ПРАВОВЫЕ АСПЕКТЫ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ

Карцхия А. А.[1]

Ключевые слова: *кибератаки, киберпреступность, кибербезопасность, информационно-коммуникационные технологии (ИКТ), цифровые технологии, программное обеспечение, мошенничество, способ, информационно-телекоммуникационные сети (ИТС), Интернет, трансграничность, персональные данные, сфера компьютерной информации.*

Аннотация

Цель работы: определение актуальных правовых аспектов и особенностей киберпреступности в сфере информационно-коммуникационных технологий (ИКТ) с учетом российского и зарубежного опыта и правоприменительной практики.

Методы: сравнительно-правовой анализ действующего российского и зарубежного законодательства и практики их применения, а также формально-логический анализ понятийного аппарата, содержания и структуры предмета исследования.

Результаты: предлагается совокупность формализованных представлений о правонарушениях и преступлениях с использованием компьютерной техники, информационно-коммуникационного оборудования и средств, включая компьютерные программные средства, для понимания правового содержания понятия киберпреступности; исследованы новые способы совершения преступлений в киберпространстве и выявлены новые объекты киберпреступлений; определено, что киберинциденты занимают лидирующую позицию среди группы рисков, связанных с развитием современной цифровой экономики, растущей угрозой со стороны программ-вымогателей и кибермошенничества, а также геополитическим соперничеством и конфликтами, которые все чаще разыгрываются в киберпространстве; обоснован вывод о формировании особого вида преступности — в сфере кибербезопасности и ИКТ, что ставит задачу разработки технологического и правового обеспечения эффективного регулирования отношений в данной сфере.

DOI: 10.21681/1994-1404-2023-1-83-92

Введение

Наряду с экономическими и политическими последствиями пандемии COVID-19, высокими ценами на энергоносители и инфляцией, геополитической и экономической неопределенностью и изменением климата, согласно проведенному в 2022 г. аналитическому исследованию международной страховой группы *Allianz*[2], *киберинциденты занимают лидирующую позицию среди группы рисков, связанных с развитием современной цифровой экономики, растущей угрозой со стороны программ-вымогателей и кибермошенничества, а также геополитическим соперничеством и конфликтами, которые все чаще разыгрываются в киберпространстве* [3, 16]. Киберриски, такие как перебои в работе *IT*-систем, атаки программ-вымогателей или утечка данных, второй год подряд считаются наиболее важным риском во всем мире, что произошло впервые за последнее десятилетие.

Кибератаки являются одной из самых постоянных и серьезных угроз, с которыми сегодня сталкиваются многие компании. Глобальные кибератаки, спонсируемые государством, могут привести к серьезному нарушению рынков и экономики. *Киберустойчивость* становится важнейшим экономическим и политическим фактором как противовес опасностям, связанным с *киберпреступностью* [3] в виде трех взаимосвязанных угроз: уязвимости «нулевого дня», уязвимости сторонних поставщиков услуг, уязвимости программ-вымогателей.

[2] Allianz Risk Barometer 2023, 12th Edition. URL: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html#download

[1] ***Карцхия Александр Амиранович,*** *доктор юридических наук, и. о. заведующего кафедрой правового обеспечения безопасности топливно-энергетического комплекса Российского государственного университета нефти и газа (НИУ) им. И. М. Губкина, г. Москва, Российская Федерация.*

E-mail: arhz50@mail.ru

Устойчивость подразумевает способность быстро восстанавливаться после неудач, приспосабливаться. Более 2/3 глобальных финансовых компаний в 2022 г. подверглись хотя бы одной атаке программ-вымогателей. Критическая рыночная инфраструктура (биржи, расчетные центры и др.) уже сталкивается с инцидентами *кибербезопасности* [1, 3] и продолжением угроз программ вымогателей, которые уже не ограничиваются участием изощренных разработчиков программ-вымогателей и простым пользовательским интерфейсом злоумышленников, а нанимают соучастников для развертывания программы-вымогателя в целях кибератаки на жертву за вознаграждение (процент от полученного выкупа). Киберустойчивость приобретает особое значение: многие кибератаки начинаются с общих уязвимостей, которые можно устранить с помощью надлежащей кибергигиены. Попытки фишинга, атаки на программное обеспечение и системы, которые не были обновлены, доступ через удаленные соединения и попытки инсайдеров получить данные продолжают использоваться киберпреступниками[3].

По оценкам Интерпола, преступники пользуются онлайн-трансформацией для выявления слабых мест в онлайн-системах, сетях и инфраструктуре. Фишинг, программы-вымогатели и утечка данных — это лишь несколько примеров современных киберугроз, в то время как новые виды киберпреступлений появляются постоянно. Киберпреступники становятся все более гибкими и организованными: они используют новые технологии, адаптируют свои атаки и сотрудничают по-новому. *Киберпреступность* (преступность в сфере высоких технологий) не знает национальных границ. Преступники, жертвы и техническая инфраструктура охватывают несколько юрисдикций, что создает множество проблем для расследований и судебного преследования. Поэтому необходимо тесное сотрудничество между государственными и частными партнерами[4].

