УДК 343.335

П. А. Проскурякова, В. Б. Яковлев
Кузбасский государственный технический университет им. Т.Ф. Горбачева, Кемерово, Россия

ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

научный руководитель: д.ф.н., профессор кафедры истории, философии и социальных наук Золотухин В.М.

Постоянный рост информационного потока затрагивает все области деятельности человека, и как, следствие этого, ведет к снижению уровня информационной безопасности. Развитие и применение информационных технологий связаны с риском появления различных видов реагирования на эти процессы, в том числе на повышение уровня преступности и изменения правоприменительной практике, направленную на обеспечение защиты прав граждан как участников «информационного» оборота в цифровом пространстве. В статье обращено внимание на необходимость совершенствования законодательной базы в области кибербезопасности и проведен соответствующий анализ.

Ключевые слова: интернет, криминалистика, информационная безопасность, информация, киберпреступность, защита.

Вопрос противодействия угрозам информационной безопасности, и защита связанных с ними общественных отношений, в настоящее время является одним из актуальных в рамках обеспечения информационной безопасности. Это касается как сохранения национальной идентичности в правоприменительной практике [Козырева, Тарасенко, 2020, с. 70], так и различным аспектам правовой нормативности в социокультурной сфере [Золотухин В. М., Степанцова, 2015].

Актуализация этих проблем связана с процессами цифровизации почти всех сфер жизнедеятельности общества, что связано, в первую очередь с «навязываем» ее в рамках борьбы с пандемией COVID-19. Усиление данного аспекта также связано с тем, что социальные сети становятся неотъемлемой частью повседневной жизни современного человека. В 2020 году пользователями сети «Интернет» в России стали 118 млн. человек, тогда как в 2019 году их количество составляло 109,6 млн. человек [WebCanape, 2020].

В информационном пространстве ежедневно расширяется не только поток информации, но и появляются новые данные, представляющие различные угрозы и посягательства на безопасность страны, общества, человека. Особен-

но, уязвим последний относительно своей собственности, сохранности личной и семейной тайны, персональных данных при осуществлении трудовых функций, а также безопасности при совершении банковских операций и использования банковских карт [Козырева, Криони, Морозов, 2019].

В последнее время наблюдается рост преступлений, совершаемых с использованием информационных технологий. Например, за январь-июль 2020 года их количество выросло на 94,6% по сравнению с аналогичным периодом 2019 года, в том числе тяжкие и особо тяжкие – на 129,7%. При этом расчетные карты в преступлениях использовались почти в 6 раз чаще, чем в прошлом году, средства мобильной связи – более чем в 2 раза чаще [МВД России, 2020].

В 2019 году компания Positive Technologies провела исследование и выявила следующие категории жертв и объекты атак злоумышленников, категории и объекты представлены на рисунках 1 – 3 [Positive Technologies, 2019].

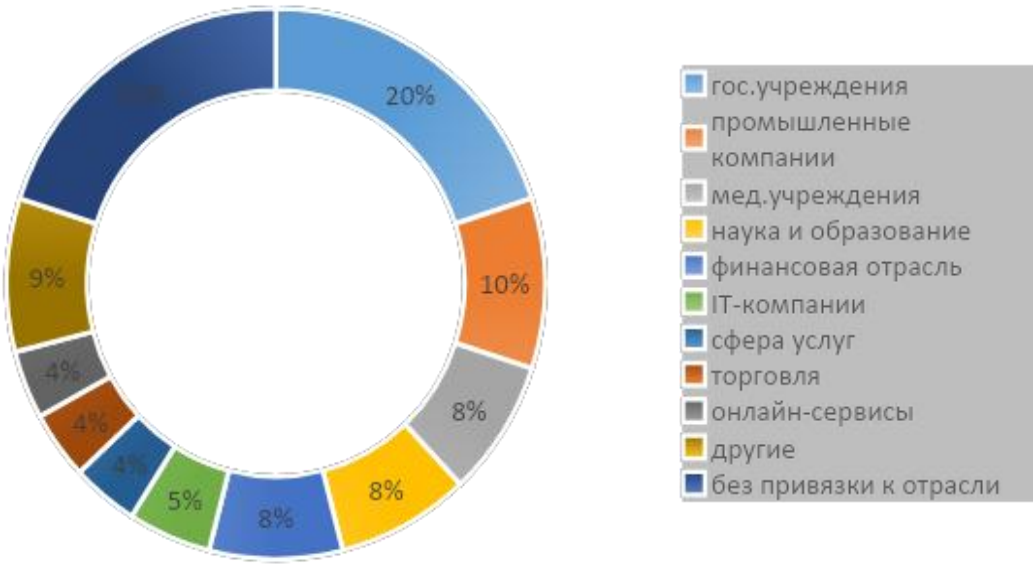

Рисунок 1. Категории жертв среди юридических лиц

Одна из причин активного роста данного вида преступлений заключена в низком уровне цифровой грамотности населения, а также безразличном отношении пользователей к собственной безопасности. Так, аналитическим центром «НАФИ» было проведено исследование, которое показало, что только 27% россиян – каждый четвертый – обладают высоким уровнем цифровой грамотности

