероприятия, а не как авторитетное заявление по обсуждавшимся темам.

© ОБСЕ 2025

Все права защищены. Содержимое данной публикации может свободно использоваться и копироваться в образовательных и других некоммерческих целях при условии, что любое такое воспроизведение будет сопровождаться признанием ОБСЕ в качестве источника.

Секретариат ОБСЕ
Департамент по противодействию
транснациональным угрозам
Отдел стратегических вопросов
полицейской деятельности
Валльнерштрассе 6
1010 Вена, Австрия

Эл. почта: SPMU@osce.org
www.osce.org/policing

Содержание

Введение	2
Трансформация уголовных расследований	3
Расширение источников оперативной информации и доказательств	3
Революция в следственных методах	4
Повышение производительности и эффективности	5
Как избежать «перегрузки» инновациями	6
Преодоление неприятия риска	6
Пересмотр профессиональной подготовки и развития навыков	7
Преодоление внутриведомственной разобщенности	9
Сотрудничество — незаменимый элемент	10
Государственно-частные партнерства	10
Обмен данными	11
(Меняющаяся) роль платформ международного сотрудничества	12
Законодательство в ногу со временем	13
От аналогового к цифровому	13
Регулирование преобразований	14
От возможностей — к ответственности	15
Выводы и программные рекомендации	15

Введение

Новые и развивающиеся технологии преобразовали практически все сферы человеческой жизни. От анализа больших данных и алгоритмов машинного обучения, через «интернет вещей», «умные» датчики и автономные беспилотные аппараты — вплоть до искусственного интеллекта (ИИ): нынешние темпы технологических инноваций беспрецедентны. На фоне такого развития событий начались дискуссии относительно преимуществ и рисков, связанных с применением новых технологий в различных профессиональных областях.

В контексте борьбы с преступностью и деятельности правоохранительных органов значительная часть дискуссий сосредоточена на опасениях, связанных с угрозами, которые могут исходить от подобных технологий — в особенности с возможностью их неправомерного использования в преступных целях. Тем не менее, потенциал этих технологий произвести революцию в работе правоохранительных органов, повысив как их результативность, так и эффективность, имеет не меньшее значение. Существуют широкие и разнообразные возможности для интеграции новых и перспективных технологий в деятельность правоохранительных структур. Например, они могут способствовать анализу тенденций и закономерностей, мониторингу угроз и рисков безопасности, содействовать выявлению подозреваемых и раскрытию преступлений, а также

оптимизировать различные административные процессы и процедуры. В то же время достижение баланса между использованием технологических достижений и обеспечением защиты прав и основных свобод человека представляет собой важную задачу, порождающую вопросы этического, правового и практического характера.

В этой связи, Отделом стратегических вопросов полицейской деятельности Департамента по противодействию транснациональным угрозам при Секретариате ОБСЕ была организована серия экспертных круглых столов посвященных применению правоохранительными органами новых и перспективных технологий. Цель данных дискуссий заключается в том, чтобы выявить возможности использования правоохранительными органами новых и перспективных технологий для поддержки своей деятельности, способствовать выработке рекомендаций по вопросам политики, а также изучить потенциальные направления поддержки со стороны ОБСЕ в области наращивания соответствующего потенциала.

Настоящий материал обобщает основные тезисы и выводы, озвученные на втором круглом столе, посвященном применению новых и перспективных технологий для расследования преступлений, и состоявшемуся 11 и 12 марта 2025 года в Фарнборо, Великобритания. Круглый стол был организован совместно с Министерством внутренних дел Великобритании и прошел в рамках мероприятия «Security & Policing 2025».

Трансформация уголовных расследований

Сегодня практически любая преступная деятельность содержит в себе цифровой компонент: от наркоторговцев, использующих зашифрованные каналы связи для организации поставок, и организаторов незаконного ввоза мигрантов, рекламирующих свои услуги в интернете, до взломщиков, отслеживающих аккаунты своих потенциальных жертв в социальных сетях. Правоохранительные органы по всему миру активно внедряют широкий спектр новых цифровых инструментов и методов, адаптируясь к постоянно меняющемуся криминальному ландшафту, что, в свою очередь, трансформирует процесс расследования преступлений. Со стратегической точки зрения влияние цифровых технологий на расследование преступлений наиболее ярко проявляется в следующих трех основных областях:

Расширение источников оперативной информации и доказательств

Следователи сталкиваются с огромным множеством устройств и платформ, генерирующих данные, которые могут быть использованы в целях расследования. Этот спектр варьируется от ноутбуков, смартфонов и наручных часов до данных о трафике домашних маршрутизаторов, показаний датчиков «интернета вещей» (IoT) в жилых помещениях, информации от бытовой техники с

поддержкой Wi-Fi и данных, записываемых бортовыми системами автомобилей. Все эти примеры уже использовались ранее при расследовании тяжких преступлений в различных государствах – участниках ОБСЕ. Опыт показывает, что такие данные зачастую позволяют получить критически важную информацию о последовательности событий, установить связи между подозреваемыми и преступной деятельностью, подтвердить показания свидетелей или наметить новые направления расследования. Своевременный и правомерный сбор и анализ таких данных не только повышают эффективность следственных действий, но и становятся все более незаменимым условием для формирования прочной, доказательной базы для судебного разбирательства.

