УДК 343.9:004
DOI: 10.19073/2658-7602-2025-22-1-128-146
EDN: OORWKV

Оригинальная научная статья

Стратегия борьбы с киберпреступностью: должное и сущее

П. А. Скобликов
Институт государства и права Российской академии наук, Москва, Российская Федерация
✉ *skoblikov@list.ru*

Аннотация. Автор привлекает внимание к тому, что в силу ряда причин правоохранительные органы не нацелены на своевременное и полное выявление преступлений, совершаемых с использованием информационно-коммуникационных технологий и в сфере компьютерной информации. Поступившие заявления о таких преступлениях зачастую не отрабатываются по горячим следам, нередко они рассматриваются по существу лишь через значительное время после приема, причем лицами, не имеющими необходимых навыков и умений, криминалистического обеспечения, оперативно-разыскных и процессуальных полномочий. Если потерпевшим не причинен материальный ущерб либо этот ущерб относительно небольшой, то, как правило, по надуманным основаниям выносятся постановления об отказе в возбуждении уголовного дела. В статье высказывается и обосновывается гипотеза о том, что фактическая преступность данного вида во много раз больше регистрируемой, а значит, субъекты уголовной политики не имеют правильного представления об обстановке в исследуемом направлении борьбы с преступностью. Подчеркивается, что в ситуации информационного дефицита невозможно принимать обоснованные управленческие решения о наиболее оптимальной расстановке имеющихся сил и средств, о потребности и масштабе их усиления, об имеющихся проблемах в организации работы и ее правовом обеспечении, об эффективных путях решения таких проблем. Сложившееся положение объясняется тем, что необходимые постулаты не закреплены в уголовно-политических документах и не воплощаются в реальной уголовной политике. Последняя настраивает правоохранителей на то, что регистрируемая преступность должна отражать пусть и сильно искаженную, но терпимую криминологическую ситуацию, а не ту неблагоприятную, которая имеет место в действительности. Автор обосновывает главные тезисы успешной борьбы с киберпреступлениями, которые должны быть закреплены концептуально и проводиться в жизнь.

Ключевые слова: информационно-коммуникационные технологии; киберпреступность; киберпреступления; стратегия борьбы с преступностью; уголовная политика; взаимодействие правоохранителей с потерпевшим; раскрытие преступлений по горячим следам; цифровая криминалистика; оперативно-розыскная деятельность; латентная преступность; отказ в возбуждении уголовного дела; участковый уполномоченный полиции

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Скобликов П. А. Стратегия борьбы с киберпреступностью: должное и сущее // Сибирское юридическое обозрение. 2025. Т. 22, № 1. С. 128–146. DOI: https://doi.org/10.19073/2658-7602-2025-22-1-128-146. EDN: https://elibrary.ru/oorwkv

Original scientific article

Cybercrime Strategy: The Ideal vs. the Reality

P. A. Skoblikov
Institute of State and Law of The Russian Academy of Sciences, Moscow, Russian Federation
✉ *skoblikov@list.ru*

Abstract. The author draws attention to the fact that, for various reasons, law enforcement agencies are not sufficiently focused on the timely and thorough detection of crimes committed using information and communication technologies or within the sphere of computer data. Reports of such crimes are often not pursued immediately, and in many cases are only addressed long after being filed – typically by personnel who lack the necessary skills, forensic tools, operational-search capacities, and procedural authority. If the victim has not suffered material damage or if the damage is relatively minor, refusals to initiate criminal proceedings are often issued on questionable grounds. The article presents and substantiates the hypothesis that the actual scale of cybercrime is many times greater than what is officially recorded. As a result, the stakeholders in criminal policy lack an accurate understanding of the situation in this area of crime control. The author emphasizes that in the face of such an information deficit, it is impossible to make informed managerial decisions regarding the optimal allocation of existing resources, the need for and extent of reinforcement, existing organizational and legal shortcomings, or effective strategies for improvement. This problematic situation is rooted in the fact that essential principles are neither established in criminal-policy documents nor reflected in real-world criminal policy. Current policy encourages law enforcement to present a distorted but tolerable picture of criminological conditions, rather than confront the unfavorable realities on the ground. The article concludes by articulating key principles for an effective cybercrime strategy – principles that must be formally outlined at the conceptual level and consistently implemented in practice.

Keywords: information and communication technologies; cybercrime; cyber offenses; crime control strategy; criminal policy; interaction between law enforcement and victims; hot pursuit crime detection; digital forensics; operational and investigative activities; latent crime; refusal to initiate criminal proceedings; district police commissioner

Conflict of interest. The Author declares no conflict of interest.

For citation: Skoblikov P. A. Cybercrime Strategy: The Ideal vs. the Reality. *Siberian Law Review.* 2025;22(1):128-146. DOI: https://doi.org/10.19073/2658-7602-2025-22-1-128-146. EDN: https://elibrary.ru/oorwkv (In Russ.)

Введение

На рубеже 2022–2023 гг. в Министерстве внутренних дел Российской Федерации и подчиненных ему подразделениях произошли некоторые существенные организационно-штатных изменения, осуществлена корректировка компетенций. Ключевое преобразование предопределено изданием Указа Президента Российской Федерации от 30 сентября 2022 г. № 688[1], согласно которому в структуре центрального аппарата МВД России появилось Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (далее – Управление, УБК), которое отнесено к подразделениям полиции. Было разработано и принято Положение

[1] *О внесении* изменений в некоторые акты Президента Российской Федерации : Указ Президента Рос. Федерации от 30 сент. 2022 г. № 688. Доступ из СПС «КонсультантПлюс».

об этом Управлении[2]. В соответствии с ним Управление выполняет функции головного подразделения МВД России в области борьбы с преступлениями, совершенными с использованием или в сфере информационно-коммуникационных технологий, а также противодействия распространению противоправной информации в информационно-телекоммуникационной сети Интернет.

Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России и подразделения по борьбе с противоправным использованием информационно-коммуникационных технологий территориальных органов МВД России на региональном уровне созданы за счет штатной численности ликвидируемого Управления «К»[3] Бюро специальных технических мероприятий и соответствующих подразделений на местах[4].

УБК МВД России должно обеспечивать и осуществлять в пределах компетенции функции своего министерства *по выработке и реализации государственной политики и нормативно-правовому регулированию в области организации противодействия противоправным деяниям, совершаемым с использованием (либо в сфере) информационно-коммуникационных технологий*. В функции УБК МВД России входит не только осуществление оперативно-разыскной деятельности в полном объеме, мониторинг и анализ оперативной обстановки, разработка мер по оперативному реагированию на ее изменение и многое другое, но также *подготовка проектов стратегических решений по вопросам его деятельности*.

Указ 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»[5] установил следующие целевые показатели и задачи, выполнение которых характеризует достижение национальной цели по цифровой трансформации государственного и муниципального управления, экономики и социальной сферы: «…создание системы эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, и снижения ущерба от их совершения» (подп. «к» п. 8). Причем процитированное положение – единственное в данном указе (всего им предусмотрено до 100 целевых показателей и задач), имеющее непосредственное отношение к вопросам борьбы с преступностью.

26 сентября 2024 г. председатель Комитета Государственной Думы по информационной политике, информационным технологиям и связи А. Е. Хинштейн в своем телеграм-канале написал, что главными задачами, стоящими перед возглавляемым им Комитетом в период осенней сессии, «является борьба с киберпреступностью и ужесточение ответственности за утечку персональных данных»[6].

Всё изложенное подчеркивает повышенную актуальность и сложность

---

[2] *Об утверждении* Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации : приказ МВД России от 29 дек. 2022 г. № 1110. Доступ из СПС «КонсультантПлюс».

