DOI: 10.18137/RNU.V9276.22.03.P.058 УДК 343.4

С.С. Симонова

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В РОССИИ И ЗАРУБЕЖНЫХ СТРАНАХ: КРИМИНОЛОГИЧЕСКИЙ И ВИКТИМОЛОГИЧЕСКИЙ АСПЕКТЫ

Аннотация. Проанализированы статистические данные по киберпреступлениям. Представлен вывод, согласно которому для профилактики преступлений, совершаемых с помощью информационно-телекоммуникационных сетей, необходим комплексный подход – сочетание правовых, социальных и технических мер. Предложено широкое толкование термина «киберпреступность» для возможности его применения не только в уголовном праве, но и в других отраслях российского права. Рассмотрен мировой, российский и региональный опыт предупреждения и виктимологической профилактики киберпреступлений.

Ключевые слова: киберпеступность, профилактика преступлений, противодействие киберпреступлениям, информационная безопасность, киберугрозы, виктимологическая профилактика.

S.S. Simonova

COUNTERACTION TO CYBERCRIME IN RUSSIA AND FOREIGN COUNTRIES: CRIMINOLOGICAL AND VICTIMOLOGICAL ASPECTS

Abstracts. Statistical data on cybercrimes are analyzed. The author comes to the conclusion that for the prevention of crimes committed with the help of information and telecommunication networks, an integrated approach is needed: a combination of legal, social and technical measures. A broad interpretation of the term «cybercrime» is proposed for the possibility of its application not only in criminal law, but also in other branches of Russian law. The world, Russian and regional experience of prevention and victimological prevention of cybercrime is considered.

Keywords: cybercrime, crime prevention, cybercrime counteraction, information security, cyber threats, victimological prevention.

Профилактика преступлений традиционно характеризуется определенной спецификой применительно к тому или иному виду преступлений. Немаловажную роль для эффективной предупредительной деятельности играют такие факторы, как уровень латентности конкретного вида преступлений и личность преступника. С этой позиции представляется важным рассмотреть отечественный и зарубежный опыт профилактики преступлений, совершаемых в сети Интернет.

В последние годы роль технологий в жизни людей значительно изменилась. Этот эволюционный процесс предоставил обществу широкий спектр возможностей, например в плане общения, развлечений и обучения, но также способствовал увеличению разнообразия киберпреступлений [3, с. 7]. Киберпреступность – один из самых динамично развивающихся видов преступных деяний, поскольку само совершение рассматриваемых преступлений тесно взаимосвязано с появлением новых компьютерных технологий.

Представляется актуальной широкая трактовка понятия киберпреступлений,

Симонова Светлана Сергеевна
кандидат юридических наук, доцент кафедры уголовного права, уголовного процесса и криминалистики, Волгоградский институт управления – филиал Российской академии народного хозяйства и государственной службы, Волгоград. Сфера научных интересов: исполнение наказаний, профилактика преступлений, криминологический портрет преступника, уголовная ответственность несовершеннолетних, киберпреступность. Автор более 110 опубликованных научных работ.
Электронный адрес: simonova.ss@mail.ru

в рамках которой противоправные деяния, совершаемые в сети Интернет, должны пониматься не только как уголовные преступления, но и как любые нарушения прав граждан. В этом контексте уместно рассматривать в качестве киберпреступлений любые нарушения цифровых прав граждан, незаконное использование персональных данных граждан, кибербуллинг и иные виды противоправного поведения во Всемирной сети.

Растущее разнообразие технических устройств, которые позволяют получить доступ к сети Интернет, способствовало общему росту пользователей Интернета в самых разных местах и обстоятельствах. Эти устройства стали частью нашей жизни, и мы используем их для достижения различных целей [2, с. 1849]. Но существует и другая сторона технологического процесса – все чаще пользователи Всемирной сети становятся жертвами киберпреступлений, то есть противоправных деяний, совершаемых в сети Интернет с использованием информационно-телекоммуникационных технологий.

На сегодняшний день ученые большинства стран признают киберпреступления крайне серьезной проблемой, угрожающей информационной безопасности как государств в целом, так и отдельных граждан. В частности, по данным Европейской комиссии, в 2019 году по крайней мере 71 % европейских интернет-пользователей стали жертвами одного или нескольких киберпреступлений.

