7. Комиссары на линии огня, 1941–1945. На земле. – М. : Политиздат, 1984. – 431 с.

8. Политработники на фронте: (Записки участников Великой Отечественной войны). – М. : Воениздат, 1982. – 222 с.

9. *Маликов В. Г.* Деятельность политорганов и партийных организаций по мобилизации личного состава авиационных частей на разгром врага в годы Великой Отечественной войны. – М. : ВПА имени В. И. Ленина, 1980. – 56 с.

УДК 373.167.1:004

Лобач Дмитрий Владимирович,
кандидат юридических наук, доцент,
Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации, г. Владивосток

Lobach Dmitry Vladimirovich,
candidate of law, associate professor, Far Eastern law institute (branch) University of the prosecutor's office of the Russian Federation, Vladivostok

dimaved85@mail.ru

Смирнова Евгения Александровна,
кандидат юридических наук, доцент,
Дальневосточный федеральный университет, г. Владивосток

Smirnova Evgenia Alexandrovna,
candidate of law, associate professor, Far Eastern Federal University, Vladivostok

smirnova.ea@dvfu.ru

КИБЕРУГРОЗЫ И КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ

CYBER THREATS AND CYBERSECURITY IN THE CONTEXT OF THE FOURTH INDUSTRIAL REVOLUTION

В статье анализируются ключевые угрозы, возникающие в сфере кибербезопасности и проявляемые в различных видах кибератак, совершаемых против информационных систем и угрожающих конфиденциальности, целостности и доступности компьютерных данных и систем, здоровью населения и общественной нравственности. Проанализированы статистические данные относительно распространения угроз в сфере кибербезопасности в мировом масштабе, а также исследована динамика компьютерных преступлений в России за последние 7 лет. Выявлены качественные характеристики киберугроз. Особое внимание об-

ращено на террористическую деятельность и смежный с ней экстремизм, распространяемые в информационном пространстве посредством использования сети Интернет.

The article analyzes the key threats arising in the field of cybersecurity and manifested in various types of cyberattacks against information systems and threatening the confidentiality, integrity and availability of computer data and systems, public health and public morality. Analyzed the statistical data on the spread of threats in the field of cybersecurity on a global scale, and also investigated the dynamics of computer crimes in Russia over the past 7 years. The qualitative characteristics of cyber threats have been identified. Particular attention is paid to terrorist activities and related extremism, spread in the information space through the use of the Internet.

Кибербезопасность, киберугрозы, терроризм, безопасность, интернет-преступность.

Cybersecurity, cyberthreats, terrorism, security, internet crime.

Четвертая промышленная революция, проявляемая в интенсификации технологического развития, быстрой интегративной адаптации общества к научным новациям и векторной динамике социальных отношений, приводит, с одной стороны, к оптимизации процессов управления и более эффективной организации субъектов социального взаимодействия, росту безопасности, экономических благ, улучшению качества жизни и росту уровня жизни населения, но с другой стороны, возникают новые риски (вероятность наступления неблагоприятных последствий при возникновении определенных условий) и угрозы (реальная опасность причинения вреда охраняемым законом интересам общества и государства, актуализируемая в свете современного научно-технологического развития), которые могут с большой долей вероятности детерминировать наступление деструктивных последствий для человека, общества, государства, всей мировой системы и международного правопорядка.

В этом ключе особый интерес вызывают угрозы, возникающие в сфере кибербезопасности и проявляемые в различных видах кибератак, совершаемых против информационных систем и угрожающих конфиденциальности, целостности и доступности компьютерных данных и систем, здоровью населения и общественной нравственности, а также общественным отношениям, возникающим в связи с правомочиями собственника и в сфере реализации авторских и смежных прав, совершенных на определенной территории в тот или иной период времени.