[3] Управление «К» создавалась по решению Министра внутренних дел, в структуру центрального аппарата МВД России не входило, то есть имело более низкий статус, нежели УБК МВД России, а также имело меньший объем функций и задач по сравнению с УБК МВД России.

[4] См., напр.: *О внесении* изменений в приказ МВД России от 30 апреля 2011 г. № 333 «О некоторых организационных вопросах и структурном построении территориальных органов МВД России : приказ М-ва внутр. дел Рос. Федерации от 31 окт. 2022 г. № 812. Документ опубликован не был.

[5] Доступ из СПС «КонсультантПлюс».

[6] *Александр* Хинштейн : телеграм-канал. 2024. URL: https://t.me/Hinshtein/7830 (дата обращения: 17.10.2024).

избранной нами темы и побуждает представить некоторые итоги наших изысканий, высказать ряд соображений относительно стратегии деятельности новой службы, образованной в МВД России, да и в целом уголовной политики государства по вопросам борьбы с правонарушениями, совершаемыми с использованием или в сфере информационно-коммуникационных технологий. При этом автор не стремится к освещению всего диапазона темы, а намерен сконцентрироваться на тех ее аспектах, которые не раскрыты или неудовлетворительно представлены в иных исследованиях.

1. Каков масштаб киберпреступности[7] и отдельных ее видов? Анализ результатов некоторых социологических исследований и сопоставление с уголовной статистикой

В 2024 году всего в России зарегистрировано 746 365 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (киберпреступлений), что почти на 13,1 % больше, чем за аналогичный период предыдущего года, и на 43 % больше по сравнению с 2022 г. Характерно также, что такой масштабный рост наблюдается на фоне общего снижения регистрируемой преступности.

В общем числе зарегистрированных преступлений удельный вес киберпреступлений увеличился до 40 %. Больше половины анализируемых преступлений (48,2 %) относится к категориям тяжких и особо тяжких (369,3 тыс.; + 7,8%), четыре из пяти (84,8 %) совершается с использованием сети Интернет (649,1 тыс.; + 23,2 %), а почти половина (45,2 %) совершена с помощью средств мобильной связи (346 тыс.; + 14,3 %)[8].

В структуре преступности рассматриваемого вида преобладают мошенничества (ст.ст. 159, 159.3, 159.6 Уголовного кодекса Российской Федерации (далее – УК РФ)), их доля составляет практически половину – 49,7 %; кражи (ст. 158 УК РФ) с долей в 14,4 %; преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) с долей в 13,8 %[9].

Столь значительная доля тяжких и особо тяжких преступлений указывает на высокую латентность интересующих нас преступлений. Какова она? Чтобы получить представление об этом, обратимся к теме так называемых телефонных мошенничеств. Ее изучение в свете поставленной нами задачи представляется перспективным по нескольким причинам. Во-первых, потому что мошенничества, как указано выше, – самые распространенные деяния в структуре регистрируемой киберпреступности. Во-вторых, по теме телефонных мошенничеств опубликовано немало социологических исследований, дающих удобный материал для криминологического анализа. В-третьих, применительно к телефонным мошенничествам гражданам проще понять, что они стали объектами преступных посягательств, даже если злоумышленнику не удалось

[7] Под киберпреступностью нами понимается совокупность уголовно наказуемых деяний, совершаемых с использованием цифровых устройств и (или) в телекоммуникационных сетях (прежде всего, в сети Интернет). Соответственно, киберпреступление – одно из таких деяний.

[8] *Состояние* преступности в России за январь–декабрь 2024 года // Офиц. сайт М-ва внутр. дел Рос. Федерации. 2025. URL: https://media.mvd.ru/files/application/9209203 (дата обращения: 24.01.2025).

[9] В этом абзаце расчет долей произведен автором, исходя из опубликованных Главным информационным центром (ГИАЦ) МВД России количественных данных. Так, всего в России в 2024 г. зарегистрировано 380 344 мошенничеств с использованием информационно-коммуникационных технологий или в сфере компьютерной информации. Из них преступлений, предусмотренных ст. 159 УК РФ – 379 762, предусмотренных ст. 159.3 УК РФ – 273, и ст. 159.6 УК РФ – 309. См.: *Состояние* преступности в России за январь–декабрь 2024 года …

реализовать свой замысел в полной мере (в ходе общения со злоумышленниками они могут задавать проверочные вопросы, сопоставлять информацию и т. д.), поэтому результаты их опросов более достоверные[10]. В-четвертых, в подобных случаях выше вероятность того, что потерпевшие обратятся в правоохранительные органы. В-пятых, телефонные мошенничества более доступны для исследования методом включенного наблюдения, который дает возможность выявить значимые подробности, ускользающие при иных подходах к исследованию.

15 февраля 2024 г. информационное агентство ТАСС опубликовало результаты опроса, осуществленного социологическим агентством «Вебер» по проекту АНО «Диалог Регионы». Опрос проводился 8 февраля 2024 г. в сети Интернет методом River Sampling среди 1300 россиян старше 18 лет. Выяснилось, что 88 % опрошенных когда-либо получали звонки или смс от телефонных мошенников, 21 % (то есть каждый пятый) – попадался на уловки телефонных мошенников, а 10 % опрошенных в результате таких махинаций теряли денежные средства[11]. В какой период произошли данные события – не сообщается. Будем исходить из того, что период не превышает 10 лет, потому что именно в это время получило широкое распространение использование россиянами интернет-банков и банковских приложений для мобильных телефонов, портала Госуслуг и других электронных сервисов, что серьезно облегчает задачу кибермошенникам. Помимо этого, надо учесть, что более отдаленные события люди зачастую забывают или, по крайней мере, не могут быстро вспомнить. И наконец, за пределами выбранного нами периода многие опрошенные являлись несовершеннолетними и в силу возраста не могли стать объектами мошеннических атак либо не располагали финансовыми активами.

Если экстраполировать приведенные результаты на всё взрослое население России[12], то можно прийти к следующему выводу: за последние годы объектами атак телефонных мошенников стали около 105 млн россиян. При этом количество таких атак многократно превосходит указанное число россиян, поскольку атаки в отношении одного и того же человека происходят не один раз в 10 лет, а много чаще, вплоть до нескольких раз в неделю. Так, по результатам проведенного SuperJob[13] опроса (эти результаты опубликованы на портале РБК[14] и продублированы на иных интернет-ресурсах),

[10] Поясним эту мысль путем сравнения с иными противоправными деяниями в рассматриваемой сфере. Допустим, персональный компьютер или смартфон гражданина был атакован преступниками посредством такой уловки, как помещение в электронное письмо или сообщение из мессенджера каким-то образом замотивированного приглашения пройти по интернет-ссылке, посмотреть фото и т. д. В случае, если пользователь гаджета воспользуется приглашением, на его устройство загрузится вредоносная программа, нацеленная на хищение персональных данных, паролей и другой информации. Однако большинство граждан не проявляют интереса или проявляют осмотрительность, не загружая вредоносную программу. В каждом таком случае имеет место незаконченное покушение на преступление, но граждане об этом не знают либо предполагают, но не уверены, и в правоохранительные органы о происшедшем не сообщают.

[11] *Каждый* пятый опрошенный россиянин становился жертвой телефонных мошенников // ТАСС. 2024. URL: https://tass.ru/obschestvo/19993285 (дата обращения: 21.10.2024).

[12] По данным Федеральной службы государственной статистики, взрослое население России на 1 января 2024 г. составило 119 305 000 чел. (84 711 500 чел. – трудоспособное население, 34 593 500 – лица старше трудоспособного возраста). См.: *Численность* населения Российской Федерации по полу и возрасту // Федер. служба гос. статистики. 2024. URL: https://rosstat.gov.ru/compendium/document/13284 (дата обращения: 20.10.2024).

