Научная статья
УДК 343.9+343.163
DOI: 10.47475/2311-696X-2024-42-3-89-95

С. 89–95

ИНФОРМАТИЗАЦИЯ В СОВРЕМЕННОМ МИРЕ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ, ПРОФИЛАКТИЧЕСКАЯ РОЛЬ ПРОКУРАТУРЫ

Игорь Михайлович Мацкевич
Университет прокуратуры Российской Федерации, Москва, Россия
mackevich2004@mail
https://orcid.org/0000-0002-4270-1599

Аннотация. Изучение вопросов, связанных с криминализацией процессов информатизации в современном мире, обусловлено, с одной стороны, закреплением уголовной ответственности за неправомерные действия в этой сфере в главе 28 Уголовного кодекса Российской Федерации (далее — УК РФ), а с другой стороны, большим кругом проблем, создаваемых всевозможными прямыми и опосредованными негативными влияниями цифровизации, проникающими во все стороны общественной жизни и государственного устройства. Парадокс ситуации заключается в том, что чем больше цифровизация проникает в повседневную реальность, чем в большей степени цифровые алгоритмы облегчают жизнь человека, тем больше возможностей для всякого рода манипуляций появляется у мошенников. Угрозами цифровизации современного мира могут выступать: а) внешние (например, природные, техногенные); б) внутренние (социальные, психологические). Безусловно, наивысшую степень опасности представляет вся совокупность угроз и их источников. Количество регистрируемых преступлений, совершенных с использованием информационно-телекоммуникационных технологий (киберпреступления), постоянно увеличивается. За истекшие пять лет их стало больше в 2,3 раза. Прокуроры посредством осуществления прокурорского надзора, иных возложенных на прокуратуру Российской Федерации функций, участвуют в выявлении, предупреждении и устранении угроз информационной безопасности, решая задачи, вытекающие из требований законов и складывающейся в стране в целом и конкретных регионах криминогенной обстановки. Особо следует отметить деятельность прокуратуры по мониторингу сети интернет с целью выявления информации, распространяемой с нарушением действующего законодательства и принятия необходимых и законных мер по ее блокированию. Делается вывод, что специалисты в области информационной безопасности должны не просто работать в органах прокуратуры, но специально готовиться для такой работы и быть аттестованными, чтобы на них распространялись все положенные социальные привилегии, а также дисциплинарная ответственность.

Ключевые слова: информатизация, цифровизация, алгоритмы, криминализация, безопасность, прокуратура, интернет, даркнет, профилактика, предупреждение

Для цитирования: Мацкевич И. М. Информатизация в современном мире: уголовно-правовые и криминологические аспекты, профилактическая роль прокуратуры // Правопорядок: история, теория, практика. 2024. № 3 (42). С. 89–95. DOI: 10.47475/2311-696X-2024-42-3-89-95

Research article

INFORMATION IN THE MODERN WORLD: CRIMINAL LEGAL AND CRIMINOLOGICAL ASPECTS, PREVENTIVE ROLE OF THE PROSECUTOR'S OFFICE

Igor M. Matskevich
University of the Prosecutor's Office of the Russian Federation, Moscow, Russia
mackevich2004@mail
https://orcid.org/0000-0002-4270-1599

Abstract. The study of issues related to the criminalization of informatization processes in the modern world is due, on the one hand, to the establishment of criminal liability for unlawful actions in this area in Chapter 28 of the Criminal Code of the Russian Federation, and, on the other hand, to a large range of problems created by all sorts of direct and indirect negative impacts of digitalization, penetrating into all aspects of social life and government. The paradox of the situation is that the more digitalization penetrates into everyday reality, the more digital algorithms make human life easier, the more opportunities fraudsters have for all kinds of manipulations. Threats to the digitalization of the modern world can be:

a) external (for example, natural, man-made); b) internal (social, psychological). Of course, the highest degree of danger is represented by the entire set of threats and their sources. The number of registered crimes committed using information and telecommunication technologies (cybercrimes) is constantly increasing. Over the past five years, their number has increased by 2.3 times. Prosecutors, through the implementation of prosecutorial supervision and other functions assigned to the prosecutor's office of the Russian Federation, participate in identifying, preventing and eliminating threats to information security, solving problems arising from the requirements of the laws and the crime situation emerging in the country as a whole and in specific regions. Of particular note is the activity of the prosecutor's office in monitoring the Internet in order to identify information disseminated in violation of current legislation and take necessary and legal measures to block it. It is concluded that specialists in the field of information security should not only work in the prosecutor's office, but be specially trained for such work and be certified so that they are subject to all the required social privileges, as well as disciplinary liability.

