Научная статья
УДК 343.988
DOI: 10.47475/2411-0590-2024-11-1-43-56

Предупреждение виктимизации дистанционных хищений и сферы его воздействия

Инна Ивановна Евтушенко

Крымский филиал Краснодарского университета МВД России, Симферополь, Россия
inna-evt@ya.ru
https://orcid.org/0000-0002-1335-5404

Аннотация. И ученые, и служащие органов власти находятся в активном поиске наиболее эффективных мер виктимологической профилактики и защиты жертв дистанционных хищений. Вместе с тем, среди российских ученых нет единого терминологического подхода к изучаемым явлениям: киберпреступность, цифровая виктимность, дистанционные хищения. Зарубежные исследователи в специализированных виктимологических журналах значительное внимание уделяют способам реализации и содержанию восстановительного правосудия. Однако в области именно виктимологической профилактики дистанционных хищений исследований мало. Значительная масса зарубежных исследований в области кибербезопасности направлена на реализацию общих криминологических мер защиты как личной, так и корпоративной информации. В исследованиях последних лет обращают внимание на необходимость контекстно-ориентированного микрообучения пользователей информационных ресурсов и технологий как метода обучения кибербезопасности. Проведенное автором и другими российскими учеными исследования в сфере виктимизации потерпевших от дистанционных хищений позволило выделить типовые виктимологические ситуации, наиболее распространённые в 2023 году и спрогнозировать их развитие в будущем. Выявленные сценарии развития виктимизации все больше получают распространение, а значит, нуждаются в быстрых предупредительных мерах со стороны государства. Большинство исследователей приходят к выводу об отсутствии у жертв дистанционных хищений индивидуальных виктимогенных признаков, поэтому в большей степени необходимо разрабатывать меры общей виктимологической профилактики, направленной на массовую виктимность жертв дистанционных хищений. Опираясь на ранее проведенные российские и зарубежные исследования, автор предлагает осуществлять предупредительное воздействие в следующих сферах общей превенции: экономической, нормативной, теоретической, практической, технической (технологической), информационной.

Ключевые слова: виктимизация, дистанционные хищения, виктимологическая профилактика, защита жертв, кибермошенничество, киберпреступность, кибервиктимология, цифровая виктимность, восстановительное правосудие, криминологические меры, кибербезопасность, типовые виктимологические ситуации, предупредительные меры, виктимогенные признаки, общая виктимологическая профилактика, превенция

Для цитирования: Евтушенко И. И. Предупреждение виктимизации дистанционных хищений и сферы его воздействия // Виктимология. 2024. Т. 11, № 1 С. 43–56. DOI: 10.47475/2411-0590-2024-11-1-43-56

Research article

Prevention of Remote Theft Victimization and its Scope of Impact

Inna I. Evtushenko,

Crimean Branch of Krasnodar University of the of the Interior Ministry of Russia, Simferopol, Russia
inna-evt@ya.ru
https://orcid.org/0000-0002-1335-5404

Abstract. Both scientists and government officials are actively searching for the most effective measures of victimological prevention and protection of victims of remote theft. At the same time, there is no single terminological approach among Russian scientists to the phenomena under study: cybercrime, digital victimization, and remote theft. Foreign researchers in specialized victimological journals pay considerable attention to the methods of implementation and content of restorative justice. However, there is little research in the field of victimological prevention of remote theft. A significant amount of foreign research in the field of cybersecurity is aimed at implementing general criminological measures to protect both personal and corporate information. Research in recent years has drawn attention to the need for context-oriented microlearning for users of information resources and technologies as a method of teaching cybersecurity. The study conducted by the author and other Russian scientists on the methods of victimization of victims of remote theft allowed us to identify typical victimological situations that are most common in 2023 and predict their development in the future. The victimization scenarios identified are becoming increasingly common and therefore require rapid preventive measures by the state. Most researchers come to the conclusion that victims of remote theft do not have individual victimogenic signs, therefore, it is more necessary to develop measures of general victimological prevention aimed at mass victimization of victims of remote theft. Based on previously conducted Russian and foreign studies, the author proposes to carry out preventive measures in the following areas of general prevention: economic, regulatory, theoretical, practical, technical (technological), informational.

Keywords: victimization, remote theft, victimization prevention, victim protection, cyberfraud, cybercrime, cybervictimology, digital victimhood, restorative justice, criminological measures, cybersecurity, typical victimization situations, preventive measures, victimogenic attributes, general victimization prevention, prevention

For citation: Yevtushenko II. Prevention of Remote Theft Victimization and its Scope of Impact. *Viktimologiya* [Victimology]. 2024;11(1):43-56. (In Russ.) DOI: 10.47475/2411-0590-2024-11-1-43-56

Введение

В современном постмодернистском информационном обществе, исходя из его ключевых сущностных характеристик, главным товаром выступает информация, получение и распространение которой одновременно является и основной угрозой безопасности данного общества.

Поэтому неудивительно, что в структуре современной преступности мы видим устойчивую тенденцию к снижению так называемых контактных форм

и способов совершения преступлений (убийств, разбоев, краж из жилых помещений и др.), с одновременным увеличением доли преступлений, совершаемых в информационном пространстве или с использованием методов удаленного воздействия на жертву.

Такое структурное изменение преступности побудило криминологов обратить пристальное внимание на новый вид преступности — киберпреступность. Активно продвигаются идеи о необходимости выделения соответствующей ей отдельной частной теории криминологии, и как следствие — отдельной теории виктимологии — «кибервиктимологии».

Предлагается введение в научный оборот соответствующих новых терминов: киберпреступность, киберугрозы, кибервиктимология, кибермошенничество, кибервиктимность, кибержертва. В этом направлении проводят исследования ученые Е. А. Антонян, Д. В. Жмуров, А. В. Майоров, А. Л. Осипенко, В. С. Соловьев, С. А. Стяжкина и другие.