Приведем статистические данные о киберпреступлениях в некоторых европейских странах. В отчете по мониторингу безопасности федеральной полиции Бельгии за 2018 год содержатся сведения, согласно которым за 2018 год 8,14 % населения стали жертвами интернет-мошенничества, а 7,82 % пострадали от взлома их компьютеров или смартфонов. По данным Статистического управления Нидерландов, в 2018 году 8,5 % граждан Нидерландов заявили, что они стали жертвами киберпреступлений, таких как хакерство, онлайн-мошенничество, кража личных данных (фишинг), программы-вымогатели и межличностные инциденты [4].

Далее проанализируем опыт европейских стран по противодействию киберпреступности. В настоящее время в исследованиях, направленных на повышение безопасности онлайн-среды, можно выделить несколько концептуальных подходов. Ряд исследований направлен на процессы виктимизации населения в сфере киберпреступлений. Так, некоторые исследователи сосредотачиваются на понимании и повышении мотивации пользователей к защите и стремятся определить, какие категории граждан могут стать жертвами киберпреступлений. Таким образом, в рамках

Вестник Российского нового университета
Серия «Человек и общество», выпуск 3 за 2022 год

рассматриваемого подхода исследуются мотивы защиты от кибермошенничества, вредоносного программного обеспечения (далее – ПО) и киберпреступности в целом, при этом используется скорректированная модель теории мотивации защиты [6, с. 147]. Полученные в ходе исследования данные свидетельствуют о существенных различиях в защите от «технических» киберпреступлений (вредоносного ПО) по сравнению с более «социальными» киберпреступлениями (кибермошенничеством).

В рамках другого подхода исследуются возможности технических улучшений для нивелирования онлайн-угроз. В частности, речь идет о такой киберугрозе, как фишинг веб-сайтов, представляющий собой серьезное онлайн-мошенничество, которое наносит серьезный финансовый ущерб онлайн-пользователям [7, с. 48].

Один из традиционных подходов к борьбе с фишингом заключается в повышении осведомленности и обучении начинающих пользователей различным тактикам, используемым фишерами, путем проведения периодических тренингов или семинаров. Однако этот подход подвергался критике за его неэффективность с точки зрения затрат, поскольку тактика фишинга постоянно меняется, к тому же он может потребовать высоких операционных затрат. Еще один подход к борьбе с фишингом – законодательно закрепить или изменить в сторону ужесточения наказания существующие законы о кибербезопасности.

Более многообещающий подход к противодействию фишингу – предотвращение фишинговых атак с использованием технологии интеллектуального машинного обучения. Данная технология предполагает интегрирование в браузер специальной системы классификации, в которой обнаруживаются фишинговые атаки, о чем немедленно сообщается конечному пользователю.

Следует отметить, что серьезной проблемой, значительно затрудняющей противодействие киберпреступлениям, является их высокая латентность. Преступники, совершающие противоправные деяния с использованием информационно-телекоммуникационных технологий, всегда, условно говоря, идут «на шаг впереди» как правовых, так и технических мер, предпринимаемых уполномоченными субъектами обеспечения информационной безопасности.

С другой стороны, высокая латентность киберпреступлений обусловлена тем, что, согласно проведенным исследованиям, значительное число жертв киберпреступлений не делится своим опытом виктимизации с семьей, друзьями или правоохранительными органами [5, с. 219]. Возможное объяснение этого вывода заключается в том, что жертвы определенных видов киберпреступлений, таких как онлайн-мошенничество, нередко обвиняются в своей виктимизации.

Обратимся к ситуации с киберпреступностью в России. Анализируя статистические данные, можно отметить, что за 2020–2021 годы число киберпреступлений значительно возросло. В 2021 году в России было зарегистрировано около 518 тыс. киберпреступлений, что составило на 1,4 % больше, чем годом ранее, и при этом в 1,8 раза превосходит показатель 2019 года. Согласно данным, полученным компанией RTM Group, проводящей на основе возбужденных уголовных дел, связанных с использованием информационных технологий, оценку ущерба, причиненного киберпреступлениями, в 2021 году общий ущерб от преступлений с использованием компьютерных технологий в России превысил 150 млрд руб. Примечательно, что, по оценкам экспертов, в 2022 году он может составить уже 165 млрд руб. [1].

