УДК 343.988

Д.В. Жмуров

КИБЕРМОШЕННИЧЕСТВО: ВИКТИМОЛОГИЧЕСКИЙ АСПЕКТ

В статье рассмотрены отдельные вопросы, касающиеся жертв кибермошенничества. Автором выделены типичные формы этих преступлений и описаны соответствующие им виктимизирующие действия. Предложена сравнительная характеристика психологических особенностей мошенников и их жертв. Указаны некоторые особенности потерпевших от кибермошенничеств (гендерные, возрастные, психологические).

Ключевые слова: кибервиктимология, жертвы кибермошенничества, кибервиктимность, потерпевшие от интернет-мошенничеств.

D.V. Zhmurov

CYBERFRAUD: A VICTIMOLOGICAL ASPECT

The article discusses certain issues related to victims of cyberfraud. The author highlights the typical forms of these crimes and describes the corresponding victimizing actions. A comparative characteristic of the psychological characteristics of fraudsters and their victims is offered. Some features of victims of cyberfraud (gender, age, psychological) are indicated.

Keywords: cyber victimology, victims of cyber fraud, cyber victimization, victims of online fraud.

Кибермошенничество не является отдельным преступлением, оно включает в себя широкий спектр компрометирующих деяний, совершаемых в виртуальной среде.

По одним данным эти преступления ограничиваются причинением материального или иного ущерба путем хищения личной информации пользователя, как правило платежной или идентификационной [3]. По другим сведениям, пределы мошеннической активности не ограничены исключительно присвоением персональных сведений. Эта сфера чрезвычайно диверсифицирована. Она включает в себя десятки преступных схем: начиная от сокрытия или предоставления неверной информации (в брачных объявлениях, при купле-продаже на торговых площадках, инвестировании, ставках) и заканчивая сбором или использованием конфиденциальных данных (нелегальным в Даркнете, полулегальным в открытых источниках, в форме заимствования цифровых идентификаторов и т.д.). В любом случае все эти примеры являют собой разные виды манипулирования информацией в результате чего жертва остается без денег или имущественных прав.

Можно говорить о появлении целой индустрии виртуальных мошенничеств. Несмотря на их значительное количество способами совершения таких преступлений по-прежнему остаются *обман* (активный – намеренное введение

в заблуждение; пассивный – утаивание истинной информации) и *злоупотребление доверием*. На этой почве продолжают разрастаться многообразные формы мошеннической активности. Только в сети интернет их насчитывается более тридцати (см. табл. 1).

Несмотря на новизну технологий и не всегда знакомую терминологию суть этих действий остается неизменной. Указанные лица, как и десятки лет тому назад, поступают одинаково. Они:

1) предлагают совершить какую-либо сделку на условиях, которые значительно выгоднее обычных;

2) сулят без особых усилий получить материальные ценности и блага;

3) мотивируют потерпевших действовать в спешке, без тщательного обдумывания своих поступков;

4) выдают себя за тех, кем не являются (за богатых, влиятельных, преуспевающих людей, либо бедных и больных, чиновников, врачей, работодателей, продавцов и пр.);

5) используют человеческие страхи и непросвещенность для манипулирования своими жертвами.

Мошенники в меру умны, технически грамотны, изобретательны и уверены в своей безнаказанности. Наиболее успешные характеризуются словами Дона Винченцио из к/ф «Операция Святой Януарий». Про ловкого жулика он заметил: «Настоящий виртуоз! Успел обчистить автобус с иностранцами, пока те разглядывали в окна дым над Везувием. – Над Везувием нет дыма...– Перед этим он его там разжег…».

Таблица 1

Виды кибермошенничества и сопутствующий им алгоритм виктимизации

Наименование		**Описание виктимизирующих действий**
В сфере трудоустройства	Ложное трудоустройство	Различные формы предложения работы для поступления на которую требуется уплатить взнос, конкурсную комиссию и пр. В другом варианте предлагается погасить стоимость услуг рекрутингового агентства, которое выступит посредником при устройстве на высокооплачиваемую должность (в России, либо за ее границей)
	Работа на дому	Предоставление реальной работы, но без разъяснения ее криминальной специфики. Например, черные и серые схемы дроповодства, когда человеку предлагается получать по почте посылки и отправлять их другим адресатам. При этом, как правило, не упоминается, что в посылках товар оплаченный с краденных банковских карт (для разводных дропов). Таким образом, человек наверняка того не зная может принять участие в реализации преступной схемы
	Трудоустройство без оплаты	Выдача задания (платных заказов) на выполнение тех или иных услуг для самозанятых (фрилансеров) в интернете без дальнейшей оплаты за работу
В кредитно-финансовой сфере	Кредитные аферы	Включает всевозможные предварительно оплаченные консультации, обязательства оформить кредит заемщику с плохой кредитной историей, снизить процент по платежам, пересмотреть долги перед банками и пр.

