ПРАВОВЫЕ АСПЕКТЫ СОВРЕМЕННОЙ КИБЕРБЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Карцхия А.А.[1], Макаренко Г.И.[2]

Аннотация

Целью исследования *является рассмотрение правовых аспектов и актуальных вопросов кибербезопасности и особенностей киберпреступности в сфере информационно-коммуникационных технологий в российском и зарубежном праве.*

Методы исследования *заключаются в сравнительно-правовом анализе действующего российского и зарубежного законодательства и практики его применения, а также формально-логическом исследовании понятийного аппарата, содержания и структуры предмета исследования.*

Результаты исследования *позволяют авторам сформулировать оригинальное понимание правового содержания киберпреступности, которое охватывает не только правонарушения, совершенные с использованием компьютерной техники, но и иного информационно-коммуникационного оборудования и средств, включая компьютерные программные средства. Стремительное распространение киберпреступности, появление новых форм организованной преступности, использующей глобальную сеть Интернет, спланированные и хорошо организованные кибератаки на критическую инфраструктуру государства и частных компаний свидетельствует о формировании особого направления преступности – преступность в сфере кибербезопасности и информационных технологий, которая выходит за рамки традиционного понимания преступности в сфере информационных технологий и средств связи. Авторы пришли к выводу о необходимости концептуального оформления теоретических и методологических начал, разработки основ правопорядка в сфере кибербезопасности, уточнение понятийного аппарата и специфики регулирования как в сфере публично-правового, так и частно-правового регулирования сферы кибербезопасности, а также формирования нового направления криминологии в сфере киберпреступности (киберкриминологии) как социального феномена, во многом порожденного цифровизацией и информатизацией общества.*

Научная новизна *исследования заключается в обосновании концептуальной оценки противодействия киберпреступности как элемента национальной кибербезопасности, а также обоснованию специального направления криминологии – киберкриминологии.*

Ключевые слова: *защита информации, безопасность в киберпространстве, кибератаки, киберкриминология, киберправо, киберпреступность, информационное право, цифровое право, персональные данные, частное право, кибербезопасность.*

DOI:10.21681/2311-3456-2023-1-58-74

Введение

Законодательство в сфере кибербезопасности продолжает совершенствоваться по всему миру в ответ на стремительно развивающиеся новые угрозы в киберпространстве и возрастающие размеры ущерба, причиняемого в результате инцидентов с применением новых цифровых технологий, а также активизации деятельности государственных регуляторов и правоохранительных органов по защите интересов государства и общества, потребителей, инвесторов и компаний в этой сфере. Экспоненциальный рост Интернета вещей, облачных технологий, других многочисленных революционных инноваций и цифровых технологий создают виртуальную действительность в формате информационных пулов, целых виртуальных миров, порождающих новые риски и новые угрозы. Растущая зависимость и уязвимость человечества от технологий, их постоянное развитие значительно увеличили нашу подверженность киберугрозам, которая

1 Карцхия Александр Амиранович, доктор юридических наук, и.о. заведующего кафедры правового обеспечения безопасности ТЭК РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва, Россия. E-mail: arhz50@mail.ru

2 Макаренко Григорий Иванович, старший научный сотрудник НЦПИ при Минюсте РФ, Москва, Россия. E-mxail: t7920518@yandex.com

только расширяется, а число и скорость кибератак только увеличивается [5,6].

Преступность в киберпространстве, как отмечалось в докладе ООН[3], является одной из самых сложных проблем, с которыми международное сообщество сталкивается в последние годы в связи с развитием информационных и коммуникационных технологий.

Многие страны предприняли общегосударственные меры реагирования на риски кибербезопасности, устанавливая жесткую уголовную ответственность, а также стратегии кибербезопасности и меры расследования, как в национальном праве, так и на международном уровне. Стратегии кибербезопасности представляют собой документы, определяющие государственную политику, направленную на обеспечение безопасности государства в киберпространстве. Такие национальные стратегии приняты в многих государствах, включая Россию, США, КНР, Японию, Великобританию. Стратегии альянсов государств приняты в ЕС и НАТО (хотя у блока НАТО нет официальной стратегии кибербезопасности, но фактически им является «Таллинское руководство по международному праву, применимому к кибервойне»). Существуют отраслевые стратегии, например, Стратегия гражданской ядерной безопасности Великобритании. Имеются стратегии по видам вооружений или сферам деятельности - стратегии развития искусственного интеллекта (США, Россия, КНР), стратегии информационной безопасности (Россия). Создаются стратегии конкретных мероприятий, например: стратегия кибербезопасности Олимпийских игр 2012 в Лондоне или в Стратегии кибербезопасности Японии сформирована отдельная глава, посвящённая безопасности Олимпийских игр 2020.

Единообразного понятия кибербезопасности пока не принято. В стратегических документах России, уголовном и административном законодательстве применяется термин «информационная безопасность» как более широкое понятие, включающее также и кибербезопасность.

Кибербезопасноть включает, как отмечают аналитики, следующие элементы:

— *физическая безопасность* — защита от физических угроз, которые могут влиять на состояние киберсистемы, т.е. физический доступ к серверам, внедрение вредоносного ПО в сеть или принуждение к этому пользователей
— *национальная безопасность* — защита от угроз в киберпространстве, которые могут угрожать физическим активам и кибератывам таким образом, что злоумышленник может получить политическую, военную или стратегическую выгоду, т.е. атаки на системы связи или другую промышленную инфраструктуру;
— *безопасность коммуникаций* — защита от угроз воздействия на техническую инфраструктуру киберсистем, которое может привести к изменению конфигураций для выполнения действий, не предусмотренных её владельцами, разработчиками или пользователями;
— *безопасность операций* — защита от преднамеренного искажения рабочих процессов, которые могут привести к результатам, не предусмотренным владельцами, разработчиками или пользователями;
— *информационная безопасность* — защита от угрозы кражи, удаления или изменения хранящихся и передаваемых данных в киберсистеме. В этом смысле кибербезопасность (безопасность киберпространства) может быть определена как сохранение конфиденциальности, целостности и доступности информации в киберпространстве.

При этом киберпространство представляет собой сложную среду, формирующуюся в результате взаимодействия людей, программного обеспечения и услуг в сети Интернет с помощью технологических устройств и подключённых к нему сетей, не существующих в какой-либо физической форме[4].

Киберпреступность носит трансграничный характер, а Интернет все чаще становится сферой террористических и экстремистских деяний, вовлечения и вербовки молодежи в преступную деятельность, областью целенаправленных кибератак на государственные и коммерческие структуры в преступных целях, включая посягательства на критически важную инфраструктуру, а также дестабилизацию международной информационной безопасности. Современная действительность доказывает, что киберпреступность при определенных условиях переформатируется в информационную войну.

[5], что в борьбе с киберпреступностью нельзя ограничиваться сферой компьютерных преступлений,

3 Доклад о работе двенадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию, 2010. С.68-71. https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053830r.pdf

4 Стратегии кибербезопасности: аналитический отчет. Центр InfoWatch, 2022. URL: infowatch.ru/analytics

5 Борьба с информационной преступностью: международно-правовые инструменты// Ведомости, от 29.06.2022, https://www.vedomosti.ru/press_releases/2022/06/29/borba-s-informatsionnoi-prestupnostyu-mezhdunarodno-pravovie-instrumenti

Рис.1. Цели кибератак в России в 2022г. (по данным Positive Technologies)

которые составляю 1,5% от всех преступлений, совершаемых с помощью информационно-коммуникационных технологий в России. Сфера киберпреступлений предполагает использование всех доступных информационно-коммуникационных технологий в преступных целях, включая не только компьютеры, но и современные телефоны, факсы, спутниковую связь и другие IT технологии.

