

7. Федеральный закон № 73-ФЗ от 31 мая 2001 г. «О государственной судебно-экспертной деятельности» (ред. от 26.07.2019). URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102071320> (дата обращения: 30.11.2021).

УДК 34

Ковтун Карина Александровна,
студент, Санкт-Петербургский государственный
политехнический университет,
г. Санкт-Петербург, Российская Федерация
wertoment@mail.ru

**Осуществление прокурорского надзора
в сфере киберпреступности
в информационно-телекоммуникационной сети Интернет.
Актуальные тенденции развития**

В статье предоставлен анализ влияния информационных технологий на состояние преступности в Российской Федерации. В первой части проводится сопоставление статистических данных, свидетельствующих о повышении уровня преступности в информационной сфере. Опираясь на Концепцию, предоставленную Генеральной Прокуратурой Российской Федерации, производится анализ неутешительного прогнозирования, представленного в рамках данной Концепции, а также возможные пути противодействия информационной преступности. Во второй части статьи выделяется проблематика необходимости урегулирования законодательной базы, осуществляющей контроль за информационной сферой. В заключении предоставляется вывод о проделанном исследовании, а также приводятся примеры усовершенствования деятельности прокуратуры в сфере информационной безопасности.

Ключевые слова: статистика, угрозы, информационные технологии, деятельности прокуратуры, тенденции развития, мошенничество, государственная поддержка, эффективные способы правового воздействия.

Kovtun Karina Alexandrovna,
student, Saint Petersburg State Polytechnic University,
Saint Petersburg, Russian Federation

**Implementation of prosecutorial supervision in the field of cybercrime
in the information and telecommunications network of the Internet.
Current development trends**

The article provides an analysis of the impact of information technology on the state of crime in the Russian Federation. In the first part, a comparison of statistical data indicating an increase in the level of crime in the information sphere is carried out. Based on the Concept provided by the Prosecutor General's Office of the Russian Federation, the analysis of the disappointing forecasting presented within the framework of this Concept, as well as possible ways to counter in-

formation crime, is carried out. The second part of the article highlights the problems of the need to regulate the legislative framework that controls the information sphere. The conclusion provides a conclusion about the research done, as well as examples of improving the activities of the prosecutor's office in the field of information security.

Keywords: *statistics, threats, information technologies, prosecutor's office activities, development trends, fraud, state support, effective ways of legal influence.*

Исходя из статистики, предоставленной в сборнике Генеральной Прокуратуры Российской Федерации, уровень преступлений, совершаемых в сфере информационных технологий, вырос в 25 раз по сравнению с показателями пятилетней давности. Данные статистические материалы подтверждают актуальность изучаемой проблематики, которая требует усовершенствованного подхода в правовом регулировании. Такой рост киберпреступлений связан, в первую очередь, с внедрением информационных технологий практически во все сферы жизни общества. Сложно представить деятельность любого лица без использования удобств, использование которых стало возможным в связи с цифровизацией жизни. Несмотря на ряд положительных аспектов внедрения информационных технологий во все сферы жизни общества, данное явление послужило поистине колоссальной возможностью для возникновения новой категории преступлений, а именно киберпреступности.

Политика государства в рамках данной проблематики направлена на оптимизацию информации, предоставленной в сети интернет, а именно на осуществление безопасного доступа и фильтрацию потребляемых интернет-ресурсов [1].

Отражение необходимости в модернизации правового регулирования информационных технологий и киберпреступности наиболее подробно раскрыта в Доктрине информационной безопасности Российской Федерации, которая была утверждена приказом Президента РФ № 646 от 05.12.2016 года. Содержание данной доктрины отражает актуальность усовершенствования механизмов, выступающих в качестве регуляторов общественных отношений, возникающих в сфере информации и информационных технологий.

Говоря о Генеральной Прокуратуре Российской Федерации, как об основном государственном органе, осуществляющем надзор за соблюдением норм законодательства на государственном уровне, играет важнейшую роль в реализации противодейственных мер, направленных на нарушение целостности правового порядка в киберпространстве. Одним из основных направлений, необходимых для осуществления правильной правовой политики, является анализ состояния законности.

Наиболее значимым моментом, произошедшим в сфере анализа информационной преступности, является Координационное совещание руководителей правоохранительных органов Российской Федерации, которое состоялось в 2020 году. Выводы, которые были вынесены по окончании данного мероприятия, являлись неутешительными, так как 2020 год характеризуется в уголовном судопроизводстве как год банковских кибер атак. Повсеместное распространение такого печального феномена связана с недостаточной финансовой грамотностью населения, которая и послужила основной причиной для та-

кого масштабного распространения краж банковских средств со счетов граждан. Но данное направление кибер преступности является далеко не единственным. Наряду с хищением банковских средств, получили свое распространение махинации, связанные с передачей личных данных, содержащихся в сети интернет, сторонним лицам. Особую опасность неутешительной статистике придает не только повышение уровня кибер преступлений, но и низкий процент раскрываемости, который составил $\frac{1}{4}$ от ее общего числа.

Игорь Викторович Краснов, Генеральный прокурор Российской Федерации, выдвинул свои неутешительные прогнозы о дальнейшем распространении киберпреступности и обозначил необходимость осуществления прокурорского обзора в рамках данной проблематики.

Борьба, осуществляемая органами государственной власти по борьбе с преступлениями в информационной сфере, не соответствует масштабам данной проблемы. В первую очередь, это связано с использованием преступниками таких сервисов, как VPN, такой интернет-ресурс позволяет злоумышленникам скрывать свое истинное местоположение, что затрудняет их поиск и раскрытие преступлений. Следующей причиной, которая не позволяет регулировать информационную сферу в полной мере, является возможность анонимного пользования интернетом во множестве браузеров, данная проблема также осуществляет прямое влияние на низкий уровень раскрываемости киберпреступности.