[13] Один из самых крупных в России IT-сервисов по поиску работы и подбору сотрудников. С 2005 г. на базе портала SuperJob создан исследовательский центр. Отдельное направление деятельности – социологические исследования в форме опросов экономически активного населения.

[14] РБК – РосБизнесКонсалтинг – российская медиагруппа.

подозрительные телефонные звонки от людей, похожих на мошенников, *регулярно* получают восемь из десяти россиян, причем 13 % респондентов сообщили, что получают такие звонки ежедневно, 20 % – несколько раз в неделю, а еще 23 % – несколько раз в месяц. В данном опросе приняли участие 1600 респондентов из 507 городов во всех федеральных округах страны. Опрос проходил 26–29 сентября 2021 г.[15]

В свете изложенного количество мошеннических атак посредством телефона сложно подсчитать даже приблизительно, но в любом случае это число за 10 предшествующих лет превысило миллиард и составляет, возможно, десятки или даже сотни миллиардов; по крайней мере, в течение года количество мошеннических атак такого рода может насчитывать от нескольких сотен миллионов до миллиарда и более.

Каждая подобная атака – неудавшееся покушение на мошенничество с использованием информационно-коммуникационных технологий, которое, как правило, не было доведено до конца по не зависящим от посягающего лица обстоятельствам[16]. Следовательно, виновные должны нести уголовную ответственность, даже если не смогли завладеть имуществом потерпевших и (или) причинить им имущественный вред (ч. 3 ст. 30 УК РФ). *В уголовной статистике подобные деяния должны отражаться наряду с оконченными преступлениям*.

Между тем уголовная статистика показывает кардинально иную картину. Согласно сведениям ГИАЦ МВД России, в 2023 г. в целом по стране выявлено и зарегистрировано чуть более 356 тыс. мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. По сравнению с предыдущим годом рост составил + 38,2 % (то есть в 2022 г. зарегистрировано лишь 257,6 тыс. анализируемых мошенничеств)[17]. Данный результат приблизительно в тысячу раз меньше того количества деяний, на которое указывают социологические опросы, и это при том, что телефонные мошенничества, с одной стороны, и мошенничества, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, с другой, соотносятся между собой как часть и целое (мошенники также атакуют своих потенциальных жертв через электронную почту, мессенджеры и другие каналы электронных коммуникаций). Иначе говоря, число зарегистрированных телефонных мошенничеств еще меньше приведенных статистических данных.

Но даже если абстрагироваться от покушений на телефонные мошенничества и принимать во внимание лишь оконченные преступления (в результате которых телефонным мошенникам удалось завладеть деньгами потерпевших), то социологические опросы дают основания ожидать отражения в уголовной статистике последнего десятилетия примерно 1,2 млн таких преступлений за год, но никак не около 100–200 тысяч. Таким образом, есть веские доводы предполагать крайне высокую степень латентности рассматриваемых преступлений – на несколько порядков больше зарегистрированных.

---

[15] *Каждый* шестой россиянин пострадал из-за телефонных мошенников // РБК. 2021. URL: https://www.rbc.ru/technology_and_media/02/10/2021/6156e99a9a794778904993ed (дата обращения: 21.10.2024).

[16] Согласно результатам опроса, осуществленного 8 февраля 2024 г. социологическим агентством «Вебер», 81 % россиян прекращают разговор, если начинают подозревать, что с ними общаются телефонные мошенники. См.: *Каждый* пятый опрошенный россиянин становился жертвой телефонных мошенников …

[17] *Состояние* преступности в Российской Федерации за январь–декабрь 2023 года // Офиц. сайт М-ва внутр. дел Рос. Федерации. 2024. URL: https://media.mvd.ru/files/application/5095078 (дата обращения 21.10.2024).

2. Насколько актуальны изменения антикриминального и иного законодательства?

У нас нет оснований считать, что для эффективного противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий (киберпреступлениям), требуется разработка и принятие каких-либо специальных федеральных законов. По мере осуществления практической деятельности правоохранительными органами определенные проблемы, связанные с пробелами и противоречиями антикриминального законодательства, а также упускаемые возможности будут выявляться, что потребует периодического внесения точечных изменений в это законодательство.

Могут быть оправданными некоторые дополнения Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ). Например, в научной литературе обсуждается целесообразность включения в уголовный процесс принципиально нового следственного действия – онлайн-обыска. Суть данного мероприятия заключается в тайном внедрении в компьютер подозреваемого/обвиняемого специальной вирусной программы, которая затем передает следствию сведения о доступе к облачному хранилищу и операциях с ним в режиме текущего времени. В этом случае доказательства получаются органом предварительного расследования в режиме онлайн, по аналогии с уже предусмотренным в ст. 186 УПК РФ контролем и записью переговоров [1, с. 120–121]. Возможно, если будет разработан и принят выверенный законопроект о соответствующем дополнении УПК РФ, это благоприятно скажется на ходе и результатах предварительного расследования киберпреступлений, схема подготовки и совершения которых предполагает использование облачного хранилища.

Не исключается криминализация и пенализация некоторых новых или уже известных деяний, но только если для этого будут усматриваться достаточные основания. Фиксация совершаемых с использованием информационно-коммуникационных технологий деяний, способ осуществления которых отличается от ранее известных, но укладывается в его уголовно-правовое описание из той или иной статьи Особенной части действующего УК РФ, не является достаточным основанием криминализации (введения специальных норм) или пенализации, если вариативные деяния не отличаются от иных преступлений по характеру и степени общественной опасности и нет иных серьезных обстоятельств для модернизации законодательства[18].

На состоявшемся 25 сентября 2024 г. заседании Общественного совета при МВД России глава министерства В. Колокольцев сообщил, что разработан законопроект, предусматривающий введение уголовной ответственности за передачу электронного средства платежа или предоставление к нему доступа иным лицам на возмездной основе[19]. Вероятно, речь идет о том, чтобы таким путем нарушить условия анонимности лиц, занимающихся выведением и обналичиванием похищенных денежных средств. В связи с этим полезно отметить, что *если уже существующие в какой-то сфере деятельности уголовно-правые запреты, обоснованность которых не ставится под сомнение, не исполняются, виновные лица не устанавливаются, не привлекаются к ответственности и не подвергаются*

[18] Похожая мысль уже высказывалась в юридической литературе, но в связи с частной проблемой и с другими акцентами [2, с. 57].

[19] *Владимир* Колокольцев принял участие в заседании Общественного совета при МВД России, на котором обсуждались вопросы противодействия киберпреступности // МВД Медиа. 2024. URL: https://mvdmedia.ru/news/official/vladimir-kolokoltsev-prinyal-uchastie-v-zasedanii-obshchestvennogo-soveta-pri-mvd-rossii-na-kotorom-/ (дата обращения: 22.10.2024).

справедливым наказаниям, то введение новых запретов в этой сфере теряет практический смысл.

Преступные схемы, применяемые в настоящем (установленные в ходе оперативно-разыскной деятельности и предварительного расследования) и прогнозируемые в будущем, при соответствующем анализе указывают на то, какие изменения целесообразно вносить в законодательство, регулирующее сферу информационных технологий, для минимизации преступных проявлений[20].

Однако *назревшие изменения нельзя внести в законодательство раз и навсегда, потому что прогресс в развитии и внедрении в жизнь данных технологий идет (и будет идти) в высоком темпе; необходима планомерная законотворческая работа, исходящая из актуальных, достаточно полных и точных результатов правоохранительной деятельности*.