Представляется особенно важным проводить профилактические мероприятия по предупреждению преступлений, совершаемых в сети Интернет, среди подростков и лиц преклонного возраста, ведь, по статистике, именно данные категории населения наиболее часто становятся жертвами киберпреступлений. При этом в отношении пенсионеров чаще всего совершаются мошеннические действия, а в отношении несовершеннолетних пользователей – также кибербуллинг, фишинг, моральное, психическое и сексуальное насилие. Также в качестве рекомендаций по предупреждению киберпреступлений следует особо выделить повышение правовой и компьютерной грамотности, особенно среди рассмотренных выше возрастных категорий граждан, наиболее подверженных угрозам их информационной безопасности.

В качестве примера рассмотрим региональный опыт профилактической работы по предупреждению киберпреступлений. Так, преподаватели и студенты Волгоградского института управления в рамках работы Юридической клиники не только оказывают бесплатную юридическую помощь гражданам, но и проводят просветительские лекции для школьников, пенсионеров, читателей библиотек, где повышают их правовую грамотность в контексте защиты от киберугроз. В рамках изучения учебной дисциплины «Криминология» студенты составляют памятки по киберугрозам для различных категорий граждан.

Таким образом, считаем необходимым для успешной профилактики киберпреступлений слаженную практическую реализацию различных субъектов предупреждения преступлений, причем как специализированных, так и неспециализированных. Также важно учитывать индивидуальные особенности потенциальных и реальных жертв киберпреступлений для их эффективной виктимологической профилактики.

Литература

1. *Мингазов С.* Эксперты назвали низкую цифровую грамотность россиян причиной роста киберпреступности // ForbesLife. URL: https://www.forbes.ru/tekhnologii/455881-eksperty-sprognozirovali-rost-userba-ot-kiberprestupnosti-v-rossii-do-165-mlrd-rublej
2. *Carvalho J.V., Carvalho S., Rocha Á.* European strategy and legislation for cybersecurity: implications for Portugal // Cluster Computing. 2020. No. 23(3). Pp. 1845–1854.
3. *De Kimpe L., Walrave M., Ponnet K., Van Ouytsel J.* Internet safety. The International Encyclopedia of Media Literacy. 2019. Pp. 1–11.
4. Digitale Veiligheid & Criminaliteit 2018. URL: https://www.cbs.nl/nl-nl/publicatie/2019/29/digitale-veiligheid-criminaliteit-2018
5. *Jansen J., Leukfeldt E.R.* Coping with cybercrime victimization: An exploratory study into impact and change // Journal of Qualitative Criminal Justice and Criminology. 2018. Vol. 6. Iss. 2. Pp. 205–228.
6. *Martens M., De Wolf R., De Marez L.* Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general // Computers in Human Behavior. 2019. Vol. 92. Pp. 139–150.
7. *Qabajeh I., Thabtah F., Chiclana F.* A recent review of conventional vs automated cybersecurity anti-phishing techniques // Computer Science Review. 2018. Vol. 29. Pp. 44–55.

Вестник Российского нового университета
Серия «Человек и общество», выпуск 3 за 2022 год

References

1. Mingazov S. (2022) Eksperty nazvali nizkuyu tsifrovuyu gramotnost' rossiyan prichinoy rosta kiberprestupnosti [Experts called the low digital literacy of Russians the reason for the growth of cybercrime]. *ForbesLife.* URL: https://www.forbes.ru/tekhnologii/455881-eksperty-sprognozirovali-rost-userba-ot-kiberprestupnosti-v-rossii-do-165-mlrd-rublej (In Russian).
2. Carvalho J.V., Carvalho S., Rocha Á. (2020) European strategy and legislation for cybersecurity: implications for Portugal. *Cluster Computing*. No. 23(3). Pp. 1845–1854.
3. De Kimpe L., Walrave M., Ponnet K., Van Ouytsel J. (2019) Internet safety. *The International Encyclopedia of Media Literacy*. Pp. 1–11.
4. Digitale Veiligheid & Criminaliteit (2018) URL: https://www.cbs.nl/nl-nl/publicatie/2019/29/digitale-veiligheid-criminaliteit-2018
5. Jansen J., Leukfeldt E.R. (2018) Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*. Vol. 6. Iss. 2. Pp. 205–228.
6. Martens M., De Wolf R., De Marez L. (2019) Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*. Vol. 92. Pp. 139–150.
7. Qabajeh I., Thabtah F., Chiclana F. (2018) A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review.* Vol. 29. Pp. 44–55.