УДК 343.97 DOI: 10.14451/2.183.15

Современные методы противодействия компьютерной преступности

© 2023 **Агаджанян Армен Аркадьевич**
Адвокат. Адвокатская палата Краснодарского Края.
E-mail: a65303980@gmail.com

Ключевые слова: развитие права, цифровая среда, современная компьютерная преступность, криминологические тенденции, противодействие компьютерной преступности.

Важность и актуальность проблемы, поднимаемой в данном исследовании, объясняются несколькими существенными правовыми и общественными трудностями, которые делают недостаточно результативными меры по предотвращению противозаконных действий в цифровой компьютерной среде. Величина урона, который приносят отечественной экономике данные правонарушения, выходит за рамки понимания. В качестве объекта исследования выступает анализ криминологических тенденций, связанных с появлением, развитием и прогрессом российской преступности в цифровой среде, а также изучение юридических аспектов, касающихся борьбы с данными противозаконными общественными действиями. Главной целью нашего исследования является формирование методической, правовой и прикладной базы для борьбы с противозаконными действиями в цифровой компьютерной среде в России, особенно с учетом тенденции ее превращения в неуправляемое технокриминальное явление. Методологическая основа строится на диалектическом подходе и использовании комплекса общенаучных и частных методов исследования. Научная новизна работы заключается в определении направлений и формулировании конкретных мер по борьбе с противозаконными действиями в цифровой среде, а также действий по профилактике, снижению и ликвидации возможностей реализации преступлений в области информационных технологий на территории России.

В настоящее время в нашей стране четко прослеживается негативный тренд в развитии противозаконных действий в цифровой среде. Эта динамика охватывает разнообразные аспекты такой преступности, включая её состав, понятие, различные характеристики, а также другие факторы. Эти изменения приводят к тому, что компьютерная преступность становится все более технологически сложной, скрытой, носящей международный характер, организованной, ориентированной на экономическую выгоду и даже вмешательство в политические процессы. Важно подчеркнуть, что уровень урона, который такие противозаконные действия наносят России, продолжает увеличиваться [7, с. 76].

На взгляд автора, в качестве наиболее перспективного способа противостояния данной негативной динамике, особенно в контексте её превращения в технотронную форму, является развитие отечественного уголовного правового поля. Такой подход считается результативным

инструментом в рамках всей системы противодействия таким противозаконным поступкам.

На данный момент актуальность борьбы с нарушениями законодательства в компьютерной среде на территории Российской Федерации неоспорима, так как ее последствия наносят существенный ущерб как экономическим, так и социальным сферам. Однако следует отметить, что в процессе уголовного преследования граждан, нарушивших закон в данной области, возникают определенные правовые трудности [12, с. 401].

Существует неопределенность в толковании некоторых ключевых терминов, прописанных в статьях 272–2741 Уголовного кодекса Российской Федерации. Такие термины, как «вредоносная компьютерная программа» и ряд других, содержащихся в данной статье, не имеют четких, закрепленных в законодательстве определений.

Несмотря на эти сложности, результативность уголовного преследования нарушений законодательства в компьютерной среде может обеспечиваться через регулярное развитие и улучшение уголовного законодательства, принимая во внимание развитие российского общества, динамику цифровых процессов, а также продолжающиеся активности в области формирования, накопления, анализа и передачи цифровых данных и методов их незаконного использования [2, с. 79].

На данный момент недостаток четких рекомендаций российского Пленума Верховного Суда относительно дел, связанных с нарушениями законодательства в цифровых технологиях, приводит к недоразумениям и разночтениям в правоприменении. Это сбивает с толку многих судей, прокуроров и работников правоохранительных структур при выявлении подобного рода противозаконных действий на различных этапах уголовного разбирательства.

Исходя из накопившегося судебного опыта в делах о нарушениях законодательства в цифровой сфере, необходимо выделить наиболее существенные трудности, которые встают перед правоохранительными структурами в данной области.