Keywords: informatization, digitalization, algorithms, criminalization, security, prosecutor's office, Internet, darknet, prevention, prevention

For citation: Matskevich IM. Information in the modern world: criminal legal and criminological aspects, preventive role of the procecutor`s office. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(3):89-95. (In Russ.) DOI: 10.47475/2311-696X-2024-42-3-89-95

Введение

В современных геополитических и социальных экономических условиях преступность как известное социальное отрицательное негативное явление трансформировалось в одну из угроз национальной безопасности для нашего государства и приобретает все новые формы, используя ранее неизвестные средства и инструменты воздействия на все элементы общественной жизни. Ее транснациональный и организованный характер преобразуется во все более сложные формы и разновидности. Современные преступники, преступники будущего, о появлении новых типов которых я говорил на одной из конференций Ковалевских чтений не так давно, используют современные, в том числе высокие технологии, включая искусственный интеллект [4; 5; 11], информационно-телекоммуникационные сети [7; 10] и расширяющиеся возможности нейросетей. Более того, преступники первыми начинают использовать возможности современных цифровых технологий в своих корыстных целях, пока эти самые технологии только начинают использоваться в интересах всего общества. Будучи по своей природе явлением социальным, о чем я только что говорил, преступность обладает таким свойством как изменчивость. Преступность способна встраиваться в объективные социальные процессы и оказывать на них колоссальное обратное влияние. Таким образом, имеет место негативное обратное влияние преступности на внешние объективные обстоятельства, что еще более увеличивает степень ее опасности и вредоносности. При этом преступность как явление динамичное и способное к трансформации использует как достижения, так и недостатки, а зачастую и слабости общества, паразитирует на естественных недочетах в государственном управлении и тем самым усиливает свои негативные последствия.

Для понимания сути имеющихся и складывающихся угроз национальной безопасности, безопасности личности, общества и государства, в том числе, важное значение имеют источники таких угроз. В качестве таковых могут выступать: а) внешние угрозы (например, природные, техногенные); б) внутренние угрозы (социальные, психологические). Безусловно, наивысшую степень опасности представляет вся совокупность угроз и их источников. Вместе с тем каждая из перечисленных угроз требует к себе отдельного внимания с учетом присущих им особенностей, свойств и качеств.

Одной из определяющих все развитие государства и общества в современный период является угроза информационной безопасности. Поэтому перед государством наряду с задачей создания информационного цифрового государства, неизбежно появляется задача обеспечения собственной информационной безопасности. При этом рассматриваемая проблема может быть сопряжена с ее преувеличением и с ее преуменьшением. И это и другое не только вредно, но и опасно.

Отмечу, что в сфере информационных технологий в 2023 г. прокурорами было выявлено 45,8 тыс. нарушений законодательства.

Понятие информационной безопасности

Если следовать Федеральному закону «Об информации, информационных технологиях и о защите информации»[1], то легальными признаками информационной безопасности следует считать: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации.

При этом защита информации должна обеспечиваться: 1) предотвращением несанкционированного доступа к информации и/или передачи ее лицам, не имеющим права на доступ к информации; 2) своевременным обнаружением фактов несанкционированного доступа к информации; 3) предупреждением возможности неблагоприятных последствий нарушения порядка доступа к информации; 4) недопущением воздействия

[1] Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

на технические средства обработки информации, в результате которого нарушается их функционирование; 5) возможностью незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней; 6) постоянным контролем за обеспечением уровня защищенности информации; 7) наконец, нахождением на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации[1].

Очевидно, что соблюдением всех этих (а также многих других) императивных предписаний должны заниматься органы прокуратуры.

