Батюкова Вера Евгеньевна

ст. научный сотрудник сектора уголовного права,
уголовного процесса и криминологии
Федерального государственного бюджетного учреждения
науки Институт государства и права Российской академии наук
(ИГП РАН),
119019 Москва, ул. Знаменка, д.10
к.ю.н., доцент
e-mail: Batuykova@yandex.ru

Киберпреступность в условиях пандемии COVID-19.

Настоящее время- эпоха расцвета информационного общества. Время, когда во все сферы жизни проникли информационные технологии, связанные со сверхбыстрой передачей данных, их хранением и обработкой в огромных масштабах. Так, человечество создало и поставило себе на службу технологии, которые предыдущие поколения и представить себе не могли, принесшие с собой невероятные возможности и огромные проблемы, так как новая, стремительно развивающаяся отрасль, которую можно при желании назвать «новой реальностью» в прямом и переносном смысле, открывает людям доселе невиданные возможности для совершения преступлений. Все большее количество населения становятся жертвами мошенников, особенно это обострилось во время пандемии COVID-19. Изощренными стали формы девиантного поведения в киберпространстве, все больше становится жертв такого поведения, однако, меры, направленные на противодействие таких преступных действий не приводят к желаемому результату.

В современном мире киберпреступность является опасностью, угрожающей всему миру, России в том числе. Малочисленная группа преступников может посягать на безопасность тысяч обычных людей и даже целых государств. Количество преступлений в киберпространстве растет пропорционально увеличению числа людей, так или иначе взаимодействующих в своей жизни с информационными технологиями и

пользующихся компьютерными сетями. Также проблемой является то, что появление любых новых технологий вызывает расширение сфер для действия киберпреступников и создает условия для повышения эффективности производимых ими атак. Киберпреступность- результат глобализации, расширения международных информационных сетей и развития IT-технологий. В результате, IT-преступность показывает наибольший среди других видов преступности рост.

Также исследователями отмечается высокий уровень латентности киберпреступлений в следствие несовершенства правового регулирования, недостаточности технических средств и, как уже ранее отмечалось, сверхбыстрого роста и развития данного типа преступности. В связи с чем, точную статистику по всем IT-преступлениям составить практически невозможно.

Законодательного закрепления понятие киберпреступности не имеет. В своей работе В.А. Номоконов и Т.Л. Тропин определяют киберпреступность как: ««преступность, связанную как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей»¹.

Самый распространенный вид преступлений в сфере информационных технологий - это хищение. Мошенничество совершается путем обмана или злоупотребления доверием, под воздействием которых имущество или право на него может быть передано владельцем другим лицам. Одной из тенденций в этой области преступности является все более широкое использование телефонов, мобильной связи и других устройств для доступа к конфиденциальной информации, в частности, за счет использования вредоносного программного обеспечения, предназначенного для кражи средств с банковских счетов с использованием систем мобильного банкинга и различных типов социальной инженерии.

¹ Номокова В.А. Киберпреступность как новая криминальная угроза / В.А. Номокова, Т.Л. Тропина. – 2012.

Согласно данным, приведенным в отчете о состоянии преступности, составленном Генеральной Прокуратурой Российской Федерации на январь-март 2021 года, в первом квартале зарегистрировано примерно 85 тысяч различных мошенничеств, составив 17% в структуре всей преступности. Почти 70% из них были совершены с использованием информационно-коммуникационных технологий или в сфере компьютерной информации. Также отмечается их значительный прирост (+33,7%) по сравнению с предыдущим периодом. Отмечается, что в 1,7 тысяч случаев жертвами стали несовершеннолетние, в 17,2 тысячах - пенсионеры¹.

Правовые системы многих стран мира имеют ряд механизмов и норм, противодействующих мошенничеству с применением информационных технологий. В Российском праве подобной нормой выступает статья 159. 6 Уголовного кодекса. В ней дается понятие мошенничества в сфере компьютерной информации, носящее описательный и криминологический характер.

Все киберпреступления можно разделить на две группы. Первая - преступления, где компьютерная информация является предметом преступления. В данном случае преступниками используется различное вредоносное программное обеспечение, целью которого является заражение устройства и остановка или повреждение их работы. Такие действия принято называть атаками отказа в обслуживании или DoS. Вторую группу составляют преступления, в которых информация является лишь средством для их совершения².

Интернет-мошенничество представляет собой совокупность преступлений, которые характеризуются единством способа совершения, а

¹ Состояние преступности в России // https://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf Электронный ресурс [дата доступа 8.05.2021г.]

² Титарева, Е. Г. Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий / Е. Г. Титарева // Научный альманах. – 2015. – № 7(9). – С. 1158-1161.

именно использованием возможностей компьютерных систем и сети Интернет для совершения обмана человека или совершения неправомерных манипуляций с другими компьютерными системами с целью получения чужого имущества или права на него. Отдельного внимания заслуживает мошенничество с пластиковыми картами, необходимыми условиями которого является получение преступником данных о данных банковской карты жертвы. Часто преступники посредством получения информации о пин-коде карты завладевают всеми денежными средствами на ней, либо тем или иным способом просят у владельца карты подтвердить перевод денежных средств с карты.

При рассмотрении темы киберпреступлений нельзя не затронуть такое явление как социальная инженерия, технологии которой являются своеобразной «головной болью» для правоохранительных органов. Под социальной инженерией принято понимать систему способов воздействия и контроля людей, побуждающая их совершать определенные действия, применяемая с целью получения персональных данных личности

Одним из способов компьютерного мошенничества является фишинг-получение путем обмана или методов социальной инженерии персональных данных для использования в корыстных, преступных целях¹. Реализовываться фишинг может как посредством получения данных у самого владельца, так и путем посредничества в их получении. Проблемой является то, что сами по себе фишинг и социальная инженерия не содержат в себе состава преступления, однако последствия данных действий, такие как неправомерный доступ, использование или распространение вредоносных программ имеют квалификацию как преступления. Таким образом фишинг-лишь инструмент для совершения противоправных деяний.