3. Главные проблемы и ключевые моменты

Главные проблемы в рассматриваемом направлении борьбы с преступностью видятся нам в неудовлетворительной организации работы (выдвижении второстепенных задач в качестве главных и игнорировании задач первостепенных, неудовлетворительной системе оценки результатов проведенной работы, плохо продуманной расстановке имеющихся сил и средств и т. д.), а также в недостаточном количестве и качестве сил и средств, привлекаемых для борьбы с киберпреступлениями (что требует адекватного расширения штатов, создания надлежащих стимулов для привлечения на работу людей, обладающих необходимой подготовкой и морально-деловыми качествами, переподготовки имеющихся кадров, укрепления материально-технической базы, оснащения передовым криминалистическим оборудованием и т. п.).

Ключевые моменты, которые, на наш взгляд, *должны быть отражены в Концепции государственного противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий* (далее – Концепция), *– это основные проблемы данной сферы и обусловленные ими первостепенные задачи, основные способы их решения.* Соответственно, одно из направлений реализации положений будущей Концепции после ее разработки и принятия – ревизия и корректировка действующих ведомственных и межведомственных правовых актов с учетом концептуальных положений.

4. Первостепенная задача

Наипервейшей задачей в области борьбы с преступлениями, в основе которых лежит использование информационно-коммуникационных технологий, является максимально полное выявление и точная фиксация всех обнаруженных фактов такого рода.

Особая важность названной задачи обусловлена тем, что успешное ее решение является непременным условием выполнения иных задач, которые объективно стоят перед субъектами уголовной политики и правоохранительными органами в рассматриваемой области деятельности.

1. Полная и точная картина совершаемых киберпреступлений и правонарушений позволит получить правильное представление о том, какие требуются силы и средства для раскрытия, расследования и предупреждения таких деяний

[20] Наглядный пример – самозапрет на получение онлайн-кредитов и отправление денежных переводов. Подробнее см., напр.: *С 2025 года* россияне смогут устанавливать самозапрет на выдачу кредитов: как он будет работать // Банки.ру. 2023. URL: https://www.banki.ru/news/daytheme/?id=10980251 (дата обращения: 22.10.2024). (Причем информативным является не только редакционный материал, но и комментарии пользователей.)

в стране в целом и в отдельных регионах в частности.

2. Полная и точная картина совершаемых киберпреступлений и правонарушений даст возможность проанализировать структуру данного вида преступности, вычленить узловые звенья и расставить имеющиеся силы и средства правоохранительных органов наилучшим образом, обеспечивающим наибольший эффект на выходе.

3. Подавляющее большинство киберпреступлений совершаются серийно; зачастую в течение только одного дня преступники предпринимают десятки подходов к различным лицам в поисках перспективной и податливой жертвы. Поэтому фиксация всех подобных фактов в оптимально структурированной базе данных позволит при помощи соответствующих компьютерных программ (или, как модно ныне выражаться, искусственного интеллекта) из отдельных фрагментов составить и прояснить используемые преступные схемы, свести воедино разрозненные улики, относящиеся к одной и той же группировке, проследить движение похищенных активов, с большей вероятностью установить и задержать причастных лиц, а в результате резко повысить реальную раскрываемость данных преступлений, более полно возмещать причиненный преступлениями вред.

4. В ходе расследования преступлений рассматриваемого вида зачастую становится понятно (даже если расследование не приводит к раскрытию), что многие преступники действуют на территории определенных стран, или перемещаясь по нескольким конкретным странам. Эта информация после обобщения позволит решить, с правоохранительными органами каких стран требуется наладить эффективное взаимодействие прежде всего, а также каким должно быть это взаимодействие применительно к разным странам.

5. Полная и точная картина обращений пострадавших от противоправных деяний с использованием информационно-коммуникационных технологий, выявленных преступлений и правонарушений в данной области вкупе с результатами производства по соответствующим делам позволит объективно оценить адекватность действующего антикриминального законодательства (уголовного, уголовно-процессуального, оперативно-разыскного, уголовно-исполнительного и проч.), а равно ведомственного и межведомственного нормативного регулирования; затем при необходимости позволит обосновать инициативы о внесении назревших изменений.

5. Задачи быстрого реагирования на киберпреступления и эффективного взаимодействия с потерпевшими

К задаче максимально полного выявления и точной фиксации противоправных деяний, в основе которых лежит использование информационно-коммуникационных технологий, примыкает *задача оптимально быстрого реагирования на их совершение, с тем чтобы попытаться задержать причастных лиц по горячим следам, закрепить эти следы, пока они не «остыли».* Такая же задача объективно стоит перед правоохранительными органами при организации борьбы с иными (назовем их классическими или традиционными) преступлениями[21], но в рассматриваемом случае несколько новых обстоятельств повышают ее актуальность.

С *одной стороны*, преступники, совершающие свои деяния с использованием информационно-телекоммуникационных технологий, значительно легче и быстрее могут уничтожить следы своих

[21] На эту тему проведено множество исследований и обоснованные в их рамках рекомендации давно стали аксиомой [3].

противоправных деяний, применяя соответствующие меры заблаговременно или постфактум: использовать методы шифрования и самоуничтожающиеся программы, маскировать IP-адреса, стереть состоявшуюся электронную переписку, удалить аккаунты, использованные в преступных схемах, сменить телефонные номера и IP-адреса [4], избавиться от скомпрометированных гаджетов, полностью и навсегда прекратить контакты с лицами, оказывающими им содействие втемную, и т. д. При этом, в отличие от ситуаций, складывающихся при совершении классических преступлений, в которых вся цепочка событий разворачивается офлайн, здесь для уничтожения улик преступнику не нужно приезжать на место преступления или присылать туда кого-то; как совершать преступления, так и уничтожать их следы он может и находясь за сотни и тысячи километров от своих жертв.

С *другой стороны*, при совершении рассматриваемых преступлений объективно возрастает значимость своевременного установления и поддержания оперативными работниками контактов с лицами, которые стали объектами атак со стороны мошенников и других преступников, действующих дистанционно, использующих в своих схемах информационно-телекоммуникационные технологии. Как показывает наше изучение, после первой попытки через несколько часов или дней в развитие своей схемы они могут совершать дополнительные действия, присылать потенциальной жертве новые сообщения, продолжать разыгрывать различные роли, вводить новых персонажей. Если же удалось установить контроль над жертвой и первоначальное преступление доведено до конца, то позже с новым сценарием, учитывающим опыт взаимодействия с жертвой, ее могут вновь атаковать, чтобы до конца исчерпать те имущественные активы, к которым у жертвы есть доступ. Помимо этого, жертву могут побудить к оказанию содействия преступникам в иных преступных схемах (против иных лиц), требующих определенных действий офлайн (забрать и передать деньги, документы, технические устройства) и даже исполнения неких ролей перед новыми жертвами. Наконец, как показывает практика, внушаемые жертвы уже состоявшихся корыстных преступлений способны стать исполнителями политических акций, диверсий и других деяний в интересах враждебных России сил.

После совершении традиционных преступлений виновные, как правило, не заинтересованы в новых контактах со своими жертвами и, более того, стремятся их избегать; следствием такой тактики является то, что для совершения традиционных преступлений (карманных и квартирных краж, грабежей, изнасилований и проч.) профессиональные и серийные преступники выезжали и выезжают в другие районы, города, дабы свести к минимуму вероятность последующих встреч со своими жертвами. Однако грамотные сотрудники уголовного розыска всегда инструктировали потерпевших от указанных преступлений о поведении при случайной встрече и опознании злоумышленника, оговаривали способы оперативной связи, чтобы при такой удаче установить личность и задержать подозреваемого.

