УДК 343.163

Тухтарова Елена Владимировна
студент,
кафедра уголовного процесса
и прокурорского надзора,
Байкальский государственный университет,
г. Иркутск, Российская Федерация,
e-mail: elen.tukhtarova@gmail.com

ПРОКУРОРСКИЙ НАДЗОР ЗА ПРОТИВОДЕЙСТВИЕМ КИБЕР-ПРЕСТУПЛЕНИЯМ

Аннотация. Статья посвящена анализу роли прокуратуры в борьбе с кибер-преступностью. Рассмотрены поставленные Генеральным прокурором задачи для противодействия преступлениям, связанными с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий. В статье приведена статистика совершения кибер-преступлений за последние три года, проанализированы причины низкой раскрываемости кибер-преступлений с учётом мнения IT-специалистов, предложены меры по решению проблемы с учётом зарубежного опыта.

***Ключевые слова*:** прокурорский надзор, сеть «Интернет», Генеральная прокуратура Российской Федерации, киберпреступность, противодействие преступности.

Elena V. Tukhtarova
Student,
Department of Criminal Procedure
and Prosecutor's Supervision,
Baikal State University,
Irkutsk, Russian Federation,
e-mail: elen.tukhtarova@gmail.com

PROSECUTOR'S SUPERVISION OVER CYBERCRIME CONTROL

Abstract. The article is devoted to the analysis of prosecutor's role over cybercrime control. The article contains main objectives in the fight with cybercrime, planned by Prosecutor-General of Russia, cybercrime statistics for the last three years, analysis of reasons of low clearance rate according to IT-experts' opinion. Author also proposes measures to solving the problem based on foreign experience.

***Keywords*:** prosecutor's supervision, the Internet, the Prosecutor General's Office of the Russian Federation, cybercrime, crime control.

Процесс информатизации, возникший во второй половине 20 века оказывает влияние на все сфере общества, в том числе и на криминальную. С того момента количество способов совершения этих преступлений увеличивалось в геометрической прогрессии. Сегодня каждое седьмое преступление в России

совершается с помощью IT-технологий, а ущерб от них в России в 2020 году составил 69 млрд рублей [1]. Информационная инфраструктура открывает широкий спектр возможностей для современных преступников: сокрытие личности, совершение преступления на расстоянии, общение с сообщниками на международном уровне. Одно из самых первых преступлений с использованием электронно-вычислительной машины (ЭВМ) на территории СССР было совершено в 1979 году в Вильнюсе [2]. В 1986 г. в Париже группой экспертов Организации экономического сотрудничества и развития было дано определение компьютерного преступления, под которым понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных [3]. С того момента в Уголовный Кодекс Российской Федерации был внесен ряд изменений, закрепляющих виды преступлений в информационно-телекоммуникационной сети Интернет. Надзор за соблюдением данных норм уголовного законодательства является одним из направлений деятельности прокуратуры. В частности, кибер-преступлениям посвящена глава 28 Кодекса:

272 УК РФ «Неправомерный доступ к компьютерной информации»;

273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»;

274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»;

274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»;

а также ст. 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности»; 159.6 УК РФ «Мошенничество в сфере компьютерной информации» и 187 УК РФ «Неправомерный оборот средств платежей».

Согласно проведенным нами расчетам, удельный вес , за последние три года почти в два раза выросло количество преступлений совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (14 % в 2019 году и 25 % в 2021)*.

Условиями такой динамики является повсеместное распространение информационных технологий, под причинами эксперты выделяют влияние пандемии и карантинный режим в связи с распространением новой коронавирусной инфекции COVID – 19. Кроме того, по всему миру организации здравоохранения фиксируют повышение уровня тревожности и паники у населения, на чем успешно спекулируют преступники. Популярным стало распространение в мессенджерах вредоносных ссылок в сообщениях с информацией о коронавирусе.

На фоне таких изменений в структуре преступности последних лет, возрастает роль правоохранительных органов в борьбе с кибер-преступлениями. Генеральная прокуратура Российской Федерации как единая федеральная централизованная система органов, осуществляющая надзор за соблюдением Конституции Российской Федерации и исполнением действующих в России законов, играет ключевую роль в борьбе с киберпреступностью в сфере информации. сфере,

обеспечивающей защиту интересов и прав человека и гражданина в информационном пространстве, безопасности общества и государства.

