ВИКТИМОЛОГИЧЕСКИЕ ОСОБЕННОСТИ КИБЕРПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВА

Айнутдинова К.А.,*, канд. юрид. наук, доцент,*
Университет управления «ТИСБИ», г. Казань;
Айнутдинова И.Н., *д-р пед. наук, профессор, ИМО КФУ, г. Казань*

Аннотация. Цель статьи - проанализировать состояние киберпреступности с позиции виктимологии в условиях цифровой трансформации российского общества. На основе изучения статистических данных МВД РФ и тематической литературы выявлены наиболее распространенные виды киберпреступлений, совершаемые в результате виктимного поведения жертв; определены виктимогенные факторы, способствующие совершению мошенничества в сети Интернет с использованием социальной инженерии; дана характеристика виктимного поведения жертв; внесены предложения по организации виктимологической профилактики мошенничества в сети Интернет на общесоциальном, специальном и индивидуальном уровнях.

Abstract. The purpose of the article is to analyze the state of cybercrime from the standpoint of victimology in the context of the digital transformation of Russian society. Based on the study of the statistical data of the Ministry of Internal Affairs of Russia and thematic literature, the most common types of cybercrime committed as a result of victim behavior were identified; victimogenic factors that contribute to the commission of fraud on the Internet using social engineering were determined; characteristics of victim behavior were given; proposals were made on organization of victimological prevention of cybercrime at the general social, special and individual levels.

Ключевые слова: киберпреступность, кибермошенничество, жертва, виктимизация, виктимное поведение, социальная инженерия, виктимологическая профилактика.

Key words: cybercrime, cyber fraud, victim, victimization, victim behavior,

social engineering, victimological prevention.

Обращение к теме исследования обусловлено ростом темпов цифровой трансформации российского общества, что порождает как позитивные, так и негативные изменения в экономике, политике, управлении, науке, образовании, здравоохранении, культуре, сфере потребления, формах взаимодействия и пр. [1]. С одной стороны, повсеместное внедрение цифровых технологий во все сферы жизни способствует оптимизации и автоматизации рутинных задач и процессов, что ведет к улучшению и упрощению доступа к информации, новым цифровым продуктам и услугам. С другой стороны, становятся очевидными потенциальные риски активно развивающейся цифровой среды, влекущие появление новых форм киберпреступности с уникальными схемами и недостаточно изученными способами совершения преступлений и создающие угрозы кибербезопасности для государственных органов, учреждений, бизнеса и отдельных граждан [2].

Несмотря на то, что в своих отчетах за январь-сентябрь 2022 г. МВД РФ и Прокуратура РФ [3] зафиксировали снижение темпов роста количества киберпреступлений (-6,1%; 378,5 тыс.), их доля в общей структуре и массиве преступности по-прежнему высока и составляет около четверти (25%) от всех зарегистрированных преступлений (-1,5 %; 1,5 млн.). При сокращении общего количества случаев хищения денежных средств у граждан в III квартале 2022 г., по сравнению с таким же периодом прошлого года – на 10,3% (229,8 тыс.) и снижением на треть числа краж с банковских счетов (с 121,1 тыс. до 84,7 тыс.), в стране наблюдается рост количества зарегистрированных мошенничеств (с 249,9 тыс. до 250,7 тыс.), в том числе в сфере компьютерной информации (ст. 159.6) и с использованием электронных средств платежа (ст. 159.3). По данным Банка России, опубликованным в ноябре в «Обзоре отчетности об инцидентах информационной безопасности при переводе денежных средств» [4], ущерб от мошеннических операций без согласия клиентов (ОБС) за июль-сентябрь 2022 г. вырос на 23,9% и составил почти 4 млрд. руб. (точнее, 3 973 456,54 руб.).