Согласно статистике Банка России, в первом полугодии 2020 г. мошенники украли у банковских клиентов примерно 4 *млрд руб.*, совершив 360 тыс. несанкционированных операций. Из этой суммы банки смогли вернуть клиентам только 12,1% похищенных средств (около 485 *млн руб.*)[5].

Почти четверть криптовалютных токенов, выпущенных в 2021 г., продемонстрировали явные признаки мошеннической схемы. По оценкам аналитиков *Chainalysis*, схемы накачки и сброса распространены в традиционных финансах. Мошенники обычно продвигают активы, которыми они владеют, другим инвесторам, быстро повышая цену. Когда она достигает определенной точки, они продают переоцененные акции с прибылью, в результате чего цена резко падает (*Pump-and-Dump*). Криптовалюты, торгуемые цифровые активы, построенные на блокчейне другой криптовалюты, становятся все более популярными среди тех же мошенников, что часто связано с относительной легкостью, с которой злоумышленники могут запустить новый токен и установить для него искусственно высокую цену и рыночную капитализацию «на бумаге», задав первоначальный объем торговли и контролируя оборотное предложение[6]. Мошеннические объявления о продаже криптовалюты могут размещаться в социальных сетях и на законных веб-сайтах СМИ или появляться в списках онлайн-поиска.

Как только пользователи делятся своими личными данными, с ними можно связаться по телефону, электронной почте или в сообщении в социальных сетях и предложить высокую прибыль с минимальным риском или без него. На этом этапе мошенники обычно используют тактику продаж с высоким давлением. Но, как только деньги будут внесены, мошенники заморозят счет и украдут средства. Они получат доступ, обманом заставив жертву загрузить *троянскую* программу удаленного доступа (*Remote Access Trojan — RAT*), что позволит им захватить компьютер пользователя[7]. Согласно сообщениям, в 2021 г. жертвы мошенничества с криптовалютой уже потеряли более 146 *млн* фунтов стерлингов (200 *млн* долларов США), что на двузначное число больше, чем в 2020 г.[8]

Недавние кибератаки доказали, что киберпреступность представляет собой реальную и непосредственную опасность для большинства компаний в сегодняшнюю цифровую эпоху. Даже традиционные компании, не зависящие от *IT*, в том числе, например, в горнодобывающей и обрабатывающей промышленности, все чаще подключают свои компьютерные системы к своим *IT*-сетям и тем самым подвергают данные и системы рискам, связанным с киберугрозами.

Преступность в киберпространстве, как отмечалось в докладе ООН [6], является одной из самых сложных проблем, с которыми международное сообщество сталкивается в последние годы в связи с развитием информационных и коммуникационных технологий (ИКТ).

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 показывает, что методы киберпреступности

---

[3] См.: CFTC Commissioner Christy Goldsmith Romero identified cybercrime and climate risk as severe threats to financial markets and called for collaborative action to strengthen resiliency in both areas. URL: https://www.cftc.gov/PressRoom/SpeechesTestimony/oparomero

[4] URL: https://www.interpol.int/Crimes/Cybercrime

[5] URL: https://www.cbr.ru/press/event/?id=8238

[6] URL: https://www.chainalysis.com/

[7] URL: https://www.infosecurity-magazine.com/news/santander-warns-of-87-surge-uk/

[8] URL: https://www.infosecurity-magazine.com/news-features/us-government-open-source-security/

могут эффективно использоваться в *информационной борьбе (войне)* [2, 8].

Стремительное распространение киберпреступности, появление новых форм организованной преступности, использующей глобальную сеть Интернет, спланированные и хорошо организованные кибератаки на критическую инфраструктуру государств и частных компаний свидетельствуют 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 [6, 17].

Виды и особенности киберправонарушений

Киберпреступления совершаются с использованием компьютеров и компьютерных сетей и могут быть нацелены на отдельных физических лиц, компании и бизнес-структуры, государственные органы и управленческие структуры, а также объекты критической инфраструктуры. *Киберпреступником*, как правило, является лицо (группа лиц), использующее свои навыки в области компьютерных технологий для совершения злонамеренных действий и незаконной деятельности в противоправных целях. Киберпреступниками могут быть лица, торгующие незаконным онлайн-контентом или нарушающие права *интеллектуальной собственности* [9], кибермошенники, наркоторговцы, кибертеррористы. Чаще всего киберпреступления совершаются по мотивам личной мести, корыстным мотивам (мошенничество, вымогательство, кража цифровых активов или данных и др.), а также таким как шантаж, кибертерроризм и угрозы или идеологическая мотивация. К наиболее распространенным способам совершения киберпреступлений можно отнести следующие[9].