Причем в своих исследованиях каждый из авторов изучает киберпреступность с «разных сторон одной медали»: А. Л. Осипенко [9], А. Н. Игнатов и В. С. Соловьев [6] — с точки зрения криминологии, А. В. Майоров [6; 7], Д. В. Жмуров [4; 5], С. А. Стяжкина [11] — с точки зрения виктимологии. При этом Д. В. Жмуров широко использует в наименовании новых терминов приставку «кибер», а другие исследователи более осторожно подходят к употреблению этого термина, используя различные словоформы: «цифра», «информационно-телекоммуникационные технологии», «дистанционные».

Причем все исследователи обоснованно говорят об отсутствии единой терминологии, и как следствие, единого объекта изучения. Наличию путаницы в понятиях — какие же преступления считать цифровыми, или с приставкой «кибер», способствует и путаница в нормативных документах, письмах, специальных базах данных учета как МВД России, так и Центробанка России.

Отсутствие единства терминологии приводит и к путанице в предлагаемых уровнях и видах виктимологического предупреждения, этапах виктимизации потерпевшего, субъектов их осуществляющих, конкретных мерах по предупреждению дистанционных хищений.

Изучение зарубежных публикаций в специализированных виктимологических журналах, таких как Revista de Victimología / Journal of Victimology и Società Italianadi Vittimologia за 2022–2024 гг., показало, что исследователи в основном интересуются вопросами защиты жертв насильственных преступлений, а именно домашнего насилия, сексуального насилия, сексуальной эксплуатации, в том числе детей, защите мигрантов как отдельной группы жертв. Другая значительная часть публикаций связана с реализацией идеи восстановительного правосудия.

Предупреждению различных форм киберпреступлений посвящены криминологические исследования, в основном направленные на обеспечение общих мер криминологической профилактики. Шашанк Ядав (Shashank Yadav) обращает внимание на актуальные, но постоянные угрозы кибербезопасности (APT), которые являются первоочередной задачей при разработке и реализации национальной политики кибербезопасности. Эти угрозы часто также связаны со сложными тактиками социальной инженерии, которые претерпевают количественную и качественную революцию благодаря растущим возможностям искусственного интеллекта. Однако атрибуция этих действий APT может быть обусловлена техническими и политическими соображениями. Им изучаются последствия такого распределения политических угроз для национальных сред кибербезопасности [16].

Материал и методы исследования

В качестве материалов исследования были использованы научные работы отечественных и зарубежных исследователей по заявленной теме, статистические данные и информация о способах совершения дистанционных хищений из открытых источников и сети интернет.

Методологию исследования составили такие методы как анализ и синтез, дедукция и индукция, контент-анализ, прогнозирование, моделирование и изучение документов. Использование указанных методов позволило автору предложить модель системы предупреждения виктимизации дистанционных хищений.

Описание исследования

Анализ способов совершенных дистанционных хищений за 2023 г. позволяет отметить следующие особенности. Только на территории Республики Крым в 2023 г. мошенники выманили у крымчан более 665 млн рублей. Причем это не только хищение у граждан наличных или безналичных денежных средств с их счетов, это и оформленные самими потерпевшими кредиты на миллионы рублей, которые они в последующем переводили или отдавали мошенникам. В среднем за одну неделю, не смотря на все предпринимаемые сотрудниками полиции меры профилактики и пресечения противоправной деятельности мошенников, последним удавалось выманить у потерпевших порядка 20 млн рублей.

С. А. Стяжкина, анализируя способы взаимодействия преступника и жертвы кибермошенничества, выделает два типа жертвы: «жертвы технического воздействия и жертвы информационного воздействия. Для первого типа жертв характерно активное использование электронных систем платежей, внедрение новых информационных технологий в сфере оплаты товаров, услуг, как правило, приобретаемых через маркетплейсы, интернет-ресурсы с активным использованием сервисов заказов и т. д. Это молодые, активные люди, пользующиеся современными достижениями информационного пространства, владеющие навыками работы с информационными ресурсами и техническими средствами… Второй тип жертвы практически ничем не отличается от жертв обычных мошенничеств. Следует отметить, что в данном случае речь идет не о каких-то специфических особенностях кибержертв, а об особенностях личности потерпевшего от мошеннических действий. Для второго типа жертв мошенничества, независимо от сферы его совершения, характерна чрезмерная доверчивость, небрежность и легкомысленность» [11, с. 549].

Причем все больше исследователей приходят к одним и тем же выводам, что виктимологические признаки потерпевших от дистанционных хищений не отличаются ни какими особенностями: в равной мере страдали от действий мошенников и мужчины, и женщины, и молодые, и среднего возраста (пожилые граждане — значительно реже), как с высшим образованием и большим жизненным опытом, так и без них, как рабочие, так и служащие.

Таким образом, профилактические мероприятия должны быть направлены не на какие-то отдельные группы населения или индивидуумы, а на всех жителей в равной мере. То есть необходимо вести речь в большей степени о массовой виктимности всех жителей России и общих мерах виктимологической профилактики.

Как справедливо указывает О. А. Старостенко в своем диссертационном исследовании, механизм виктимизации потерпевшего условно можно представить в виде трех видов взаимодействия: «преступник-техника», «преступник-техника-жертва», «преступник-жертва». Причем на первый вид взаимодействия при дистанционных хищениях приходится всего 8% виктимогенных ситуаций. Взаимодействие «преступник-техника-жертва» более распространено и составляет уже 24% дистанционных хищений. Однако самую большую группу составляют все-таки, ситуации взаимодействия «преступник-жертва» — 68% [10, с. 51].

Такие показатели связанны в первую очередь со сложностью технологического взаимодействия преступника и защищаемой владельцем информации. Вместе с тем, и все остальные виды виктимологических ситуаций связаны с наличием у преступника доступа к базам данных различных организаций, к персональным данным о потерпевшем, его фотографиям, служебной и личной информации, переписке в рабочих «чатах» различных мессенджеров.