¹ Батюшкин М.В. "Фишинг" - компьютерное мошенничество? // Символ науки. 2021. №1. URL: <https://cyberleninka.ru/article/n/fishing-kompyuternoe-moshennichestvo> (дата обращения: 07.05.2021).

Принцип работы фишинга состоит в создании поддельной копии интернет-ресурса с последующим перенаправлением пользователя на него. Созданные злоумышленниками ресурсы ничем внешне не отличаются от оригиналов, чаще всего копируя сайты магазинов, банков или социальных сетей. Путем ввода на сайте-подделке своих логина и пароля, пользователь отдает их в руки преступников, которые, в свою очередь, переводят денежные средства со счетов пользователя, тем самым совершая хищение.

Проблема квалификации по статье 159.6 в данном случае заключается в том, что фишинг никак не воздействует на компьютер жертвы. Потерпевший добровольно переходит по ссылке вводит логин и пароль, тем самым открывая доступ к своим средствам. Хищение производится при помощи логина и пароля, а не в результате воздействия на устройство, из-за чего данное деяние не может быть квалифицировано как мошенничество в сфере компьютерной информации.

Другой техникой, использующей социальную инженерию, является, так называемый, «троянский конь». Эта техника основывается на любопытстве, доверчивости и желании получить выгоду. Примерно действие выглядит так: злоумышленник отправляет жертве письмо с информацией, к примеру, о выигрыше суммы денег и прикрепленным файлом или ссылкой, содержащими в себе вредоносную программу. После открытия ссылки или файла, устройство пользователя может быть заражено вирусом, избавление от которого потребует перевода мошенникам денежной суммы, или произойдет иной сценарий, вследствие которого преступник получит доступ к персональным данным жертвы. Характерными чертами техники являются использование интересной для человека информации в сообщении, массовая рассылка писем, наличие вирусной программы в прикрепленном файле или ссылке¹.

¹ Старостенко Н. И. Криминалистический аспект техник социальной инженерии при совершении преступлений // Вестник Краснодарского университета МВД России. № 1 (47), 2020, с. 80-83.

Для правоприменения является основной задачей обеспечение информационной безопасности. Во многом злоумышленники, использующие техники, связанные с социальным инжинирингом, опираются на недостаточную грамотность населения в этой сфере и низкую осведомленность о новых способах мошенничества. Тема широко обсуждается как в научных кругах, так и в средствах массовой информации, однако законодательного закрепления аспекты проблемы не имеют.

Помимо вышеописанных преступлений существует множество других, направленных как непосредственно на компьютерную информацию, так и использующих ее для иных целей. К ним относятся: разработка и распространение вирусов- вредоносных программ, препятствующих нормальной работе устройств и сетей; создание логических бомб в программном обеспечении- программ, которые запускаются при определенных информационных условиях с целью обеспечения несанкционированного доступа или оказания вредоносного воздействия на данные; халатная небрежность при разработке, создании, эксплуатации компьютерной техники; подделка и фальсификация информации; хищение программного обеспечения; несанкционированное копирование, изменение или уничтожение информации; несанкционированный просмотр или хищение информации из банков данных, баз данных и баз знаний, а также многие другие¹.

Ввиду того, что киберпреступления- серьезная угроза как для обычных людей, так и для государств, борьба с ними становится важнейшей задачей. На сегодняшний день преступления в сфере компьютерной информации входят в положения главы 28 уголовного кодекса. В эту группу включены следующие составы: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 «Нарушение правил эксплуатации средств

¹ Чакрян В.Р., Кешишян В.В. Понятие компьютерных преступлений и их классификация // Символ науки, № 12-2. 2020, с. 71-75.

хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»; ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Тем не менее, данные статьи вызывают ряд вопросов, касающихся применения и квалификации, также, как обстоит ситуация со статьей 159.6 и квалификацией фишинга.

В случаях, когда преступления были совершены в отношении кредитно-финансовых организаций, огромную роль в противодействии киберпреступникам играет обратная связь кредитно-финансовых организаций со специалистами по обнаружению киберугроз, а также правоохранными органами. Важной составляющей информационной безопасности государства также является международное сотрудничество, прямо проистекающее из того факта, что киберпреступность интернациональна. Для эффективного противодействия киберпреступникам государство должно создать многоуровневую систему кибербезопасности, которая могла бы защищать интересы как обычных граждан, так и государственных или частных организаций.

Также немаловажным является поддержания высокого уровня используемых правоохранными технологиями для расследования преступлений, обучение и набор высококвалифицированных кадров, способных наравне бороться с угрозами информационной безопасности.

Список, использованных источников

1. Батюшкин М.В. "Фишинг" - компьютерное мошенничество? // Символ науки. 2021. №1. URL: <https://cyberleninka.ru/article/n/fishing-kompyuternoe-moshennichestvo> (дата обращения: 07.05.2021).
2. Номокова В.А. Киберпреступность как новая криминальная угроза / В.А. Номокова, Т.Л. Тропина. – 2012.

3. Старостенко Н. И. "Криминалистический аспект техник социальной инженерии при совершении преступлений" // Вестник Краснодарского университета МВД России, № 1 (47), 2020.
4. Титарева, Е. Г. Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий / Е. Г. Титарева // Научный альманах. – 2015. – № 7(9). – С. 1158-1161.
5. Чакрян В.Р., Кешишян В.В.. "Понятие компьютерных преступлений и их классификация" // Символ науки, № 12-2, 2020