I. *Кибермошенничество* (*Internet fraud)* или кража личных данных как форма мошенничества в отношении потребителей (*identity theft*) — незаконное присвоение или использование киберпреступниками *персональных* или иных данных другого человека (номера кредитных карт, личные фотографии, имя, аккаунта в соцсети и др.) без разрешения владельца этих данных в целях совершения мошенничества или иного преступления.

К этой категории, в частности, относится фишинг (*fishing & scams*) — разновидность онлайн-мошенничества, которое нацелено на завладение персональными и иными данными потребителей путем отправки им электронного письма якобы от хорошо известного и доверенного источника (например, от интернет-провайдера, банка или ипотечной компании), и которым просят потребителя предоставить личную идентификационную информацию. Затем мошенник использует эту информацию в противоправных целях — для открытия новых учетных записей или вторжения в существующие учетные записи потребителя. Разновидностями такого рода афер (*scams*) в целях получения персональных данных являются, например:

(а) мошенничество с автогарантией или медицинским страхованием — мошенническое предложение о продлении гарантии на автомобиль, страховой или медицинский полис для завладения персональными данными;

(б) мошенничество с благотворительностью — мошеннические звонки с просьбой о благотворительных пожертвованиях в адрес выдуманных фальшивых благотворительных организаций или имитация настоящей благотворительности для выманивания денежных средств;

(в) мошенничество с оказанием помощи при несчастных случаях или стихийных бедствиях, когда преступник запрашивает деньги или персональные данные для якобы попавшего в беду родственника или члена семьи;

(г) мошенничество с предложением о трудоустройстве по онлайн-объявлениям, часто с незаконным использованием официальных названий известных компаний;

(д) мошенничество с подарочными картами или сертификатами;

(е) мошенничество с государственными грантами, с предложением перевести на расчетный счет потребителя денежные средства, как только он предоставит информацию о своей учетной записи, которую впоследствии мошенники продают или используют для кражи денег;

(ж) мошенничество с самозванцем (звонка, робозвонка, электронной почты или другого сообщения) от имени налоговой социальной или иной государственной службы с требованием немедленной оплаты задолженности, часто с помощью неотслеживаемых способов;

(з) мошенничество с технической поддержкой или бесплатной пробной версией компьютерной программы путем ложного заявления о том, что устройство пользователя заражено вирусом, иной вредоносной программой с последующим требованием оплаты за «исправление» несуществующего дефекта или удаление подключения к внешнему устройству для кражи личной информации.

В США, например, у физических лиц нет официального удостоверения личности, но номер социального страхования долгое время служил де-факто идентификационным номером. Налоги взимаются на основе номера социального страхования каждого гражданина, и многие частные учреждения используют этот номер для отслеживания своих сотрудников, студентов и пациентов. Доступ к номеру социального страхования человека дает возможность собрать все документы, относящиеся к гражданству этого человека, т. е. «украсть» его личность. Даже украденная информация кредитной карты может быть использована для восстановления личности[10].

[9] URL: https://www.ftc.gov/news-events/topics/identity-theft

[10] M. Aaron Dennis. Alternate titles: computer crime: Article History. URL: https://www.britannica.com/topic/cybercrime

По данным Банка России[11], за первое полугодие 2020 г. доля социальной инженерии в общем числе атак на банковских клиентов составила 83,8%. По оценкам Сбербанка, с начала 2020 г. мошенники позвонили клиентам около 15 *млн* раз. В сутки число мошеннических звонков в России достигает 100 *тыс*.

II. *Создание и применение шпионских и вредоносных компьютерных программ*, включая вирусы и «шпионские» программы в целях кражи персональных данных и иных личных данных (в том числе биометрические данные [11] и сведения о геноме [5] конкретного человека, сведения личного аккаунта в соцсетях или личного банковского и иного счета), рассылки спама и совершения мошеннических действий. Используя привлекательные веб-сайты, желаемые загрузки и убедительные истории, преступники заманивают потребителей по ссылкам, по которым загружается вредоносное программное обеспечение (ПО), особенно на компьютерах, где не используются ПО безопасности. «Шпионское» ПО как вид вредоносного ПО способно отслеживать использование чужого компьютера или контролировать его, а также позволяет отправлять потребителям всплывающие окна, перенаправлять их компьютеры на нежелательные веб-сайты, отслеживать их интернет-серфинг или записи нажатий клавиш в целях кражи личных данных.

III. *Кражи персональных данных или иных данных военнослужащих* и членов их семей составляют особую категорию, направленную на подрыв боеспособности Вооруженных сил.