Эта *задача – достижения эффективного взаимодействия оперативных работников с потерпевшими – становится более сложной и более актуальной, когда граждане оказываются объектами атак преступников, действующих дистанционно.* Если первую атаку своевременно не выявить, преступная деятельность против первоначального потерпевшего и с его участием, а также против новых жертв будет продолжаться и масштабироваться. Если же оперативные работники без промедления встретятся с человеком, который стал объектом преступного интереса, обсудят варианты новых активностей

злоумышленников против него, дадут эффективные рекомендации для действий при том или ином варианте, будут постоянно находиться на связи, то возникнет благоприятная ситуация не только для предупреждения новых преступлений, но и для ведения оперативной игры, проведения оперативных комбинаций. Посредством таких методов, используя азарт и стремление злоумышленников умножить противоправные доходы, можно побудить их совершить ошибки, раскрыться, а в итоге – установить личности и задержать виновных.

6. Практика реагирования на заявления о киберпреступлениях. Выборочное исследование

Какова же современная правоприменительная практика в части реагирования на заявления граждан, столкнувшихся с деяниями, совершаемыми с использованием информационно-коммуникационных технологий? В какой мере обоснованные выше задачи решаются в деятельности правоохранительных органов?

Выборочное и углубленное исследование, проведенное нами в 2018–2024 гг., позволяет в качестве предварительного результата описать фактический порядок реагирования органов МВД России на обращения граждан, в отношении которых неизвестные лица при помощи информационно-коммуникационных технологий предприняли действия, содержащие признаки ряда преступлений.

Прежде чем описать обнаруженный порядок, целесообразно сделать несколько пояснений. Данное небольшое исследование проводилось путем опроса граждан, изучения предоставленных ими документов, а также посредством использования методов включенного наблюдения и правового эксперимента.

Во всех изученных случаях к пострадавшим гражданам по мобильной телефонной связи, через мессенджеры или электронную почту обращались некие лица, которые располагали более или менее полным набором персональных данных о гражданах, выдавали себя за представителей различных финансовых или коммерческих организаций, должностных лиц государственных органов либо представлялись известными в той или иной сфере деятельности персонами. Далее разыгрывались различные сценарии, направленные на то, чтобы побудить граждан предоставить какие-то сведения о себе и организации, в которой работают, совершить какие-то действия финансового и иного характера и др.

Высока вероятность, что в каждом таком случае против граждан совершено и закончено преступление, предусмотренное ч. 2 ст. 272 УК РФ, – неправомерный доступ к охраняемой законом компьютерной информации, поскольку деяние повлекло копирование информации и совершено с корыстной целью (это может объяснить, каким образом неизвестные завладели персональными данными граждан), и (или) другое преступление, предусмотренное ст. 137 УК РФ «Нарушение неприкосновенности частной жизни». Кроме того, в большинстве указанных случаев усматриваются признаки покушения на мошенничество либо иные преступления, которые не были доведены до конца по не зависящим от посягающего лица обстоятельствам (ч. 3 ст. 30 УК РФ), а следовательно, виновные должны нести уголовную ответственность, даже если не причинили материальный ущерб потерпевшим.

Кто-то из потерпевших в изученных случаях обращался в правоохранительные органы, оформив соответствующее заявление на бумаге и отправив его традиционной почтой. Иные в целях быстроты доставления и рассмотрения отправляли свои заявления по электронной почте или через интернет-сайт

правоохранительного органа, заполнив там специальную форму. Граждане обращались с данными заявлениями к руководству разных уровней – МВД России, управлений (главных управлений) МВД России по соответствующему субъекту Российской Федерации, специализированного Управления «К» МВД России. Заявления имели различную степень проработанности, часть из них тщательно выверялась с помощью подготовленного юриста, имеющего опыт оперативно-следственной работы. Действия злоумышленников анализировались, им давалась правовая оценка. К заявлениям прилагались копии состоявшихся переписок, аудиофайлы с записью речи злоумышленников, справки от мобильного оператора и провайдера об имевших место соединениях (с кем, когда, по чьей инициативе) и т. д. В резолютивной части заявлений некоторые граждане формулировали ходатайства о проведении целесообразных и неотложных, с их точки зрения, проверочных и следственных действий, оперативно-разыскных мероприятий, об установлении иных потерпевших и сопоставлении полученных данных с теми, что изложены в заявлениях, и т. д.

7. Негативные результаты и последствия

Все обозначенные вариации обращений не влияли на конечный результат, он был единообразным: после прохождения длительной административной процедуры (занимавшей несколько недель) все заявления поступали в отделы полиции по месту жительства подавших заявления граждан и поручались для рассмотрения участковым уполномоченным полиции. В свою очередь последние оформляли письменные объяснения граждан (которые в основном дублировали сведения, изложенные в заявлениях) либо справки о том, что с гражданами не удалось связаться, а *затем по надуманным основаниям выносили постановления об отказе в возбуждении уголовного дела.* В отдельных случаях прокуроры в рамках надзора за соблюдением установленного порядка разрешения заявлений и сообщений о совершенных и готовящихся преступлениях отменяли постановления об отказе в возбуждении уголовного дела и назначали дополнительную проверку. Однако такая проверка выражалась, как правило, лишь в отобрании от заявителей дополнительных объяснений, затем повторно выносились постановления об отказе в возбуждении уголовного дела; о вынесении таких повторных постановлений заявители не извещались, их копии не получали[22].

Это закономерный результат, поскольку участковые уполномоченные полиции не имеют необходимых знаний, умений, инструментов, полномочий и времени для доследственной проверки и расследования преступлений, тем более таких сложных и высокотехнологичных.

Итак, *есть основания предполагать, что если в органы МВД России поступают*

[22] Довольно давно в правоприменительной практике сложилась система приемов и уловок правоохранителей, направленных на противодействие возбуждению тех уголовных дел, которые по каким-то причинам представляются нежелательными. Среди таких приемов: нерегистрация в установленном порядке принятого заявления о преступлении; нерассмотрение принятого и зарегистрированного заявления о преступлении в установленном процессуальном порядке; неуведомление в установленном порядке заявителя о принятом процессуальном решении (о направлении заявления по подследственности либо об отказе в возбуждении уголовного дела); ненаправление или направление с большим опозданием заявителю копии постановления об отказе в возбуждении уголовного дела (что препятствует подготовке заявителем мотивированной жалобы на принятое решение), согласно действующему закону такая копия должна быть направлена в течение 24 часов с момента вынесения соответствующего постановления, независимо от желания/нежелания заявителя. Подробнее см.: *Скобликов П. А.* Противодействие правоохранителей возбуждению уголовных дел: система типичных приемов и уловок // Закон. 2016. № 7. С. 92–105.

заявления о преступлениях (либо покушениях на преступления), предусмотренных ст.ст. 137, 272, 159, 159.3, 159.6 УК РФ, совершенных с использованием информационно-коммуникационных технологий, которые не причинили потерпевшим существенного материального ущерба, то работа по их проверке с привлечением оперативных работников, следователей и экспертов-криминалистов не проводится, методы оперативно-разыскной деятельности и цифровой криминалистики не применяются, следы преступлений не фиксируются, предварительное расследование не осуществляется; априори выносятся постановления об отказе в возбуждении уголовного дела.

Описанная практика опасна не только тем, что происходит фактическое укрытие преступлений, а виновные получают возможность безнаказанно продолжать преступную деятельность (хотя это, конечно, главное). Нужно также указать на то, что участковые уполномоченные полиции отвлекаются от исполнения своих основных функций[23] и не оправдывают ожидания граждан на обслуживаемых участках, а также на то, что разъяснения прокуратуры[24] и обоснованные рекомендации специалистов[25] о том, кто и как должен расследовать киберпреступления, оказываются невостребованными – к следователям материалы попросту не попадают.