Наименование		Описание виктимизирующих действий
	Денежные переводы	Оповещение о том, что сделан перевод средств, но он попал не к тому получателю, либо средства значительно завышена и часть денег необходимо вернуть. После этого транзакция со стороны мошенника отменяется, либо ее вообще не было
	Нарушение приватности финансовых операций	Человека убеждают в том, что его средства пытаются (пытались) похитить и предлагают помощь в решении этой проблемы (карта взломана, заблокирована, идут подозрительные списания и пр.)
	Инвестиции в бизнес	Предложение вложить денежные средства в развивающийся бизнес-проект (например, стартапы на краудфандинговых площадках), либо купить «прибыльную» франшизу
	Инвестиции в финансовые инструменты	Предложение инвестировать в сомнительные высокодоходные ценные бумаги, криптовалюты, операции на валютном рынке и пр. (инвестиционный механизм ICO, форекс, несуществующие криптографические средства платежа)
	Обмен валют	Выходят с предложением обменять валюту онлайн по выгодному курсу. В конечно итоге, комиссия оказывается значительно выше первоначально заявленной, либо обменник оказывается фейковым
	Страхование	Прямая продажа страховых полисов (поддельных, недействительных, продажа страховых полисов компаний, либо уже ушедших с рынка, либо тех, у кого приостановлена лицензия; искажение данных страхователя, получение денежных средств за страховой полис и непередача их в страховую компанию, а также намеренные ошибки при заполнении бланка полис)
В сфере азартных игр	Лотереи и тотализаторы	Оповещают о победе в розыгрыше, лотерее и предлагают забрать выигрыш. Для этого необходимо оплатить налог или сбор после чего, якобы, будет осуществлена выплата призового фонда
	Казино	Осуществляют сбор средств игроков и под разными предлогами не выплачивают выигранные деньги (якобы на основании блокировки аккаунта, вновь появившихся требований службы безопасности, использования игроком недопустимых криптовалют, обвинения их в читерстве и пр.)
	Букмекерские услуги	Приглашают заработать деньги на различных ставках по беспроигрышной «авторской» методике (ставки на спорт, продажа договорных матчей, продажа прогнозов, раскрутка счета в букмекерской конторе и т.д.)
В сфере здоровья и медицинского обслуживания	Продажа медицинского оборудования и препаратов	Создание ресурсов, продающих некачественную продукцию (БАДы, медицинские препараты и приборы для здоровья) под видом дорогостоящих и эффективных средств лечения
	Консультационные услуги медицинских работников	Проведение консультаций и дистанционного лечения от имени дипломированных специалистов в области медицинских наук

Наименование		Описание виктимизирующих действий
	Консультационные услуги колдунов, магов, целителей	Проведение консультаций и удаленного лечения от имени представителей альтернативной (народной) медицины
	Помощь в оформлении справок, рецептов, записи на прием, получении медицинских документов	Посреднические услуги в медицинской сфере, как правило, ограничивающиеся реализацией фальшивых бланков, рецептов, заведомо невыполнимыми обещаниями и пр.
В сфере цифровых и информационных прав	Кража личных данных	Любые формы мошенничества с целью получения доступа к конфиденциальным данным пользователей (фишинг, спуфинг, кьюшинг, фальшивые доменные имена, и пр.)
	СМС-мошенничества	Оформление платных подписок без согласия пользователя; ложная верификация телефона, когда необходимо отправить обратное смс, а оно оказывается чрезвычайно дорогостоящим
	Фейковые курсы и интернсивы	Серии бесполезных и малоэффективных учебных занятий по какой-либо теме («как похудеть за несколько дней?», «накачать собственное тело», «заработать миллион», стать авитологом, сделать «карту собственных желаний», чтобы они исполнились; запустить воздушный шарик с «долгами» или «обидами»; курсы по влюблению в себя мужчин; курсы успешности и пр.)
	Доступ к ресурсам	Предоставление возможности использовать бесплатную версию интересного пользователю ресурса. После получения платежных средств, мошенник присваивает их и подписывает клиента на стандартную платную версию. В других случаях, жертву заинтересовывают чем-либо (например, продолжением общения с девушкой) и за продолжения этой деятельности требуют оформления премиум аккаунта
	Доступ к программам	Продажа фиктивных программ для взлома чужих интернет-кошельков, бесплатного использования ресурсов интернет-провайдера и пр.
В сфере предоставления услуг и продажи товаров	Продажа несуществующих товаров и оказание мнимых услуг	Осуществление услуг и продажа товаров по заниженным ценам (глобальные распродажи, карженная техника, конфискат, продажа со склада, продажа билетов на мероприятия, квартиры посуточно, туристические сертификаты или таймшеры и т.д.). Кроме этого, может выражаться в оформлении несуществующих подписок (на книги, кино, музыку)
	Покупка реальных товаров и услуг	Приобретение товаров и услуг с имитацией оплаты (несуществующими чеками, фальшивыми деньгами, отзывными транзакциями и проч.), либо с оплатой с украденных кредитных карт для последующей перепродажи
	Мошенничество с программами лояльности	Получение информации, касающейся подарочных карт, которые были выпущены, но не были использованы. Хищение данных накопительных карт с остатком. Манипуляции