Согласно приведенной выше информации, в качестве часто осуществляемого нарушения законодательства в сфере информационных технологий, особенно при тенденции их превращения в технотронную форму, является DDoS-атака на веб-сайты или порталы государственных органов, СМИ, различных корпораций и так далее. Содержание этого противозаконного действия заключается в применении специальных вредоносных программ, посылающих на серверы корпоративных цифровых комплексов огромное число запросов от несуществующих пользователей. Серверы, в свою очередь, не могут справиться с такой нагрузкой, что ведет к их блокировке или создает серьезные проблемы с доступом к сайтам или порталам для обычных граждан. Эти преступления чаще всего реализуются за счет использования больших локально-вычислительных сетей, так называемых bot-сетей. Такие сети представляют собой группы ПЭВМ, зараженные компьютерными вирусами, которые дают возможность нарушителю закона управлять ими удаленно, без согласия и уведомления их собственников с целью проведения атак на целевые Интернет-ресурсы [3, с. 158].

Проведение исследования судебных действий приводит к заключению, что существует разногласие в решениях относительно оптимального определения DDoS-атак в рамках уголовного законодательства.

Некоторые судебные органы определяют данный вид преступлений как нарушение статьи 272 Уголовного кодекса Российской Федерации, которая регулирует незаконный доступ к законодательно защищенным цифровым данным. Другие суды ориентируются на статью 273 Уголовного кодекса, которая предусматривает применение вредоносного программного обеспечения с целью незаконного изъятия, изменения и прочих противозаконных действий с цифровыми данными или обхода методов их защиты.

По мнению автора, более точной характеристикой DDoS-атаки является статья 273 Уголовного кодекса Российской Федерации, так как она

наилучшим образом отражает специфику и механизм этого преступления. Точка зрения автора заключается в том, что необходимо разъяснение определения DDoS-атаки в решении российского Пленума Верховного Суда, посвященного судебной работе в области противозаконных действий, связанных с цифровыми данными.

Итак, рассматриваемое преступление характеризуется применением некоторого вредоносного программного обеспечения (или вируса) с целью противозаконного воздействия на защищенные цифровые данные. По мнению автора, нет необходимости во вспомогательной квалификации таких поступков в соответствии со статьей 272 Уголовного кодекса Российской Федерации, так как с правовой позиции, преступники взаимодействуют с веб-ресурсами, находящимися в общем доступе и предназначенными для оказания комплекса услуг, получения сведений или обмена сообщениями, что не нарушает законодательство [5, с. 23].

Согласно ранее упомянутой информации, данное противозаконное действие реализуется с помощью вредоносного программного обеспечения, и вся объективная сторона преступления описывается в части 1 статьи 273 Уголовного кодекса Российской Федерации.

Тем не менее, важно отметить, что при незаконном воздействии на цифровые данные, отнесенные к категории критических для России, поступки нарушителя закона рассматриваются согласно части 1 статьи 2741 Уголовного кодекса Российской Федерации. Это означает применение цифровых технологий, преднамеренно разработанных для незаконных атак на критические цифровые объекты России, включая DDoS-атаки, незаконное изъятие, изменение и прочие противозаконные действия.

Судьи, прокуроры и сотрудники правоохранительных органов сталкиваются с рядом непростых проблем, связанных с классификацией преступлений в области цифровых данных. Некоторыми из таких дискуссионных вопросов является следующие: стоит ли позиционировать, как уничтожение цифровых данных, действие, при котором они изначально были стерты (удалены), но затем восстановлены? Как правильно определить удаление цифровых данных с применением мощных излучений, которые физически не повреждают источник их хранения? Можно ли рассматривать как операцию копирования цифровых данных такие поступки злоумышленника, когда он создает их дубликат, например, путем печати данных или осуществления фото- и видеосъемки экрана монитора? [9, с. 137]

Также возникает важный вопрос о том, как правильно определять противозаконный доступ к цифровым данным. Например, когда злоумышленник запоминает защищенные данные (личную информацию, банковские счета, номера пластиковых карт, адреса электронной почты и т. д.), а затем переносит их на другой источник хранения, формируя таким образом дубликат (например, записывая на бумагу, на жесткий диск ПЭВМ или любого вида гаджета).