Не менее существенно то, что с высокой степенью вероятности заявители впредь не станут обращаться в правоохранительные органы за помощью, если вновь станут жертвами преступных атак, а кроме того, расскажут о своем негативном опыте родственникам и знакомым, которые сделают соответствующие выводы. Таким образом, *латентность рассматриваемых преступлений будет возрастать, равно как растет безопасность и привлекательность преступной деятельности в сфере высоких технологий. А еще увеличивается отчуждение граждан от государства, недоверие первых ко второму.*

8. Показательный пример из современной правоприменительной практики

Для более полного раскрытия темы настоящей статьи было бы полезным сравнить практику рассмотрения заявлений граждан о покушении на мошенничество с использованием информационно-коммуникационных технологий и о неправомерном доступе к компьютерной информации в периоды до создания УБК МВД России (см. предыдущие разделы статьи) и после того, как это Управление и соответствующие подразделения территориальных органов МВД России на региональном уровне были сформированы и развернули свою работу в полном объеме. Для этого нами выявлен и приводится показательный пример.

[23] На условиях анонимности некоторые участковые уполномоченные полиции, проходящие службу в столичном регионе, пояснили нам, что в течение месяца им приходится проверять и разрешать несколько десятков заявлений о преступлениях, каждый раз вынося постановления об отказе в возбуждении уголовного дела. И это отнюдь не только и не столько заявления о киберпреступлениях: подобным образом канализируются зарегистрированные сообщения о любых преступлениях, которые по тем или иным причинам неудобны лицам, осуществляющим или контролирующим уголовно-процессуальную деятельность. Исследование о мотивах таких решений ранее было представлено в юридической литературе. Подробнее см.: *Скобликов П. А.* Мотивы необоснованных и незаконных отказов в возбуждении уголовных дел // Уголовный процесс. 2013. № 4 (100). С. 68–75.

[24] См., напр.: *Особенности* расследования уголовных дел в сфере информационных технологий. Разъясняет аппарат прокуратуры области // Офиц. сайт Правительства Свердлов. обл. 2020. URL: https://midural.ru/normative_documents/100615/100629/page2/document166027/ (дата обращения: 09.10.2024).

[25] Из-за ограничений по объему настоящей статьи мы не имеем возможности назвать все публикации такого рода (их насчитываются уже сотни), но для наглядности приведем несколько [5–9].

Субботним утром, 28 сентября 2024 г., на мобильный телефон гражданина П. поступил звонок с неизвестного ему номера с префиксом 918[26]. Звонивший обратился к П. по имени-отчеству, а сам представился Беловым А. В., работником АО «Мосэнергосбыт». Белов (будем называть его так) известил, что в доме по месту жительства П. производится бесплатная («по федеральной программе») замена действующих индивидуальных электросчетчиков на трехтарифные. Для этого необходимо выбрать подходящий день и время, чтобы принять работника Мосэнергосбыта. Затем Белов попросил записать номер электросчетчика, который будет доставлен и подключен[27]. После этого он сообщил, что будет оформлен договор на установку электросчетчика, огласил дату рождения П. (привел ее точно)[28], и заявил, что, помимо имеющихся данных, гражданин должен указать свой СНИЛС. На вопрос «зачем?» Белов ответил, что новый счетчик будет оснащен сим-картой для автоматической передачи данных[29], поэтому нужны дополнительные персональные данные.

П., являющийся пенсионером МВД России и имеющий опыт оперативной работы, затем спросил, принимает ли телефон, с которого позвонил Белов, входящие звонки. Белов ответил утвердительно и предложил проверить. П. перезвонил, услышал голос Белова, и они ненадолго продолжили разговор. П. сказал Белову, что приезжать на адрес не следует, сначала необходимо проверить достоверность поступившей от него информации. После этого завершил разговор. П. тут же выяснил, что, согласно открытым источникам, номер, с которого позвонил Белов, зарегистрирован не в столичном регионе, а в Краснодарском крае. Затем П. позвонил в контактный центр АО «Мосэнергосбыт». Оператор пояснил, что на адресе П. замена электросчетчиков не проводится. Также оператор сообщил, что П. не первый, кто получил звонки от лжеработников Мосэнерогосбыта.

В тот же день П. подготовил заявление о преступлении и направил его через сайт МВД России в УБК. В заявлении описал приведенные выше факты и предположил,

[26] Вряд ли указанное время выбрано случайно. Если бы звонок поступил в будний день и в рабочее время, то высока вероятность, что трудоустроенный гражданин не отреагировал бы на звонок с незнакомого номера. Кроме того, в этот день и на следующий сотрудники правоохранительных органов отдыхают, на службе находятся лишь дежурные.

[27] Оглашение всех этих подробностей и концентрация внимания гражданина на них («запишите») призвана внушить потенциальной жертве, что действительно готовится замена электросчетчика, в то время как это лишь легенда, используемая для формирования доверия, выманивания конфиденциальной информации и побуждения жертвы к нужным мошеннику действиям.

[28] Демонстрация осведомленности о персональных данных жертвы также есть элемент подтверждения легенды мошенников по схеме, которая работает на психологическом уровне: «вот видите, мы знаем ваши персональные данные, мы ими правомерно обладаем, ведь у нас с вами юридически значимый договор, будет нормальным эти данные уточнить и расширить их объем».

[29] Здесь следует заметить, что действительно в столице в рамках программы, утвержденной Департаментом экономической политики и развития г. Москвы, АО «Мосэнергосбыт» с 2019 г. совместно с подрядной организацией проводит работы по созданию системы беспроводного сбора данных показаний приборов учета электроэнергии. Однако персональный обзвон граждан в связи с этим не проводится. АО «Мосэнергосбыт» за 1–2 дня до начала работ извещает жителей домов о предстоящих работах путем расклейки объявлений в подъездах и на информационных стендах. Работники имеют при себе фирменное удостоверение и копию письма АО «Мосэнергосбыт» о проведении работ (см.: *В Москве* проводятся работы по установке «умных» счетчиков // АО «Мосэнергосбыт». 2019. URL: https://www.mosenergosbyt.ru/individuals/news/v-moskve-provodyatsya-raboty-po-ustanovke-umnykh-schyetchikov/ (дата обращения: 29.10.2024)). Чтобы выяснить эти подробности, подвергшийся мошеннической атаке гражданин должен взять паузу и заняться поиском информации. Между тем преступная схема рассчитана на то, что уже в ходе первого разговора мошенник решит намеченные задачи, а гражданин ничего не заподозрит и будет ожидать визита лжеработников АО «Мосэнергосбыт», которые, якобы, сделают режим потребления электроэнергии более удобным и экономным. На самом же деле личную встречу с гражданином преступная схема не предполагает.

что дополнительные персональные данные, которые пытался выведать Белов, нужны для дальнейшей реализации преступной схемы. Например, для взлома личного кабинета жертвы на сайте «Госуслуги», последующего получения кредитов от имени жертвы и завладения полученными таким образом денежными средствами, либо завладения телефонным номером жертвы и получения посредством него доступа к банковским счетам и т. д.