Поскольку люди все активнее используют онлайн-сервисы и платформы во всех сферах своей повседневной жизни, они оставляют после себя «цифровые следы», которые могут быть использованы в целях расследования. Разведка по открытым источникам (OSINT) стала важной частью инструментария правоохранительных органов, зачастую дополняя другие, традиционные источники оперативной информации и доказательств. Хотя OSINT сопряжена с определенными сложностями — особенно в вопросах надежности и проверяемости данных — огромный массив доступных данных и информации, а также скорость, с которой их можно получить, существенно повышают эффективность расследований и способствуют

созданию надежной доказательной базы для последующего уголовного преследования.

Цифровые технологии также позволяют правоохранным органам более предметно вовлекать общественность в текущие расследования посредством краудсорсинга оперативной информации. Привлекая граждан к участию в расследовании, следователи могут получить ценные наводки, подсказки или доказательства, которые в противном случае могли бы остаться невыявленными. Будь то опознание подозреваемых по записям с камер видеонаблюдения, поиск пропавших без вести или отслеживание похищенного имущества — краудсорсинг позволяет мобилизовать поддержку общественности и расширить охват следственных мероприятий. При ответственном использовании и соблюдении надлежащих мер предосторожности краудсорсинг оперативной информации способен укрепить доверие граждан к правоохранным органам и повысить уровень их вовлеченности, дополняя при этом традиционные методы расследования знаниями и информацией, которыми располагает местное сообщество.

Революция в следственных методах

Поскольку большинство современных преступлений имеют цифровую составляющую, умение работать с цифровыми доказательствами стало одной из ключевых компетенций для сотрудников правоохранных органов. Цифровая криминалистика

(компьютерно-техническая экспертиза) становится краеугольным камнем современных уголовных расследований, играя столь же преобразующую роль, какую в свое время сыграло появление дактилоскопии или анализа ДНК. Подобно тому как анализ ДНК произвел революцию в способности с научной точностью устанавливать связь между конкретными лицами и совершенными преступлениями, цифровая криминалистика позволяет следователям извлекать, анализировать и интерпретировать электронные данные для реконструкции событий, выявления скрытых взаимосвязей и выстраивания цепочек доказательств. В эпоху, когда большая часть человеческой деятельности оставляет цифровой след, цифровая криминалистика предоставляет незаменимые инструменты для установления истины, укрепления доказательной базы и привлечения к ответственности.

Еще одной областью, где влияние современных технологий носит преобразующий характер, является возможность быстрой обработки огромных массивов данных с помощью приложений на базе ИИ. Примерами успешного применения ИИ в ходе расследований служат автоматизированный анализ записей с камер видеонаблюдения, а также обработка крупных наборов данных, полученных в результате перехвата зашифрованной переписки между преступниками. Инструменты на базе ИИ позволяют интерпретировать и использовать эти данные в расследованиях за ничтожную долю того времени, которое потребовалось бы при ручном анализе.

Тем не менее, по-прежнему необходима проверка со стороны человека для выявления и устранения потенциальной предвзятости в моделях ИИ. В настоящее время отсутствует международная правовая или нормативная база, гарантирующая прозрачность использования ИИ в следственной работе.

Широкомасштабное внедрение ИИ в практику уголовных расследований потребует создания механизмов, позволяющих отслеживать логику рассуждений ИИ и проводить аудит следов в процессе формирования ими итоговых результатов.

Цифровые технологии также трансформируют методы документирования и анализа мест преступлений. Используя высокоточные лазерные сканеры, следователи имеют возможность создавать весьма детализированные и точные трехмерные (3D) цифровые копии мест происшествий, сохраняя пространственные взаимосвязи, размеры и визуальные ракурсы именно в том виде, в каком они существовали на момент обнаружения.

Эти реконструкции позволяют следователям, прокурорам и даже присяжным виртуально возвращаться на место преступления, анализировать траектории или проверять гипотезы, не присутствуя там физически. 3D-сканирование не только повышает качество и достоверность документирования места преступления, но и снижает риск утраты, искажения или неверной интерпретации улик с течением времени, что делает его мощным инструментом при проведении сложных или масштабных расследований.

Повышение производительности и эффективности

Использование цифровых технологий позволяет существенно сократить дублирование усилий и повысить производительность в работе правоохранительных органов. Благодаря цифровизации рабочих процессов, автоматизации рутинных задач и обеспечению обмена данными между подразделениями в режиме реального времени, правоохранительные органы могут избежать проведения избыточных расследований, оптимизировать управление делами, улучшить оперативное планирование и принимать более обоснованные решения. Например, централизованные базы данных и автоматизированные системы отслеживания дел позволяют сотрудникам выяснить, не расследуются ли аналогичные дела уже где-либо еще, что позволяет сэкономить ценное время и ресурсы. Кроме того, они могут помочь выявить взаимосвязи между расследованиями, которые в противном случае могли бы остаться незамеченными.