Как указывает Международная организация уголовной полиции (Интерпол), появляются и новые виды киберпреступлений. В частности, криптоджекинг (*cryptojacking*), при котором преступник тайно использует вычислительную мощность жертвы для создания криптовалюты, когда жертва непреднамеренно устанавливает программу с вредоносными скриптами, позволяющими киберпреступнику получить доступ к компьютеру или другому устройству, подключенному к Интернету, (например, нажав на неизвестную ссылку в электронном письме или посетив зараженный веб-сайт). Затем преступники используют программы для создания («майнинга») криптовалют[6]. Создаются и новые способы совершения преступлений по схеме «преступление как услуга» («*crime as a service*»), которые предлагаются в даркнете как сервисы по организации «коммерческих» DDoS-атак, аренде бот-сетей, продаже или аренде программных кодов вредоносного ПО для мошенничества. Интерпол также отмечает, что террористы и экстремистские группы используют Интернет и платформы социальных сетей для общения и координации своей деятельности, привлечения новых участников, продвижения своего присутствия с помощью фотографий и видео или сбора средств. Также существует реальная опасность того, что боевики-террористы будут использовать приобретенный на полях сражений и в зонах конфликтов тактический опыт, чтобы использовать уязвимости в новых технологиях для планирования и/или осуществления террористических атак. Платформы социальных сетей могут использоваться для определения целей, планирования и проведения атак, а также для распространения руководств по изготовлению бомб и распространению химического и биологического оружия [7].

Актуальность противодействия киберпреступности во всех ее формах, включая предупреждение, выявление и расследование такого рода преступлений и судебного преследования по делам о них неоднократно подчеркивалось ООН, выражавшей обеспокоенность тенденцией роста киберпреступности и преступного использования информационно-коммуникационных технологий для совершения различных преступлений[8].

В специальном докладе о глобальных трендах преступности (2022 INTERPOL Global Crime Trend Report) Интерпол на основе проведенного исследования академических институтов и аналитических центров и IT-компаний по безопасности информационных технологий выделил пять областей преступности, которые доминируют в глобальном ландшафте угроз преступности, включая: организованную преступность, незаконный оборот (в т.ч. незаконный оборот наркотиков, торговлю людьми и незаконный ввоз мигрантов), фи-

6 https://www.interpol.int/Crimes/Cybercrime/Cryptojacking

7 https://www.interpol.int/Crimes/Terrorism/Counter-terrorism-projects/Project-CT-Tech

8 Резолюция, принятая Генеральной Ассамблеей 23 ноября 2020 года (A/RES/75/10) «Сотрудничество между Организацией Объединенных Наций и Международной организацией уголовной полиции (Интерпол)».

нансовую преступность (в т.ч. отмывание денег, финансовое мошенничество и коррупцию), киберпреступность (в т.ч., программы-вымогатели, фишинг и онлайн-мошенничество) и терроризм. Особая группа составляют преступления против детей (сексуальная эксплуатация и надругательство в сети[9]

В рамках масштабной операции HAECHI III (июнь-ноябрь 2022г.)[10] с участием многих государств мира Интерпол изъял деньги и виртуальные активы на сумму более $130 млн., полученных в результате киберпреступлений и операциями по отмыванию денег. В этой связи особую значимость приобретает международное сотрудничество по линии Интерпола[11].

Современную киберпреступность отличает особая организация кибератак (DDOS-атак) высокой интенсивности и длительности. Как отмечает ряд экспертов[12], кибератаки носят не только избирательный или сезонный характер, но организованные хакерами бот-сети атакуют даже те организации, которые ограничили у себя использование международного трафика и закрылись от международных ботнетов и злоумышленники используют нестандартные способы DDoS-атак с территории РФ (например, за счет заражения видеоплеера на популярном видеохостинге хакеры включили в свой ботнет устройства ничего не подозревающих российских зрителей). Особыми целями кибератак стали корпоративные сети и иные частные объекты. К примеру, созданная инфраструктура ИТ-армии Украины в период СВО использовалась не только для DDoS каналов связи, но и для массовых атак уровня веб-приложений. При этом, целями становятся не только адреса конкретной организации, но и все российские IP-адреса, а на текущий момент в российском интернете содержится несколько десятков тысяч уязвимых корпоративных ресурсов и забытых веб-консолей, опубликованных на ИТ-периметрах госструктур и коммерческих компаний, которые в дополнении ко всему еще и давно устарели. Наряду с использованием уязвимостей программных продуктов, современные хакеры применяют дезинформацию или фейковые новости, которые активно внедряют под видом новостной информации, рекламы или аналитических материалов. Причем, если такого рода данные раньше представлялись только за плату, то сейчас значительно больший объем материала размещается бесплатно. Вместе с тем, при хакерских атаках на компании широко продолжают использоваться и традиционные мошеннические схемы и все доступные инструменты: целевой фишинг, DDoS, различное вредоносное ПО. В корыстных целях принуждения жертвы заплатить, злоумышленники стремятся нанести максимальный ущерб: остановить операционные процессы, навредить репутации, сделать восстановление практически невозможным. Киберпреступность приобрела и особо опасные формы – направленность кибератак в интересах политических оппонентов нацеленных на дестабилизацию, разрушение инфраструктуры или максимальную компрометацию критических данных организации с использование известных уязвимостей и фишинговых рассылок с вредоносным ПО. Сохранились группировки, практикующие классический кибершпионаж, которым в текущих реалиях непрерывного вала кибератак стало проще скрываться от команд безопасности.

Как отмечается, например, в Докладе[13] Европола о киберпреступности 2021г. операторы мобильных вредоносных программ и мошенники по-прежнему представляют ключевую угрозу, пользуясь возросшей зависимостью от сервисов онлайн-покупок и мобильного банкинга; дети, проводящие больше времени в Интернете, становятся легкой добычей преступников, резко увеличился «онлайн-уход несовершеннолетних» в сети; многие угрозы в сфере киберпреступности усугубляются растущим рынком сервисов «преступление как услуга» в Dark Web («Вредоносное ПО как услуга» (MaaS) для кражи персональных данных и личной информации для последующего шантажа и вымогательства; киберпреступники более продуманно выбирают цели, операции программ-вымогателей все более сосредотачиваются на дорогостоящих атаках на крупные компании (отмечались масштабные атаки Microsoft Exchange Server, SolarWinds, Kaseya и др.); отмечается рост онлайн-криминальных рынков и мошенничества при обмене и платежей криптовалют, а также распространения материалов о сексуальном насилии над детьми (CSAM), активно продаваемых в одноранговых сетях (P2P) и в Dark Net; преступники повышают свою операционную безопасность, ис-

9 INTERPOL Global Crime Trend Report 2022. URL: https://www.interpol.int/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report

10 https://www.interpol.int/News-and-Events/News/2022/Cyber-enabled-financial-crime-USD-130-million-intercepted-in-global-INTERPOL- police-operation.

11 Internet Organized Crime Threat Assessment (IOCTA) Report, 2021.URL: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

12 Lidery rynka kiberbezopasnosti ob"edinilis' na fone vozrosshih ugroz. Cyber Media, 16.11.2022. URL: https://securitymedia.org/news/lidery-rynka-kiberbezopasnosti-obedinilis-na-fone-vozrosshikh-ugroz.html

13 Internet Organized Crime Threat Assessment (IOCTA) Report, 2021.URL: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

пользуя сквозное шифрование и криптовалюты, предпочитают размещать свои сервисы в странах, где международное сотрудничество судебных органов в правоохранительной сфере является более сложным.