В заявлении П. предложил свою правовую оценку происшедшего: имеет место совокупность двух преступлений. Первое из них – неоконченное покушение на мошенничество с целью хищения денежных средств в особо крупном размере (ч. 4 ст. 159 или ч. 4 ст. 159.3 УК РФ). Такая квалификация обоснована следующим. Исходя из обстоятельств происшедшего, умысел виновного был направлен на то, чтобы завладеть всеми денежными средствами, к которым удастся получить доступ. В таком случае деяние следует оценивать по наиболее тяжкому из возможных последствий, которые могли наступить в данном случае, но не наступили по не зависящим от виновного причинам. У потерпевшего благоприятная кредитная история, и при удачном для преступника развитии событий он мог бы оформить на потерпевшего кредит или кредиты на сумму более 1 млн руб. и завладеть кредитными средствами. Кроме того, на банковских счетах потерпевшего в сумме находилось более 1 млн руб. Поэтому виновному должно вменяться покушение на мошенничество на сумму более 1 млн руб., что следует расценивать как особо крупный размер (прим. 1 к ст. 158 УК РФ).

Второе преступление окончено и предусмотрено ч. 2 ст. 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло копирование информации и совершено с корыстной целью (только это может объяснить, откуда у мошенников обширные персональные данные о потерпевшем; возможно, преступники получили доступ к некой банковской базе данных).

П. обратил внимание правоохранителей в своем заявлении, что, по всей видимости, Белов и его соучастники обзвонили ряд иных граждан, помимо заявителя, и некоторая часть из них попалась на уловки мошенников, сообщила все запрошенные данные и уже пострадала в финансовом плане либо в ближайшее время потерпит финансовый ущерб. Поэтому *следует принять незамедлительные меры к определению локации телефона, с которого звонил Белов, задержанию последнего*, закреплению цифровых и вещественных следов противоправной деятельности, установлению и опросу потенциальных потерпевших, выявлению сообщников Белова и т. д.

П. отслеживал судьбу заявления через идентификатор, присвоенный при подаче обращения. Через два дня на сайте МВД России появилась информация, что заявление П. от 30 сентября 2024 г. зарегистрировано и находится на рассмотрении в ГУ МВД России по г. Москве. Еще через два дня появилась информация, что данное заявление зарегистрировано в Книге учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях.

Наконец, 14 октября 2024 г. П. позвонил сотрудник уголовного розыска из территориального отдела внутренних дел, обслуживающего район проживания заявителя. Сотрудник сообщил, что заявление поступило в указанный отдел, и он отрабатывает его, поскольку находится на дежурстве. Сотрудник пригласил П. к себе для дачи объяснения. П. поинтересовался, специализируется ли сотрудник на раскрытии киберпреступлений. Последовал ответ, что принцип работы лично его и дежурной группы в целом не линейный, а территориальный, приходится разбираться

с заявлениями обо всем – о грабежах, угонах, квартирных кражах и т. д. После этого никаких известий для П. о результатах рассмотрения заявления о преступлении не поступало. Через четыре недели, предполагая, что принято решение об отказе в возбуждении уголовного дела и это решение скрывается (в противном случае потерпевший был бы вызван к следователю или дознавателю на допрос или для производства иных следственных действий), П. подал жалобу на нарушение уголовного-процессуального законодательства[30]. Тем не менее по состоянию на конец января 2025 г. П. не извещен о процессуальном решении, принятом по его заявлению.

Итак, практика реагирования на заявления о киберпреступлениях, при которых потерпевшим не нанесен значительный материальный ущерб, существенным образом не изменилась. В течение 16 дней с момента приема заявления П. о преступлении правоохранительные органы не предпринимали никаких мер к пресечению преступной деятельности неизвестных, установлению иных пострадавших, раскрытию преступления по горячим следам и задержанию виновных[31]. Это позволяет мошенникам-обзвонщикам, если они используют «серые» сим-карты, периодически избавляться от них и, меняя дислокацию, находиться в относительной безопасности. Соответственно, в безопасности находятся и их сообщники.

Важно также отметить, что *тщательно продуманная и выверенная схема обзвонов, описанная выше, указывает на криминальный профессионализм. Мошенники,* по всей видимости, *входят в организованную группировку с распределением ролей.* Одни осуществляют общее руководство и контроль; другие разрабатывают (либо заимствуют) и корректируют (адаптируют заимствованные) преступные схемы; третьи добывают персональные данные граждан, необходимые для реализации преступной схемы; четвертые совершают обзвоны потенциальных потерпевших; пятые подключаются к работе, когда обзвонщики добиваются успеха; шестые занимаются легализацией преступных доходов, их сохранением и приумножением; седьмые решают вопросы материально-технического оснащения преступной деятельности; восьмые обеспечивают безопасность группировки и т. д.

Представленный выше пример наглядно демонстрирует, что главная проблема борьбы с киберпреступностью и утечкой персональных данных состоит не в мягкости уголовного законодательства или несовершенстве уголовно-процессуального законодательства, а в неудовлетворительной организации работы правоохранительных органов.

Ответственность лиц, которые незаконно копируют и торгуют персональными данными, давно закреплена в УК РФ. Необходима реальная и действенная ответственность тех руководителей правоохранительных органов, которые не могут или не желают надлежащим образом организовать работу по выявлению соответствующих преступлений, их раскрытию по горячим следам, обнаружению

[30] В части 2 ст. 144 УПК РФ содержится требование, чтобы о процессуальном решении по заявлению о преступлении без промедления сообщалось заявителю с разъяснением права на обжалование принятого решения. Причем в случае отказа в возбуждении уголовного дела копия соответствующего постановления *в течение 24 часов с момента его вынесения направляется заявителю независимо от наличия ходатайства об этом* (ч. 4 ст. 148 УПК РФ).

[31] Правоохранителей давно учат, что раскрытие преступления по горячим следам означает решение этой задачи в максимально сжатые сроки – за трое суток с момента, когда были обнаружены признаки преступления или поступило сообщение о нем; в отдельных, особо сложных случаях этот срок может быть увеличен до 10–15 суток (см., напр.: *Криминалистика* : учеб. / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская ; под ред. Р. С. Белкина. М. : НОРМА, 2000. С. 895). Таким образом, к моменту, когда заявление П. начали проверять, возможность раскрытия преступления по горячим следам была безнадежно утрачена.

и изъятию похищенного, преданию суду виновных, которые попустительствуют волоките при рассмотрении заявлений о преступлениях, в неявной форме поощряют незаконные и необоснованные отказы в возбуждении уголовных дел.

Внедрение в практику такой ответственности не требует нормотворческой деятельности, необходимая правовая база уже существует. Законодательство в описанных случаях предусматривает как дисциплинарную, так и уголовную ответственность, а также действенные меры воздействия при установлении вины. При дисциплинарной ответственности возможны, в частности, предупреждение о неполном служебном соответствии, понижение в должности и даже увольнение из правоохранительных органов по отрицательным мотивам. При уголовной ответственности за халатность возможно назначение различных уголовных наказаний вплоть до лишения свободы на срок до 7 лет. *Надо лишь сменить постулаты уголовной политики, проявить политическую волю в следовании им.*

Заключение

Крайне важно, чтобы рассматриваемое обстоятельство – очень высокий уровень латентности преступлений, совершаемых с использованием информационно-коммуникационных технологий (возможно, самый высокий, если сравнить с латентностью преступлений иных видов) – осознавали субъекты уголовной политики и принимали во внимание, ставя задачи по противодействию рассматриваемым преступлениям. Данный тезис целесообразно закрепить в Концепции государственного противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

Изложенное обстоятельство необходимо учитывать при разработке и внедрении критериев оценки эффективности работы подразделений, нацеленных на противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Выявление таких преступлений должно поощряться, даже если виновные лица не установлены. К дополнительным преференциям должны приводить своевременное выявление и фиксация улик, получение оперативно значимой информации, что может в дальнейшем способствовать установлению виновных, их задержанию, возмещению ущерба. Такие установки также целесообразно закрепить в указанной Концепции.