Вопросы обеспечения информационной безопасности включены практически во все нормативные правовые документы стратегического планирования, в том числе в Стратегию национальной безопасности Российской Федерации[2]. Закрепленные в Стратегии положения получили свое развитие в новой редакции Доктрины информационной безопасности Российской Федерации[3]. В этом документе не только дана оценка современному состоянию информационной безопасности Российской Федерации, но и определен перечень угроз, а также совокупность средств, способных обеспечить должный уровень защиты ее информационной безопасности. Более того, правовые средства обеспечения информационной безопасности отнесены к приоритетному направлению деятельности всех государственных органов, включая, естественно, органы прокуратуры.

Масштабные преобразования различных сторон человеческой жизни, связанные с информатизацией, сопровождаются ростом ее уязвимости от новых потенциальных и реальных угроз, связанных, прежде всего, с противоправными деяниями в виртуальном пространстве, связанном с цифровыми алгоритмами. Проблемы информатизации как в криминологическом, так и уголовно-правовом аспектах актуальны сегодня как никогда.

Таким образом, состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства составляют содержание информационной безопасности.

Структура преступлений с использованием информационно-телекоммуникационных технологий (киберпреступность, киберпреступления)

Количество регистрируемых преступлений, совершенных с использованием информационно-телекоммуникационных технологий (в основном это преступления в сфере компьютерной информации, закрепленные в главе 28 УК РФ, которые для краткости я в дальнейшем буду называть киберпреступлениями или киберпреступностью, понимая условность данных терминов), постоянно увеличивается. За истекшие пять лет их стало больше в 2,3 раза.

Попутно подчеркну, что глава 28 УК РФ помещена в раздел IX УК РФ, который называется «Преступления против общественной безопасности и общественного порядка», что лишний раз свидетельствует о том, что законодатель прекрасно осознает общественную опасность рассматриваемых преступлений, наносящих ущерб в первую очередь безопасности общества и государства.

Негативная тенденция киберпреступлений сопровождается ростом удельного веса этих деяний в структуре всех зарегистрированных в стране преступлений. Если в 2019 г. на них приходилось лишь 14,5 % от всех зарегистрированных в Российской Федерации преступлений, то в 2023 г. удельный вес данного вида преступности превысил треть (34,8 %).

Киберпреступность — это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. В структуре киберпреступлений преобладает мошенничество (52,2 %), кражи (17,6 %) и преступления, связанные с незаконным оборотом наркотиков 12 %). Среди остальных преступлений вымогательство (1 %) и иные преступления в рассматриваемой области (17,2 %).

Динамика киберпреступлений свидетельствует о поступательном росте их уровня от года к году. В 2019 г. удельный вес этих преступлений составлял 14,5 %, в 2020 г. — 25 %, в 2021 г. — 25,8 %, в 2022 г. — 26,5 %, в 2023 г. — уже 34,8 %[4]. К сожалению, нет никаких оснований рассчитывать, что в 2024 г. ситуация начнет меняться в лучшую сторону.

Большинство киберпреступлений совершаются с целью получения финансовой выгоды. Однако целью преступников может быть также выведение компьютеров или нейросетей из строя — из личных, политических и иных мотивов либо в террористических целях. Например, об угрозе так называемой кибервойны, т. е. развязывания масштабных и систематических кибератак, представляющих угрозу для всех критически важных информационных структур российского государства со стороны США и, скажем так, «армии» украинских хакеров (хакер и киберпреступник — понятия часто совпадающие, но не тождественные), открыто или

[1] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ст. 16).

[2] О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 02.07.2021 № 400 // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

[3] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

[4] См.: Состояние преступности 2019, 2020, 2021, 2022, 2023 гг. // Министерство Внутренних Дел Российской Федерации : [сайт]. URL: https:мвд.рф/reports (дата обращения: 12.03.2024).

опосредованно работающих в интересах специальных, в том числе разведывательных служб коллективного Запада (в первую очередь США и Великобритании), публично заявил заместитель секретаря Совета Безопасности Российской Федерации Олег Владимирович Храмов. Он подчеркнул, что эта необъявленная кибервойна является прямым следствием успешного проведения российскими Вооруженными Силами Специальной военной операции на Украине. Можно сказать и так: чем успешнее действуют российские Вооруженные Силы, тем масштабнее против Российской Федерации ведется кибервойна, тем большее число других стран и преступников пытаются втянуть в нее США и Великобритания[1].