Автор придерживается точки зрения, что вышеупомянутые сценарии представляют собой специфические варианты неправомерного воздействия на защищенные цифровые данные, что является преступлением и доказывается юрисдикцией судебных органов.

Исследование опыта рассмотрения уголовных дел и судебной практики дает возможность сделать вывод, что в ситуации, где не применяется постановление российского Пленума Верховного Суда, регулирующее порядок рассмотрения дел, связанных с нарушениями в области цифровых данных, судебные органы не каждый раз используют или вовсе не используют положения статей 183 и 187 Уголовного кодекса Российской Федерации. Это особенно актуально в контексте множества случаев хищения денег из банкоматов и цифровых средств со счетов кредитных организаций, когда злоумышленники используют фальшивые банковские карточки или электронные устройства, что в конечном итоге приводит к разглашению законодательно защищенной банковской информации [9, с. 95].

В некоторых случаях с целью извлечения выгоды злоумышленники, размещая так называемые

«скиммеры» на банкоматах, создают дубликаты данных с пластиковых карточек обычных граждан. Это не только дает им доступ к личным сведениям о клиентах банка, но и к информации, содержащейся в банковской тайне (например, номера договора, банковского счета, величина остатка по счету, хранимая на карточке и счетах, сведения о финансовых операциях, осуществлявшихся по пластиковой карточке, пин-коды и прочее).

В результате реализации таких действий, возникает нарушение отечественного законодательства, охваченное частью 3 статьи 183 Уголовного кодекса, а именно — незаконное получение информации, входящей в сферу банковской тайны, с целью личной выгоды.

В дальнейшем ходе развития событий, злоумышленники создают фальшивые банковские карты и несанкционированно записывают на них добытые данные. Далее они используют эти банковские карты для извлечения наличных денег из банкоматов или для их удаленных транзакций на собственные счета, осуществляя таким образом незаконные финансовые операции.

На взгляд автора исследования, в таких ситуациях поступки злоумышленников попадают под действие части 1 статьи 187 Уголовного кодекса, а именно, под пункты, касающиеся создания, хранения, перемещения для применения фальшивых банковских карточек, а также технических устройств, программного обеспечения и прочих средств, предназначенных для незаконных финансовых операций [4, с. 79].

По мнению автора, если «скиммеры» используют созданные фальшивые пластиковые карточки для извлечения средств из банкоматов, то, принимая во внимание решения российского Верховного Суда, поступки злоумышленников должны рассматриваться как комплекс противозаконных действий, и, следовательно, подпадать под такие статьи Уголовного кодекса, как статьи о краже, незаконном доступе к компьютерной информации, использовании вредоносных программ и др.

Важно акцентировать, что существует разнообразие судебных решений в отношении определения преступлений, связанных с кражей денег из банкоматов с применением специального программного обеспечения.

Проблемой в определении таких действий судебными органами, где имущественное правонарушение осуществляется через незаконный доступ к цифровым данным и применение программного обеспечения, а также других информационно-технических средств, остается неоднозначной и пока не имеет четкого разрешения в решениях Верховного Суда.

В Постановлении №6 Пленума Верховного Суда, принятого 5 апреля 2012 года, касающегося предложений по совершенствованию Уголовного кодекса и других правовых актов, можно выделить интересный аспект. В частности, речь идет о создании отдельной категории противозаконных действий в области цифровых данных, а именно — мошенничества, согласно статье 1596 Уголовного кодекса. Подобные деяния характеризуются не стандартными методами обмана или использования доверчивости людей, а доступом к цифровым технологиям и проведением операций, которые подразумевают вмешательство в компьютерные данные и информационные системы. По сути, такие действия приводят к незаконному приобретению имущества или прав на него, и все это реализуется через получение доступа к компьютерным системам, а не через типичные методы мошенничества или нарушения доверия конкретных лиц [6, с. 195].