Зарубежные исследователи так же обращают внимание на тот факт, что значительная часть угроз кибербезопасности пользователей исходит от самих пользователей. Они обращают внимание на ненадлежащее поведение в области кибербезопасности, отмечая, что гражданам не хватает знаний в области кибербезопасности при использовании интернета и цифровых устройств, и в целом существует несоответствие между возможностями интернета и поведением людей. Они предлагают использовать теорию мотивации защиты (PMT) для поощрения надлежащего поведения в области кибербезопасности. Теория предполагает, что оценка угрозы и оценка преодоления — это два основополагающих механизма, лежащих в основе поведенческих действий, когда люди сталкиваются с угрожающими событиями. Таким образом, они предлагают практику модели кибербезопасности, ориентированной на граждан [14].

Пользователи постоянно становятся мишенями злоумышленников, и им требуется обладать достаточными знаниями, чтобы выявлять такие атаки и избегать их. Поэтому часть зарубежных криминологических исследований посвящена снижению виктимности у населения путем их обучения, повышения осведомленности в области кибербезопасности [12; 13].

Гарри Л. Уайт (Garry L. White) предлагает рассматривать грамотность в области безопасности как разную на разных уровнях управления. Им представлена модель грамотности в области безопасности с точки зрения уровня управления и того, как различные методы грамотности в области безопасности (осведомленность, обучение, просвещение) поддерживают модель различных потребностей в области информационной безопасности для стратегического (*почему*), тактического (*как*) и оперативного (*что*) управления. Модель предполагает, что безопасность выходит за рамки технических знаний и вместо этого предполагает критическое осмысление того, что делать [13, с. 29–37].

Поэтому одно из направлений виктимологической профилактики — использование различных методов обучения безопасного поведения пользователей. Однако, как отмечают исследователи, недостаточно один раз научить пользователя, объяснить ему угрозы и показать способ их преодоления. Они предлагают использовать контекстно-ориентированное микрообучение (CBMT). Этот подход предполагает, что обучение должно проводиться в коротких последовательностях, когда информация имеет прямое отношение к деятельности пользователя. Цель состоит в том, чтобы провести обучение, непосредственно связанное с текущей ситуацией пользователя, а также обеспечить эффект повышения осведомленности. Кибербезопасность — это социально-техническая область, в которой осведомленность и поведение пользователей являются решающими аспектами. Готовым решением для улучшения поведения пользователей является обучение безопасности (SETA), включающем три элемента: *осведомленность*; *обучение; образование*, целью которого является интеграция навыков и компетенций в совокупность знаний. Причем знания не всегда преобразуются в поведение, о чем свидетельствуют постоянные инциденты с использованием человеческого фактора. Существенных различий между респондентами мужского и женского пола авторами исследования выявлено не было, поэтому универсальный подход к обучению действительно возможен. Респонденты упоминают, что реализация сама по себе должна быть простой в использовании и не должна быть навязчивой. Исследование также показывает, что около 40 % респондентов, прошедших обучение, считают, что оно изменило их поведение, связанное с безопасностью [15, с. 121–137].

В настоящий момент Центробанком России проводятся с целевой аудиторией — сотрудники правоохранительных органов и преподаватели учебных заведений, бесплатные онлайн обучающие семинары, посвященные различным аспектам корпоративной и частной кибербезопасности. Это, конечно, в некоторой степени повышает осведомленность слушателей этих семинаров, однако для основной массы обучающихся транслируемые знания

остаются непонятными, поскольку используется специальная узкопрофессиональная терминология. Кроме того, такое обучение не включает выработку практических навыков, закрепление их и систематическое повторение.

Поэтому и эффективность таких обучающих семинаров, согласно теории контекстно-ориентированного микрообучения, крайне низкая. Целевая аудитория, которая призвана к обучению, в последующем не может масштабировать полученные знания, передавать их обучающимся или потенциальным потерпевшим. Именно поэтому широкое разъяснение и предупреждение граждан о новых способах мошенничества и даже вручение им текстовой памятки практически не влияют на уровень виктимности потерпевших. Эти знания для них не актуализированы и хорошо известные способы виктимизации потерпевших оказываются очень результативными со стороны мошенников.

Так, по данным МВД по Республике Крым, в 2023 г. самым «популярным» способом обмана стало мошенничество посредством телефонных звонков — таким образом граждане лишились 473 млн рублей.

В 25 % случаев такие звонки произведены на телефонные номера операторов сотовой связи. Наиболее популярны у преступников в прошлом году были «легенды»: «ваш родственник попал в ДТП (СИЗО)», «служба безопасности банка (Центробанка России)», «главный следователь Главного управления МВД (ФСБ)», «звонок от оператора мобильной связи».

Но подавляющее большинство — 75 % звонков — поступили через мессенджеры — Вотсап, Телеграм, Вайбер. При таком способе виктимизации потерпевшего самыми распространенными были две «легенды»: звонок с логотипом банка и звонок (сообщение) от босса (начальника).

Механизм совершения дистанционного мошенничества с использованием мобильной связи

Рассмотрим более подробно механизм совершения таких мошенничеств в целях выявления наиболее значимых факторов виктимизации потерпевшего.

Целью преступников при звонке потерпевшему — поставить его в тупик, запугать. Поэтому назовем первый этап виктимизации потерпевшего — «испуг». Например, при звонке от «службы безопасности банка» потерпевшей узнает, что в этот самый момент кто-то от его имени пытается оформить на него кредит или обналичить денежные средства с его счета, карты и поэтому нужно незамедлительно принять меры безопасности, «спасти» свои деньги. Или, например, «главный следователь Главного следственного управления» сообщает, что в отношении потерпевшего, или некоего заявителя проводятся следственные действия, возбуждено уголовное дело, и счета потерпевшего использовались в преступной схеме и возможно привлечение его к уголовной ответственности как соучастника. После того, как потерпевший «испугался», он уже не способен воспринимать критически получаемую информацию, всецело полагается на своего нового телефонного «спасителя» и выполняет его указания.