В марте 2023 г. США обнародовали новую редакцию стратегии по кибербезопасности, носящую откровенно агрессивный характер, причем не только в отношении России, но и, по сути, любых третьих стран. В стратегии прямо говорится о якобы заведомой легитимности наступательных кибероперациий в качестве превентивной или ответной меры для подавления хакерских группировок в информационном пространстве третьих стран[2].

Киберпреступления могут совершаться различными способами через интернет и/или сети Даркнет (теневого сегмента интернета) с использованием: а) фишингового (поддельного) сайта; б) поддельных мошеннических ссылок; в) вредоносных компьютерных программ; г) «программ-шифровальщиков»; д) бот-сетей (ботнет); е) расчетных (пластиковых) карт; ж) социальных сетей; и) электронных платежных систем; к) технологий «дипфейк» и др.

Необходимо отметить негативную тенденцию с точки зрения тяжести совершения рассматриваемых преступлений: если в 2019 г. доля особо тяжких преступлений из общего числа киберпреступлений составляла 8,5 %, то в 2023 г. она увеличилась до 12,3 % при одновременном уменьшении доли преступлений небольшой тяжести с 18,3 в 2019 г. до 16,4 % в 2023 г. При этом количество зарегистрированных преступлений, предусмотренных главой 28 УК РФ («Преступления в сфере компьютерной информации»), за последние 5 лет увеличилось с 2883 в 2019 г. до 37 101 в 2023 г. Наиболее значительный рост числа зарегистрированных преступлений наблюдается по ст. 274.1 УК РФ («Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»), с 2019 г. по 2023 г. их число увеличилось с 4 до 114. Не менее существенный рост преступлений наблюдается по ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), в 2019 г. их число составило 2420, в 2023 г. — 36 788[3].

Борьба с преступлениями в сфере компьютерной информации

Очевидно, законодателю необходимо стремиться адаптироваться к новым вызовам и продолжать совершенствовать уголовно-правовые меры противодействия информационным угрозам.

Например, составляющей для расследования и борьбы с киберпреступлениями стала компьютерная экспертиза. Так называемые компьютерные эксперты занимаются тем, что анализируют данные с компьютеров и других устройств, восстанавливают удаленную информацию и определяют следы преступной деятельности хакеров.

Не меньшее значение имеют электронные доказательства, которые включают в себя данные с компьютеров, мобильных устройств, систем видеонаблюдения и других источников электронной информации (спектр этих источников постоянно обновляется и расширяется).

Кроме этого, позволяет выявлять закономерности в поведении потенциальных преступников и их жертв анализ больших данных, что, в свою очередь, помогает разрабатывать эффективные меры по предотвращению преступлений вообще и киберпреступлений в частности.

В Российской Федерации и других странах создаются специализированные подразделения, занимающиеся борьбой с киберпреступностью. Накопленная и собираемая информатизация позволяет правоохранительным органам осуществлять контроль/надзор и мониторинг сети Интернет для выявления потенциальных угроз информационной безопасности исовершаемых преступных действий. Представители правоохранительных органов Российской Федерации и других стран сотрудничают друг с другом по вопросам непосредственного расследования киберпреступлений.

В то же время любое действие, направленное на защиту интересов государства и его граждан, при несоблюдении норм закона может привести к обратным результатам. Любое проникновение в сферу информационной безопасности, в том числе с благими намерениями, неизбежно поднимает вопросы защиты личной жизни и прав граждан, поэтому необходимо соблюдать баланс между безопасностью государства и человека и защитой его прав, интересов и интимных стороны жизни.

Таким образом, создание специализированных служб и налаживание сотрудничества между ними в разных странах является неотъемлемой частью борьбы с киберпреступлениями.

Искусственный интеллект

Не могу не остановиться на таком важном вопросе, как искусственный интеллект. На пресс-конференции 14 декабря 2023 г. Президент Российской Федерации Владимир Путин сказал, что «предотвратить развитие искусственного интеллекта невозможно и надо сделать все, чтобы Россия была одним из лидеров в этом направлении»[4].