Задачи своевременного выявления всех противоправных деяний, совершаемых с использованием информационно-коммуникационных технологий, незамедлительного изъятия цифровых устройств, извлечения из них значимых данных, закрепления иных улик и задержания виновных по горячим следам, точной фиксации основных параметров выявленных преступлений (как раскрытых, так и не раскрытых), обеспечивающей последующий быстрый и удобный системный анализ такого рода деяний, предполагают комплексный подход к их решению.

Помимо быстрой проверки, правильного разрешения соответствующих заявлений от граждан и юридических лиц с подключением к работе оперативных уполномоченных и следователей, обладающих необходимыми навыками, инструментами и полномочиями, требуется налаживание системы информирования потенциальных пострадавших, иных осведомленных лиц о том, куда и в каком порядке они могут сообщить ставшую известной им информацию о преступлениях и причастных к ним лицах. Надлежит разворачивать креативную социальную рекламу, создавать и совершенствовать цифровые платформы с дружественным интерфейсом, при помощи которых граждане могут легко и быстро оформить, а затем моментально отправить свои обращения.

Необходима планомерная работа правоохранительных органов по инициативному выявлению противоправных деяний. Важная часть такой работы – регулярный сетевой мониторинг, то есть исследование сетевой активности для выявления подозрительного поведения и идентификации угроз (анализ контента и трафика, поиск аномалий и обнаружение вторжений и т. п.).

Целесообразно действовать в сети Интернет не только реактивно, но и проактивно: создавать сайты, аккаунты-ловушки, проводить оперативные эксперименты и иные оперативно-разыскные мероприятия. В свою очередь, это направление правоохранительной деятельности должно гармонично дополняться и сочетаться с агентурно-оперативной работой.

Установленные преступные схемы необходимо тщательно изучать, должны разрабатываться меры по их нейтрализации (путем оповещения потенциальных потерпевших, устранения обнаруженных уязвимостей и т. д.). Нужно также работать на опережение, моделировать новые преступные схемы, которые могут появится в будущем, и принимать меры по недопущению их распространения.

Список литературы

1. Зазулин А. И. Онлайн-обыск как самостоятельное следственное действие: предпосылки, перспективы и недостатки // Казанские уголовно-процессуальные и криминалистические чтения : материалы междунар. науч-практ. конф. (Казань, 28 апр. 2022 г.) : в 2 ч. / [редкол.: Ю. Н. Кулешов (отв. ред.) и др.] ; Казан. ин-т (фил.) ВГУЮ. Казань : ЮрЭксПрактик, 2022. Ч. 1. С. 117–123.

2. Каракулов Т. Г. К вопросу о допустимости лишения специального, воинского или почетного звания, классного чина и государственных наград за киберпреступления // Уголовная политика в условиях цифровой трансформации : сб. ст. материалов II всерос. науч.-практ. конф. / отв. ред. М. А. Ефремова. Казань : Отечество, 2023. С. 52–59.

3. Кардашевская М. В. Раскрытие преступлений по горячим следам // Вестник экономической безопасности. 2018. № 1. С. 142–145.

4. Зуев С. В., Зазулин А. И. IT-следователь в цифровой среде уголовного судопроизводства // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 48–54. DOI: https://doi.org/10.47475/2311-696X-2024-41-2-48-54

5. Бастрыкин А. И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий // Вестник Российской правовой академии. 2022. № 4. С. 88–94. DOI: https://doi.org/10.33874/2072-9936-2022-0-4-88-94

6. Киселев А. С., Горбунова К. А. Особенности тактики допроса обвиняемых при расследовании преступлений в сфере компьютерной информации // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 67–74. DOI: https://doi.org/10.47475/2311-696X-2024-41-2-67-74

7. Романова Г. В. Информационные технологии в деятельности следователя // Вестник Волжского университета им. В. Н. Татищева. 2023. Т. 1, № 2 (104). С. 159–168. DOI: https://doi.org/10.51965/2076-7919_2023_1_2_159

8. Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. Т. 17, № 3 (136). С. 102–111. DOI: https://doi.org/10.17803/1994-1471.2022.136.3.102-111

9. Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2 (38). С. 131–135.

References

1. Zazulin A. I. Online Search as an Independent Investigative Action: Preconditions, Prospects and Disadvantages. In: Kuleshov Yu. N. (Ed.). *Kazan Criminal Procedure and Forensic Readings. Part 1.* Kazan: YurEksPraktik Publ.; 2022. P. 117–123. (In Russ.)

2. Karakulov T. G. On the Question of the Admissibility of the Deprivation of a Special, Military or Honorary Title, Class Rank and State Awards for Cybercrime. In: Efremova M. A. (Ed.). *Criminal Policy in the Context of Digital Transformation*. Kazan: Otechestvo Publ.; 2023. P. 52–59. (In Russ.)

3. Kardashevskaya M. V. Disclosure of Crimes in Hot Pursuit. *Vestnik of Economic Security*. 2018;1:142-145. (In Russ.)

4. Zuev S. V., Zazulin A. I. IT-Investigator in the Digital Environment of Criminal Proceedings. *Legal Order: History, Theory, Practice*. 2024;2:48-54. DOI: https://doi.org/10.47475/2311-696X-2024-41-2-48-54 (In Russ.)

5. Bastrykin A. I. Identification and Investigation of Crimes Committed Using Information and Communication Technologies. *Herald of the Russian Law Academy*. 2022;4:88-94. DOI: https://doi.org/10.33874/2072-9936-2022-0-4-88-94 (In Russ.)

6. Kiselev A. S., Gorbunova K. A. Features of the Tactics of Interrogation of the Accused In the Investigation of Crimes in the Field of Computer Information. *Legal Order: History, Theory, Practice*. 2024;2:67-74. DOI: https://doi.org/10.47475/2311-696X-2024-41-2-67-74 (In Russ.)

7. Romanova G. V. Information Technologies in the Investigator's Activity. *Vestnik of Volzhsky University named after V. N. Tatishchev.* 2023;1(2):159-168. DOI: https://doi.org/10.51965/2076-7919_2023_1_2_159 (In Russ.)

8. Smushkin A. B. Forensic Aspects of the Dark Net Study for Crimes Investigation Purposes. *Actual Problems of Russian Law*. 2022;17(3):102-111. DOI: https://doi.org/10.17803/1994-1471.2022.136.3.102-111 (In Russ.)

9. Yangaeva M. O., Pavlenko N. O. OSINT. Obtaining Forensic Significant Information from the Internet. *Altai Law Journal*. 2022;2:131-135. (In Russ.)

Информация об авторе

Пётр Александрович Скобликов, ведущий научный сотрудник сектора уголовного права, уголовного процесса и криминологии Института государства и права Российской академии наук (ул. Знаменка, 10, Москва, 119019, Российская Федерация), доктор юридических наук; ORCID: https://orcid.org/0000-0001-7875-7036; SPIN-код: 8001-2807; e-mail: skoblikov@list.ru

About the Author

Petr A. Skoblikov, Leading Researcher of the Criminal Law, Criminal Procedure, and Criminology Sector at the Institute of State and Law of The Russian Academy of Sciences (10 Znamenka str., Moscow, 119019, Russian Federation), Doctor of Legal Sciences; ORCID: https://orcid.org/0000-0001-7875-7036; SPIN-code: 8001-2807; e-mail: skoblikov@list.ru

Поступила | Received 26.01.2025

Поступила после рецензирования и доработки | Revised 12.03.2025

Принята к публикации | Accepted 26.03.2025