Далее преступники переходят ко второму этапу виктимизации потерпевшего — «снятие денег»: потерпевшему предлагается перевести деньги на безопасные счета, или потерпевшему предлагается заблокировать доступ к личному кабинету в интернет-банкинге путем сообщения индивидуального одноразового кода, приходящего потерпевшему на телефон, или установить по присланной ссылке специальную программу-защитник. Причем в таких ситуациях бессильны оказываются и настоящие сотрудники полиции, службы безопасности, кассовые операторы банков, которые пытаются потерпевшего вернуть к объективной действительности, предупреждают, что с ним говорит мошенник, приостанавливают операции, давая жертве время одуматься.

Далее преступники переходят к третьему этапу преступной деятельности — выводу денег. На этом этапе потерпевший зачисляет денежные средства на счет мошеннику, или передает наличные

денежные средства курьеру, или, передав мошенникам код (установив программу), он утрачивает контроль над личным кабинетом в интернет-банкинге, и уже от его имени переводятся денежные средства, оформляются и выводятся кредиты на дроп-счета.

Таким образом, виктимологическая профилактика должна касаться всех трех этапов, затрудняя с одной стороны преступнику доступ к жертве, а с другой стороны блокируя снятие и вывод его денег.

Дистанционное мошенничество посредством интернет-сайтов

Еще одна распространенная схема дистанционного мошенничества — через интернет-сайты. Чаще всего речь идет о различных торговых площадках, сайтах бесплатных объявлений: о продаже товаров, предложения о работе, легком заработке, инвестировании. Также к этой группе относятся и фишинговые сайты (сайты-двойники) отелей, авиакомпаний, турагенств и т. п., которые предлагают услуги бронирования, предварительной или полной оплаты поставляемых товаров или услуг.

В таких ситуациях первая стадия виктимизации потерпевшего — «испуг» — отсутствует. Вместо нее присутствует иная, но аналогичная стадия, цели которой — заинтересовать, обратить внимание потерпевшего на контекстную рекламу, красивые картинки, истории о «чудесном» инвестировании и т. п. По аналогии с ловлей рыбы эту стадию можно называть «приманка». Аналогичным образом осуществляется «приманка» жертв в социальных сетях, в том числе многочисленных объявлениях о сборе денег на помощь больному ребенку (а на самом деле — финансирование терроризма, экстремизма, или армии сопредельного государства).

После того как потерпевший обратил внимание, он должен «наживку заглотить», то есть не просто перейти по ссылке, проявив свой интерес, а начать общение (переписку, телефонный разговор) с продавцом. На этой стадии продавец предлагает жертве самые выгодные для него уникальные предложения, после чего потерпевший уже готов перейти к следующей стадии — перечислении денег на счет продавца. Как правило, при таком способе мошенничества денежные средства переводятся в безналичной форме на банковские счета подставных лиц или электронные кошельки. Последующая стадия — вывод денег не имеет отличий от иных видов дистанционных хищений.

Предпринимаемые кредитными организациями, полицией усилия по пресечению и предупреждению дистанционных хищений, повышению технической и финансовой грамотности потерпевших приводит к тому, что и преступники вынуждены использовать для совершения обмана все больше сведений, похожих на правду. При всех вышеперечисленных ситуациях получает все большее распространение не просто «прозвон» по случайным номерам, или номерам из базы данных банка, оператора связи, службы такси, доставки еды и т. п. Преступники персонализируют свое общение с жертвой, которая для него уже не случайная, а целенаправленно выбранная. Причем теперь преступники готовятся к общению с жертвой, собирают о ней информацию, разговаривают на привычном для жертвы языке, используя обращение по имени и отчеству, фамилии, приводя факты из жизни, службы или работы потерпевшего, фотографии с его социальной страницы или фотографии его ближайшего окружения.

Такие сведения они могут получить как из открытых источников — например, социальных страниц потерпевшего, официальных сайтов образовательной организации или публичных сведений о должностных лицах органов власти, так и похищенных у операторов персональных данных — ГИБДД, поликлиник, страховых организаций, баз миграционного и паспортного учета. Таким образом, преступник может собрать информацию, показывающую почти полную картину жизни любого человека, не прибегая к сложным техническим устройствам или программным средствам. Такие базы продаются на «черном рынке информации»

и пока каналы их поступления и продажи не перекрыты в полной мере.

Особое беспокойство у общества и профессиональных участников рынка информационных услуг вызывает все большее проникновение в нашу повседневную жизнь технологий искусственного интеллекта, цифровой обработки информации и ее последующей подмены — так называемые технологии DeepFake, когда с помощью новейших программных средств искусственный интеллект подменяет один голос на другой, или даже потоковое видео. С одной стороны, такие технологии способны значительно упрощать нашу жизнь, позволяя управлять голосом различными устройствами и банковскими приложениями, как в фантастическом фильме, который уже стал нашей реальностью. Однако и преступники все чаще используют подмену голоса или изображения для обмана потерпевшего, вызывая у него доверие при виде знакомого изображения или голоса.

Таким образом, рассматривая механизм виктимизации потерпевшего, мы приходим к выводу, что создание преступником условий в предкриминальной ситуации значительно повышает эффективность и так высокоэффективной деятельности дистанционных мошенников. А значит и меры предупреждения таких деяний должны быть направлены на устранение таких благоприятных для преступника условий.

Соответственно выявленным факторам и условиям необходимо разрабатывать меры виктимологической профилактики на первом этапе виктимизации потерпевших от дистанционных хищений.