---

[1] Егоров И. Совбез РФ: США рассматривают возможность глобального кибердара по России // Российская газета. URL: https://rg.ru/2023/10/09/cifra-cveta-haki.html (дата обращения: 12.03.2024).

[2] Овчинский В., Жданов Ю. О новой американской стратегии кибербезопасности // Газета Завтра. 2023. 5 марта. URL: https://zavtra.ru/blogs/o_novoj_amerikanskoj_strategii_kiberbezopasnosti (дата обращения: 12.03.2024).

[3] См.: Состояние преступности 2019, 2020, 2021, 2022, 2023 гг. // Министерство Внутренних Дел Российской Федерации : [сайт]. URL: https:мвд.рф/reports (дата обращения: 12.03.2024).

[4] Путин прокомментировал развитие ИИ // РИА Новости. 2023. 14 дек. URL: https://ria.ru/20231214/razvitie-1915817736.html (дата обращения: 12.03.2024).

В 2023 г. уже разработаны предложения по актуализации национальной стратегии развития страны до 2030 г. В национальном проекте «Экономика данных» искусственный интеллект (далее — ИИ) станет центральным направлением развития.

Следует отметить, что в Российской Федерации нормативное и этическое регулирование рынка ИИ является одним из самых прогрессивных в мире. В частности, это наглядно видно на примере использования ИИ в медицине, в сфере высокоавтоматизированных транспортных средств и беспилотных летательных аппаратов. Новый этап развития ИИ в Российской Федерации заключается в переходе к активному внедрению проектов с использованием цифровых технологий в экономические и хозяйственные процессы. В 2023 г. Российская Федерация, согласно оценкам некоторых экспертов, вошла в ведущие 5 стран мира, где в полной мере используются технологии, связанные с ИИ[1].

В науке выделяются четыре основных направления развития ИИ.

1. Решение проблем, связанных с приближением специализированных систем ИИ к возможностям человека и их интеграция с жизнедеятельностью человека и общества (человека в обществе).

2. Создание искусственного (технологического) разума, представляющего интеграцию уже созданных подсистем ИИ в единую систему, способную решать глобальные проблемы человечества (подсказывать направления решения глобальных проблем).

3. Исследование возможностей использования ИИ в сфере борьбы с преступностью (алгоритмы для расследования однотипных преступлений).

4. Изучение вопроса о возможности/невозможности признания ИИ субъектом преступления.

С другой стороны, юристы приводят самые различные примеры фактического использования ИИ в повседневной жизни рядового гражданина Российской Федерации: а) автомобили с автоматическим управлением; б) плотность дорожного движения (трафик), регулируемая ИИ; в) техническое обслуживание интеллектуальных сетей и т. д.

Приложения на мобильных телефонах/устройствах стали неотъемлемой частью нашей повседневной жизни: голосовые помощники (Алисе и Google Assistant); реклама; алгоритмы для заказа такси; распознавание по лицам как способ пользования общественным транспортом; финансовые услуги в банках и финансовая безопасность (уведомление клиентам об обнаруженном или потенциальном мошенничестве) и т. д.

Роль прокуратуры в решении вопросов информационной безопасности

В настоящее время все более заметной становится роль органов прокуратуры в обеспечении информационной безопасности. Прокуроры посредством осуществления прокурорского надзора, иных возложенных на прокуратуру Российской Федерации функций принимают непосредственное участие в выявлении, предупреждении и устранении угроз информационной безопасности, решая задачи, вытекающие из требований законов и складывающейся в стране в целом и конкретных регионах в частности криминогенной обстановки, связанной с киберпреступностью. Особо следует отметить деятельность прокуратуры по мониторингу сети Интернет с целью выявления информации, распространяемой с нарушением ст. 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации»[2].

К сожалению, практика свидетельствует, что в условиях современного развития информационных технологий одним ограничением доступа к информации, распространяемой с нарушением закона, добиться нужного результата удается далеко не всегда. Установленные запреты киберпреступники легко обходят, размещая запрещенную информацию на других ресурсах в интернете, а когда информация запрещается на этих ресурсах, открываются другие и/или информация размещается в даркнете, блокировка которого крайне затруднена.