Европол делает вывод о том, что цифровизация затрагивает все формы преступности, а используемые киберпреступниками методы и инструменты, все чаще применяются в других областях преступности, и цифровая криминальная экосистема продолжает развиваться тревожными темпами. Конфиденциальность и удобство, предлагаемые коммуникационными, распределительными и криптовалютными платформами, выгодны при любой противоправной деятельности. Анонимность в Интернете усугубляется широкомасштабным внедрением технологий шифрования, которые могут принести пользу как законным пользователям, так и преступникам одновременно, создавая парадоксальную ситуацию для политиков. Пристальное внимание правоохранительных органов направлено также на VPN и криптотелефонных провайдеров, которые обслуживают преступные элементы общества. Для борьбы с растущими угрозами сотрудники правоохранительных органов должны иметь возможность своевременно получать доступ к данным и проводить законную работу под прикрытием, чтобы обеспечить безопасность общества. Компаниям необходимо совершенствовать методы по принципу “Знай своего клиента” (KYC) и раскрытия информации. Наконец, жизненно важно продолжать повышать коллективную грамотность и осведомленность граждан в области информационных технологий (IT), поскольку киберпреступность прочно укоренилась в обществе.

В этой связи следует отметить, что вопросы обеспечения безопасности в киберпространстве на международном уровне рассматривались уже в Международной конвенции о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 1981, ратифицирована РФ в 2005 г.) и Европейской конвенции о порядке использования персональных данных полицией (2001, РФ не ратифицировала). Эти международные конвенции направлены на повышение эффективности мер, принимаемых международным сообществом в сфере обеспечения информационной безопасности, противодействию преступлениям против целостности, конфиденциальности, доступности компьютерных систем и данных. Однако, Российская Федерация не ратифицировала Европейскую конвенцию в силу того, что предусматривалась возможность доступа и получения следственными органами через компьютерную систему к хранящимся на территории другой стороны компьютерным данным. Европейская Конвенция о преступности в сфере компьютерной информации (ETS N 185) (Будапешт, 2001 с изм. Протокол от 28.01.2003)[14] Россией не ратифицирована, поскольку Конвенция не в полной мере отвечает реально существующим угрозам и рискам [7]. Эта Конвенция признает преступлениями противозаконный доступ к компьютерной системе и неправомерный перехват компьютерных данных, неправомерное воздействие на компьютерные системы и противозаконное использование компьютерных устройств и данных, подлог и мошенничество с использованием компьютерных технологий, а также регламентирует международное сотрудничество стран-участниц в сфере противодействия киберпреступности.

Серьезность значения киберпреступности непосредственно связана, в том числе, с проблемой защиты прав человека в эпоху цифровых технологий, которая стала одной из злободневных тем в правозащитной деятельности. Ввиду трансграничного характера Интернета, его способности влиять на различные области права сформировалась потребность в принятии международно-ориентированного подхода для оценки влияния новых технологий, таких как алгоритмы и интеллектуальные искусственные системы, на гражданские, политические и социальные права людей не только в цифровом, но и в физическом мире. Поскольку появление Интернета ставит под сомнение устоявшиеся правовые категории, необходимы серьезные исследования этого явления с точки зрения мировых перспектив развития [9].

В последние два десятилетия, как отмечают зарубежные исследователи [10], кибербезопасность стала неотъемлемым компонентом международных отношений, хотя в данной сфере до сих пор не созданы надлежащие механизмы международного регулирования ввиду неопределенности масштаба, природы, сущности и понятийного аппарата кибербезопасности. Также не существует универсального подхода к определению кибербезопасности, а эксперты используют этот термин по-разному, в зависимости от контекста. Само понятие «кибербезопасность» sensu stricto, включает такие вызовы безопасности, как киберпреступность, кибертерроризм и использование кибертехнологий в военных целях.

Учитывая общемировые тенденции в сфере кибербезопасности, в июне 2021 года Российская

14 https://rm.coe.int/1680081580

Таблица 1

Последствия кибератак (доля в %) (по данным Positive Technologies)

Для организаций	Для физических лиц
Утечка конфиденциальной информации - 45%	Утечка конфиденциальной информации - 55%
Нарушение основной деятельности – 30%	Нарушение основной деятельности – 1%
Ущерб интересам государства – 9%	Ущерб интересам государства – 2%
Прямые финансовые потери - 7%	Прямые финансовые потери - 25%
Использование ресурсов организации для атак 7%	Использование ресурсов лица для атак 7%
Другое 2%	Другое 10 %

Федерация внесла в Спецкомитет ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях российский проект первого в истории универсального договора по борьбе с киберпреступностью, который учитывает современные вызовы и угрозы в сфере международной информационной безопасности, включая использование криптовалюты, вводит новые составы преступлений, совершаемых с использованием ИКТ (распространение фальсифицированной медицинской продукции, оборот наркотиков, вовлечение несовершеннолетних в совершение противоправных деяний, опасных для их жизни и здоровья, и др.), а также расширяет сферу международного сотрудничества в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов. В ноябре 2022 года Первый Комитет Генеральной Ассамблеи ООН утвердил решение о принятии российского проекта резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», который закрепляет конструктивные итоги первого года деятельности Рабочей группы открытого состава (РГОС) ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025 и нацеливает государства на продолжение конструктивных переговоров во исполнение ее мандата[15].

Обратной стороной активного технологического развития и цифровизации бизнес-процессов, глобального роста объема обрабатываемых финансовыми организациями данных пользователей финансовых услуг, как отмечается в Стратегии развития финансового рынка РФ до 2030 года[16], является рост киберпреступности и кибермошенничества, что порождает встречный тренд в виде развития технологий борьбы с такого рода преступлениями и соответствующих изменений в законодательстве Российской Федерации и правоприменении.

2. Право кибербезопасности и аспекты киберпреступности в РФ

Киберпреступность (преступность в сфере высоких технологий) в настоящее время является одной из наиболее серьезных угроз национальной безопасности Российской Федерации в информационной сфере. В связи с этим развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия, обеспечение информационной безопасности, в том числе в целях установления международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий, а также совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий определено одним из важнейших направлений национальной безопасности РФ в соответствии со Стратегии национальной безопасности Российской Федерации[17].

Эксперты отмечают [13, 14] особые характеристики киберпреступности: высокая латентность, специальная подготовка преступников, трансграничность, автоматизированность преступлений, нетрадиционность средств противодействия киберпреступности. Наиболее значимые негативные последствия кибератак в России в 2022 году приведены в Табл. 1.

Российское законодательство и судебная практика определили новые группы преступлений, связанных с использованием современных компьютерных техно-

15 https://mid.ru/ru/foreign_policy/un/1837378/

16 Распоряжение Правительства РФ от 29.12.2022 N 4355-р «Об утверждении Стратегии развития финансового рынка РФ до 2030 года».

17 Указ Президента РФ от 02.07.2021 N400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ, 05.07.2021, N 27 (часть II), ст. 5351

логий, которые формируют особую группу преступлений – преступления в сфере компьютерной информации. К этой категории относятся преступления, квалифицированные в УК РФ как: неправомерный доступ к компьютерной информации (ст.272 УК); создание, использование и распространение вредоносных компьютерных программ (ст.273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ); а также нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст.274.2 УК РФ), введенный в июле 2022 года.