Предупреждение виктимизации дистанционных хищений

Д. В. Жмуров выделяет следующие «уровни виктимологической превенции: 1) легальный (формирование виктимологического законодательства); 2) академический (активизация виктимологических исследований); 3) институциональный (администрирование и организация процессов виктимологической превенции в цифровой среде); 4) технический (внедрение перспективных разработок, направленных на девиктимизацию субъектов информационно-технологического мира); 5) идеологический (выработка системы идей и взглядов, в которых осознаются отношения людей, как субъектов виртуальной жизни, способных пострадать от правонарушений)» [4, с. 135].

Предложенная классификация уровней виктимологической превенции не безупречна с точки зрения теории виктимологии. В данном случае автор ведет речь идет о таком уровне виктимологической профилактики как общая. Но если мы говорим об общей профилактике как уровне принятия управленческих решений, формирования системы мер, направленной на неопределенный круг потерпевших лиц (массовой виктимности) и затрагивающей деятельность органов власти общей компетенции, то правильнее было бы говорить не о дополнительных уровнях, а о сферах деятельности субъектов профилактики, в которых такие решения одного уровня должны приниматься.

В связи с чем полагаем более терминологически верным говорить о сферах воздействия общей превенции: экономической, нормативной, теоретической, практической, технической (технологической), информационной.

В части экономической превенции необходимо создать такие условия, что бы всем профессиональным участникам денежного оборота было бы невыгодно участвовать прямо или косвенно в хищениях денежных средств у граждан. И тут огромную превентивную роль должны сыграть меры финансовой ответственности кредитных организаций, которые на сегодняшний день возлагают бремя ответственности за сохранность денег потерпевшего на него самого, получая проценты от мошеннических транзакций и выданных потерпевшему кредитов в любом случае. Однако ситуация стала меняться к лучшему, на что указывают последние данные ЦБ России: «в 2023 году кредитные организации возвратили клиентам 8,7 % (1378,8 млн руб.) от всего объема операций по переводу денежных средств, совершенных без согласия

клиентов (в 2022 году данный показатель составил 4,4%, или 618,4 млн руб.)»[1]. Ранее мы предлагали ввести понятие «презумпции вины» кредитной организации [3, с. 86–88] как профессионального участника финансового рынка, обладающего огромными ресурсами и способного обеспечить безопасность денежных средств клиентов.

О больших рисках такой безответственности для самой финансовой системы ранее говорила председатель ЦБ России Э. Набиулина, которая 14 февраля 2024 года на сессии форума «Кибербезопасность в финансах» особенно выделила легкость, с которой банки и иные кредитные организации выдают кредиты гражданам. Учитывая, что быстро выданные многомилионные кредиты достаются мошенникам, а бремя выплаты их ложится на потерпевших, это в целом снижает доверие клиентов и устойчивость финансово-кредитной системы, поскольку приводит к закредитованности граждан и их последующему банкротству, то есть к прямым убыткам самой кредитной организации.

Соответственно, в данной сфере необходимо усложнять процедуру выдачи кредитов, позволять гражданам устанавливать личный запрет на онлайн подачу заявки и оформление кредитов, чтобы никто от имени клиента без его ведома не смог оформить такой кредит, или ввести процедуру согласования выдачи кредита с доверенным лицом (супругом, взрослыми детьми, родителями). В данном случае это, конечно же, приведет к замедлению оборота денег, но снизит риски и повысит стабильность всей системы, что гораздо более ценно, чем выгоды и интересы отдельно взятой кредитной организации. Также высказаны предложения об ограничении суммы единовременно вносимых денежных средств через банкомат, поскольку мошенники, зная об уже предпринятых ограничениях, заставляют клиента не переводить кредитные деньги, а снять их со своего счета в наличной форме и внести на счет мошенника через банкомат, исключая таким образом сотрудника банковской организации из круга общения мошенник-потерпевший и не давая таким образом пресечь мошенническую операцию.

В сфере нормативного предупреждения дистанционных хищений в настоящий момент сделано уже много, но все равно недостаточно, о чем свидетельствует постоянный рост показателей таких преступлений и попыток их совершения. Какие слабые места в этой сфере можно выделить? Вариативность отраслевого законодательства: основные предложения по виктимологической профилактики рассылаются Центробанком России как рекомендации к кредитным организациям, а не обязательные требования, влекущие ответственность за их неисполнение. До сих пор забота о безопасности своей и своих клиентов находится «на совести» самих кредитных организаций, они могут реагировать на возникающие угрозы, а могут и использовать их к своей выгоде. А изменения, внесенные в июне 2023 г. в Федеральный закон «О национальной платежной системе», вступят в силу только в июне 2024 года! Федеральный закон от 20.10.2022 № 408-ФЗ «О внесении изменений в статью 26 Федерального закона „О банках и банковской деятельности“ и статью 27 Федерального закона „О национальной платежной системе“»[2], который с 21 октября 2023 года обязал Банк России предоставлять в МВД России информацию о случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, в рамках банковской автоматизированной системы «ФинЦЕРТ» не подкреплен ведомственными приказами и инструкциями практического осуществления такого обмена информацией, не решены вопросы обеспечения безопасности доступа в данную систему со стороны сотрудников МВД России. На момент вступления

[1] Обзор операций, совершенных без согласия клиентов финансовых организаций // Банк России. URL: https://cbr.ru/analytics/ib/operations_survey/2023/ (дата обращения: 14.02.2024)

[2] URL: https://www.consultant.ru/document/cons_doc_LAW_429413/ (дата обращения: 14.02.2024).

в силу данных изменений ни сотрудники Центробанка России, ни сотрудники низовых подразделений ОВД не могли сказать, как они будут обмениваться данной информацией, обеспечивая при этом безопасность самой системы «ФинЦЕРТ» и защищенных банковской тайной сведений о клиентах.

В сфере теоретического обоснования предупреждения дистанционных хищений мы отмечаем усиление внимания ученых к данной проблеме. В частности, большое количество научных статей и новых диссертационных исследований посвящены как институциональным проблемам виктимологической профилактики хищений, так и выработке практических мер, так необходимых сотрудникам органов внутренних дел.