IV. *Навязанные платежи* *(mobile cramming)* — взимание несанкционированных платежей третьими лицами со счетов мобильных телефонов за сторонние услуги без ведома или согласия потребителей (например, предложение бесплатных призов, а затем взимания с телефонных счетов потребителей периодических платежей в пользу третьих лиц за услуги, не связанные с предложением).

V. *Кибератаки программ-вымогателей* *(ransomware attack)* — кибератаки с использованием программ-вымогателей, вредоносного ПО, которое способно препятствовать доступу пользователей к их личным данным (аккаунтам) в системе, шифруя эти данные, а затем запрашивая выкуп за открытие доступа к зашифрованным данным.

VI. *Взлом/блокировка доступа в компьютерных сетях* *(hacking/misusing computer networks)*, т. е. несанкционированный доступ к частным компьютерам или иным *IT-сетям* и последующем их неправомерном использовании либо путем их отключения, либо путем изменения хранимых данных, либо другими противоправными способами.

VII. *Киберзапугивание* *(cyber bullying)* — онлайн- или интернет-издевательства, включающие отправку или совместное использование вредоносного и унизительного контента о каком-либо лице, направленное на то, чтобы вызвать его смущение, что может быть причиной возникновения психологических проблем — это в последнее время стало распространенным явлением, особенно среди подростков.

VIII. *Киберпреследование* *(cyber stalking)* — использование лицом нежелательного и постоянно нацеленного на других людей онлайн-контента с целью контроля и/или запугивания (например, нежелательные и систематически продолжающиеся звонки и сообщения).

IX. *Киберпиратство,* пиратское программное обеспечение (*software piracy*), нарушения прав интеллектуальной собственности (*intellectual property infringements*) — незаконное использование или копирование платного ПО с нарушением авторских прав или лицензионных ограничений. Например, загрузка нелицензированной копии *Windows* и ее взлом; неправомерное использование в сети музыки, фильмов, фотографий и иных объектов авторских или смежных прав, патентных прав и прав на товарные знаки и др. [12].

X. *Мошенничество в социальных сетях* *(social media frauds)* — использование поддельных аккаунтов в социальных сетях для совершения любого рода неправомерных и вредоносных действий (выдача себя за других пользователей или отправка устрашающих сообщений, распространение спама по электронной почте).

XI. *Онлайн-торговля наркотиками* *(online drug trafficking)*. Существенный рост сбыта наркотиков в Интернете, особенно в «теневом Интернете» (*Darknet*) связан с развитием технологий криптовалют, облегчающих перевод денег и заключение сделок с наркотиками, не привлекая внимания правоохранительных органов.

XII. *Отмывание электронных денег* *(electronic money laundering)* — наиболее распространенный онлайн-бизнес, использующий противоправные способы оплаты и транзакции по кредитным картам или криптовалютам с предоставлением неполной или противоречивой платежной информации для приобретения запрещенных к обороту объектов или сокрытия источников финансирования, денежных средств.

XIII. *Кибервымогательство* (*cyber extortion*) — требование выкупа киберпреступниками за возврат неправомерно полученных ими важных документов или личных данных либо за прекращение совершения вредоносных действий (кибератаки типа «отказ в обслуживании»).

XIV. *Мошенничество с наймом на работу, подбором персонала онлайн* *(online recruitment fraud)* — получающее распространение киберпреступление, заключающееся в предложении онлайн поддельных трудовых вакансий, предоставляемых поддельными компаниями с целью получения финансовой выгоды от соискателей или даже использования их личных данных, по типу операции «программа-вымогатель как услуга»[12].

[11] URL: https://www.rbc.ru/society/12/12/2020/5fd446c49a7947746aba6e19

[12] L. Fair. Taking the "ploy" out of employment scams. January 25, 2023. URL: https://www.ftc.gov/business-guidance/blog/2023/01/taking-ploy-out-employment-scams

XV. *Мошенничество с банкоматами*, через которые многие люди получают наличные. Для доступа к учетной записи пользователь предъявляет карту и персональный идентификационный номер (ПИН — *PIN*). Преступники разработали средства для перехвата как данных на магнитной полосе карты, так и *PIN*-кода пользователя. В свою очередь, информация используется для создания поддельных карт, которые затем используются для снятия средств со счета ничего не подозревающего человека.

XVI. *Мошенническая романтическая афера (romance scam)*[13] — использование онлайн-приложений в соцсетях, мессенджерах или Интернете для романтического знакомства в мошеннических целях, где мошенники-любовники под различными предлогами выманивают деньги у лица за мнимое оказание услуги или для преодоления выдуманной сложной жизненной ситуации и др., либо личные фото и/или иную личную информацию для последующего шантажа.