Для причинения материального или иного ущерба и получения выгоды

кибермошенники используют сеть Интернет, различные технические средства и устройства, а также активно практикуют методы и технологии социальной инженерии с целью психологического воздействия на потенциальных жертв и манипулирования ими. Делается это для извлечения незаконной выгоды через обман и принуждение пользователей предоставить доступ к защищенным системам, раскрыть личную или конфиденциальную информацию (коды, пароли, номера кредитных карт, банковских счетов и пр.) или же добровольно перевести деньги злоумышленникам в нарушение мер безопасности обслуживания банком. Интенсивность применения кибермошенниками социальной инженерии крайне высока; например, при совершении ОБС их доля в III квартале 2022 г. составила 54,1% [4]. Инциденты чаще происходят при оплате товаров и услуг в Интернете, дистанционном банковском обслуживании (ДБО), переходе по ссылке на подложные сайты, имитирующие известные ресурсы (фишинг), телефонном разговоре с мошенниками (вишинг), открытии поддельного SMS (смишинг) и др.

Во всех перечисленных случаях социальные инженеры еще до совершения атаки обычно владеют элементарными данными о потенциальной жертве, которые они получают через соцсети и информационные базы с персональными данными, оказавшиеся по какой-либо причине в коммерческом или свободном доступе в сети. Для достоверности сценария махинаторы маскируются под представителей реально существующих государственных или финансовых организаций, компаний и Интернет-магазинов и, пользуясь определенными психологическими уловками, играя на чувствах и слабостях людей, обманывая, злоупотребляя доверием, вводя в заблуждение, дезинформируя или шантажируя их, зачастую превращают даже самых умных и осторожных людей в жертв своих злонамеренных посягательств, направленных на получение конфиденциальных данных, завладение ими и дальнейшее их использование в корыстных целях [5].

Парадоксально, но виктимизация при кибермошенничестве происходит, в основном, спонтанно и/или на добровольной основе, при этом жертвы в момент совершения преступления не осознают сути конкретной преступной ситуации или заблуждаются относительно реальной картины происходящего, что лишь

способствует совершению в отношении данных лиц противоправных действий и превращению их в реальные жертвы. Установлено, что манипулятивные методы и технологии социальной инженерии воздействуют, в первую очередь, на интеллект и волю в структуре личности жертвы и тем самым уравнивают шансы виктимизации лиц с разным потенциалом виктимности (набором личных качеств и уязвимостей). Таким образом, жертвами кибермошенников в равной степени могут стать как наивные, доверчивые, некритичные лица любого возраста и пола с низким уровнем цифровой грамотности и правовой информированности, так и молодые высокообразованные, азартные, любящие риск, ведущие активную жизнь и включающиеся во множество новых видов деятельности индивиды [6; 7].

Напрашивается вывод о том, что наличие определенных характеристик и уязвимостей отдельной личности, отражающих ее социальное, психологическое или биофизическое состояние, не может служить единственным и неоспоримым доводом о виктимности жертвы и ее предрасположенности к последующей виктимизации в отсутствие определенной жизненной ситуации и действия важных объективных и субъективных виктимогенных факторов. Цифровизация и виртуализация всех сфер жизнедеятельности общества; внедрение высоких технологий в экономику, образование и повседневную жизнь; общедоступность сети Интернет и цифровых гаджетов (компьютеров, планшетов, мобильных телефонов, смартфонов и пр.); популярность социальных сетей для общения, обмена и размещения в открытом доступе информации личного характера; распространенность сервисов по определению геолокации (местонахождения) пользователей; торговля на черных рынках конфиденциальной информацией из похищенных источников и открывающая махинаторам доступ к персональной информации потенциальной жертвы еще на этапе подготовки к преступлению – все это и многое другое можно рассматривать как объективные или внешние по отношению к жертве виктимогенные факторы кибермошенничества [6; 8].

