О. Г. Ковалев профессор кафедры организации режима и оперативно-розыскной деятельности в уголовно-исполнительной системе Псковского филиала Академии ФСИН России, доктор юридических наук, кандидат психологических наук, профессор, академик РАЕН

СОВРЕМЕННАЯ КИБЕРПРЕСТУПНОСТЬ: КРИМИНОЛОГИЧЕСКИЙ И УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ

Повсеместное внедрение научно-технического прогресса в жизнедеятельность современного человека, взрывное, скачкообразное развитие информационных технологий (IT), последующая цифровизация функционирования органов государственной власти и управления, военных, финансовых институтов, производственных и коммерческих организаций неизбежно включили граждан в киберпространство, сделав их активными участниками и пользователями различных информационных ресурсов. Современное киберопространство способно влиять не только на экономическую, но и политическую, социальную, правоохранительную, оборонную, экологическую, национальную и другие сферы функционирования государства. Все большее распространение получают криминальные кибератаки, киберпреступность, базирующиеся на применении информационных технологий в интернет-пространстве. В 2019 году, по оценкам специалистов, ущерб от кибератак, осуществленных на государственные, оборонные, финансовые, коммерческие, производственные организации и граждан, в мировом масштабе составил около 2,5 трлн долларов [1]. В Российской Федерации аналитики Сбербанка ожидают ущерб от киберпреступлений в 2020 году в размере 3,5 трлн руб., в 2021 году — 7 трлн рублей, тогда как в 2018 году он составил менее 1,3 трлн рублей [2]. Согласно статистике МВД России, за последние 5 лет отмечается взрывной рост киберпреступности. Ежегодный прирост составляет более 70 %, а по отдельным видам преступлений — в 3–5 раз. В прошедшем году зарегистрировано больше на 75 % преступлений в сфере информационных технологий. Более чем в пять раз увеличилось число преступлений, связанных с использованием данных банковских карт. Вместе с тем существенно сократилось количество квартирных краж, разбоев и грабежей (на 22,2 %, 21,3 % и 14,6 % соответственно) [3]. Таким образом, каждое пятое преступление совершается сегодня в России с применением IT-технологий. Если же учесть, что, по данным аналитиков, латентность этих преступлений достигает 80–85 %, ситуация выглядит еще более угрожающей для внутренней и внешней безопасности государства, общества и граждан. Киберпреступления совершаются на всей территории Российской Федерации. В большей степени им подвержены такие регионы, как Ямало-Ненецкий и Ханты-Мансийский автономные округа (почти треть от всех регистрируемых), Республики Чувашия и Коми, Пензенская область. Меньше всего подобных преступлений совершается в северокавказских республиках: Чечне, Дагестане и Ингушетии [4]. Актуальность проблемы предопределила проведение комплексного теоретико-эмпирического исследования криминологических и уголовно-правовых проблем киберпреступности. С этой целью была разработана специальная исследовательская программа, состоящая из 4 этапов, на которых применялись методы толкования правовых норм посредством контент-анализа нормативных правовых актов и информационных источников по проблеме, сравнительно-правовой метод, анкетирование и интервьюирование более 90 сотрудников МВД и работников органов прокуратуры Российской Федерации. Внедрение инновационных технологий в определенной мере повлияло на изменение структуры преступности, предопределило появление новых составов уголовных преступлений, развитие специфической криминальной деятельности, совершаемой в том числе организованными преступными киберсообществами. Рассматривая киберпреступность как систему однородных, умышленных, хорошо законспирированных преступных действий лица (группы лиц) с использованием IT-технологий в информационном пространстве, можно выделить основные виды преступлений в сфере компьютерной информации. Им законодатель посвятил 28 главу Уголовного кодекса Российской