В части практической деятельности подразделений ОВД основу составляет ведомственная система учета дистанционных хищений, которая названа «Дистанционные мошенничества»[1]. Однако учету в этой базе данных подлежат не только деяния, квалифицируемые органами следствия как все разновидности ст. 159 УК РФ, но и дистанционные кражи. В рамках выполнения планов проведения профилактических мероприятий ведется активная работа по предупреждению потенциальных жертв дистанционных мошенничеств о новых и ранее известных способах обмана путем распространения социальной рекламы на телевидении, радио, в интернете, по номерам сотовых операторов, на стендах в социальных учреждениях, общественном транспорте, кредитных организациях, на экранах банкоматов.

Также в рамках оперативного реагирования и предупреждения дистанционных мошенничеств в Республике Крым с ведущими кредитными организациями и местными операторами стационарной, сотовой связи, агрегаторами такси заключены соглашения об оказании содействия об оперативном информировании полиции о попытках потерпевших снять большие суммы денег со своих счетов или их перевода, длительного разговора абонента по номеру телефона, использования такси для собирания денег у потерпевших. Это позволило пресечь и раскрыть по горячим следам уже не один десяток таких мошенничеств, при которых вывод денег осуществлялся при помощи курьеров.

Более того, в феврале этого года абонентам на номера операторов сотовой связи, оказывающих услуги в Республике Крым, с номера 102 стали приходить сообщения-предупреждения о самых распространенных способах мошенничеств и действиях потерпевшего по пресечению совершения в отношении них преступлений.

В сфере технического (технологического) предупреждения дистанционных хищений широко используются технологии блокировки подмены номеров как стационарной, так и сотовой связи, в связи с чем и были приняты соответствующие нормативные акты. В части административного регулирования деятельности операторов связи с 1 марта 2023 г. вступили в силу изменения в части статей 13.29 и 13.30 КоАП РФ, предусматривающих административные штрафы для операторов связи, которые допускают «неисполнение установленных законодательством Российской Федерации в области связи требований к заключению договоров об оказании услуг связи, несоблюдение порядка проверки достоверности сведений об абоненте и сведений о пользователях услугами связи абонента — юридического лица либо индивидуального предпринимателя, либо оказание услуг связи в случае отсутствия в федеральной государственной информационной системе «Единая система идентификации и аутентификации» в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» сведений, внесение

[1] Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3 км : приказ МВД России от 25.11.2019 № 878 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=519451&ysclid=lsmxip6bvu620632413#p2Q8L4UPZXEvh7wP (дата обращения: 14.02.2024)

которых является обязательным»[1]. Так по инициативе прокуратуры Республики Крым на 500 тыс. руб. был оштрафован оператор сотовой связи, который не защитил абонента от подмены номера, в результате чего потерпевший стал жертвой дистанционного мошенничества, совершенного с территории сопредельного государства[2]. Еще ранее в 2021 г. вступили в силу изменения в Федеральный закон «О связи», предусматривающие, в том числе, что абоненты — юридические лица и ИП, заключающие договор об оказании услуг подвижной радиотелефонной связи, могут предоставлять физлицам возможность пользоваться услугами корпоративной связи в рамках данного договора только при условии внесения в ЕСИА самим корпоративным абонентом или по его решению пользователем услугами связи сведений о таких пользователях. Однако, как мы видим в настоящий момент, мошеннические звонки по-прежнему осуществляются по многочисленным «серым сим-картам», информация о которых отсутствует в ЕСИА. «В 2023 г. Банк России направил операторам связи с целью принятия соответствующих мер реагирования 575 669 номеров телефонов, используемых злоумышленниками для хищения средств у граждан»[3].

Каждому из участников финансово-кредитных отношений необходимо повышать уровень защищенности самих устройств доступа в интернет и данных владельца, имеющихся на них. Приложения интернет-банкинга должны постоянно обновляться разработчиками, а на официальных сайтах кредитных организаций в качестве бесплатной и обязательной опции необходимо размещать доступные для скачивания антивирусные программы, а не продавать их клиентам как дополнительную опцию (как это делают некоторые банки, предлагая клиентам дополнительные страховки от похищения денег, платные антивирусы, платные защитники от спам-звонков).

На сегодняшний день именно техническая блокировка звонков на номера потерпевших является одной из самых эффективных мер предупреждения (пресечения) дистанционных хищений. Свои технические решения пресечения возникающих угроз от телефонных мошенников предлагают ведущие кредитные организации при помощи цифрового определителя номера, а также мессенджеры — Вотсап, Телеграм, Вайбер. В них абонент самостоятельно может настроить уровень своей конфиденциальности, сделав невидимым для злоумышленника номер своего телефона, фото в аккаунте, запретить звонки с неизвестных номеров.

Однако очень незначительная часть пользователей данных мессенджеров реально пользуется имеющимися техническими способами самозащиты. Поэтому помимо технической, необходимо вести речь и об информационной профилактике. В этой части необходимо не только разъяснять гражданам наиболее распространенные способы дистанционных хищений, а через эти же мессенджеры распространять информациюо возможностях защиты устройств и своих аккаунтов в них, рассказывать о рисках. Подавляющее большинство граждан открыты и добропорядочны, и в силу таких своих личных качеств полагают, что и все остальные в мире тоже добропорядочны, а значит с точки зрения виктимности — уязвимы для злоумышленников, некритичны и доверчивы.

Кроме того, необходимо учитывать, что «в условиях постоянного появления новых финансовых инструментов, криптовалют, NFT (токенов), развития инвестиционных площадок и краудфандинговых платформ человек оказывается в состоянии постоянного дефицита знаний о них. При помощи информационно-когнитивных

[1] Кодекс Российской Федерации об административных правонарушениях : от 30.12.2001 № 195-ФЗ : Статья 13.30. Утратила силу // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34661/c85334785978d8398b3ff32f4b68ddbbd7a217a7/ (дата обращения: 14.02.2024).