Самостоятельным преступлением являются неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст.272 УК РФ). Следует иметь в виду, что понятие доступа к информации содержится в п. 6 статьи 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: доступ к информации – возможность получения информации и ее использования. В УК РФ, тем не менее, этой ссылки не имеется. Однако, под охраняемой законом, как предусмотрено в Методических рекомендациях Прокуратуры РФ[18], понимается информация, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.). Неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты. Другими словами, неправомерный доступ к компьютерной информации - это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее).

Важное значение для правоприменительной практики имеет новое постановление Пленума Верховного Суда РФ от 15.12.2022 г. №37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационной-телекоммуникационных сетей, включая сеть «Интернет» (далее - Постановление), принятое для обеспечения единообразного применения законодательства об уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные статьями 272, 273, 274 и 274.1 Уголовного кодекса Российской Федерации, а также за иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». В п.2 Постановления разъясняется, что под «компьютерной информацией, указанной в ст.272 УК РФ понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах (далее – компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе жестких дисках – накопителях, флеш-картах и т.п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи. При этом к числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом».

18 Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» (утверждены Генпрокуратурой России. Источник: http://genproc.gov.ru по состоянию на 15.04.2014.

Кроме того, в качестве охраняемой законом компьютерной информации (п.1 ст.272 УК РФ) рассматривается как информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности.

Постановление содержит ряд ключевых для применения главы 28 УК РФ определений, включая следующие:

- *компьютерной программой* с учетом положений статьи 1261 Гражданского кодекса Российской Федерации, является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения;
- *уничтожением компьютерной информации* понимается приведение такой информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена;
- *блокированием компьютерной информации* является воздействие на саму информацию, средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме (искусственное затруднение или ограничение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением);
- *модификация компьютерной информации* представляет собой внесение в нее любых изменений, включая изменение ее свойств, например целостности или достоверности;
- *копированием компьютерной информации* понимается перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме (в том числе отправка по электронной почте, распечатывание на принтере, фотографирование, переписывание от руки и т.п.);
- *нейтрализацией средств защиты компьютерной информации* является воздействие, в частности, на технические, криптографические и другие средства, предназначенные для защиты компьютерной информации от несанкционированного доступа к ней, а также воздействие на средства контроля эффективности защиты информации (технические средства и программы, предназначенные для проверки средств защиты компьютерной информации, например, осуществляющие мониторинг работы антивирусных программ) с целью утраты ими функций по защите компьютерной информации или контролю эффективности такой защиты.

В качестве широко используемых вредоносных программ наиболее часто используются шифровальщики и вредоносные инструменты для удаления управления или данных, либо проведения DDoS-атак. В табл. 2 приведены данные.

Применительно к статье 272 УК РФ, как указано в п.5 Постановления, неправомерным доступом к

Таблица 2

Типы вредоносного ПО (Россия, 1 кв.2022г.) (доли в % от общего числа)

Организации	**Физические лица**
Шифровальщики – 44%	Шифровальщики – 2%
ВПО для удаленного управления – 31%	ВПО для удаленного управления – 13%
Загрузчик – 22%	Загрузчик – 10%
Шпионское ПО – 18%	Шпионское ПО – 38%
ПО, удаляющее данные – 3%	ПО, удаляющее данные – 2%
Банковский Троян – 2%	Банковский Троян – 32%
Майнер – 2%	Майнер – 2%
Другие – 2%	Другие – 10%

компьютерной информации является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа).

Важно также, что преступления, предусмотренные статьями 272 и 274 УК РФ, признаются оконченными, когда указанные соответственно в части 1 статьи 272 УК РФ или в части 1 статьи 274 УК РФ деяния повлекли наступление общественно опасных последствий (одного или нескольких) в виде уничтожения, блокирования, модификации либо копирования такой информации, а по статье 274 УК РФ также в виде причинения крупного ущерба (п.6 Постановления). Если лицо, намереваясь осуществить уничтожение, блокирование, модификацию или копирование охраняемой законом компьютерной информации, выполнило все действия, необходимые для неправомерного доступа к компьютерной информации, либо осуществило такой доступ, однако ни одно из последствий, предусмотренных частью 1 статьи 272 УК РФ, не наступило по независящим от него обстоятельствам (например, в результате срабатывания автоматизированных средств защиты информации или действий лиц, осуществляющих ее защиту), такие действия следует квалифицировать как покушение на совершение данного преступления.

В соответствии с п.7 Постановления к иной компьютерной информации (ст.273 УК РФ), заведомо предназначенной для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, могут быть отнесены любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить достижение целей, перечисленных в части 1 статьи 273 УК РФ, например ключи доступа, позволяющие нейтрализовать защиту компьютерной информации, элементы кодов компьютерных программ, способных скрытно уничтожать и копировать информацию.

Уголовную ответственность по ст.273 УК РФ влекут действия по созданию, распространению или использованию только вредоносных компьютерных программ либо иной компьютерной информации, то есть заведомо для лица, совершающего указанные действия, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Создание вредоносных компьютерных программ или иной вредоносной компьютерной информации представляет собой деятельность, направленную на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютерной информации, предназначенных для несанкционированного доступа, то есть совершаемого без согласия обладателя информации, лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты (п.9 постановления).

Распространение вредоносных компьютерных программ или иной вредоносной компьютерной информации состоит в предоставлении доступа к ним конкретным лицам или неопределенному кругу лиц любым способом, включая продажу, рассылку, передачу копии на электронном носителе либо с использованием сети «Интернет», размещение на серверах, предназначенных для удаленного обмена файлами (п.11 Постановления).

При квалификации действий лица по незаконному воздействию на критическую информационную инфраструктуры (ст. 274.1 УК РФ) предполагается нарушении установленных федеральными законами и подзаконными нормативными правовыми актами правил, а также инструкций или иных локальных нормативных актов организаций, если они приняты в развитие указанных законов и подзаконных актов, не противоречат им и не изменяют их содержание. Обязанность соблюдения правил, установленных локальным нормативным актом, должна быть доведена до сведения лица, которому вменяется совершение соответствующего преступления (например, при подписании трудового договора, соглашения на использование сетей или оборудования либо отдельного акта ознакомления с такими правилами). Действия лиц квалифицируются по части 1 статьи 274.1 УК РФ, если установлено, что компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, определение понятия которой содержится в статье 2 Федерального закона от 26 июля 2017 года N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В ином слу-

чае действия лица при наличии на то оснований могут быть квалифицированы по статье 273 УК РФ (п.13 Постановления).

В сфере противодействия киберпреступности особое значение имею Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также международные акты по вопросам борьбы с преступлениями в сфере компьютерных технологий. В частности, Соглашение стран СНГ от 2001г. о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, которое рекомендовало странам-участницам признавать уголовно наказуемыми следующие деяния, если они совершены умышленно: 1) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; 2) создание, использование или распространение вредоносных программ; 3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия; 4) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб [19].

Уточнение и унификация понятий в сфере кибербезопасности служит необходимой основой для повышения эффективность правоприменения и защиты законных государственных, общественных и частных интересов в киберпространстве.

Понятия критической информационной инфраструктуры, которое содержится в ст.2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», могут служить объектом преступного посягательства при квалификации действий лиц по ч. 1 ст. 274.1 УК РФ, когда компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, в том числе в случае, когда осуществляется распространение этих программ на объекты критической информационной инфраструктуры исключительно для их последующего использования.