[Цифровая грамотность россиян: исследование, 2020]. Стоит отметить, что, несмотря на низкий уровень цифровой грамотности населения, наблюдается тенденция к ее увеличению. Остальные 73% россиян либо не задумываются о киберугрозах, поскольку не ожидают, что с ними это может произойти, либо не принимают никаких действий по защите своих персональных данных, либо по незнанию отдают свои же персональные данные злоумышленникам.

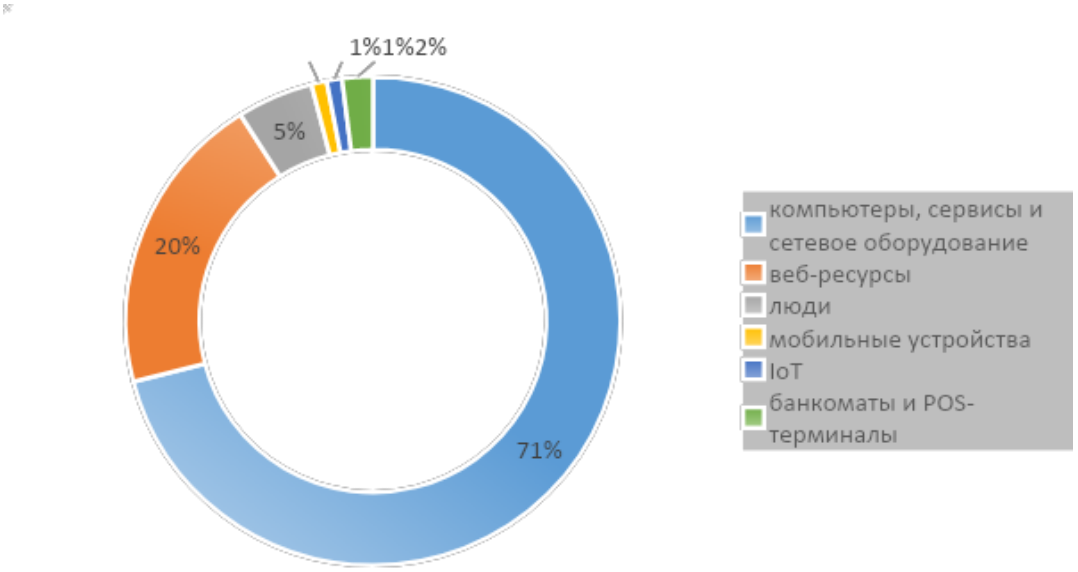

Рисунок 2. Объекты атак юр. лиц

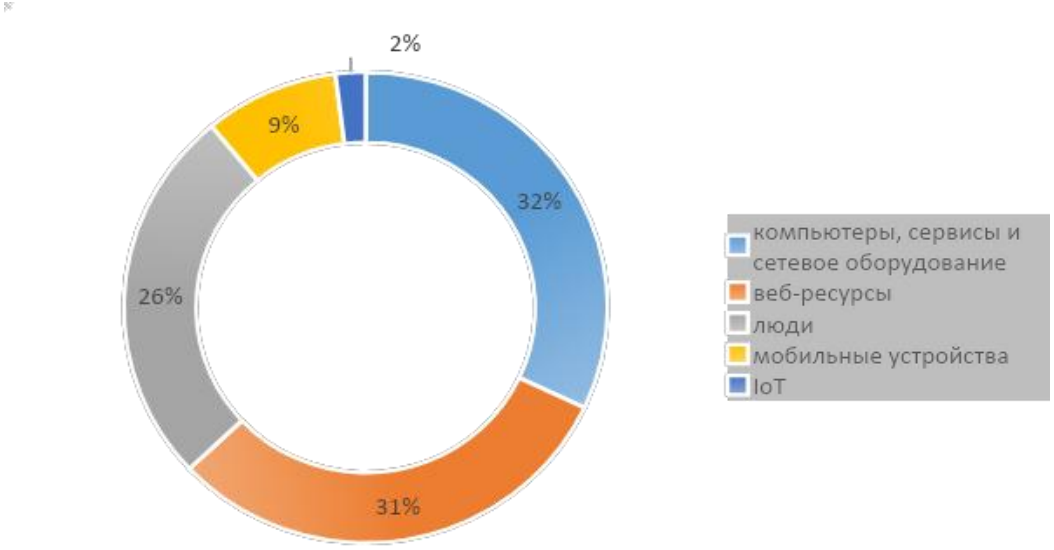

Рисунок 3. Объекты атак частных лиц

Негативно на данную статистику влияет то, что при расследовании данных преступлений проведение необходимых судебных экспертиз как способа