К субъективным виктимогенным факторам кибермошенничества можно отнести весь массив черт, слабостей и уязвимостей жертв кибермошенничества, обусловленных психическими особенностями личности и актуализированных в

процессе социализации жертвы под влиянием социальной среды и условий проживания в ней. Окружающий человека мир, его нормы, правила и ценности также постоянно развиваются и меняются под воздействием геополитических, социально-экономических, технологических, культурных факторов и несут как позитивные, так и негативные последствия для отдельного индивида. Издержки экономических кризисов и иные ситуации неопределенности (катастрофы, стихийные бедствия, эпидемии, военные конфликты и пр.) обнажают слабости и личностные деформации людей (наивность, доверчивость, невнимательность, беспечность, мнительность, самонадеянность жадность, страх, низкая правовая и информационная грамотность, консьюмеризм (потребительство) и др.), делают их беззащитными перед кибермошенниками, которые, в отличие от своих жертв, легко адаптируются к новым условиям и используют любые «бреши» для преступного обогащения [7]. Обман, злоупотребление доверием, введение в заблуждение и дезинформация служат отправной точкой виктимизации их жертв.

Для понимания особенностей виктимизации жертв кибермошенничества следует также обратить внимание на основные типы виктимного поведения, присущие жертвам данного преступления и провоцирующие кибермошенников на преступные деяния. Для первого типа жертв характерно активное поведение в сети Интернет, которое проявляется в их навыках работы с информационными ресурсами и техническими средствами; чрезмерном потреблении Интернет-услуг для жизни, работы и отдыха; в использовании сервисов заказов в Интернет-магазинах и маркетплейсах; оплате товаров и услуг через электронные системы платежей; переходе из реальной коммуникации в виртуальную через чаты, блоги, форумы, сетевые сообщества, социальные сети и пр., где они нередко оставляют о себе информацию личного и конфиденциального характера. Для них характерны самоуверенность, самонадеянность, бравада и беспечность, а игнорирование норм безопасности в информационной среде, отказ от обеспечения безопасности своих денежных средств и, в целом, легкомысленное поведение становятся основными виктимологическими факторами их уязвимости перед кибермошенниками [8; 9].

Для второго типа жертв характерно агрессивное поведение в сети

Интернет, которое может быть и проактивным, и реактивным. В первом случае агрессия проявляется в рассылке оскорбительных сообщений, использовании провокаций или демонстрации агрессивных действий, направленных на вызов эмоций, прежде всего возмущения, гнева и ответной агрессии оппонентов. Испытывая чувство ложной вседозволенности, безнаказанности и анонимности в сетевом общении, некоторые ожесточенные, беспокойные и неуверенные в себе пользователи считают нормой нарушать все допустимые границы этики и морали и позволяют в сетевом взаимодействия оскорбления, ожесточенность по отношению к незнакомым оппонентам и прямую агрессию. Реактивная модель поведения в сети проявляется вспышками агрессии, раздражения, недовольства и гнева в ответ на провокационное поведение других лиц [10]. Лица с проактивным и реактивным агрессивным поведением в сети в равной степени привлекают кибермошенников своей неустойчивой психикой, а такие люди для снятия напряжения обычно ищут помощь, хоть и мнимую, в социальной среде.

В результате проведенного исследования было установлено, что процессы цифровой трансформации, в целом, оказывают позитивное влияние на развитие общества и способствуют повышению благосостояния и качества жизни россиян. При этом отмечается, что цифровая среда и ее пользователи все чаще становятся мишенью и жертвами киберпреступников, которые умело используют цифровые технологии как средство и способ достижения своих преступных намерений. Одним из распространенных киберпреступлений является кибермошенничество, а усиленное технологиями социальной инженерии оно становится особенно опасным, так как здесь используются человеческие ошибки, а не уязвимости ПО (программного обеспечения). К тому же, жертвой кибермошенников может стать каждый, независимо от возраста, уровня достатка, социального положения и пр. Ведь, несмотря на разнообразие проявлений кибермошенничества и способов их совершения, их объединяет общий специфический способ посягательства на собственность жертвы – злоупотребление доверием в сочетании с обманом [7].