Самостоятельным составом преступления является мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), определяемое как хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. При этом Пленум Верховного Суда РФ от 30.11.2017 № 48[20] (в ред. от 29.06.2021) указал, что под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Вместе с тем, если хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т.п.), подлежит квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, происшедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием.

19 URL: http://www.cis.minsk.by/page.php?id=866

20 Пункт 20 Постановления Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 29.06.2021)»О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ, N 2, февраль, 2018.

Если же хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет» (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159, а не ст. 159.6 УК РФ.

В соответствии с Кодексом об административных правонарушениях РФ установлена ответственность за административные правонарушения в области связи и информации (гл.13 КоАП РФ), которые предусматривают административную ответственность, и в том числе, за нарушение правил защиты информации (ст. 13.12 КоАП РФ), нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (ст. 13.12.1 КоАП РФ), злоупотребление свободой массовой информации (ст.13.15. КоАП РФ), нарушение порядка ограничения доступа к информации, информационным ресурсам, доступ к которым подлежит ограничению в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, и (или) порядка удаления указанной информации (13.41 КоАП РФ), Нарушение требований законодательства к установке технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования либо технических средств контроля за соблюдением операторами связи, собственниками или иными владельцами технологических сетей связи требований законодательства, предусматривающих ограничение доступа к информации (ст. 13.42 КоАП РФ) и др.

Особое регулирование осуществляется в сфере оборота персональных данных – Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

3. Зарубежное законодательство в сфере кибербезопасности

В зарубежных юрисдикциях проблемы борьбы с компьютерными преступлениями также являются очень актуальными. В частности, **Европейский союз** уделяет большое внимание принятию единых правил для обеспечения достаточной кибербезопасности, основные из которых содержаться в Директиве о конфиденциальности (ред.2009 г.), Директива NIS (2016), Закон о кибербезопасности (2019) и Директива об атаках на информационные системы (2013). Директивы не применяются непосредственно в государствах – членах ЕС, но требуют обязательного преобразования в национальное законодательство этих стран. В последние годы законодательство ЕС в сфере кибербезопасности нуждается в кардинальном обновлении из-за растущего уровня цифровизации и взаимосвязанности европейского общества, из-за растущего количество злонамеренных действий, совершаемых в киберпространстве на общеевропейском и глобальном уровнях. В дополнение к нормативным актам, которые непосредственно касаются кибербезопасности, существуют также связанные нормативные акты, например, Общие правила защиты данных в ЕС (GDPR), содержащие набор мер безопасности, которые должны быть приняты компаниями при обработке персональных данных.

Принятая в декабре 2020 года Стратегия кибербезопасности ЕС предусматривает создание сети операционных центров безопасности в странах ЕС для отслеживания и предупреждения атак на сети, создание совместного подразделения по кибербезопасности, развитие технологии 5G в ЕС, обеспечение безопасности сетей 5G и развитие будущих поколений сетей, ускорение внедрения ключевых стандартов безопасности в Интернете, развитие надежного шифрования, повышение эффективности и действенности «кибердипломатии» с особым вниманием на предотвращение и противодействие кибератакам на критическую инфраструктуру, создание рабочей группы по киберразведке для усиления потенциала EU INTCEN (разведывательный и ситуационный центр ЕС), укрепление сотрудничества с международными организациями и странами-партнерами для продвижения общего понимания ландшафта киберугроз, разработка программы наращивания внешнего киберпотенциала ЕС для повышения киберустойчивости и возможностей во всём мире [11,12].

В марте 2022года ЕС объявил о разработке стратегии по кибербезопасности и космосу в рамках реализации оборонной программы «Стратегический компас»[21]. ЕС намерен разработать кибердипломати-

21 Борьба с информационной преступностью: международно-правовые инструменты// Ведомости, от 29.06.2022, https://www.vedomosti.ru/press_releases/2022/06/29/borba-s-informatsionnoi-prestupnostyu-mezhdunarodno-pravovie-instrumenti

ческий инструментарий [2, 15], разработать стратегию ЕС по киберзащите, чтобы лучше подготовиться к кибератакам… Разработать стратегию Евросоюза по обороне и безопасности в космосе». А в ноябре 2022 года Еврокомиссия представила проект новой стратегию кибербезопасности и план упрощения военных перевозок по всем странам Евросоюза.

15 сентября 2022 г. Европейская комиссия опубликовала проект предложения по Закону о киберустойчивости (Cyber Resilience Act –CRA). Законопроект является одним из нескольких законов и инициатив ЕС в области кибербезопасности, которые в настоящее время обсуждаются и дорабатываются в рамках более широких усилий по формированию цифровой стратегии ЕС. Это, в частности, включает в себя более широкие требования к управлению кибербезопасностью, предложенные в соответствии с Директивой ЕС «Правила Евросоюза по безопасности сетевых и информационных систем» (NIS 2), которая предназначена для применения в критически важных отраслях, регламентом DORA для индустрии финансовых услуг и Законом ЕС о кибербезопасности (EU Cybersecurity Act, 2019).

Законопроект служит ответом на все более частые кибератаки, а также с учетом прогнозов, что глобальные затраты на противодействие и компенсанции от кибератак для компаний достигнут $10,5 трлн. в год к 2025 году, по сравнению с $3 трлн. в 2015г. Основная цель законопроекта — установить минимальный стандарт кибербезопасности для разработки программного и аппаратного обеспечения с конкретными обязательствами для различных участников цепочки поставок. Производители (включая разработчиков) соответствующих продуктов несут наиболее значительные обязательства, и от них ожидается обеспечение соответствия их продуктов основным требованиям кибербезопасности. Эти требования в первую очередь включают набор технических стандартов, которые соответствуют другим организационным и управленческим требованиям. Акцент на оценке рисков и принципах управления занимает центральное место в подходе предложения, наряду с тщательным вниманием к управлению уязвимостями и раскрытию информации.

Как и Закон ЕС об искусственном интеллекте (Artificial Intelligence Act), внесенный законопроект увеличит нормативные обязательства в зависимости от уровня риска, связанного с продуктом. Производители должны будут разрабатывать продукты (включая стандартные и критические продукты) в соответствии с “основными требованиями кибербезопасности”, включающие требования о безопасной конфигурации по умолчанию, поддержание конфиденциальности и механизмы целостности данных, а также возможность отзыва продукта в случае обнаружения определенных уязвимостей. Кроме того, производители должны будут проводить оценку рисков кибербезопасности на протяжении всего жизненного цикла продукта, чтобы свести к минимуму эти риски кибербезопасности и смягчение последствий инцидентов. Производители также должны устранять уязвимости, в том числе с помощью “скоординированных политик раскрытия уязвимостей”. Наконец, производители должны будут пройти процедуру оценки соответствия, чтобы показать, что их продукция соответствует их нормативным обязательствам, наряду с “декларацией о соответствии”. Законопроект устанавливает максимальный штраф в размере до €15 млн. или до 2,5% от общего годового оборота за предыдущий финансовый год за несоблюдение любых существенных требований кибербезопасности. Нарушение других обязательств может привести к штрафам в размере до €10 млн. или 2% от общего оборота за последний финансовый год. Предоставление вводящей в заблуждение информации органам по надзору за рынком также может повлечь за собой штрафы в размере до € 5 млн. или 1% от общего оборота, полученного за последний финансовый год.