XVII. *Мошеннические рекламные акции в Интернете*[14] **—** использование сомнительных заявлений для рекламы мошенниками столь же сомнительных продуктов: таблетки для похудения или лекарства от всех болезней, рекламные акции быстрого обогащения и др. Отличие таких рекламных акций в якобы одобрении рекламируемых продуктов знаменитостями или известными лицами в деловом мире. Например, Федеральная комиссия по торговле США в 2019 г. возбудила административное производство в защиту прав потребителей по факту ложной рекламы новостных сайтов «умных» таблеток *Geniux*, якобы повышающих деятельность мозга, с неправомерным использованием имен и фото Билла Гейтса и покойного профессора Стивена Хокинга[15] — обман, который стоил большого штрафа.

XVIII. *Нарушение сохранности данных несовершеннолетних* *в сети Интернет*[16]. *В* частности, в соответствии с Законом США о защите частной жизни детей в Интернете (Children's Online Privacy Protection Act of 1998, COPPA) операторы сайтов и онлайн-сервисов, ориентированных на детей (определение делается путем оценки предмета, визуального контента, использования анимированных персонажей или ориентированных на детей действий и стимулов, а также других факторов), которые собирают или хранят личную информацию детей младше 13 лет, обязаны среди прочего получить поддающееся проверке согласие родителей, прежде чем собирать, использовать или раскрывать личную информацию детей (включая полные имена, адреса электронной почты и имена пользователей). Нарушение этих требований закона владельцем популярной игры *Fortnite* (*Epic Games*) стало предметом расследования в 2019 г. Федеральной комиссией по торговле США, на которую возложен контроль за обеспечением защиты конфиденциальности детей в цифровом мире. Этот контроль распространяется не только на онлайн-игры, но и на защиту конфиденциальности детей в сфере онлайн-образования, оказание онлайн медицинских услуг и иных потребительских услуг. Следует заметить, что точная геолокация (данные о точном местоположении) детей при онлайн-играх, телереклама также подпадают под определение персональных данных, защищаемых *COPPA*[17].

XIX. *Кибертерроризм и экстремизм*. Интернет широко используется для пропаганды различных экстремистских идей и движений, кибермошенничества, информационных блокад, компьютерного шпионажа и иных противоправных действий [14, 15].

Особая сфера противоправных действий в сфере ИКТ — *кибервойна*, использование ложной, фейковой информации, обработка сознания человека и общества, целью которого может быть конкретное лицо (государственный или общественный деятель, популярный политик и др.), а также в целях получения глобального результата (массовые беспорядки или гражданское неповиновение, формирование негативного образа публичной власти и др.).

Однако следует заметить, что сфера кибервойны постоянно расширяется. Например, ряд исследований исходит из того, что культура как таковая определяется как коллективное программирование разума, которое отличает членов одной группы или категории людей от другой[18] [18], что оказывает огромное влияние на жизнь людей и в результате влияет на события, в которых участвуют представители разных культур. Распространение новостей представляет один из наиболее эффективных механизмов трансграничного распространения информации.

В связи с постоянно растущим числом событий, имеющих значительный международный резонанс, все бóльшее значение для профессионалов и исследователей во многих дисциплинах, включая цифровые гуманитарные науки, медиа-исследования и журналистику, приобретает *кросс-культурная аналитика*. Самые последние примеры таких событий включают COVID-19 и Brexit. Существует несколько детерминант, которые оказывают существенное влияние на процесс отбора,

---

[13] E. Fletcher. Romance scammers' favorite lies exposed. February 9, 2023. URL: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

[14] L. Fair. A warning to marketers about testi-phony-als, including ads falsely claiming a "Shark Tank" connection. February 17, 2023. URL: https://www.ftc.gov/business-guidance/blog/2023/02/warning-marketers-about-testi-phony-als-including-ads-falsely-claiming-shark-tank-connection

[15] URL: https://www.ftc.gov/business-guidance/blog/2019/04/bogus-celebrity-testimonials-and-phony-formats-donts-advertisers-and-affiliates

[16] L. Fair. Record-setting FTC settlements with Fortnite owner Epic Games are the latest "Battle Royale" against violations of kids' privacy and use of digital dark patterns. December 19, 2022. URL: https://www.ftc.gov/business-guidance/blog/2022/12/record-setting-ftc-settlements-fortnite-owner-epic-games-are-latest-battle-royale-against-violations

[17] L. Fair. Updating you on FTC privacy and data security initiatives. 25 May, 2021. URL: https://www.ftc.gov/business-guidance/blog/2021/05/updating-you-ftc-privacy-data-security-initiatives

[18] Abdul Sittar, Dunja Mladenic. Classification of Cross-cultural News Events. January 2023. URL: https://arxiv. org/abs/2301.05543

анализа и распространения информации. К ним относятся культурные ценности и различия, экономические условия и связи между странами. Например, если две страны более схожи в культурном отношении, больше шансов, что между ними будет более интенсивный поток новостей. Анализ новостных событий может применяться с использованием реестра событий, т. е. системы, которая анализирует новостные статьи, идентифицирует группы статей, описывающих одно и то же событие, и представляет их как единое событие.