доказательств совершения преступлений осложняется тем, что появляются новые объекты исследования, предполагающие новые методы и формы. Прежде всего, это касается усовершенствования известных видов преступлений и появление абсолютно новых, ранее не известных и возникших в результате развития информационных технологий [Шелупанов, Смолина, 2020]. Такие факторы влияют на срок проведения расследований, затягивания делопроизводства на неопределенный срок.

Еще одной причиной является сбор улик. Форензик должен обладать специальными знаниями и понимать все тонкости сбора улик из различных источников. Собираемые им в компьютере улики – это по большей части нематериальные сведения.

Для эффективной работы специалисту требуются отлаженные механизмы и методики сбора улик, подкрепленные еще и соответствующими инструментами, например, специальным программным обеспечением The Forensic Toolkit Imager (FTK Imager) – данная утилита поддерживает около полутора десятков форматов образов и позволяет подключить их к системе, как настоящий физический диск.

Правовая основа борьбы с киберпреступностью в России впервые появилась с принятием Уголовного кодекса Российской Федерации, который вступил в силу 1 января 1997 года. В нем появилась глава 28 «Преступления в сфере компьютерной информации» [УК РФ, 1996], но стоит отметить, что подобные законопроекты появлялись ранее, однако они не были приняты. Например, 6 декабря 1991 года был представлен проект Закона РСФСР «Об ответственности за правонарушения при работе с информацией», который предлагал введение в УК РСФСР норм ответственности за совершение преступлений, связанных с компьютерной информацией [Гребеньков, 2012]. При этом до сих пор на законодательно отсутствует определение «киберпространство» и «киберпреступность» как на международном уровне, так и в законодательстве РФ.

Так, УК РФ устанавливает следующие виды преступлений в сфере компьютерной информации:

– неправомерный доступ к компьютерной информации;

– создание, использование и распространение вредоносных компьютерных программ;

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

– неправомерное воздействие на критическую информационную инфраструктуру РФ [УК РФ, 1996].

Вместе с этим преступления, связанные с информационными технологиями, не ограничиваются данными видами. В УК РФ также закреплены соответствующие признаки совершения общественно опасных деяний, в которых используются электронные и информационно-телекоммуникационные сети.

Раскрытие киберпреступлений – довольно сложная задача для сотрудников органов предварительного расследования. Это обусловлено спецификой данных преступлений, а именно:

–трудности с обобщением материалов следственной и судебной практики по каждому виду рассматриваемых правонарушений;

– отсутствие методических рекомендаций по организации расследований преступных деяний и тактике производства следственных действий;

– недостаточная квалификация следователей для работы со специфическими источниками доказательной информации, оцифрованной в виде электронных сообщений, страниц, сайтов [Шевченко, 2016].

Наряду с проблемами предварительного расследования существуют криминалистические проблемы расследования киберпреступлений, в частности: обоснование информационно-следовой картины преступных деяний, связанных с виртуальными следами; выделение данных преступлений в отдельную группу в системе криминалистической классификации противоправных деяний и другие вопросы рассматривались многими учёными. Например, в своих работах Ю. В. Гаврилин исследовал особенности тактических приёмов при производстве следственных действий, которые направлены на получение вербальной и не-

вербальной криминалистически значимой информации [Гаврилин, 209]; В. А. Мещеряков исследовал особенности обыска, выемки, допроса следственного эксперимента, возможности компьютерно-технической экспертизы и тактические рекомендации по ее назначению [Мещеряков, 2001].

Рассматривая киберпреступность с точки зрения криминалистики, стоит отметить, что наиболее важной методологической спецификой является исследование любых предметов материального и идеального, или же мысленного, моделей макро- и микромира. Иначе говоря, состав задач, подлежащих решению при исследовании киберпреступлений и киберпространства, обусловлен разнообразием существующих экспертных и следственно-судебных ситуаций. Для этого необходим соответствующий методологический потенциал для изучения виртуальных преступлений содержащийся специфику общенаучного, частнонаучного и специального разделов криминалистические знания.