Еще одним перспективным направлением применения технологий является внедрение локальных ИИ-агентов, обученных на специализированных массивах данных (таких как инструкции, методические пособия, законодательные акты или материалы конкретных дел), для предоставления следователям практических рекомендаций и консультаций — особенно по вопросам технического характера. В настоящее время, например, проводится тестирование таких агентов в сфере цифровой криминалистики.

И хотя широкомасштабное использование ИИ непосредственно в ходе текущих расследований, вероятно, останется ограниченным в обозримом будущем — главным образом из-за опасений касательно целостности доказательств — его потенциал в качестве «умного» технического помощника или консультанта способен существенно повысить продуктивность работы отдельных следователей.

В конечном счете цифровые технологии могут способствовать переходу правоохранительной деятельности от ручных, разрозненных процессов к более скоординированной, эффективной и основанной на аналитических данных оперативной работе.

Как избежать «перегрузки» инновациями

Цифровые инновации, несомненно, открывают колоссальные возможности для повышения эффективности и результативности уголовных расследований, но они также порождают и серьезные вызовы. В данном контексте инновации выходят за рамки простого внедрения новых инструментов: они требуют фундаментального переосмысления подходов к правоохранительной деятельности, включая адаптацию организационных структур, рабочих процедур и институциональной культуры. Правоохранительные органы вынуждены продолжать выполнять трудоемкие задачи в рамках широкого спектра полицейских функций, одновременно внедряя инновации,

необходимые для реагирования на изменения в криминогенной обстановке. На практике идеал плавного и беспрепятственного инновационного процесса зачастую вступает в противоречие с повседневной реальностью, характеризующейся устоявшимися рабочими практиками, конфликтующими интересами и нежеланием принимать перемены.

Успешное внедрение инноваций требует совместных усилий, готовности учиться и понимания того, что неудачи и ошибки являются неотъемлемой частью этого пути. Этот процесс редко бывает линейным; как правило, он начинается с необходимости решения конкретной насущной проблемы, а не с реализации заранее продуманной долгосрочной стратегии. При рассмотрении вопросов цифровых инноваций в контексте уголовных расследований особого внимания заслуживают три ключевые области:

Преодоление неприятия риска

Неприятие риска — явление, весьма распространенное в государственном секторе, и правоохранительные органы здесь не являются исключением. Полицейские организации — и на то есть веские причины — традиционно строят свою работу таким образом, чтобы минимизировать риски, обеспечить подотчетность и избежать ошибок. Разумеется, такой подход вполне объясним, учитывая необходимость поддерживать уверенность в эффективности работы полиции и сохранять доверие общественности, однако он может сдерживать инновации и замедлять внедрение новых технологий.

Оценка рисков, связанных с применением новейших технологий, является для правоохранительных органов ключевым фактором при принятии решения об их использовании. Многие сотрудники полиции и лица, принимающие решения, с опаской относятся к опробованию незнакомых инструментов или методов, опасаясь возможных правовых, операционных или репутационных последствий.

Несмотря на то, что ответственное и надежное управление рисками должно оставаться приоритетом для любого правоохранительного органа, важно не допустить, чтобы стремление избежать рисков стало препятствием для необходимых инноваций. Это требует формирования такой институциональной культуры, которая поощряет обучение, допускает контролируемые неудачи и вознаграждает за успешное решение проблем. Сюда относится создание безопасной среды для апробации новых подходов, инвестирование в пилотные проекты, а также формирование лидерства, основанного на понимании того, что не любой риск представляет собой угрозу — некоторые риски открывают возможности для прогресса. Слишком часто лишь трагические инциденты в сфере безопасности или крупные провалы становятся тем толчком, который запускает культурные сдвиги, необходимые для внедрения инноваций.

Одним из примеров неприятия риска в правоохранительной сфере является склонность отдавать предпочтение уже зарекомендовавшим себя коммерческим инструментам. Зачастую

это объясняется их широкой популярностью, что, в свою очередь, повышает их приемлемость и значимость в ходе судебных разбирательств по уголовным делам.

Тем не менее в условиях ограниченности ресурсов сотрудникам правоохранительных органов все чаще приходится полагаться на разработанные сообществом решения из открытых источников или даже на самостоятельно созданные программные инструменты, чтобы заменить или дополнить функционал дорогостоящих коммерческих средств. Несмотря на то, что открытый код подобных инструментов предоставляет более широкие возможности для анализа и аудита, их обширное внедрение нередко вызывает настороженность: такие решения считаются недостаточно проверенными и испытанными, а потому — более уязвимыми для оспаривания в судебном порядке.

В принципе, оценка значимости и достоверности доказательств, а также результатов, полученных с помощью новых технологических инструментов, должна основываться на научном методе — в частности, на проверке воспроизводимости и верифицируемости результатов в аналогичных случаях.

Пересмотр профессиональной подготовки и развития навыков

Технологии способны существенно повысить эффективность расследования уголовных дел, однако они не могут заменить необходимость в обоснованной следственной логике и методах.

Следователи должны продолжать действовать, сохраняя четкое понимание сути следственного процесса, и одновременно осваивать новые навыки, позволяющие ориентироваться в постоянно меняющемся цифровом пространстве. По мере роста объема и сложности цифровых доказательств специализированная подготовка станет обязательным условием для всех сотрудников, участвующих в расследовании уголовных дел, обеспечивая им возможность эффективно работать в следственной среде, насыщенной современными технологиями.