После Директивы об электронной торговле ЕС в 2000 г. в ноябре 2022 года вступил силу Закон о цифровых услугах в ЕС (The Digital Services Act, 2022) (далее -Закон DSA), который распространяется на следующие категории участников е-торговли: онлайн-посредники; услуги хостинга (такие как облачные услуги и услуги веб-хостинга); онлайн-платформы (объединяющие продавцов и потребителей и распространяющие информацию среди населения по их запросу, такие как онлайн-рынки, магазины приложений, платформы совместной экономики и платформы социальных сетей); а также VLOP/VLOSE. Закон DSA обязывает все онлайн-платформы внедрять механизмы уведомлений и действий, которые позволят третьим сторонам уведомлять платформу о незаконном контенте в своих услугах, а также механизм идентификации пользователей услуг этих онлайн-платформ, обеспечивающий четким, кратким и недвусмысленным образом и в режиме реального времени. Закон DSA устанавливает режим, который должен эффективно обеспечивать защиту от ответственности за незаконный контент в отношении онлайн-посредников, которые просто

предоставляют «канал» для информации, выполняют рутинное «кэширование» информации или «размещают» информацию в обстоятельствах, когда они не знать о незаконном содержании. Закон предусматривает создание нового органа ЕС - *Европейский совет по цифровым услугам* для координации соблюдения и обеспечения соблюдения и выполнения функций консультативного совета. Кроме того, поставщики посреднических услуг, которые добросовестно принимают решение о добровольном принятии мер по обнаружению и удалению незаконного контента, не будут лишены возможности воспользоваться защитой от ответственности (принцип «доброго самаритянина»).

Несоблюдение норм Закона DSA может привести к штрафам в размере до 6% от мирового годового дохода или оборота провайдера или платформы. Размер штрафа будет зависеть от серьезности нарушения, а также продолжительности и частоты нарушения. Государства-члены ТЕС или Комиссия могут также налагать штрафы в размере до 1% от годового дохода или оборота провайдера или платформы за предоставление неверной, неполной или вводящей в заблуждение информации в ответ на запрос информации и непрохождение проверки. Получатели услуг, регулируемых DSA, также имеют право подать жалобу на поставщика-посредника Координатору цифровых услуг государства-члена, в котором находится или учрежден получатель услуги, о несоблюдении DSA. Получатель имеет право потребовать компенсацию от поставщика посреднических услуг за ущерб или убытки, понесенные из-за несоблюдения поставщиком, в соответствии с национальным законодательством или законодательством ЕС.

В **США** действует несколько ключевых федеральных уголовных законов способствующих обеспечению кибербезопасности, в том числе Закон о компьютерном мошенничестве и злоупотреблениях (CFAA), раздел 1030 18 USC, запрещающий взлом и другие компьютерные преступления, Закон об экономическом шпионаже (1996), Закон о защите коммерческой тайны (2016), Закон о конфиденциальности электронных коммуникаций (ECPA), Закон о кибербезопасности (2015), разд. 2510 18 USC, запрещающий определенный доступ к информации при передаче или хранении у поставщика услуг сохраненной связи или службы удаленных вычислений (включая облачных провайдеров). Во всех штатах также есть законы о компьютерных преступлениях, касающиеся несанкционированного доступа и компьютерного вторжения, и во многих штатах есть дополнительные законы, касающиеся шпионских программ, фишинга, программ-вымогателей и других кибератак. Закон о кибербезопасности регулирует области важнейшей инфраструктуры (определенных в Президентской директиве 21 (PPD-21), включая безопасность и устойчивость критической инфраструктуры, секторы здравоохранения и финансовых услуг, для которых установлены подробные требованиям кибербезопасности. В мае 2021 года президент Байден издал указ «Об улучшении кибербезопасности страны», направленный на дальнейшее повышение кибербезопасности критической инфраструктуры для государственных органов и частных компаний, включая обмен информацией, отчетность об инцидентах, условия контрактов, связанные с кибербезопасностью и безопасностью цепочки поставок, которые уже применяются к компаниям оборонно-промышленного комплекса США.

В сфере энергетики структуры Министерства энергетики США отвечают за обеспечение кибербезопасности, энергетической безопасности и реагирования на чрезвычайные ситуации, при контроле безопасности энергосистем и предпринимает меры кибертестирования на устойчивость программ промышленных систем управления. Аналогичным образом, программа стандартов борьбы с терроризмом на химических объектах осуществляется Министерством внутренней безопасности посредством установления стандартов кибербезопасности, основанных на рисках, для объектов, которые производят, обрабатывают или хранят химические вещества, представляющие повышенную опасность.

Президентская директива 21 президента Обамы (PPD-21) «Безопасность и устойчивость критической инфраструктуры» определила 16 областей критической инфраструктуры и поручила министру внутренней безопасности возглавить объединенные национальные усилия по защите этих областей в координации с соответствующим основным федеральным регулирующим органом для этого сектора. Так, Федеральная комиссия по регулированию энергетики отвечает за обеспечение надежности основной энергосистемы Северной Америки, а Североамериканская корпорация электрической надежности обеспечивает кибербезопасность в энергетическом секторе, путем оповещения Центра обмена и анализа информации об электричестве, а также внедрением Стандартов надежности защиты критически важной инфраструктуры. Администрация транспортной безопасности также может издавать правила, касающиеся кибербезопасности трубопроводов, и директивы о защите от кибернетических вторжений. Аналогичным образом, SEC и

несколько других федеральных агентств рассматривают киберугрозы для финансовой инфраструктуры. Недавний исполнительный указ президента Байдена.

Орган национальной кибербезопасности NIST предоставляет рекомендации, помогающие организациям управлять рисками кибербезопасности, основанной на оценке пяти 'функций' эффективной программы кибербезопасности:

— идентификация – способность выявлять и понимать организационные киберриски;
— защита – разработка и внедрение надлежащих мер предосторожности для обеспечения безопасности критически важной инфраструктуры.;
— обнаружение – действия и возможности для обнаружения вторжений в кибербезопасность и попыток вторжения;
— реакция – способность реагировать и реагировать на обнаруженный инцидент кибербезопасности; и
— восстановление – деятельность по планированию отказоустойчивости и способности поддерживать или восстанавливать службы, которые были повреждены в результате инцидента кибербезопасности.

Закон об экономическом шпионаже, Закон о компьютерном мошенничестве и злоупотреблениях, законы о компьютерных преступлениях штатов предусматривают уголовную ответственность за широкий спектр правонарушений. Закон о компьютерном мошенничестве и злоупотреблениях устанавливает уголовную и гражданскую ответственность лиц, получающих информацию путем преднамеренного несанкционированного доступа к 'защищенному компьютеру' без разрешения или при превышении разрешенного доступа. Взлом, несанкционированный доступ, незаконное проникновение, вирусы, вредоносные программы, атаки типа «отказ в обслуживании», программы-вымогатели, компьютерное вымогательство, фишинг и шпионские программы также являются уголовными преступлениями в соответствии с различными законами, также как запрет на мошенничество с средствами связи, банковское мошенничество и мошеннические схемы в целом, предусмотренные федеральными законами и законами штатов.

FTC может возбудить гражданско-правовые иски против компаний, которые не осуществляют разумный контроль безопасности конфиденциальных данных, если это бездействие причиняет или может нанести существенный вред потребителям, которого они не могут разумно избежать, а также в случае нарушения организациями стандартов безопасности, которые они обязуются соблюдать. Комиссия по ценным бумагам и биржам (SEC) также является важным регулятором благодаря своей роли в обеспечении того, чтобы участники публичных рынков ценных бумаг предоставляли инвесторам всю существенную информацию.