Наименование		Описание виктимизирующих действий
		с банковскими кэшбэками и профессиональный возврат товаров. Участие в партнерских программах крупных сайтов и нелегальное оформление на них рефералов
В сфере осуществления государственных полномочий	Мошенничество в области социальной помощи	Предоставление социальной помощи, выплат на ребенка, компенсационных платежей, льготных займов (осуществляется для сбора персональной информации и получения с клиентов сборов за несуществующие льготы)
	Лжеответственность	Имитация исполнения карательных функций государства с назначением штрафов в пользу бюджета (за нарушение режима самоизоляции, правил дорожного движения и т.д.)
	Официальная помощь в реализации государственных услуг	Посредничество в получении официальных документов, ускорение очереди на получение каких-либо благ, запись в детские сады и т.п.
	Неофициальная помощь в реализации государственных услуг	Полулегальное или откровенно криминальное посредничество в получении государственных услуг (оформление загранпаспорта на другую фамилию, внеочередное снятие судимости, оформление документов на льготы, которые не положены; организация выезда за границу невыездным лицам)
В сфере межличностных отношений	Мошенничества на доверии	Датинг-скам или мошенничества в сфере знакомств и интимных отношений (краткосрочные и долгосрочные), связаны с просьбами финансового характера со стороны партнера
	Лжеблаготворительность	Интернет попрошайничество, обращение с просьбами пожертвовать определенную сумму на благую цель (помощь приюту животных, лечение ребенка и много другое)

Каждое из перечисленных мошенничеств рассчитано на определенный тип жертвы. В любом случае за мошенниками и пострадавшими от их действий отмечаются некие основополагающие или ключевые характеристики. Сравнительное соотношение этих психологических черт представлено в табл. 2.

Таблица 2

Соотношение психологических особенностей мошенника и его жертвы

Мошенник	Жертва
Убедительный, обходительный, хороший психолог, манипулирует жертвой, навязчивый, хитрый, стратегически мыслящий, грамотный, уравновешенный, бессовестный, психологически доминирует над жертвой, изворотливый, скрытный, предприимчивый	Неопытный, легкомысленный, доверчивый, хочет легко и быстро «заработать» деньги, хочет купить товар намного дешевле, чем в магазине, невнимательный, простодушный, не задумывается о последствиях своих действий, самоуверенный, суетливый, алчный, наивный, безответственный

Главным образом, мошенничество строится на обещаниях достижения потребностей потерпевшего.

Вместе с тем, не всегда следует признавать интернет-мошенничеством различного рода виртуальные вымогательства, например, использование Ransomware, троянов-вымогателей или блокировщиков компьютера. Немалая

часть авторов некритично относят эти деяния к кибермошенничествам. Но в данном случае обмана не происходит. Программа попадя на компьютер жертвы, ограничивает доступ к файлам пользователя и требует выкуп за продолжение работы. Сходные ситуации, без установки вредоносного ПО, все-таки можно отнести к мошенническим. Ими являются порно-вымогательства, когда потерпевшему приходит письмо примерно следующего содержания: «Кажется, *** – это ваш пароль. Вы меня не знаете и наверняка очень удивились, получив это письмо. Дело в том, что я взломал порносайт, на который вы заходили… Если не хотите, чтобы эта информация стала общеизвестной, придется заплатить». В данном случае преступник обманывает и рассчитывает на панику жертвы, а ее реальный пароль, использованный для придания правдоподобия происходящему, как правило, берется из базы паролей, купленной в сети.