Однако, невзирая на то, что, с позиции автора, использование статьи 1596 Уголовного кодекса Российской Федерации комплексно охватывает правовую оценку противозаконных действий, связанных с кражей имущества или прав на него при помощи различного вида операций с цифровыми данными или вмешательства в работу технических средств, обеспечивающих накопление, хранение и движение цифровых данных и компьютерных сетей, российский Верховный Суд поменял свою точку зрения по этому вопросу в своем решении от 30 ноября 2017 года № 48.

В рамках данного решения Верховный Суд настоятельно рекомендовал судебным органам рассматривать факт хищения денег, совершенный с использованием фальшивых банковских карточек, как традиционную кражу, в случае, если наличные финансовые средства были получены злоумышленником через банкомат без каких-либо действий со стороны работника банка.

Также он признал необходимым квалифицировать такие случаи, как хищение чужих денежных средств, когда злоумышленник получил доступ к законодательно защищенным сведениям владельца банковской карточки (например, личные данные, номер карты, контрольные данные, пин-код), предоставленные непосредственным владельцем данной карты под влиянием обманных действий или из-за излишней доверчивости.

Кроме того, указывается, что хищение денежных средств, осуществленное с помощью применения личной информации собственника имущества, вне зависимости от способа обретения этой информации (например, злоумышленник использовал смартфон человека с установленным банковским приложением, прошел идентификацию в платежной системе с помощью переданных личных данных и так далее), должно квалифицироваться по статье 159 Уголовного кодекса Российской Федерации, если такое действие было реализовано вследствие предоставления изначально ложной информации в компьютерных сетях (через «фишинговые» сайты, поддельные e-mail, торговые площадки и т.д.) [10, с. 154].

Итак, согласно авторской позиции, решение российского Верховного Суда абсолютно игнорирует устоявшуюся судебную деятельность в период с 2015 по 2017 год. Оно связано с использованием статьи 1596 Уголовного кодекса Российской Федерации в делах, связанных с хищением денег из банкоматов с использованием фальшивых банковских карточек. Это также включает в себя ситуации, где с банковских счетов осуществляется хищение при помощи «мобильного банка» или при использовании данных для входа, таких как логины и пароли. Важно подчеркнуть, что подавляющее большинство таких действий в области цифровых данных на территории РФ были осуществлены именно с использованием таких методов.

Наши рассуждения основаны на том, что отказ от использования статьи 1596 Уголовного кодекса Российской Федерации в таких ситуациях, и, следовательно, от добавочного определения противозаконных действий согласно части 2 статьи 272 Уголовного кодекса или части 2 статьи 273 Уголовного кодекса, является существенным упущением. Это вызывает вопросы об актуальности интеграции в Уголовный кодекс нормы, делающей преступлением факт мошенничества в области цифровых данных, как было рекомендовано Верховным Судом [11, с. 152].

Более того, проблемы в особенностях определения противозаконных действий согласно статье 274 Уголовного кодекса Российской Федерации и в актуальности уголовного преследования за пренебрежение нормами использования технических средств накопления или передачи цифровых данных, вызывает оживленные дебаты в научных кругах. Некоторые эксперты придерживаются мнения, что рассматриваемый вид противозаконных действий не требуется в российском Уголовном кодексе и его следует переквалифицировать в разряд административных, так как необходимые задачи можно реализовать с использованием административных процедур и инструментов.

Автор данного исследования придерживается абсолютно противоположного мнения и полностью поддерживает точку зрения экспертов, рассматривающих нарушения пренебрежения нормами использования технических средств как социально небезопасные поступки, в ряде случаев позиционируя их даже как форму цифрового бунта.