Важные аспекты режима кибербезопасности США также подлежат отраслевому саморегулированию. Например, стандарт безопасности данных индустрии платежных карт (PCI-DSS) описывает меры защиты, необходимые для платежных карт, используемых торговцами или поставщиками. Хотя США официально не приняли обязательные стандарты, связанные с кибербезопасностью, Национальный институт стандартов и технологий (NIST) разработал систему кибербезопасности, инициированную исполнительным указом президента Обамы в феврале 2013 года, которая основывается на нескольких международных стандартах, включая ISO / IEC 27001. Стандарт соответствия требованиям безопасности NIST является обязательным для всех федеральных информационных систем США, за исключением тех, которые связаны с национальной безопасностью, которые должны соответствовать более высоким стандартам. Закон Сарбейнса Оксли (2002г.) обязывает публичные компании поддерживали надлежащее управление своими ключевыми информационными системами, чтобы сотрудники могли гарантировать целостность существенных данных, а также выявлять, устранять и раскрывать существенные недостатки кибербезопасности. Должностные лица и директора корпораций также обязаны по общему праву выполнять фидуциарные обязанности в отношении акционеров, которые включают в себя обязательство контролировать риски кибербезопасности. Невыполнение этого требования может привести к искам о ценных бумагах или искам акционеров о деривативах. Хотя на федеральном уровне не существует единого набора обязательных защитных мер, структура кибербезопасности NIST, разработанная для организаций частного сектора, описывает лучшие практики соблюдения требований кибербезопасности.

На государственном уровне многочисленные законы налагают обязательства по кибербезопасности, которые защищают информацию от несанкционированного использования. Каждый штат принял свой закон о недобросовестных или вводящих в заблуждение действиях, и многие штаты также приняли законы, включающие требования соблюдения «разумной безопасности». К примеру, Правила кибербезопасности

штата Массачусетс предъявляют особые требования к безопасности в отношении личной информации, включая внедрение письменной программы безопасности и шифрование определенных данных. В Калифорнии закон о защите прав потребителей, который будет расширен новым законом о правах потребителей на неприкосновенность на неприкосновенность частной жизни, предусматривает право на возмещение ущерба в размере $100-750 для жителя штата, если компания не внедрила разумные протоколы безопасности для защиты персональных данных, что повлекло нарушение личной информации. Несколько штатов внедрили отраслевые требования к кибербезопасности. Например, Департамент финансовых услуг Нью-Йорка (NYDFS) издал требования к кибербезопасности для компаний, предоставляющих финансовые услуги, имеющих лицензию в Нью-Йорке. Его Положение о кибербезопасности послужило моделью регулирования для FTC и других государственных страховых агентств.

Система кибербезопасности США включает систему норм общего права, разработанных и применяемых как федеральной судебной системой, так и судебной системой штатов, и относит к сложным вопросам защиты данных. В делах, связанных с деликтными концепциями халатности и незаконного проникновения, подлежит защите интересы истцов в случае ущерба, непосредственно возникший в результате нарушения обязанности по защите информации.

В **КНР** общий режим кибербезопасности и защиты данных включает Закон о кибербезопасности, правила и меры по его применению. В Китае также существуют различные отраслевые регулирующие органы, которые издают отраслевые правила и регулируют вопросы кибербезопасности и защиты данных в своих соответствующих секторах. Вступивший в силу 1 января 2021 года Гражданский кодекс КНР, заменивший ранее действовавшие Общие принципы гражданского законодательства, предусматривает право на защиту персональных данных. Любые организации и частные лица, которые собирают и обрабатывают персональные данные, должны обеспечивать безопасность персональных данных. Незаконный сбор, использование, обработка или передача персональных данных запрещены. Уголовный кодекс КНР содержит определенные действия, которые могут представлять собой преступление нарушения права на защиту персональных данных, а также составы преступлений, включая вторжение в информационные системы и другие киберпреступления.

Первым национальным законом КНР о защите безопасности в сети Интернет стал Закон о кибербезопасности 2016 года, который считается основным краеугольным камнем системы кибербезопасности и защиты данных. Закон регулирует строительство, эксплуатацию, техническое обслуживание и использование сети сетевыми операторами на территории Китая, устанавливает понятия «сети» и «сетевых операторов», включающие большинство информационных систем в Китае и их владельцев, операторов и администраторов. В 2021 году в КНР приняты Закон о безопасности данных и Закон о защите личной информации (Закон о защите персональных данных), знаменующий собой создание китайской сети кибербезопасности и защиты персональных данных.

В сентябре 2022 года в КНР опубликован проект поправок в Закон и кибербезопасности, предусматривающий существенное повышение размеров штрафных санкций и введение оборотных штрафов для организаций за правонарушения, включая незаконное вторжение или нарушение работы сети или кражу данных, Проект направлен на обеспечение стабильности бизнеса и его непрерывной работы, внедрению мер защиты, сохранению конфиденциальности закупок сетевых продуктов и услуг, а также проведению регулярных проверок и оценок мер безопасности. Проект поправок предлагает скорректировать штрафы за нарушение обязательств по управлению информацией, публикуемой пользователями, и установить механизмы жалоб и сообщений, а также запрет на установку вредоносных программ или публикацию незаконной электронной информации. Проект также ужесточил юридические наказания за незаконную публикацию и передачу информации, вводит суровые наказания при особо серьезных обстоятельствах, а также предполагает существенно ужесточить штрафы за нарушения обязательств по защите личной информации.

Выводы

Изложенный в статье анализ показывает, что стремительное распространение киберпреступности, появление новых форм организованной преступности, использующей глобальную сеть Интернет, спланированные и хорошо организованные кибератаки на критическую инфраструктуру государства и частных компаний свидетельствует о формировании особого направления преступности – преступность в сфере кибербезопасности и информационных технологий, которая выходит за рамки традиционного понимания преступности в сфере информационных технологи и средств связи.

Киберпреступность представляет особый социальный феномен, во многом порожденный процессами цифровизации и информатизации общества.

Это дает основание авторам сформулировать понимание правового содержания киберпреступности, которое охватывает не только правонарушения, совершенные с использованием компьютерной техники, но и иного информационно-коммуникационного оборудования и средств, включая программные средства. Авторы приходят к выводу о необходимости концептуального оформления теоретических и методологических начал, разработки основ правопорядка в сфере кибербезопасности, уточнению понятийного аппарата и специфики регулирования как в сфере публично-правового, так и частно-правового регулирования сферы кибербезопасности, а также формирования нового направления криминологии в сфере киберпреступности.