Таблица 1

Статистика кибер-преступлений за 2019 – 2021 годы

	2019 г.	2020 г.	2021 г.
Общее количество преступлений	2024,3 тыс.	2044,2 тыс.	2004,4 тыс.
Количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	294,4 тыс.	510,4 тыс.	517 тыс.
Удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	14 %	25 %	25 %

*Источник [4][5][6].

Согласно данным статистики МВД за 2021 год, раскрываемость преступлений в сфере компьютерной информации составила 25 %. По мнению большинства учёных причиной, определяющей такой низкий процент раскрываемости является низкая квалификация кадров правоохранительных органов в рассматриваемой сфере.

Одним из самых распространенных видов кибер-преступлений является фишинг. Суть фишинга заключается в распространении ссылок по электронной почте, переходя по которым данные банковской карты пользователя становятся известны злоумышленникам.

По мнению эксперта в области расследования кибер-преступлений, даже самый мелкий такой фишинг может расследоваться долгий период времени, поскольку дознавателю необходимо: 1) получить показания потерпевшего, сотрудников отдела информационной безопасности банка, сотрудников интернет-провайдера; 2) поручить проведение оперативно-розыскных мероприятий, направленных на установление лица, совершившего хищение; 3) получить ответы банка о перечислении денежных средств со счета потерпевшего, снятии денежных средств с банкомата; 4) получить ответы Бюро специальных технических мероприятий (подразделения МВД России) об установлении информации учетных записей в социальных сетях, электронной почтовой службы, информации об администрировании этих данных; 5) при установлении личности хакера – произвести его задержание, решить вопрос об избрании меры пресечения, допросить в качестве подозреваемого, произвести обыск, изъять компьютерную технику, которая послужит объектом исследования компьютерно-технической экспертизы и пр. Сложность данных мероприятий отталкивает недобросовестных дознавателей и

следователей [6]. Несмотря на увеличение реального количества компьютерных преступлений и причиненного ими ущерба, количество направленных в суд с обвинительным заключением преступлений сокращается. Большая часть уголовных дел приостанавливается на основании статьи 208 УПК РФ и не доходит до судебных инстанций [7].

В 2020 году было проведено совещание в Генеральной прокуратуре Российской Федерации по теме: «Борьба с преступлениями, связанными с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий». Задачи, поставленные по итогам совещания Генеральным прокурором Игорем Красновым заключаются в:

– усовершенствовании технической базы правоохранительных органов путём создания автоматизированных поисковых систем с целью расширения функционала по предупреждению и пресечению киберпреступности;

– внедрение специальной подготовки сотрудников, осуществление их профессионального отбора;

– обеспечении сотрудничества прокуроров, сотрудников оперативных, в том числе технических служб, и органов следствия на всех стадиях выявления данных посягательств и осуществления уголовного преследования;

– необходимости совершенствования действующего законодательства в части расширения признаков преступлений в сфере IT-технологий, введения в процессуальные нормы понятия «электронного доказательства», процедур внесудебной блокировки «зеркал» ранее заблокированных сайтов [8].

Полномочие, входящее в предмет прокурорского надзора, а также ключевое, по нашему мнению, направление в борьбе прокуратуры с кибер-преступностью является надзор за исполнением законов органами, осуществляющими оперативно-розыскную деятельность, дознание и предварительное следствие. В связи с этим, важнейшей, из поставленных Генеральным прокурором задач, на наш взгляд, является внедрение специальной подготовки сотрудников и осуществление их профессионального отбора.

В данном вопросе рациональным представляется анализ мнения специалистов сферы информационной безопасности.

Так, по мнению одного из бывших кибер-преступников, ныне специалиста по кибер-безопасности, Сергея Павловича, проблема низкой раскрываемости кибер-преступлений не столько в отсутствии регулирования, сколько в нежелании правоохранительных органов расследовать подобные преступления. Его поддерживает руководитель отдела аналитики российского разработчика средств информационной безопасности Алексей Парфентьев, считая, что лишь небольшой процент раскрываемости интернет-преступлений связан с недостаточной оснащенностью полиции. «Для эффективного розыска следователям требуются специальные технические познания, умение формулировать правильные вопросы для проведения экспертиз по уголовным делам, знание хода киберпроцесса и ряд других навыков в киберсфере» - считает заместитель председателя комиссии по правовому обеспечению цифровой экономики Московского отделения Ассоциации юристов России Екатерина Ипполитова.