В настоящее время многие правоохранительные органы по-прежнему полагаются исключительно на специалистов по цифровой криминалистике в решении любых вопросов, связанных с цифровыми технологиями; это создает риск перегрузки ограниченного штата экспертов и возникновения «узких мест» в процессе следствия. Вместо этого сотрудников первичного реагирования и следователей необходимо наделить базовыми цифровыми компетенциями — такими как выявление, фиксация и обеспечение сохранности цифровых доказательств в ходе обысков или задержаний, — чтобы они могли выступать в роли «цифровых специалистов первичного реагирования». Кроме того, они должны уметь выполнять простые задачи (например, проверять биткоин-адреса), чтобы специалисты могли сосредоточиться на более сложных видах деятельности — таких как восстановление удаленных данных с изъятого жесткого диска.

Несмотря на то, что знания и навыки, необходимые для выполнения следственных функций, отличаются от требований к техническим специалистам, фундаментальное понимание цифровых технологий и владение минимальным набором цифровых навыков сегодня становятся ключевой компетенцией. Следовательно, непрерывное повышение квалификации должно быть неотъемлемой частью профессионального развития и карьерного роста всех сотрудников правоохранительных органов, участвующих в расследованиях; это позволит гарантировать, что их профессиональные возможности будут развиваться синхронно с технологиями, с которыми им приходится сталкиваться в работе. Учебные программы полицейских академий также должны отражать эту тенденцию, интегрируя практические цифровые навыки и основы цифровой криминалистики в базовый курс подготовки сотрудников полиции.

Учитывая сложный характер цифровых технологий и их постоянное развитие, крайне необходим структурированный и системный подход к обновлению профессиональной подготовки и повышению квалификации. Вместо того чтобы полагаться на ситуативные или стандартные учебные курсы, правоохранительным органам следует разрабатывать рамочные модели компетенций для обучения, четко определяющие, кто, что, на каком уровне и в какой должности должен знать и уметь. Подобные модели помогают выявить конкретные компетенции, необходимые для выполнения различных функций — от сотрудников передовой линии, обеспечивающих фиксацию

цифровых доказательств, до специалистов, проводящих цифровые криминалистические экспертизы. Разрабатывая учебные программы в соответствии с этими четко определенными компетенциями, правоохранительные органы получают возможность более эффективно распределять ресурсы, отслеживать прогресс и гарантировать, что их персонал будет готов к решению меняющихся оперативных задач на последовательной и устойчивой основе.

Преодоление внутриведомственной разобщенности

Цифровая трансформация, необходимая для противодействия текущим и возникающим угрозам безопасности, требует не только общего понимания технологических изменений, но и фундаментального переосмысления устоявшихся методов и процессов работы полиции. Однако во многих случаях правоохранительные органы склонны рассматривать технологический прогресс с точки зрения конкретных инструментов, а не как глубокое изменение среды, в которой они действуют.

Это тоннельное зрение зачастую усугубляется организационной разобщенностью, при которой подразделения и отделы функционируют изолированно, практически не поддерживая контактов и не взаимодействуя друг с другом в смежных областях. Подобные структуры препятствуют свободному обмену информацией, снижают оперативную эффективность и тормозят внедрение инноваций.

Сотрудники могут проявлять нерешительность в вопросах освоения новых технологий или подходов просто потому, что те выходят за рамки их привычных должностных обязанностей или воспринимаемой ими зоны ответственности. В ряде случаев технические специалисты стремятся сохранить единоличный контроль над специализированными знаниями и инструментами, тем самым непреднамеренно создавая зависимость и ограничивая возможности для более широкого институционального обучения.

В то же время растущая сложность и объем цифровых улик, фигурирующих в делах о большинстве видов преступлений, со всей очевидностью демонстрируют: традиционных методов расследования, основанных исключительно на ручном труде, более недостаточно. Даже если бы правоохранительные органы располагали ресурсами для значительного увеличения штата следователей, это не решило бы проблему. Необходим стратегически выверенный баланс между привлечением квалифицированных кадров и расширением масштабов автоматизации. Автоматизация способна помочь в обработке огромных массивов рутинных данных и оптимизации повторяющихся операций, высвобождая время следователей для сосредоточения на более значимой аналитической работе. Для того чтобы автоматизация была по-настоящему эффективной, она должна внедряться на масштабируемой и воспроизводимой основе, а также строго соответствовать нормам права и принципам соблюдения прав человека.

Преодоление внутриведомственной разрозненности требует смены организационной культуры в сторону сетевого взаимодействия, при котором происходит активный обмен экспертными знаниями, поощряется создание межфункциональных команд, а решение проблем осуществляется на коллективной основе. Это требует более тесного сотрудничества между оперативными подразделениями и техническими специалистами (такими как цифровые криминалисты, аналитики данных и прочие ИТ-эксперты) для выявления решений, которые могут быть масштабированы для различных случаев и контекстов, и где человеческие и технологические возможности дополняют друг друга. Инновации должны восприниматься не как сфера ответственности лишь отдельных сотрудников или отделов, а как общая институциональная цель. Эффективно отвечать на вызовы современной следственной работы правоохранительные органы смогут только путем создания структур, поддерживающих междисциплинарное сотрудничество, инвестиций в масштабируемые процессы и формирования культуры открытости и обмена знаниями.