Рассматривая позицию Международного валютного фонда, как отмечается в исследованиях [7], следует поддержать призыв международного сообщества к решению вопроса регулирования цифровых валют как стратегически важного этапа развития мировой экономики, поскольку цифровая валюта может использоваться для легализации денежных средств, полученных преступным путем и кибермошенничеством.

Российское законодательство и правоприменение в сфере противодействия киберпреступности

В настоящее время киберпреступность является одной из наиболее серьезных угроз национальной безопасности Российской Федерации в информационной сфере. Эксперты отмечают [3, 4, 13] особые характеристики киберпреступности: высокая латентность, специальная подготовка преступников, трансграничность, автоматизированность преступлений, нетрадиционность средств противодействия киберпреступности.

Российское законодательство и судебная практика определили группы преступлений, связанных с использованием современных компьютерных технологий, которые формируют особую группу преступлений — *преступления в сфере компьютерной информации* (по состоянию на июль 2022 г.): неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ИТС) (ст. 274); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1), а также нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации ИТС Интернет и сети связи общего пользования (ст. 274.2).

Важной вехой формирования *единой судебной практики* стало Постановление Пленума Верховного Суда РФ от 15 декабря 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 ИТС, 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 УК РФ, а также за иные преступления, совершенные с использованием электронных или ИТС.

Постановление разъяснило понятие «компьютерной информации» в ст. 272 УК РФ, которая включает любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Эти 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 др.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электросвязи. 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 гл. 28 УК РФ определений, включая следующие:

- *компьютерной программой* с учетом положений ст. 1261 ГК РФ 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 является 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 является 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 др.);
– *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 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 ч. 1 ст. 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, т. е. заведомо для лица, совершающего указанные действия, предназначенные 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*[19] [10], т. е. 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).

Особая ответственность установлена за незаконное воздействие на критическую информационную инфраструктуру (ст. 274.1 УК РФ), что представляет собой нарушение установленных законом и подзаконными актами правил, 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 ст. 2 Федерального закона от 26 июля 2017 г. № 187- ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В ином случае действия лица при наличии на то оснований могут быть квалифицированы по ст. 273 УК РФ.

В сфере противодействия киберпреступности особое значение имеют: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26 июля 2017 г. № 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 2001 г. 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 пра-

[19] Начиная с 70-х гг. прошлого века несанкционированный доступ к особо привилегированной информации осуществляется, как правило, по так называемым скрытым каналам (covert channel), эффективная защита от которого представляется крайне затруднительной. См.: ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. М. : Ростехрегулирование, 2008. 24 с.; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 2. Рекомендации по организации защиты. М. : Ростехрегулирование, 2009. 26 с.

ва, а равно присвоение авторства, если это деяние причинило существенный ущерб[20].

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 ИТС. При этом Пленум Верховного Суда РФ от 30 ноября 2017 г. № 48[21] (в ред. от 29.06.2021) указал, что под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или ИТС 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 ПО, или на ИТС, 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, то, 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 др.), оно подлежит квалификации как кража, если виновным не было оказано незаконного воздействия на ПО серверов, компьютеров или на сами ИТС. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, произошедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием. Если же хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в ИТС, включая сеть Интернет (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159, а не по ст. 159.6 УК РФ.

В соответствии с Кодексом об административных правонарушениях (КоАП) РФ установлена ответственность за административные правонарушения в области связи и информации (гл. 13 КоАП РФ), которые предусматривают административную ответственность, в том числе за нарушение правил защиты информации (ст. 13.12), нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (ст. 13.12.1), злоупотребление свободой массовой информации (ст. 13.15), нарушение порядка ограничения доступа к информации, информационным ресурсам, доступ к которым подлежит ограничению в соответствии с информационным законодательством Российской Федерации, и (или) порядка удаления указанной информации (ст. 13.41), нарушение требований законодательства к установке технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации ИТС 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), и др.

Особое регулирование осуществляется в сфере оборота персональных данных: принят Федеральный закон от 27 июля 2006 г. № 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.