ISSN 2658-7823

Таким образом, тезис об определяющей роли профессиональной подготовки кадров правоохранительных органов в борьбе с кибер-преступностью подтверждается. В связи с чем, по данной проблеме среди других направлений деятельности прокуратуры надзор за исполнением законов органами, осуществляющими оперативно-розыскную деятельность, дознание и предварительное следствие считаем приоритетным.

Для повышения раскрываемости кибер-преступлений, а также снижения преступной активности в сфере компьютерной информации представляется целесообразным использование зарубежного опыта в части ужесточения наказания за кибер-преступления. В Соединенных Штатах Америки лицу, будучи осужденному за киберпреступление, но повторно совершившему несанкционированный доступ к компьютеру, что повлекло тяжкие последствия, может быть назначено тюремное заключение сроком до 20 лет, в то время как ст. 272 УК РФ предусматривает максимальное наказание в виде семи лет лишения свободы [9]. Кроме того, на наш взгляд важнейшим шагом в борьбе с кибер-преступлениями является сотрудничество правоохранительных органов с IT-специалистами, а также внедрение профессиональной подготовки следователей, дознавателей, оперуполномоченных. Учитывая тот факт, что предметом прокурорского надзора является надзор за исполнением законов органами, осуществляющими оперативно-розыскную деятельность, дознание и предварительное следствие, необходимо на законодательном уровне закрепление признаков преступлений в сфере IT-технологий, введения в процессуальные нормы понятия «электронного доказательства», процедур внесудебной блокировки «зеркал» ранее заблокированных сайтов. Еще одной необходимой мерой является объединение всех стран для совместной борьбы с кибер-преступностью. Так как в свете глобализации мира, многие механизмы и уловки, преступники заимствуют из практики злоумышленников других стран. Стоит отметить, что по всем предложенным мерам государство уже начало активную работу. В частности, в июле 2021 года Россия внесла в ООН первый в мире проект конвенции о противодействии киберпреступности и криминальному использованию криптовалюты.

Список использованной литературы

1. Ущерб от киберпреступности в РФ в 2020 году составил 69 млрд рублей / Гункель Елена. – Текст : электронный // Deutsche Welle : [сайт]. – URL: https://www.dw.com/ru/ushherb-ot-kiberprestupnosti-v-rossii/a-56568904 (дата обращения: 20.02.2022).

2. Батурин, Ю. М. Проблемы компьютерного права / Ю. М. Батурин. – Москва : Юрид.лит., 1991. — 272 с.

3. Волеводз, А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. / А. Г. Волеводз. – Москва : Юрлитинформ, 2002. – 496 с.

4. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года // Министерство внутренних дел Российской Федерации : офиц.сайт. – URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 20.02.2022).

5. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2020 года // Министерство внутренних дел Российской Федерации : офиц.сайт. – URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 20.02.2022).

6. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2019 года // Министерство внутренних дел Российской Федерации : офиц.сайт. – URL: https://мвд.рф/reports/item/19412450/ (дата обращения: 20.02.2022).

7. Киберпреступлений становится все больше, однако их раскрываемость уменьшается. // Адвокатская газета : офиц.сайт. – URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения: 20.02.2022).

8. Александрина Н. М. Виктимологическая характеристика компьютерных преступлений, совершенных в отношении юридических лиц / Н. М. Александрина // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2019. – № 1 (45). – С. 223–227. — URL: https://cyberleninka.ru/article/n/viktimologicheskaya-harakteristika-kompyuternyh-prestupleniy-sovershennyh-v-otnoshenii-yuridicheskih-lits (дата обращения: 20.02.2022).

9. Потапов, А. А. Прокурорский надзор за противодействием киберпреступности в информационно-телекоммуникационной сети Интернет / А. А. Потапов. — Текст : непосредственный // Молодой ученый. – 2020. – № 49 (339). – С. 292–297. — URL: https://moluch.ru/archive/339/76047/ (дата обращения: 20.02.2022).

10. Закон и общество: история, проблемы, перспективы: мат-лы XXIV Межвуз. науч.- практ. конф. студентов и аспирантов (в дистанционном формате). Часть 2 / Краснояр. гос. аграр. ун-т. – Красноярск, 2020. – 244 с.