Сотрудничество — незаменимый элемент

Помимо внедрения культуры внутреннего взаимодействия, все более важным для выполнения всех функций правоохранительных органов — от обеспечения общественного порядка

и проведения уголовных расследований до оказания узкоспециализированных услуг — становится эффективное сотрудничество с внешними субъектами как в государственном, так и в частном секторе. Для выполнения своих обязанностей правоохранительные органы должны взаимодействовать с общественностью, другими органами системы уголовного правосудия на всех уровнях, государственными учреждениями, а также с частным сектором. Доверие остается краеугольным камнем эффективного партнерства, особенно в контексте деятельности полиции и системы уголовного правосудия.

Государственно-частные партнерства

Поскольку цифровые элементы сегодня являются неотъемлемой частью большинства — если не всех — преступлений, правоохранительным органам необходимо и далее укреплять сотрудничество с субъектами частного сектора. В частности, ключевыми партнерами выступают технологические компании, поскольку предоставляемые ими платформы и инструменты зачастую используются преступниками в своих целях.

Модели государственно-частного партнерства получают все более широкое распространение, предлагая структурированные платформы, посредством которых правоохранительные органы могут взаимодействовать с ключевыми заинтересованными сторонами. Подобные форумы уже существуют на международном уровне

в таких сферах, как борьба с киберпреступностью, а также экономическими и финансовыми преступлениями, однако они обладают потенциалом для применения в более широком спектре видов преступлений и отраслей деятельности. Эти партнерства позволяют правоохранительным органам и субъектам частного сектора выстраивать доверительные отношения, разрабатывать протоколы действий и формализовывать сотрудничество в рамках единой, последовательной системы. Кроме того, они могут служить катализаторами инноваций в сфере полицейской деятельности.

Прежде всего, государственно-частные партнерства способствуют налаживанию коммуникации. Правоохранительным органам, проводящим сложные расследования, зачастую требуется доступ к данным, находящимся в распоряжении частных организаций. Ведение стратегического диалога — как в контексте отдельных уголовных дел, так и применительно к более широким оперативным потребностям — помогает формировать взаимопонимание и обеспечивать более эффективное сотрудничество.

В ряде случаев правоохранительным органам может потребоваться привлечение внешних экспертов для восполнения нехватки внутренних ресурсов, особенно при проведении узкоспециализированных или масштабных расследований. Подобные партнерства могут представлять значительную ценность, но они при этом должны опираться на надежные процедуры проверки и механизмы, основанные на доверии, чтобы

гарантировать целостность расследований и обеспечить защиту конфиденциальных данных. Создание сбалансированной и масштабируемой модели цифровых знаний — как внутренней, так и внешней — является ключевым фактором для поддержания эффективности расследований в условиях стремительно меняющейся технологической среды.

Обмен данными

Растущая значимость цифровых доказательств в современных расследованиях, теоретически, должна сделать процесс обмена данными более быстрым и простым. По крайней мере, на уровне сотрудничества между полицейскими ведомствами переход к цифровизации открывает возможности для снижения зависимости от длительных юридических процедур, позволяя следователям уделять больше внимания оперативной (в том числе трансграничной) кооперации и совместным мероприятиям — сфере, важность которой неуклонно возрастает по мере того, как преступность приобретает все более транснациональный характер. Однако на практике по-прежнему существует множество сложностей с доступом к цифровым данным, находящимся у третьих лиц, особенно если они базируются в иностранной юрисдикции.

Во многих государствах-участниках ОБСЕ правоохранительные органы поддерживают давние отношения с определенными субъектами, хранящими данные, такими как интернет-провайдеры, платформы социальных сетей или файлообменные сервисы.

Однако цифровизация повседневной жизни сегодня означает, что совершенно новые категории субъектов — например, автопроизводители или производители устройств IoT — также генерируют данные, которые могут представлять ценность для следствия. В связи с этим для правоохранительных органов крайне важно расширить взаимодействие с частным сектором, включив в него и этих новых участников. В некоторых государствах-участниках ОБСЕ практика запроса цифровых доказательств у частных организаций все еще является относительно новой, и правоохранительным органам зачастую не хватает институциональной и процессуальной базы, а также практического опыта для получения таких данных.

С точки зрения частных компаний, процесс обмена данными с правоохранительными органами нередко воспринимается как односторонний, поскольку они выполняют поступающие запросы, но взамен получают лишь минимальную обратную связь. Налаживание механизмов обратной связи способно повысить мотивацию и укрепить взаимопонимание, помогая компаниям осознать, какой вклад их данные вносят в обеспечение общественной безопасности. Подобный обмен информацией может даже повлиять на процесс проектирования продуктов и привести к внедрению усовершенствований, приносящих пользу как государственным, так и частным субъектам. Частный сектор можно и нужно стимулировать к дальнейшему инвестированию в сотрудничество с правоохранительными органами, делая акцент на социальной

ответственности и подчеркивая ощутимую ценность вклада, который вносят эти компании.