Современные реалии и потребности защиты информационной безопасности Российской Федерации диктуют необходимость совершенствования существующего порядка возбуждения уголовных дел, который бы позволял в скорейшие сроки не только возбудить уголовное дело, но одновременно привлечь виновное лицо к ответственности, не допустив тем самым продолжения им своей преступной деятельности. Оптимально было бы, если бы это делалось одновременно. В этой связи представляется целесообразным наделение прокурора полномочиями по возбуждению уголовных дел в связи с выявлением им признаков деятельности, направленной против информационной безопасности Российской Федерации. Актуальность и необходимость такой меры обусловлены в первую очередь сложившейся геополитической обстановкой вокруг страны и не простой криминогенной ситуацией внутри страны.

Последовательное расширение круга прокурорских полномочий повлечет за собой дальнейшее усиление роли прокуратуры в системе обеспечения информационной безопасности Российской Федерации. В соответствии со ст. 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» Генеральный прокурор Российской Федерации или его заместители обращаются в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) с требованием о принятии мер по ограничению доступа к следующей распространяемой с нарушением закона информации: а) призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых мероприятиях с нарушением порядка;

[1] См.: Чернышенко оценил перспективы развития ИИ в России // РИА Новости. 2023. 23 нояб. URL: https://ria.ru/20231123/chernyshenko-1911313936.html (дата обращения: 12.03.2024).

[2] Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

б) ложные сообщения об актах терроризма и иная недостоверная информация, распространяемая под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и здоровью граждан, имуществу; в) распространяемая под видом достоверных сообщений недостоверная информация, содержащая данные об использовании ВС РФ; г) предложения о финансировании противника в условиях вооруженного конфликта, военных действий; д) призывы к введению в отношении РФ и ее граждан санкций; е) обоснования или оправдания осуществления экстремистской деятельности, включая террористическую деятельность; ж) предложения о приобретении поддельного документа, предоставляющего права или освобождающего от обязанностей; и) материалы нежелательной иностранной или международной неправительственной организации; к) информация о получении банковских услуг со стороны неуполномоченных лиц; л) информация об осуществлении сбора религиозных пожертвований; м) сведения, позволяющие получить доступ к указанным видам информации[1].

Настоящие положения закона реализуются через приказ Генерального прокурора Российской Федерации от 26.08.2019 № 596 «Об утверждении Инструкции о порядке рассмотрения уведомлений и заявлений о распространяемой с нарушением закона информации в информационно-телекоммуникационных сетях, в том числе в сети „Интернет“»[2]. При обнаружении на интернет-ресурсе распространяемой с нарушением закона информации исполнитель инициирует его экспертное исследование. Материалы о результатах предварительного рассмотрения уведомлений прокурорами городов, районов направляются для дальнейшей работы прокурорам. На основании полученной информации составляется заключение, которое утверждается прокурором субъекта, которое вместе с материалами направляется в Генеральную прокуратуру Российской Федерации. В Генеральной прокуратуре Российской Федерации по результатам рассмотрения уведомлений и заключений готовится требование в Роскомнадзор о принятии мер по удалению информации и/или по ограничению доступа к информационным ресурсам. Занимаются этой работой прокуроры субъектов, городов, районов.

Таким образом, прокуратура в силу возложенных на нее законом полномочий и специфики выполняемых ею функций является полноправным субъектом системы обеспечения информационной безопасности и предупреждения киберпреступности. Обеспечивая информационную безопасность, прокуратура, во-первых, осуществляет прокурорский надзор за исполнением законов органами, отвечающими за информационную безопасность, и, во-вторых, реализует собственные полномочия, направленные на обеспечение информационной безопасности Российской Федерации.

Заключение

Поскольку напряженная криминогенная обстановка в сфере использования информационно-коммуникационных технологий очевидно будет сохраняться (возможно даже ухудшаться), большое значение приобретает повышение уровня осведомленности граждан в вопросах обеспечения личной информационной безопасности. Работники прокуратуры проводят соответствующую разъяснительную работу в рамках правового просвещения и правового информирования населения. Для формирования безопасного информационного пространства прокуроры налаживают взаимодействие с органами публичной власти и добровольческими движениями, оказывающими содействие в выявлении деструктивного информационного материала, распространяемого в интернете/даркнете, готовят информационные справочные материалы по вопросам повышения уровня правосознания граждан, разъясняют нормы законодательства в сфере информационной безопасности.