Заключение

Особенности современной киберпреступности проявляются в следующем:

- мотивы и цели совершения преступления — использование цифровых технологий и компьютерных устройств для достижения противоправных целей;
- место совершения преступления — определяется глобальным, трансграничным характером преступности в силу трансграничности Интернета, *IT* и цифровых технологий;
- способы (средство) совершения преступлений — использование технологически нейтральных *IT* и цифровых технологий для достижения самых различных противоправных целей от кражи или мошенничества до преступлений против государственного строя и военных преступлений;
- субъекты совершения преступлений — преступления могут совершаться как отдельными физическими лицами или группой лиц, так и специалистами (хакерами) или хакерскими организованными сообществами в Интернете, а в отдельных случаях — с использованием средств (технологий или объектов), принадлежащих другим лицам без их ведома и согласия.

[20] URL: http://www.cis.minsk.by/page.php?id=866

[21] См.: Пункт 20 Постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2018. № 2. Фев.

*Рецензент: Т**ерентьева Людмила Вячеславовна,** доктор юридических наук, доцент, доцент кафедры международного частного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА).*
E-mail: terentevamila@mail.ru

Литература

1. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5. С. 39—42.
2. Глазов Б.И., Ловцов Д.А. Информационная борьба как система отношений в информационной среде // Военная мысль. 1997. № 5. С. 36—41.
3. Государство и право в новой цифровой реальности : монография / Под общ. ред. И.А. Конюховой-Умновой, Д.А. Ловцова. М. : ИНИОН РАН, 2020. 259 с. ISBN 978-5-248-00959-6.
4. Далгалы Т.А. Киберкриминология: вызовы XXI века // Российская юстиция. 2020. № 10. С. 19—21.
5. Запольский С.В., Пестрикова А.А., Сморчкова Л.Н. Информационно-правовой режим получения, хранения и использования биологического материала человека // Правовая информатика. 2022. № 4. С. 4—14. DOI: 10.21681/1994-1404-2022-4-4-14 .
6. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1. С. 28—44.
7. Кузнецова А.Д., Калмакова Н.А. Становление законодательной базы Российской Федерации в сфере оборота криптовалюты: цифровизация рубля // Финансовое право. 2022. № 3. С. 21—24.
8. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
9. Ловцов Д.А., Галахова А.Е. Защита интеллектуальной собственности в сети Интернет // Информационное право. 2011. № 4 (27). С. 13—20.
10. Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 2. Информ. процессы и системы. 2006. № 9. С. 1—9.
11. Ловцов Д.А., Князев К.В. Защищённая биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100—103.
12. Мельников В.С. Защита авторских и смежных прав в сети Интернет: проблемы теории и правоприменительной практики // Российское правосудие. 2013. № 5 (85). С. 46—56.
13. Мордвинов К.В., Удавихина У.А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1 (11). С. 83—88.
14. Савенкова Д.Д. Правовое обеспечение информационной безопасности Российской Федерации и развитие института ответственности за правонарушения в информационной сфере // Динамика институтов информационной безопасности. Правовые проблемы : сб. науч. трудов / Отв. ред. Т.А. Полякова, В.Б. Наумов, Э.В. Талапина. М. : Канон Плюс, РООИ «Реабилитация», 2018. С. 118—124.
15. Смирных С.Е. Международная информационная безопасность как гарантия осуществления права народов на самоопределение // Международное право и международные организации. 2022. № 2. С. 20—30.
16. Терентьева Л.В. Понятие киберпространства и очерчивание его территориальных контуров // Правовая информатика. 2018. № 4. С. 66—71. DOI: 10.21681/1994-1404-2018-4-66-71 .
17. Терентьева Л.В. Управление киберпространством в условиях противостояния России и стран североатлантического альянса // Правовая информатика. 2022. № 3. С. 51—60. DOI: 10.21681/1994-1404-2018-3-51-60 .
18. Rampersad G., Althiyabi T. Fake news: acceptance by demographics and culture on social media. Journal of Information Technology & Politics, 2020, 17.1, pp. 1–11.

LEGAL ASPECTS OF MODERN CYBERCRIME

***Aleksandr Kartskhiia,** Ph.D. (Law), Acting Head of the Department of Legal Support for Fuel and Energy Industry Security of Gubkin Russian State University of Oil and Gas, Moscow, Russian Federation.*
E-mail: arhz50@mail.ru

***Keywords:** cyberattacks, cybercrime, cyber security, information and communication technologies (ICT), digital technologies, software, fraud, information and telecommunication networks (ITN), Internet, crossborderness, personal data, sphere of computer information.*

Abstract

Purpose of the paper: identifying topical legal aspects and specific features of cybercrime in the sphere of information and communication technologies (ICT) considering Russian and foreign experience and law enforcement practice.

Methods used: comparative legal analysis of current Russian and foreign laws and the practice of applying them as well as formal logical analysis of the conceptual framework, content and structure of the subject under study.