Трудности, связанные с определением цифровых противозаконных действий во время следствия и судебного разбирательства, подчеркивают высокую актуальность немедленной разработки Верховным Судом решения, касательно особенностей судебной практики в области цифровых противозаконных действий. Это необхо-

димо для получения более высокого результата борьбы с нарушениями закона в цифровой среде в рамках уголовного законодательства.

Также автор придерживается позиции, что статья 273 Уголовного Кодекса, касающаяся разработки и применения вредоносного программного обеспечения, недостаточно учитывает характер и суть указанных преступлений.

По авторскому мнению, применение так называемых «компьютерных ботов», актуально лишь на начальной стадии, когда ПЭВМ заражаются и формируется «ботнет». Однако после создания «ботнета» злоумышленники могут осуществлять незаконный доступ и дистанционное управление данными ПЭВМ. Следовательно, они перестают пользоваться этими вирусами, а вместо этого обращаются к ресурсам зараженных ПЭВМ для реализации противозаконных действий. Этот аспект не учтен в статьях 272 и 273 Уголовного Кодекса Российской Федерации [8, с. 23].

Следовательно, автор утверждает, что применение «ботнетов» является отдельным преступлением, определяющимся созданием и использованием «кибероружия» для осуществления различных видов противозаконных действий. Автор также предлагает ужесточить наказание за цифровые преступления, особенно, когда они имели серьезные последствия или сформировали такую угрозу. Высшее наказание предлагается ограничить 15 годами лишения свободы.

Данные инициативы позволят улучшить законодательство России в сфере борьбы с цифровой преступностью, делая его более соответствующим текущим вызовам и более результативным в противодействии таким видам противозаконной деятельности.

Библиографический список

1. *Аносов А. В.* Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Труды Академии управления МВД России. — 2018. — 4 (48). — С. 93—97.
2. *Воронин Ю. А.* Преступления в сфере обращения цифровой информации и их детерминанты // Виктимология. — 2020. — 1 (23). — С. 74—80.
3. *Иванова Л. В., Пережогина Г. В.* Цифровое пространство как место совершения преступления в условиях глобальных ограничений // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. — 2020. — Т. 6, № 4. — С. 155—171.
4. *Каримов А. М.* Преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационно-коммуникационных технологий: сравнительно-правовой аспект // Вестник Казанского юридического института МВД России. — 2023. — 1 (51). — С. 75—82.
5. *Кондрашов А.* Искусственный интеллект идет в разведку. Как спецслужбы используют новейшие технологии // Аргументы недели. — 2019. — 25 (669). — С. 19—28.
6. *Пинкевич Т. В., Рахманова Е. Н.* Понятие цифровой преступности // Современные тенденции управления и цифровая экономика: от регионального развития к глобальному экономическому росту : Материалы 2-й Международной научно-практической конференции. — Москва, 2020. — С. 193—196.
7. *Поляков В. В., Милич И. Д.* Применение методов машинного обучения в криминалистике на примере противодействия высокотехнологичной преступности // Проблемы правовой и технической защиты информации. — 2020. — № 8. — С. 73—80.
8. *Поляков И. В.* Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. — 2020. — № 4. — С. 21—25.
9. *Смольянинов Е. С., Воронин М. Ю.* Проблемы реализации уголовной политики по противодействию преступлениям в сфере высоких технологий // Вестник РГГУ. Серия: Экономика. Управление. Право. — 2018. — 3 (13). — С. 134—141.
10. *Топольскова И. А.* Усовершенствование методов противодействия преступност // Вестник Луганской академии внутренних дел имени Э. А. Дидоренко. — 2023. — 1(14). — С. 150—158.
11. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения / Ю. В. Грачева [и др.] // Lex russica (Русский закон). — 2020. — 1 (158). — С. 145—159.
12. Цифровизация уголовной политики как инструмент преодоления ее асистемности / С. В. Максимов [и др.] // Всероссийский криминологический журнал. — 2019. — Т. 13, № 3. — С. 395—407.