Можно сказать, что применение системного подхода для повышения эффективности выявления и расследования киберпреступлений обусловлено необходимостью создания определенной, четкой классификации не только киберпреступлений, но и киберпространства, что потребует внедрение их механизмов, обоснование иерархии связей, например, внутренних и внешних. При этом изучение данных явлений должно происходить с учетом выявления и рассмотрения всех факторов, условий и специфики, в том числе, степени влияние человека на информационные процессы [Золотухин, 2020] и, вместе с ним трансформации его сознания [Zolotukhin, Zhukova, 2019; Яцевич, 2020]. Для этого необходимо постоянное совершенствование методик расследования инцидентов, содержащих в себе признаки преступления в киберпространстве.

Обобщение различных аспектов совершения и расследования преступлений в киберпространстве дает возможность утверждать, что данный вид преступлений, существующих в производной (искусственной) среде необходимо изучать через взаимодействие и взаимопроникновение с точки зрения системного подхода как сложного явления. Взаимосвязанные элементы совершаемых

преступлений в киберпространстве имею свою специфику и структуру, которые необходимо рассматривать с точки зрения единого целого.

Библиографический список

Гаврилин, Ю. В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: Дис… д-ра юрид. наук. М., 2009.

Гребеньков А. А. История формирования норм об ответственности за компьютерные преступления в России // Известия Юго-Западного государственного университета. Серия: История и право. – Курск: ГОУ ВПО "Юго-Западный гос. ун-т", 2012, – № 1. – Ч. 2. – С. 53–56.

МВД России – [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/20901417/ (дата обращения 10.11.2020).

Золотухин В. М. Социально-философский и культурологический аспекты деятельности человека в рамках цифровой реальности // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2020. – Т. 4. – № 4. – С. 323–329. DOI: https://doi.org/10.21603/2542-1840-2020-4-4-323-329

Золотухин В. М., Степанцова Е. В. Социокультурный аспект правовой нормативности в России. // Вестник Кемеровского государственного университета культуры и искусств. 2015. – № 31. – С. 105–111.

Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: Дис. ... д-ра юрид. наук. Воронеж: ВГУ, 2001

Козырева М. В., Криони А. Е., Морозов Н. В. Социокультурный и правовой аспекты социальной деятельности субъектов в банковской сфере. // Вестник Кемеровского государственного университета. Серия Гуманитарные и общественные науки, 2019. – Т 3 – № 2 (10). – С. 159-164.

Козырева, М. В., Тарасенко А .А. Трансформация российской идентичности и ее влияние на специфику уголовного правоприменения. / Проблемы экономики и управления: социокультурные, правовые и организационные аспекты : сборник статей магистрантов и преподавателей КузГТУ Посвящается 300-летию Кузбасса и 70-летию КузГТУ. (второй выпуск) / под ред. В. М. Золотухина, В. Г. Михайлова ; КузГТУ – Кемерово, 2020. – 319 с. С. 69-75.

Шевченко Е.С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений // Актуальные проблемы российского права. – 2016. – № 10. – С. 160–69.

Шелупанов А. А., Смолина А. Р. Форензика. Теория и практика расследования киберпреступлений. – М.: Горячая линия – Телеком, 2020. – 104 с.

Уголовный Кодекс Российской Федерации : федер. закон от 13 июня 1996 г. N 63-ФЗ : [ред. от 31.07.2020] // Собрание законодательства Рос. Федерации. – 1996. – № 25. – Ст. 2954.

Цифровая грамотность россиян: исследование 2020 – [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ (дата обращения 10.11.2020).

WebCanape. [Электронный ресурс]. – Режим доступа: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ (дата обращения 10.11.2020).

Яцевич М. Ю. Экологическое мировоззрении в условиях становления научных парадигм. // Вестник Томского государственного университета. Философия. Социология. Политология. 2020. – № 56. – С. 53–62.

Positive Technologies [Электронный ресурс].– Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/ (дата обращения 10.11.2020).

Zolotukhin, V. M., Zhukova, O. I. Man and Transformation of His Socio-Cultural Values in the Ethnic-National Aspect Smart Innovation, Systems and Technologies. 2019, T. 139, c. 772-777.

P. A. Proskuryakova, V. B. Yakovlev
T.F. Gorbachev Kuzbass State Technical University, Kemerovo, Russia

LEGAL ASPECTS OF INFORMATION SECURITY IN THE RUSSIAN FEDERATION

supervisor: D. F. N., Professor of history, philosophy and social Sciences Zolotukhin V. M.

The constant increase in the flow of information affects all areas of human activity and, as a consequence, leads to a decrease in the level of information security. The development and application of information technology poses the risk of different types of responses to these processes, including increased levels of crime and changes in law enforcement practices aimed at protecting the rights of citizens as participants «information» turnover in digital space. The article draws attention to the need to improve the legislative framework in the area of cybersecurity and analyses it accordingly.

Keywords: the Internet, forensics, information security, information, cybercrime, information protection.