Об актуальности заявленной проблемы свидетельствуют следующие показатели угроз в сфере кибербезопасности в мировом масштабе. Так, за период 2009–2019 гг. наблюдается экспоненциальный рост количества заражений вредоносным программным обеспечением. Если в 2009 г. было зарегистрировано 12,4 млн инцидентов, то уже в 2010 г. – 29,97 млн инцидентов, в 2011 г. – 48,17 млн инцидентов, в 2012 г. – 82,62 млн инцидентов, в 2013 г. – 165,81 млн, в 2014 г. – 308,96 млн, в 2015 г. – 452,93 млн, в 2016 г. – 580,40 млн, в 2017 г. – 702,06 млн, в 2018 г. было зарегистрировано 812,67 млн соответствующих фактов заражений, а в 2019 г. – было зарегистрировано более 900 млн фактов зара-

жений [3]. За последнее время беспрецедентная пандемия коронавируса глубоко повлияла на распространение киберугроз по всему миру. Глобальный кризис здравоохранения усугубляется резким ростом киберпреступной деятельности, связанной с COVID-19, что создает значительную нагрузку на работу правоохранительных органов по всему миру. В целом киберпреступность, связанная с пандемией COVID-19, проявляется в следующих формах: интернет-мошенничество и фишинг; программы-вымогатели и DDoS-атаки против объектов критически важной инфраструктуры и учреждений здравоохранения; использование вредоносного программного обеспечения для несанкционированного сбора данных; создание вредоносных веб-сайтов; дезинформация и распространение фейковых новостей [2].

На национальном уровне также наблюдается быстрый рост количества совершаемых преступлений в сфере компьютерной информации. Так, если анализировать динамику компьютерных преступлений в России за последние 7 лет, то в репрезентативном виде обнаруживается следующая картина: в 2014 г. было совершено 44 тыс. компьютерных преступлений; в 2015 г. – 58 тыс. компьютерных преступлений; в 2016 г. – 66 тыс. компьютерных преступлений; в 2017 г. – 90 587 компьютерных преступлений; 2018 г. – 174 675 компьютерных преступлений; в 2019 г. – 294 409 компьютерных преступлений; 2020 г. (январь – сентябрь) – 363 035 компьютерных преступлений [4]. Темпы роста с 2014 г. по 2020 г. составили 825 %. В среднем темпы прироста компьютерных преступлений составили 107 %. По состоянию на сентябрь 2020 г. удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий в структуре всей преступности составил 23,6 %.

Анализ качественных характеристик киберугроз позволяет прийти к следующим выводам.

Во-первых, наблюдается качественная диверсификация хакерских атак, что выражается в появлении новых вредоносных программ, которые ориентированы не только на кражу данных, но и в случае необходимости способны уничтожить или подорвать работу всей системы. Современные вредоносные программы моделируются по принципу превентивного обезвреживания антивирусных программ и виртуальных сред для анализа вирусов. Наблюдается тенденция к распространению программ, используемых в противоправном майнинге криптовалюты. При этом среди всего разнообразия используемых методик хакерских атак программы-вымогатели и DDoS-атаки остаются главной угрозой киберпреступности в 2019 году, приносящей наибольший ущерб потерпевшим и позволяющей извлечь наибольшую прибыль [1].

Во-вторых, наблюдается криминальная специализация и функциональная дифференциация хакерских атак, что выражается в появлении новых криминальных IT-профессий (дидосеры, дропперы, фишеры, кардеры, вирусописатели, заливщики).

В-третьих, увеличиваются виктимологические риски относительно вероятных кибератак, что объясняется устареванием оборудования и слабым софтом, готовностью потерпевших платить и появлением новых технологий в структуре потребительского спроса (например, майнинг криптовалюты, облачные технологии). Кроме того, хакерская практика эволюционирует сообразно с нарождающимися социальными проблемами. Так, эксперты отмечают, что сегодня электронная почта активно используется для фишинга, связанного с эпидемией новой коронавирусной инфекции. Преступники все чаще имитируют видеоконференции, стриминговые платформы, подделывают сайты, связанные с займами и различными выплатами, а также создаются домены, имитирующие сайты ВОЗ, и площадки, где распространяются антивирусные препараты и рецептура.