По половому признаку жертвами мошенничеств чаще становятся женщины. В ходе опроса интернет-пользователей, проведенного В.С. Соловьевым, из одиннадцати типов мошеннических действий в девяти случаях наблюдается существенное превышение доли пострадавших лиц женского пола [1]. Шесть видов мошеннических действий характеризуются значительной долей несовершеннолетних потерпевших. Среди них виктимизация вследствие обмана на валютном рынке Форекс (36,5 %); приобретения программ для бесплатной мобильной связи и интернета (33,3 %); денежной помощи друзьям, «обратившимся» со взломанных аккаунтов (33,3 %); потерянной предоплаты (32,3 %); фишинга (26,6 %); отправления денег на «волшебный кошелек» (25 %).

Таким образом, жертвы мошенничеств – это неоднородная группа потерпевших, поскольку криминальные стратегии преступников чрезвычайно разнообразны. Женщины, согласно выводам локальных опросов, в большей степени подвержены виктимизации от данного вида преступлений. Пожилые люди, несмотря на то, что являются одной из групп риска мошенничества вообще [2], в интернет-сегменте представлены не столь значительно. Это связано с небольшим распространением интернет-технологий в этой возрастной группе и не является сущностным признаком. Через несколько поколений, когда состарятся люди, воспитанные на кибертехнологиях, статистика, вероятно, выровняется. Критерием классификации жертв кибермошенничества могут быть способы его совершения. В соответствии с ними можно выделить:

– *коммуникационных жертв,* т.е. пострадавших в ходе использования различных коммуникативных приемов (социальная инженерия; методы, основанные на использовании фобий и страхов потерпевшего; его легковерности, асоциального поведения и неадекватных ожиданий);

– *жертв подлога* – людей, которых ввели в заблуждение путем намеренных фальсификаций (подделка сайтов, фальшивые объявления, имитация интернет-продаж, инвестиций, трудоустройства и пр.);

– *жертв инсценировки*, которые были убеждены в правдоподобности неких событий, разыгрываемых преступником (социальная помощь, интернет-попрошайничество);

– *комбинированных жертв*, пострадавших в результате использования всех вышеназванных способов.

В конечном итоге, остается констатировать, что мошенники эксплуатируют самые разные качества людей: доверчивость, зависть, алчность, стремление бесплатно получить то, что имеет материальную стоимость, азарт, гуманизм и стремление помочь другим, страх потерять свою собственность и проч. Наиважнейшим в данном контексте является отсутствие у потерпевших критического мышления, которое требует рефлексии и внимательности к принятию решений. Как выразился Ж. Лабрюиер: «водись на свете поменьше простаков, было бы меньше и тех, кого называют хитрецами и ловкачами». Потерпевшие от интернет-мошенничеств – это перевоплощение традиционных жертв преступного обмана, но только совершенного в виртуальном пространстве.

Список использованной литературы

1. Соловьев В.С. Мошеннические действия в социальном сегменте сети Интернет (криминологическое исследование по результатам интернет-опроса пользователей) / В.С. Соловьев // Известия Юго-Западного государственного университета. Серия: История и право. – 2018. – Т. 8. – № 3 (28). – С. 100–108.

2. Кабанов. П.А. Жертвы российской преступности: геронтологический аспект (криминологический анализ виктимологической статистики за 2014–2015 гг.) / П.А. Кабанов // Виктимология. – 2016. – № 1. – С. 9–16.

3. Что такое кибермошенничество и какая наступает за него уголовная ответственность // Отдел МВД России по Белоглинскому району. – URL: https://белаяглина.23.мвд.рф/news/item/20243491 (дата обращения: 17.03.2021).

Информация об авторе

Жмуров Дмитрий Витальевич – кандидат юридических наук, доцент кафедры уголовного права и криминологии Байкальского государственного университета экономики и права, руководитель проекта «Национальная энциклопедическая служба России», Иркутск, Россия, e-mail: zdevraz@ya.ru.

Author

Dmitriy V. Zhmurov – Candidate of Law, Assosiate Professor of the Chair of Criminal Law, Criminology and Criminal Process, Law Institute of Baikal State University, Coordinator, Project «National Encyclopedic Service of Russia», Irkutsk, e-mail: zdevraz@ya.ru.