[2] Оператор связи оштрафован на полмиллиона за пропуск звонка мошенника // РИА Новости. URL: https://crimea.ria.ru/20231021/operator-svyazi-oshtrafovan-na-polmilliona-za-propusk-zvonka-moshennika-1132221005.html?ysclid=lsls1i6epl75638735 (дата обращения: 21.10.2023).

[3] Обзор операций, совершенных без согласия клиентов финансовых организаций.

технологий этот дефицит с легкостью возмещается «нужной» для субъекта виктимогенного воздействия информацией, что является ключевым этапом виктимизации» [8, с. 66].

А значит, информационное воздействие на жертву должно включать и обогащение его понятными правильными сведениями о сущности новых финансовых институтов. В этой части Центробанком России предприняты меры по повышению уровня финансовой грамотности населения, проводятся онлайн обучающие курсы с фокусными группами населения, в частности с сотрудниками полиции, финансовых учреждений, образовательных организаций всех уровней, в школьную программу вводятся курсы «Основы финансовой грамотности». И это тоже дает свои положительные результаты. Однако в данном случае разъяснительная, обучающая и предупредительная деятельность всех субъектов виктимологической профилактики оказывается в роли «догоняющей», а не опережающей. Поэтому и разработчикам новых финансовых инструментов необходимо, прежде чем они выдут на рынок, разъяснять гражданам возможные сценарии их использования и риски, с этим связанные.

Заключение

Проведенное нами и другими исследователями изучение механизма виктимизации жертв дистанционных хищений позволили прийти к следующим выводам.

Виктимологические признаки потерпевших от дистанционных хищений не отличаются никакими особенностями: в равной мере страдали от действий мошенников и мужчины, и женщины, и молодые, и среднего возраста. Поэтому профилактика дистанционных хищений главным образом должна быть направлена на массовую виктимность и необходимо вести речь в большей степени об общих мерах виктимологической профилактики.

К аналогичным выводам приходят и зарубежные криминологи, обращая внимание на необходимость контекстно-ориентированного микрообучения корпоративной и личной кибербезопасности, отмечая, что сами потерпевшие в виду недостаточности имеющихся у них знаний создают угрозы своей кибербезопасности.

Рассматривая механизм виктимизации потерпевшего, мы приходим к выводу, что создание преступником условий в предкриминальной ситуации значительно повышает эффективность деятельности дистанционных мошенников. А значит и меры предупреждения таких деяний должны быть направлены на устранение таких благоприятных для преступника условий.

В связи с чем полагаем более терминологически верным говорить о сферах воздействия общей превенции: экономической, нормативной, теоретической, практической, технической (технологической), информационной. Соответственно каждой из сфер превентивного воздействия должна строиться единая система виктимологической профилактики дистанционных хищений.

Список источников

1. Базаров Р. А. К вопросу о прикладной направленности криминологической и виктимологической теории, виктимологической профилактике в широком смысле // Виктимология. 2023. Т. 10, № 2. С. 128–137. DOI: https://doi.org/10.47475/2411-0590-2023-10202

2. Дамм И. А., Тарбагаев А. Н. Политика противодействия преступности: вопросы понятийно-категориального аппарата // Всероссийский криминологический журнал. 2023. Т. 17, № 5. С. 397–410. DOI: https://doi.org/10.17150/2500-4255.2023.17(5).397-410 EDN: SOIXAZ.

3. Евтушенко И. И. Виктимологическая защита жертв дистанционных хищений // Виктимология. 2023. Т. 10, № 1. С. 78–88. DOI: https://doi.org/10.47475/2411-0590-2023-10108

4. Жмуров Д. В. Общая виктимологическая профилактика киберпреступности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 135–142. DOI: https://doi.org/10.36511/2078-5356-2022-4-135-142

5. Жмуров Д. В. Кибержертва: особенности классификации // Всероссийский криминологический журнал. 2022. Т. 16, № 4. С. 463–472. DOI: https://doi.org/10.17150/2500-4255.2022.16(4).463-472

6. Игнатов А. Н., Соловьев В. С. Информационно-когнитивные технологии в механизме цифровой виктимизации // Вестник Казанского юридического института МВД России. 2023. Т. 14, № 1 (51). С. 59–66. DOI: https://doi.org/10.37973/KUI.2023.20.15.008

7. Майоров А. В. Влияет ли цифровизация на виктимизацию в современном обществе? // Виктимология. 2022. Т. 9, № 2. С. 148–156. DOI: https://doi.org/10.47475/2411-0590-2022-19202

8. Майоров А. В. Теория и методология виктимологического противодействия преступности в Российской Федерации : автореф. дис. … д-ра юрид. наук. Екатеринбург, 2022. 49 с.

9. Осипенко А. Л., Соловьев В. С. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. Т. 15, № 6. С. 681–691. DOI: https://doi.org/10.17150/2500-4255.2021.15(6).681-691

10. Старостенко О. А. Виктимологическое предупреждение хищений, совершаемых дистанционно : дис. … канд. юрид. наук. Краснодар, 2023. 232 с.