Хотя представители правоохранительных органов порой воспринимают вопросы защиты данных как препятствие для сотрудничества, наличие четко определенных и всеобъемлющих рамок в этой сфере на самом деле способно облегчить процесс обмена информацией. Устанавливая ясные правовые границы и формируя единое понимание того, что является допустимым, надежные механизмы защиты прав человека помогают как правоохранительным органам, так и частным субъектам действовать с большей уверенностью и ответственностью.

(Меняющаяся) роль платформ международного сотрудничества

Цифровые технологии могут стать серьезным подспорьем для международного сотрудничества правоохранительных органов. Эти инструменты способны помочь в устранении коллизий между следственными действиями, расширении трансграничного обмена данными, поддержке оперативной координации и оптимизации взаимодействия между ведомствами. Международные конвенции — такие как Конвенция Совета Европы о киберпреступности и Конвенция Организации Объединенных Наций против киберпреступности — содержат общие определения, рамочные положения и принципы, способствующие гармонизации процедур и согласованию ожиданий в различных юрисдикциях.

Эти правовые инструменты формируют единый понятийный аппарат, что оказывается особенно полезным в тех случаях, когда правоохранительные органы проводят трансграничные расследования.

Международные организации, такие как Интерпол, УНП ООН, Совет Европы и ОБСЕ, играют важную роль — не только поддерживая сотрудничество, но и стимулируя инновации посредством обмена передовым опытом и примерами успешной практики, в том числе в сфере государственно-частного партнерства. Выступая в качестве платформ для диалога и совместного наращивания потенциала, они помогают избежать дублирования усилий и гарантировать, что опыт, накопленный в одной стране, принесет пользу и другим. Они могут способствовать более справедливому доступу к новым технологиям — особенно для стран с ограниченными ресурсами — и тем самым поддерживать создание более сбалансированной и основанной на сотрудничестве инновационной экосистемы, которая укрепляет коллективную безопасность и обеспечивает более равномерное распределение нагрузки, связанной с внедрением инноваций в правоохранительном секторе.

Законодательство в ногу со временем

Следственная деятельность строго регламентирована и регулируется постоянно расширяющимся массивом законодательных актов и судебных прецедентов, которые определяют соответствующие практики, стандарты и требования.

Виды доказательств, получаемых в ходе уголовных расследований и используемых в судебных процессах, эволюционируют вслед за развитием технологий. Например, если раньше перехват телефонных разговоров служил ценным источником доказательств при расследовании громких дел, связанных с организованной преступностью, то сегодня преступники обмениваются ключевой информацией посредством зашифрованных онлайн-звонков и приложений для обмена сообщениями. Этот сдвиг имеет глубокие последствия для следователей, которым теперь приходится ориентироваться в более сложных и децентрализованных цифровых средах для выявления доказательств.

От аналогового к цифровому

Во многих юрисдикциях к цифровым доказательствам по-прежнему зачастую применяются правовые режимы, изначально разработанные для регулирования использования вещественных доказательств, при этом соответствующие нормы применяются по аналогии. Такой подход, несомненно, обеспечивает определенную преемственность, однако в нем не учитываются уникальные характеристики цифровых доказательств — такие как их изменчивость (нестабильность), возможность неограниченного копирования и сложность определения четкой юрисдикции.

Транснациональный характер цифровых доказательств — когда данные зачастую хранятся на серверах, расположенных в разных странах, — создает дополнительные правовые и процессуальные трудности.

Для устранения этих пробелов необходимы специальные правовые нормы, обеспечивающие ясность и единообразие в вопросах выявления, сбора, хранения и использования цифровых доказательств. Кодификация ключевых стандартов в национальном законодательстве — в частности, требование о том, чтобы сбор цифровых доказательств осуществлялся в строгом соответствии с правами человека и процессуальными гарантиями, — способствовала бы повышению правовой определенности. В то же время принцип соразмерности, регулирующий использование вещественных доказательств, должен оставаться руководящим ориентиром и при работе с электронными доказательствами. Масштаб и доступность цифровых данных не должны служить обоснованием для неоправданного или чрезмерного вмешательства в права личности.

Многие государства-участники ОБСЕ, в частности те, которые являются сторонами Конвенции Совета Европы о киберпреступности, уже включили процедуры использования цифровых доказательств в свои уголовно-процессуальные кодексы и внедрили соответствующие защитные механизмы. Другие же лишь приступают к этому процессу.

Регулирование преобразований

Эффективное регулирование использования новых технологий — в особенности ИИ — в ходе уголовных расследований и судебных разбирательств является одной из наиболее актуальных задач, стоящих перед системами уголовного правосудия.

Несмотря на то, что чрезмерное регулирование чревато риском сдерживания инноваций, отсутствие четких правовых рамок представляет собой не менее серьезную проблему. Грамотно выстроенное регулирование обеспечивает прозрачность, защищает основные права и способствует укреплению общественного доверия. Правовые гарантии помогают обеспечить, чтобы сбор и обработка данных носили ограниченный и соразмерный характер, а также были обусловлены законными потребностями следствия. Кроме того, четкие правовые нормы должны закреплять права на неприкосновенность частной жизни и обеспечивать защиту лиц, сообщающих о нарушениях (осведомителей), с целью поощрения подотчетности и предотвращения злоупотреблений в ходе расследований с использованием цифровых технологий.