Study findings: a system of formalised views on offences and crimes committed using computers, information and communication equipment and means including software is proposed, to the end of understanding the legal content of the concept of cybercrime. New ways to commit crimes in cyberspace are studied and new objects of cybercrime are identified. It is found that cyber incidents hold a leading position within the group of risks related to the development of modern digital economy, a growing threat from ransomware and cyber fraud as well as geopolitical rivalry and conflicts happening ever more often in cyberspace. A conclusion is justified that a new, special type of crime is emerging, that is, crime in the field of cyber security and ICT, which poses a problem of developing technological and legal support for efficient regulation of relations in this sphere.

References

1. Alpeev A.S. Terminologiia bezopasnosti: kiberbezopasnost', informatsionnaia bezopasnost'. Voprosy kiberbezopasnosti, 2014, No. 5, pp. 39–42.
2. Glazov B.I., Lovtsov D.A. Informatsionnaia bor'ba kak sistema otnoshenii v informatsionnoi srede. Voennaia mysl', 1997, No. 5, pp. 36–41.
3. Gosudarstvo i pravo v novoi tsifrovoi real'nosti : monografiia. Pod obshch. red. I.A. Koniukhovoi-Umnovoi, D.A. Lovtsova. M. : INION RAN, 2020. 259 pp. ISBN 978-5-248-00959-6.
4. Dalgaly T.A. Kiberkriminologiia: vyzovy XXI veka. Rossiiskaia iustitsiia, 2020, No. 10, pp. 19–21.
5. Zapol'skii S.V., Pestrikova A.A., Smorchkova L.N. Informatsionno-pravovoi rezhim polucheniia, khraneniia i ispol'zovaniia biologicheskogo materiala cheloveka. Pravovaia informatika, 2022, No. 4, pp. 4–14. DOI: 10.21681/1994-1404-2022-4-4-14 .
6. Kartskhiia A.A., Makarenko G.I. Pravovye aspekty sovremennoi kiberbezopasnosti i protivodeistviia kiberprestupnosti. Voprosy kiberbezopasnosti, 2023, No. 1, pp. 28–44.
7. Kuznetsova A.D., Kalmakova N.A. Stanovlenie zakonodatel'noi bazy Rossiiskoi Federatsii v sfere oborota kriptovaliuty: tsifrovizatsiia rublia. Finansovoe pravo, 2022, No. 3, pp. 21–24.
8. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
9. Lovtsov D.A., Galakhova A.E. Zashchita intellektual'noi sobstvennosti v seti Internet. Informatsionnoe pravo, 2011, No. 4 (27), pp. 13–20.
10. Lovtsov D.A., Ermakov I.V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. NTI, ser. 2. Inform. protsessy i sistemy, 2006, No. 9, pp. 1–9.
11. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2013, No. 1, pp. 100–103.
12. Mel'nikov V.S. Zashchita avtorskikh i smezhnykh prav v seti Internet: problemy teorii i pravoprimenitel'noi praktiki. Rossiiskoe pravosudie, 2013, No. 5 (85), pp. 46–56.
13. Mordvinov K.V., Udavikhina U.A. Kiberprestupnost' v Rossii: aktual'nye vyzovy i uspeshnye praktiki bor'by s kiberprestupnost'iu. Teoreticheskaia i prikladnaia iurisprudentsiia, 2022, No. 1 (11), pp. 83–88.
14. Savenkova D.D. Pravovoe obespechenie informatsionnoi bezopasnosti Rossiiskoi Federatsii i razvitie instituta otvetstvennosti za pravonarusheniia v informatsionnoi sfere. Dinamika institutov informatsionnoi bezopasnosti. Pravovye problemy : sb. nauch. trudov. Otv. red. T.A. Poliakova, V.B. Naumov, E.V. Talapina. M. : Kanon Plius, ROOI "Reabilitatsiia", 2018, pp. 118–124.
15. Smirnykh S.E. Mezhdunarodnaia informatsionnaia bezopasnost' kak garantiia osushchestvleniia prava narodov na samoopredelenie. Mezhdunarodnoe pravo i mezhdunarodnye organizatsii, 2022, No. 2, pp. 20–30.
16. Terent'eva L.V. Poniatie kiberprostranstva i ocherchivanie ego territorial'nykh konturov. Pravovaia informatika, 2018, No. 4, pp. 66–71. DOI: 10.21681/1994-1404-2018-4-66-71 .
17. Terent'eva L.V. Upravlenie kiberprostranstvom v usloviiakh protivostoianiia Rossii i stran severoatlanticheskogo al'iansa. Pravovaia informatika, 2022, No. 3, pp. 51–60. DOI: 10.21681/1994-1404-2018-3-51-60 .
18. Rampersad G., Althiyabi T. Fake news: acceptance by demographics and culture on social media. Journal of Information Technology & Politics, 2020, 17.1, pp. 1–11.