В-четвертых, следует отметить увеличение различных убытков от кибератак, которые оцениваются в 500 млрд долл. США – ежегодные убытки, которые несет бизнес из-за кибератак. Интенсивное распространение кибератак и их вредоносный характер создают условия для активного инвестирования значительных средств в сферу кибербезопасности в целях обеспечения сохранности данных, предупреждения прямого взлома их систем со стороны преступников, а также непреднамеренных сбоев в цифровой инфраструктуре. Опыт таких компаний, как Sony Pictures, TalkTalk, Target и Barclays, показывает, что потеря контроля над служебной информацией предприятия и над конфиденциальными клиентскими данными приводит к значительному падению стоимости акций. Это объясняет, почему Банк Америки Мерилл Линч полагает, что рынок кибербезопасности вырастет более чем в два раза: с 75 млрд долл. США в 2015 году до 170 млрд долл. США к 2020 году, т. е. ежегодный рост отрасли в ближайшие пять лет составит более 15 % [6, с. 99].

Особое внимание также необходимо обратить на такое явление социальной действительности, как террористическая деятельность и смежный с ней экстремизм, распространяемые в информационном пространстве посредством использования сети Интернет. В современных условиях цифровой трансформации общества террористические организации и группы все больше используют возможности Интернета в целях распространения идеологии терроризма, рекрутирования новых членов преступного подполья, создания условий для коммуникаций, обучения, подготовки диверсионной деятельности и привлечения средств для финансирования терроризма [5]. Актуализируется постановка проблемы о возможной будущей трансформации традиционного терроризма (терроризма в физическом мире) в терроризм в киберпространстве, т. е. в кибертерроризм. Закономерен вопрос: может ли террористический акт быть совершен посредством использования ИКТ в случае совершения компьютерной атаки на критическую информационную инфраструктуру России? Действительно, развитие информационно-телекоммуникационных технологий способствует трансформации отдельных видов криминальных деяний (если говорить относительно объективной стороны таких преступлений), которые могут совершаться

посредством использования новых технологий в информационно-телекоммуникационном пространстве. Если российский законодатель криминализировал неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, то ничто не мешает сделать разумное допущение о возможной кибератаке на объекты критической информационной инфраструктуры, совершаемой в террористических целях.

Проблема обеспечения кибербезопасности в современных условиях также заключается в юридической неопределенности ряда ключевых понятий. Например, отсутствует единообразное определение таких понятий, как «кибербезопасность», «киберпреступность», «суверенитет в информационном пространстве», «кибератака», «кибервойна», «кибертеракт», «вмешательство во внутренние дела другого государства», «границы юрисдикции» и др.). Нельзя не отметить проблему регулирования Интернета как всемирной системы объединенных компьютерных сетей для хранения и передачи информации.

Обобщая все вышеизложенное, необходимо признать, что цифровая трансформация социальных отношений в фокусе активного использования и широкого распространения технологических новаций сопровождается новыми рисками и угрозами, которые имплицитно возникают в сетевом пространстве (киберпространстве) и выражаются в различных видах кибератак, совершаемых против информационных систем и угрожающих конфиденциальности, целостности и доступности компьютерных данных и систем, а также частным и публичным интересам.

СПИСОК ИСТОЧНИКОВ

1. Cybercrime is Becoming Bolder with Data at the Centre of the Crime Scene. – URL: https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene(дата обращения: 25.07.2021).

2. Official Annual Cybercrime Report 2019. – URL: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (дата обращения: 10.08.2021).

3. The Ultimate List OfCyber Security Statistics For 2019. – URL: https://purplesec.us/resources/cyber-security-statistics/ (дата обращения: 14.08.2021).

4. Статистика и аналитика. – URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics (дата обращения: 14.08.2021).

5. *Туронок С. Г.* Информационный терроризм: выработка стратегии противодействия // Общественные науки и современность. – 2011. – № 4. – С. 131–140.

6. *Шваб К.* Четвертая промышленная революция. – URL: http://ncrao.rsvpu.ru/sites/default/files/library/k._shvab_chetvertaya_promyshlennaya_revolyuciya_2016.pdf (дата обращения: 14.08.2021).