Литература:

1. Авдеев В.А., Авдеева О.А. Основные направления совершенствования правовой политики по обеспечению в условиях глобализации информационной безопасности // Российская юстиция. 2021. N 3. С. 3-10.
2. Алешин.А .Евросоюз разработал свою первую оборонную стратегию URL:https://www.imemo.ru/publications/relevant-comments / text/evrosoyuz-razrabotal-svoyu-pervuyu-oboronnuyu-strategiyu
3. Карцхия А.А., Сергин М.Ю., Макаренко Г.И. Новые элементы национальной безопасности: национальный и международный аспект // Вопросы кибербезопасности, 2020, № 6(40), С.72-82. DOI: 10.21681/2311-3456-2020-6-72-82
4. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18-23. DOI: 10.21681/2311-3456-2019-3-16-23
5. Бочков С.И., Макаренко Г.И., Федичев А.В. Об окинавской хартии глобального информационного общества и задачах развития российских систем коммуникации // Правовая информатика. 2018. № 1. С. 4-14. DOI: 10.21681/1994-1404-2018-1-4-14
6. Карцхия А.А. Кибербезопасность в условиях новой технологической революции и опыт стран БРИКС // Пробелы в российском законодательстве. 2021. Т. 14. № 4. С. 358-365.
7. Перина А.С. Феномен использования компьютерных технологий при совершении преступлений против личности: анализ международных документов и уголовного законодательства отдельных стран // Журнал зарубежного законодательства и сравнительного правоведения. 2022. N 5. С. 115 – 126;
8. Саркисян А.Ж. Криминологическая характеристика преступлений, совершаемых в сфере информационно-коммуникационных технологий//Российский следователь.2019.N3.С.54 - 59.
9. Human Rights, Digital Society and the Law. A Research Comparison (Ed. By Mart Susi). London. Routledge, 2019.
10. Э. Верхелст, Я. Ваутерс. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций. Т. 15. № 2 (2020), с.141-172.
11. Ковалев О.Г., Скипидаров А.А. Нормативное-правовое регулирование реализации Стратегии кибербезопасности в государствах Европейского союза // Столыпинский вестник. 2021. Т. 3. № 2.
12. Ковалев О.Г., Скипидаров А.А. Правовое регулирование и особенности организации кибербезопасности в США // Столыпинский вестник. 2021. Т. 3. № 1. С. 12.
13. Мордвинов К.В., Удавихина У.А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция», № 1 (11) 2022, с.83-88.
14. Далгалы Т.А. Киберкриминология: вызовы XXI века // Российская юстиция. 2020. N 10.С.19 - 21.
15. Мороз Н.О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий // Экономические и юридические науки. Конституционное и международное право, 2011, № 14, с.143-148.

LEGAL ASPECTS OF MODERN CYBERSECURITY AND CYBERCRIME COUNTERACTION

Kartskhiya A.A.[22], Makarenko G.I.[23]

Abstract

The article analyses *contemporary legal aspects and current cybersecurity issues, cybercrime features of Russian and foreign law of information and communication technologies.*

22 Alexander A. Kartskhiya, Dr.Sc., Professor, Department of Legal security of Fuel and Energy Complex at Gubkin University, Moscow, Russia. E-mail: arhz50@mail.ru

23 Grigory I. Makarenko, leading researcher at the Scientific center for legal information under the Ministry of Justice of the Russian Federation, Moscow, Russia. E-mail: t7920518@yandex.com

The research methods *consist of comparative legal analysis of contemporary Russian and foreign legislation and law enforcement practice, as well as, a formal and logical study of a conceptual apparatus, content and structure of the research object.*

The study results *enable the authors to formulate the awareness of cybercrime legal content, that includes not only offenses committed by using computer technology, but other information and communication equipment and tools, including software either. The rapid spread of cybercrime, the emergence of new forms of organized crime using the global Internet, intended and well–organized cyber attacks on a critical infrastructure of states and private companies indicate the formation of a special area of crime - cybersecurity crime and information technology, which goes beyond a common insight of crime of information technology and communications. Therefore, the authors came to certain conclusions to conceptualize theoretical and methodological principles, develop the foundations of law and order of cybersecurity, clarify the conceptual apparatus and specifics of legal regulation of cybersecurity in public and private law, as well as the formation of a new line of criminology of cybercrime.*

The scientific novelty *of the study consists of a conceptual justification of a cybercrime countering, as an element of national cybersecurity, as well as, the substantiation of a specific line of criminology – cybercriminology.*

Keywords: cybercrime, information security, cyberspace security, cyber attacks, foreign cyber law, information law, cybercriminology, digital law, personal data, private law, cybersecurity.

References

1. Avdeev V.A., Avdeeva O.A. Osnovnye napravlenija sovershenstvovanija pravovoj politiki po obespecheniju v uslovijah globalizacii informacionnoj bezopasnosti // Rossijskaja justicija. 2021. N 3. S. 3-10.
2. Aleshin.A. Evrosojuz razrabotal svoju pervuju oboronnuju strategiju URL:https://www.imemo.ru/publications/relevant-comments / text/evrosoyuz-razrabotal-svoyu-pervuyu-oboronnuyu-strategiyu
3. Karchija A.A., Sergin M.Ju., Makarenko G.I. Novye jelementy nacional'noj bezopasnosti: nacional'nyj i mezhdunarodnyj aspekt // Voprosy kiberbezopasnosti, 2020, № 6(40), S.72-82. DOI: 10.21681/2311-3456-2020-6-72-82
4. Karchija A.A., Makarenko G.I., Sergin M.Ju. Sovremennye trendy kiberugroz i transformacija ponjatija kiberbezopasnosti v uslovijah cifrovizacii sistemy prava // Voprosy kiberbezopasnosti. 2019. № 3 (31). S. 18-23. DOI: 10.21681/2311-3456-2019-3-16-23
5. Bochkov S.I., Makarenko G.I., Fedichev A.V. Ob okinavskoj hartii global'nogo informacionnogo obshhestva i zadachah razvitija rossijskih sistem kommunikacii // Pravovaja informatika. 2018. № 1. S. 4-14. DOI: 10.21681/1994-1404-2018-1-4-14
6. Karchija A.A. Kiberbezopasnost' v uslovijah novoj tehnologicheskoj revoljucii i opyt stran BRIKS // Probely v rossijskom zakonodatel'stve. 2021. T. 14. № 4. S. 358-365.
7. Perina A.S. Fenomen ispol'zovanija komp'juternyh tehnologij pri sovershenii prestuplenij protiv lichnosti: analiz mezhdunarodnyh dokumentov i ugolovnogo zakonodatel'stva otdel'nyh stran // Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedenija. 2022. N 5. S. 115 – 126;
8. Sarkisjan A.Zh. Kriminologicheskaja harakteristika prestuplenij, sovershaemyh v sfere informacionno-kommunikacionnyh tehnologij// Rossijskij sledovatel'.2019.N3.S.54 - 59.
9. Human Rights, Digital Society and the Law. A Research Comparison (Ed. By Mart Susi). London. Routledge, 2019.
10. Je. Verhelst, Ja. Vauters. Global'noe upravlenie v sfere kiberbezopasnosti: vzgljad s pozicii mezhdunarodnogo prava i prava ES // Vestnik mezhdunarodnyh organizacij. T. 15. № 2 (2020), s.141-172.
11. Kovalev O.G., Skipidarov A.A. Normativnoe-pravovoe regulirovanie realizacii Strategii kiberbezopasnosti v gosudarstvah Evropejskogo sojuza // Stolypinskij vestnik. 2021. T. 3. № 2.
12. Kovalev O.G., Skipidarov A.A. Pravovoe regulirovanie i osobennosti organizacii kiberbezopasnosti v SShA // Stolypinskij vestnik. 2021. T. 3. № 1. S. 12.
13. Mordvinov K.V., Udavihina U.A. Kiberprestupnost' v Rossii: aktual'nye vyzovy i uspeshnye praktiki bor'by s kiberprestupnost'ju // Teoreticheskaja i prikladnaja jurisprudencija», № 1 (11) 2022, s.83-88.
14. Dalgaly T.A. Kiberkriminologija: vyzovy XXI veka // Rossijskaja justicija. 2020. N 10.S.19 - 21.
15. Moroz N.O. Dejatel'nost' Interpola po koordinacii sotrudnichestva v bor'be s prestupnost'ju v sfere vysokih tehnologij // Jekonomicheskie i juridicheskie nauki. Konstitucionnoe i mezhdunarodnoe pravo, 2011, № 14, s.143-148.