Федерации (далее — УК РФ), состоящую из 4 статей (272–274.1), регламентирующих уголовную ответственность за неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-Могилевский институт МВД www.institutemvd.by 50 телекоммуникационных сетей, а также за неправомерное воздействие на критическую информационную инфраструктуру [5]. Проведенное анкетирование сотрудников органов внутренних дел показало, что, кроме вышеперечисленных статей УК РФ, они также активно используют в своей профессиональной деятельности такой состав, как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). При этом свыше 90 % составляют случаи интернет-мошенничества с использованием персональных данных пользователей, а также их электронных кошельков, почты, банковских карт, карт лояльности и т. д. Другой статьей УК РФ, по которой опрошенные сотрудники ОВД квалифицируют действия киберпреступников, является кража, в результате которой происходит умышленное, тайное похищение и последующее незаконное использование ими финансовых и корпоративных данных, банковских карт и других носителей персональной информации. В противодействии киберпреступности активно применяются также ст. 137, 138, 183, 242.1 и 282 Уголовного кодекса Российской Федерации. К числу основных тенденций современной компьютерной преступности в России, выявленных в ходе проведения исследования, можно отнести: – существенный, прогрессирующий рост числа киберпреступлений на фоне стабилизации и некоторого снижения других уголовных деяний; – заметное увеличение доли финансовых мошенничеств с элементами социальной инженерии в общей структуре компьютерных преступлений; – значительное возрастание размера экономического ущерба от киберпреступности, исчисляемого в масштабах государства триллионами рублей; – повышение криминальной активности киберпреступников в условиях пандемии COVID-19, вызванное увеличением нагрузки на компьютерные сети, переводом сотрудников на удаленный режим работы, открывающий преступникам дополнительный доступ к серверам и сетевому обеспечению компаний и корпораций; многократное увеличение онлайн-торговли, торговых сделок, деловой переписки и т. д.; – увеличение количества сделок на электронных торговых площадках по продаже запрещенных к легальному обороту веществ и товаров (наркотиков, оружия), радиоэлектронных и специальных технических средств, ценных бумаг и др.; – использование преступными киберсообществами новых технологий в криминальной деятельности (замена кибератак на финансовые учреждения, промышленные предприятия, медицинские учреждения созданием специальных программ-шифровальщиков); дальнейшее активное использование киберпреступниками вредоносных компьютерных вирусов, заражение ими корпоративных интернет-сетей компаний и организаций, взлом их информресурсов; – объединение организованных преступных группировок для проведения кибератак на крупные нефтегазовые компании, финансовые учреждения, медицинские и туристические организации; – активный поиск преступными киберсообществами новых членов, имеющих необходимые навыки и подготовку для проведения криминальных акций в киберпространстве; – более широкое использование преступными сообществами так называемых кротов — сотрудников организаций, предприятий и корпораций, предавших интересы службы, осуществляющих незаконные действия в интересах киберпреступников. Основными субъектами противодействия киберпреступности в России в настоящее время являются Генеральная прокуратура, Министерство внутренних дел, Следственный комитет, Федеральная служба безопасности, Министерство обороны, Федеральная служба охраны Российской Федерации. Также в последнее время активно противодействует функционированию так называемых колл-центров в местах лишения свободы и Федеральная служба исполнения наказаний Российской Федерации. Проведенное исследование показало, что

в комплексном изучении нуждаются не только криминологические и уголовно-правовые проблемы современной киберпреступности, но и организационные, с привлечением ученых в области социальной инженерии, информатизации и программирования.

Список основных источников

1. Дмитрий Медведев выступил на пленарной сессии международного конгресса по кибербезопасности. 21.06.2019 [Электронный ресурс]. — Режим доступа: http://government.ru/news/37124/. — Дата доступа: 07.01.2021. Перейти к источнику Вернуться к статье 2. Сбербанк подсчитал потери роста экономики в 2021 году от киберпреступности. 18.06.2020 [Электронный ресурс]. — Режим доступа: https://tass.ru/ekonomika/ 8761953. — Дата доступа: 07.01.2021. Перейти к источнику Вернуться к статье 3. В МВД заявили о росте числа преступлений с помощью IT-технологий на 75 %. 20.11.2020 [Электронный ресурс]. — Режим доступа: https://iz.ru/1090109/2020-11-20/v-mvd-zaiavili-o-roste-chisla-prestuplenii-s-pomoshchiuit-tekhnologii-na-75. — Дата доступа: 06.01.2021. Перейти к источнику Вернуться к статьеМогилевский институт МВД www.institutemvd.by 52 4. В МВД назвали регионы с самым высоким уровнем киберпреступности. 10.02.2020 [Электронный ресурс]. — Режим доступа: https://life.ru/p/1306813. — Дата доступа: 06.01.2021. Перейти к источнику Вернуться к статье 5. Уголовный кодекс Российской Федерации [Электронный ресурс] : 13 июня 1996 г., № 63-ФЗ : принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г. : в ред. от 30.12.2020 г. — КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2021.