Виктимологическая профилактика играет особую роль в предупреждении кибермошенничества, поскольку поведение жертвы до и в момент совершения

данного преступления (в процессе ее виктимизации) является составной частью детерминации кибермошенничества. Профилактика будет эффективной, если осуществлять ее системно на общем, специальном и индивидуальном уровнях. Одной из важных задач является информирование населения для повышения уровня его правосознания, цифровой и финансовой грамотности. Цифровой портал «Кибрарий» – это успешный пример проекта для информирования населения и борьбы с кибермошенничеством, запущенный в октябре 2022 г. Сбербанком (https://promo.sber.ru/kibrary); он содержит инструкции, видеоролики, сценарии киберпреступлений, совершаемых против россиян, т.е. знакомство с ними призвано уберечь потенциальных жертв от нежелательных инцидентов. Для защиты клиентов от действий кибермошенников с 1 октября 2022 г. банки обязаны проводить идентификацию всех устройств, с которых совершаются онлайн-операции, при этом клиентам позволено самостоятельно устанавливать в банке запрет на онлайн-операции или ограничивать их параметры (сумму и др.).

Существуют все предпосылки для усиления борьбы с колл-центрами и ужесточения наказания за телефонное мошенничество (вишинг); с начала 2022 г. телеком-компаниями зафиксировано 1,5 млрд. мошеннических телефонных звонков, и, в среднем, один колл-центр совершает около 5000 звонков в сутки, при этом жертвами чаще всего становятся лица пожилого и преклонного возраста.

Безусловно, уберечься от обмана сложно, если не обладать элементарными знаниями об уловках киберпреступников и мерах противостояния им, поэтому главным инструментом виктимологической профилактики является осознание необходимости соблюдения правил и мер безопасности в киберпространстве.

Список источников:

1. Киселева Л.С., Семёнова А.А. Цифровая трансформация общества: тенденции и перспективы // Проблемы деятельности ученого и научных коллективов. - 2018. - № 4 (34). - С. 157-169.

2. Артамонов В.А., Артамонова Е.В. Кибербезопасность в условиях цифровой

трансформации // Цифровая трансформация = Digital Transformation. - 2021. - № 4 (17). - С. 42-51.

3. Состояние преступности в России за январь-сентябрь 2022 г.: Ежемесячный сб. о состоянии преступности в России за сентябрь 2022 г. (на основании ведомственного отчета МВД России формы 1-А) / Генеральная прокуратура РФ / Портал правовой статистики. - [Электронный ресурс]. - URL: http://crimestat.ru/analytics (дата обращения: 20.11.2022).

4. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за III квартал 2022 г. / Департамент информационной безопасности / Банк России. - [Электронный ресурс]. - URL: http://www.cbr.ru/analytics/ib/review_3q_2022/ (дата обращения: 23.11.2022).

5. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридич. инст. МВД России. - 2021. - № 1 (42). - С. 133-138.

6. Хоменко А.Н. К вопросу о виктимизации жертв киберпреступлений // Виктимология. - 2021. - № 2. - Т. 8. - С. 143-148.

7. Сплавская Н.В. Взаимодействие жертвы и преступника в процессе совершения мошенничества // Государство и право в XXI веке. - 2017. - № 3. - С. 16-20.

8. Стяжкина С.А. Виктимологическая профилактика мошенничества // Вестник Удмуртского ун-та. - Серия «Экономика и право». - 2022. - № 3. - Т. 32. - С. 546-552.

9. Жмуров Д.В. Кибервиктимизиция. Исследовательская матрица // Пролог: Журнал о праве. - 2021. - № 3. - С. 109-121.

10. Алистратова Е.Ю. Проактивная агрессия в Интернете: причины, последствия и возможные пути профилактики // Психолог. - 2014. - № 1. - С. 39-54.