Разработка правовых и процессуальных рамок для применения ИИ также потребует создания надежных механизмов надзора для мониторинга и регулирования его использования — особенно в таких сферах повышенной ответственности, как правоохранительная деятельность и уголовное правосудие. Человеческий контроль должен быть интегрирован в процессы, основанные на применении ИИ, для обеспечения подотчетности и предотвращения чрезмерной зависимости от непрозрачных или непроверенных систем. Органы надзора должны быть наделены достаточными полномочиями, независимостью и ресурсами для обеспечения соблюдения установленных норм — по аналогии с

моделями регулирования, принятыми в финансовом секторе. Более того, надзор должен быть проактивным — предвосхищать потенциальные злоупотребления или системные недостатки, а не реагировать лишь после возникновения проблем. Регулирование и надзор должны дополняться практическими знаниями в рамках системы правосудия. Одним из ключевых аспектов здесь является обеспечение того, чтобы юристы-практики понимали принципы функционирования систем ИИ — в том числе логику, лежащую в основе генерируемых ими результатов, а также риски, которые эти системы могут представлять для прав человека и верховенства права.

От возможностей — к ответственности

Этическое измерение всегда оставалось неотъемлемым элементом ответственной полицейской деятельности, и в цифровую эпоху его значимость лишь возрастает. По мере того, как правоохранительные органы получают доступ к все более мощным инструментам и колоссальным массивам данных, перед ними встает вопрос не только о том, что им разрешено делать с юридической точки зрения, но и о том, что им следует (а чего не следует) делать. Само по себе наличие той или иной технологической возможности не служит автоматическим оправданием для ее использования. Как следователи, так и регулирующие органы обязаны тщательно соотносить потенциальную пользу от применения конкретного инструмента с его воздействием на неприкосновенность частной жизни, принципы справедливости и общественное доверие. В то же время, этические вопросы

возникают и в тех случаях, когда доступные технологии не используются — будь то из страха, из инертности или вследствие сопротивления на институциональном уровне. Если цифровые инструменты способны оказать существенную помощь в предотвращении вреда или раскрытии тяжких преступлений, то бездействие или сознательный отказ от их применения могут повлечь за собой собственные негативные последствия — особенно когда на кону стоят человеческие жизни и фундаментальные права. Следовательно, правоохранительным органам приходится ориентироваться в сложной этической среде, соблюдая баланс между необходимостью и соразмерностью, с одной стороны, и прозрачностью, подотчетностью и уважением к личным свободам — с другой. С этой целью, четкие руководящие принципы и регулярное обучение в области прав человека должны стать неотъемлемой частью стратегий цифровой трансформации в сфере полицейской деятельности.

Выводы и программные рекомендации

Цифровая трансформация кардинально меняет характер уголовных расследований, предоставляя беспрецедентные инструменты для повышения эффективности и результативности работы, но одновременно порождая новые операционные, правовые и этические вызовы. Цифровые технологии — включая ИИ и аналитику больших данных — становятся незаменимым

подспорьем; тем не менее, их использование требует тщательного соблюдения баланса между эффективностью следственных действий и соблюдением фундаментальных прав. Ниже представлены три ключевых вывода, сделанных по итогам обсуждений за круглым столом:

- **Непрерывная адаптация:** Расследования будут продолжать развиваться вместе с технологиями, требуя гибкости в навыках, сотрудничестве и регулировании.
- **Человеческий контроль имеет решающее значение:** Безусловно, современные технологии, такие как ИИ, повышают эффективность, однако должны быть предусмотрены механизмы прозрачности и подотчетности, для защиты от предвзятости и злоупотреблений.
- **Сотрудничество имеет ключевое значение:** Укрепление партнерских отношений между правоохранительными органами, частным сектором и международными организациями необходимо для решения трансграничных и технических сложностей.

Успешное преодоление этих трудностей требует от политиков и практиков приоритетного внимания к созданию рамок, которые бы позволили гармонично сочетать инновации с защитой прав человека, обеспечивая, чтобы технологии служили правосудию, не подрывая при этом доверие общественности. В этом контексте государства-участники ОБСЕ могли бы рассмотреть следующие программные рекомендации.

Руководство на уровне организации

- Способствовать формированию в правоохранительных органах культуры инноваций, которая поощряет экспериментирование, допускает контролируемые неудачи и вознаграждает за решение проблем.
- Преодолевать ведомственную разобщенность путем развития междисциплинарного сотрудничества между оперативными подразделениями, экспертами по цифровой криминалистике, аналитиками данных и другими ИТ-специалистами правоохранительных органов.
- Создавать в структуре полицейских ведомств специализированные подразделения по инновациям или цифровой трансформации для выявления, тестирования и масштабирования новых технологий и методов, в том числе в условиях контролируемой оперативной среды.
- Разрабатывать масштабируемые и воспроизводимые рабочие процессы расследования, сочетающие человеческий опыт с автоматизацией для обработки растущих объемов цифровых доказательств.
- Поощрять руководство на всех уровнях к продвижению адаптивных изменений и подаче личного примера в освоении новых технологий и подходов.