11. Стяжкина С. А. Виктимологическая профилактика кибермошенничества // Вестник удмуртского университета. Экономика и право. 2022. Т. 32, вып. 3. С. 546–552. DOI: https://doi.org/10.35634/2412-9593-2022-32-3-546-552

12. Mungo J. Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks // Journal of Cyber Security Technology. 2024. Vol. 8, no. 2. P. 71–119. DOI: https://doi.org/10.1080/23742917.2023.2244210

13. White G. L. Education and Prevention Relationships on Security Incidents for Home Computers // Journal of Computer Information Systems. 2015. Vol. 55, no. 3. P. 29–37. DOI: https://doi.org/10.1080/08874417.2015.11645769

14. Mahlangu G., Chipfumbu Kangara C., Masunda F. (2023). Citizen-centric cybersecurity model for promoting good cybersecurity behavior // Journal of Cyber Security Technology. 2023. Vol. 7, no. 3. P. 154–180. DOI: https://doi.org/10.1080/23742917.2023.2217535

15. Kävrestad J., Furnell S., Nohlberg M. (2024). User perception of Context-Based Micro-Training — a method for cybersecurity training. Information Security Journal: A Global Perspective. 2024. Vol. 33, no. 2. P. 121–137. DOI: https://doi.org/10.1080/19393555.2023.2222713

16. Yadav Sh. Social automation and APT attributions in national cybersecurity // Journal of Cyber Security Technology. 2024. Vol. 7, no. 1. P. 1–26. DOI: https://doi.org/10.1080/23742917.2023.2300494

References

1. Bazarov RA. To the issue of applied orientation of criminological and victimological theory, victimization prevention in a broad sense. *Viktimologiya* [Victimology]. 2023;10(2):128-137. (In Russ.) DOI: https://doi.org/10.47475/2411-0590-2023-10202

2. Damm IA, Tarbagaev AN. Policy of counteraction to crime: issues of conceptual and categorical apparatus. *Vserossijskij kriminologicheskij zhurnal*=[Russian criminological journal]. 2023;17(5):397-410. (In Russ.) DOI: https://doi.org/10.17150/2500-4255.2023.17(5).397-410 EDN: SOIXAZ.

3. Evtushenko II. Victimological defense of victims of remote theft. *Viktimologiya* [Victimology]. 2023;10(1):78-88. (In Russ.) DOI: https://doi.org/10.47475/2411-0590-2023-10108

4. Zhmurov DV. General victimization prevention of cybercrime. *Yuridicheskaya nauka I praktika: Vestnik Nizhegorodskoj akademii MVD Rossii* [Legal Science and Practice: Bulletin of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia]. 2022;(4(60):135-142. (In Russ.) DOI: https://doi.org/10.36511/2078-5356-2022-4-135-142

5. Zhmurov DV. Cyber victimization: features of classification. *Vserossijskij kriminologicheskij zhurnal* = [Russian criminological journal]. 2022;16(4):463-472. (In Russ.) DOI: https://doi.org/10.17150/2500-4255.2022.16(4).463-472 EDN: QFQHWL.

6. Ignatov AN, Soloviev VS. Information and cognitive technologies in the mechanism of digital victimization. *Yuridicheskaya nauka I praktika: Vestnik Nizhegorodskoj akademii MVD Rossii* [Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia]. 2023;14(1(51):59-66. (In Russ.) DOI: https://doi.org/10.37973/KUI.2023.20.15.008

7. Mayorov AV. Does digitalization influence victimization in modern society? *Viktimologiya* [Victimology]. 2022;9(2):148-156. (In Russ.) DOI: https://doi.org/10.47475/2411-0590-2022-19202

8. Mayorov AV. Theory and methodology of victimologic counteraction to crime in the Russian Federation : [abstract of dissertation]. Ekaterinburg, 2022. 49 p. (In Russ.) EDN: HYYLTI.

9. Osipenko AL, Soloviev VS. Main directions of development of criminological science and practice of crime prevention in the conditions of digitalization of society. *Vserossijskij kriminologicheskij zhurnal* = [Russian criminological journal]. 2021;15(6):681-691. (In Russ.) DOI: https://doi.org/10.17150/2500-4255.2021.15(6).681-691

10. Starostenko OA. *Victimological prevention of thefts committed remotely*: [dissertation]. Krasnodar, 2023. 232 p. (In Russ.)

11. Styazhkina SA. Victimological prevention of cyber fraud. *Vestnik udmurtskogo universiteta. Ekonomika I pravo* [Bulletin of Udmurt University. Economics and Law]. 2022;32(3):546-552. (In Russ.) DOI: https://doi.org/10.35634/2412-9593-2022-32-3-546-552

12. Mungo J. Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks. *Journal of Cyber Security Technology*. 2024;8(2):71-119. DOI: https://doi.org/10.1080/23742917.2023.2244210

13. White GL. Education and Prevention Relationships on Security Incidents for Home Computers. *Journal of Computer Information Systems*. 2015;55(3):29-37. DOI: https://doi.org/10.1080/08874417.2015.11645769

14. Mahlangu G, Chipfumbu Kangara C, Masunda F. Citizen-centric cybersecurity model for promoting good cybersecurity behaviour. *Journal of Cyber Security Technology*. 2023;7(3):154-180. DOI: https://doi.org/10.1080/23742917.2023.2217535

15. Kävrestad J, Furnell S, Nohlberg M. User perception of Context-Based Micro-Training — a method for cybersecurity training. *Information Security Journal: A Global Perspective*. 2024;33(2):121-137. DOI: https://doi.org/10.1080/19393555.2023.2222713

16. Yadav Sh. Social automation and APT attributions in national cybersecurity. *Journal of Cyber Security Technology*. 2024;7(1):1-26. DOI: https://doi.org/10.1080/23742917.2023.2300494

ИНФОРМАЦИЯ ОБ АВТОРЕ

Евтушенко Инна Ивановна

Кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии, Краснодарский университет МВД России, Крымский филиал.

295053, Симферополь, ул. Академика Х. Х. Стевена, д. 14.

inna-evt@yandex.ru

https://orcid.org/ 0000-0002-1335-5404

INFORMATION ABOUT THE AUTHOR

Inna I. Yevtushenko

Candidate of Law Sciences, Associate Professor, Associate Professor of Department of Criminal Law and Criminology of the Crimean Branch of Krasnodar University of the of the MIA of Russia.

14 Akademika Kh. Kh. Stevena str., Simferopol 295053, Russia.

inna-evt@yandex.ru

https://orcid.org/ 0000-0002-1335-5404

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 19.02.2024.
Дата рецензирования статьи / Revised: 25.03.2024.
Дата принятия статьи к публикации / Accepted: 28.03.2024.