Университетом прокуратуры Российской Федерации последовательно и целенаправленно проводится научное обеспечение прокурорского надзора за исполнением законов о противодействии киберпреступности. На регулярной основе организовываются научные представительские мероприятия, подготовлен ряд монографий и научно-практических пособий, осуществляется образовательная деятельность в рассматриваемой области [1; 2; 3; 6; 8; 9; 12]. Новой задачей для Университета прокуратуры должна стать подготовка специалистов для борьбы с киберпреступлениями, которые одинаково хорошо знали бы цифровые технологии, умели работать с алгоритмами (так называемые IT-специалисты) и прекрасно разбирались бы в тонкостях применения законодательства и понимали бы специфику прокурорской работы.

Важно постоянно заострять внимание на научных исследованиях в вопросах обеспечения информационной безопасности и всячески популяризировать новые идеи в этом направлении. Взгляд молодежи представляется особенно ценным, в том числе тем, что отражает ее отношение к изменениям, которые происходят в Российской Федерации и мире. Новые информационные технологии априори подвластны молодым ученым, им же придется решать задачи информационной безопасности.

[1] Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

[2] СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_332385/ (дата обращения: 12.03.2024).

Список источников

1. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / editors S. P. Shcherba (Russian ed.) and P. A. Litvishko (English ed.). Moscow : Publishing House «Gorodets», 2024. 224 p.

2. Винокуров А. Ю., Винокуров Ю. Е. Прокурорский надзор : учебник. 6-е изд., пер. и доп. Москва : Юрайт, 2024. 414 с.

3. Деятельность прокуратуры по профилактике правонарушений : монография / под науч. ред. В. В. Меркурьева. Москва : Проспект, 2023. 456 с.

4. Ищенко Е. П., Кручинина Н. В. Высокие технологии и криминальные вызовы // Всероссийский криминологический журнал. 2022. Т. 16, № 2. С. 199–206. DOI: 10.17150/2500-4255.2022.16(2).199-206

5. Ищенко Е. П., Кручинина Н. В. Преступления, совершаемые с использованием высоких технологий // Всероссийский криминологический журнал. 2019. Т. 13, № 5. С. 740–746. DOI: 10.17150/2500-4255.2019.13(5).740-746

6. Концептуальные проблемы обеспечения законности в современных условиях : монография / под общ. ред. К. И. Амирбекова; науч. ред. А. Ю. Винокуров. Москва : Проспект, 2024. 320 с.

7. Коробеев А. И., Дремлюга Р. И., Кучина Я. О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. Т. 13, № 3. С. 416–425. DOI: 10.17150/2500-4255.2019.13(3).416-425

8. Максимов Е. Л., Гришин А. В., Рыжих И. В. Обзор итогов круглого стола «Особенности подготовки прокурорских работников в Университете прокуратуры Российской Федерации» // Вестник Университета прокуратуры Российской Федерации. 2024. № 2 (100). С. 198–203.

9. Научный обзор итогов конференции «Цифровые технологии в прокурорской деятельности» // Вестник Университета прокуратуры Российской Федерации. 2023. № 6 (98). С. 150–154.

10. Осипенко А. Л., Соловьев В. С. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. Т. 15, № 6. С. 681–691. DOI: 10.17150/2500-4255.2021.15(6).681-691

11. Пристансков В. Д., Харатишвили А. Г., Евстратова Ю. А. Искусственный интеллект — новая форма использования специальных знаний в расследовании и раскрытии киберпреступлений // Всероссийский криминологический журнал. 2023. Т. 17, № 6. С. 586–596. DOI: 10.17150/2500-4255.2023.17(6).586-596

12. Прокурорский надзор за исполнением законов органами предварительного расследования при выявлении и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий : науч.-практ. пособие / [А. Л. Аристархов, К. В. Камчатов и др.]; Ген. прокуратура Рос. Федерации; Ун-т прокуратуры Рос. Федерации. Москва, 2023. 122 с.

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 25.04.2024.
Дата рецензирования статьи / Revised: 16.06.2024.
Дата принятия статьи к публикации / Accepted: 15.07.2024.