Навыки и подготовка

- Разработать структурированные рамочные модели компетенций для обучения в области уголовного расследования в цифровую эпоху, определяющие требования к навыкам для различных должностей в правоохранительных органах.
- Разработать специальные стратегии — или адаптировать существующие стратегии обучения — для интеграции цифровых навыков и осведомленности на всех уровнях подготовки и образования сотрудников правоохранительных органов. Такие стратегии должны быть направлены на:
 - включение базовых цифровых компетенций и осведомленности в области цифровой криминалистики в основные учебные программы полиции как для базовой подготовки, так и для дальнейшего профессионального развития, обеспечивая всех сотрудников возможностью действовать в качестве «цифровых специалистов первичного реагирования»;
 - разработку программ непрерывного повышения квалификации, в том числе в партнерстве с учебными заведениями и технологическими компаниями, чтобы следователи шли в ногу с развивающимися технологиями;
 - содействие междисциплинарной подготовке, объединяющей сотрудников правоохранительных органов,

юристов и экспертов в области технологий для повышения взаимопонимания и обмена знаниями.

Сотрудничество

- Расширить и формализовать рамки государственно-частного партнерства, в том числе с нетрадиционными участниками, такими как поставщики IoT-услуг, автопроизводители и платформы облачных сервисов, для оптимизации обмена данными с четкими протоколами конфиденциальности и подотчетности.
- Создать механизмы обратной связи для информирования партнеров из частного сектора о том, как их сотрудничество способствует расследованиям, повышая мотивацию и доверие.
- Поощрять совместные пилотные проекты между правоохранительными органами и частным сектором/учебными заведениями для совместной разработки решений, адаптированных к реальным потребностям расследований.
- Использовать международные платформы и организации сотрудничества для распределения бремени инноваций в секторе правоохранительных органов путем активного участия в совместном наращивании потенциала и обмене опытом и извлеченными уроками.
- Рассмотреть возможности реализации совместных международных проектов с целью распределения нагрузки по разработке

и пилотированию технологий ИИ для использования в ходе уголовных расследований.

Регулирование

- Разработать или усовершенствовать национальные правовые рамки для сбора, обработки и допустимости цифровых доказательств, обеспечивая соответствие стандартам в области прав человека и согласование с соответствующими международными стандартами и конвенциями.
- Ввести четкие правовые положения, регламентирующие использование ИИ в расследованиях, включая критерии прозрачности, человеческого контроля и возможности аудита.
- Разработать системы защиты данных, которые поддерживают, а не препятствуют ответственному обмену данными внутри правоохранительных органов и между полицией и частным сектором посредством четких процедур и гарантий.
- Содействовать разработке стандартизированных правовых соглашений и процедур для облегчения трансграничного доступа к цифровым доказательствам и данным.

Права человека и надзор

- Разработать руководящие принципы использования новых и перспективных технологий в уголовных расследованиях в соответствии с правами человека, основанные на необходимости,

соразмерности и справедливости.

- Создать и/или укрепить независимые надзорные органы, обладающие мандатом и ресурсами для мониторинга использования ИИ и других высокоэффективных технологий в правоохранительной деятельности.
- Интегрировать регулярное обучение в области прав человека и этики в программы профессионального развития сотрудников правоохранительных органов с целью повышения осведомленности о потенциальных этических дилеммах и формирования навыков принятия ответственных решений.
- Содействовать обеспечению прозрачности в вопросах использования цифровых инструментов и данных в ходе расследований для поддержания общественного доверия и подотчетности.
- Укреплять механизмы защиты лиц, сообщающих о нарушениях (осведомителях), а также системы внутренней отчетности для обеспечения подотчетности в случаях неправомерного использования или превышения полномочий при проведении цифровых расследований.
- Обмениваться опытом применения эффективных стратегий по обеспечению соблюдения прав человека в ходе расследований, осуществляемых с использованием технологий, а также обсуждать возникающие в этой сфере вызовы и извлеченные уроки.

Дополнительные материалы

EU Agency for Fundamental Rights (2019):

Facial recognition technology: fundamental rights considerations in the context of law enforcement,

<https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>

EU Agency for Fundamental Rights (2022): *Bias in algorithms - Artificial intelligence and discrimination,*

<https://fra.europa.eu/en/publication/2022/bias-algorithm>

Council of Europe (2024): *HUDERIA - Risk and Impact Assessment of AI Systems,*

<https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems>

Europol (2024): *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement,*

<https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf>

INTERPOL and UNICRI (2024): *Toolkit for Responsible AI Innovation in Law Enforcement,*

<https://unicri.it/Publication/Toolkit-for-Responsible-AI-Innovation-in-Law-Enforcement-UNICRI-INTERPOL>

Europol (2025): *AI bias in law enforcement - A practical guide,*

[https://www.europol.europa.eu/cms/sites/default/files/documents/AI bias in law enforcement - practical guide.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/AI%20bias%20in%20law%20enforcement%20-%20practical%20guide.pdf)

Accountability Principles for Artificial Intelligence,

<https://ap4ai.eu/>



Организация по безопасности и сотрудничеству в Европе