Осуществление регулирования общественных отношений, которые возникают в рамках использования интернет-пространства, входят в предмет ведения Прокуратуры Российской Федерации, но имеют трансграничный характер, так как в связи с различными формами и видами проявления конкретной деятельности в киберсреде, он имеет свои пределы. В процессе реализации прокурорского надзора за соблюдением и исполнением законодательства государства первостепенное значение придается выявлению и пресечению преступной деятельности. В связи с данным фактом, стоит упомянуть отдельный компетентный орган, осуществляющий контроль за соблюдением законодательства в интернет-пространстве, а именно Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Правовая связь вышеупомянутого государственного органа и Прокуратуры Российской Федерации заключается в том, что прокурор осуществляет контроль за соблюдением и устранением нарушений законодательства в сфере информации и надзор за деятельностью Роскомнадзора, при помощи таких основных механизмов правового воздействия, как объявление предостережений и подача заявлений в суд в связи с нарушением прав человека и гражданина в сфере информационной безопасности [2].

В связи с необходимостью реализации органами прокуратуры контроля с использованием методов, указанных выше, Генеральной Прокуратурой Российской Федерации была закреплена Концепция цифровой трансформации органов и организаций прокуратуры, которая будет реализовываться до 2025 года.

В рамках данной концепции были представлены меры, необходимые для урегулирования отношений в сфере информационной безопасности. К ним была отнесена необходимость создания условий реализации прокурорского надзора в связи с цифровизацией его объектов, а также обозначена цель обеспечить функционирование отечественной инфраструктуры в цифровой среде. Кроме того, в данной Концепции было сформировано совершенно новое понятие, а именно «высокотехнологичный надзор», который представляет собой реализацию функции контроля в цифровой сфере.

Основные направления деятельности, обозначенные в Концепции Генеральной Прокуратуры Российской Федерации, безусловно, сыграют большую роль в реализации государственного контроля в сфере киберпреступности, но все же данный перечень не является исчерпывающим, так как преступность в информационной сфере постоянно развивается и требует принятия своевременных мер.

В свою очередь, необходимым направлением развития законодательства в сфере современных технологий считаем создание Информационного права, которое будет закреплено в виде кодекса, и носить общеобязательный характер. Такая мера выступит в качестве как психологического аспекта, так как лица, осуществляющие кибермахинации, обратят свое внимание на своевременно принятые государственные меры, которые представлены в виде структурированной отдельной отрасли права, так и позволит законодателю разграничить понятие дозволенного и запрещенного в информационной сфере [3].

Следующим необходимым этапом является закрепление на законодательном уровне запрета на использование сервисов, позволяющих скрывать свое местоположение, так как это является основной причиной низкого процента раскрываемости киберпреступлений.

Необходимой мерой противодействия преступлений в информационной сфере также выступает выделение отдельного государственного органа, деятельность которого будет нацелена на предотвращение киберпреступлений, на данный момент, такой законопроект уже рассматривается, а орган носит название «киберполиция».

Что касается прокуратуры Российской Федерации, то основные нововведения должны быть направлены на ужесточение мер воздействия на нарушителей законодательства в сфере информационной безопасности, так как это является необходимой мерой для снижения уровня киберпреступлений.

Основным направлением деятельности государства, которая направлена на потенциальных жертв преступников в сфере информационных технологий, является повышение финансовой грамотности населения, путем привлечения известных банков к данному вопросу. Серьезный подход к финансовой грамотности населения поможет снизить уровень доверия граждан к неизвестным лицам, представляющимся сотрудниками банков и иными уполномоченными лицами.

В заключение стоит сказать о том, что тема киберпреступности является наиболее актуальной уже на протяжении нескольких лет, и, к сожалению, не сбавляет свои обороты. Единственным способом противодействия данному виду преступности является принятие мер государственного контроля над киберпреступниками, путем комплексного подхода к данной проблематике, в том числе со стороны органов прокуратуры Российской Федерации.

СПИСОК ИСТОЧНИКОВ

1. Быков С. А. Анализ особенностей экономической преступности в России. URL: <https://www.elibrary.ru/item.asp?id=12849326> (дата обращения: 6.11.2021).

2. Гамза В. А., Ткачук И. Б. Безопасность коммерческого банка : учебно-практическое пособие. М. : Издатель Шумилова И. И., 2000.

3. Сатуев Р. С., Шраер Д. Я., Яськова Н. Ю. Экономическая преступность в финансово-кредитной системе. М. : Центр экономики и маркетинга, 2000. 259 с.

УДК 338.001

Мельников Иван Николаевич,
кандидат юридических наук, доцент,
Костромской государственный университет,
г. Кострома, Российская Федерация
melnik44@gmail.com

Журавлев Кирилл Андреевич,
магистрант,
Костромской государственный университет,
г. Кострома, Российская Федерация,
mr.Zhuravlevkirill@mail.ru

Цифровизация правоотношений гражданского общества. Проблема доверия информационным технологиям

В данной статье говорится о свойственной цифровой эпохе проблеме – проблеме цифрового доверия. В статье нами рассмотрены проблемные вопросы, которые способствуют формированию этого явления, изучены точки зрения отечественных и зарубежных исследователей, а также предложены перспективные пути решения проблемы.

Ключевые слова: правоотношения, гражданское общество, цифровизация, информационные технологии, цифровые институты, цифровые технологии, цифровые платформы, цифровое доверие.