Научная статья
Научная специальность
5.1.4 «Уголовно-правовые науки»

УДК 347.965:346:349.3
DOI https://doi.org/10.26516/2071-8136.2023.1.52

ИНДИВИДУАЛЬНАЯ ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

© Жмуров Д. В., 2023
Байкальский государственный университет, г. Иркутск, Россия

Анализируются индивидуальные меры виктимологической профилактики киберпреступности. Даны определение рассматриваемого понятия и описание его ключевых свойств. В ходе анализа специальной литературы, отечественных и зарубежных источников усматриваются три уровня индивидуальной виктимологической профилактики: 1) доинцидентный (разработка стандартов учета виктимного поведения); 2) инцидентный (разработка моделей противодействия киберпреступникам); 3) постинцидентный (разработка стандартов реагирования на кибервиктимизацию). Каждый их этих уровней описан в деталях (включая правила персональной безопасности в доинцидентном ракурсе; а также скрипты реагирования виртуальной жертвы – на постинцидентном этапе). Определено, что каждый из указанных уровней является базовой функциональной частью индивидуальной виктимологической превенции в информационно-телекоммуникационном пространстве.

Ключевые слова: кибервиктимизация, жертвы в интернете, кибервиктимность, кибервиктимология, интернет-потерпевший, жертвы цифровых преступлений, кибержертва, личность потерпевшего в виртуальном пространстве.

INDIVIDUAL VICTIMOLOGICAL PREVENTION OF CYBERCRIME

© Zhmurov D. V., 2023
Baikal State University, Irkutsk, Russian Federation

The article is devoted to the analysis of individual measures of victimological prevention of cybercrime. The paper defines the concept under consideration and describes its key properties. During the analysis of special literature, domestic and foreign sources, three levels of individual victimological prevention are identified: 1. Pre-incident (development of models for countering cybercriminals); 2. Incidental (development of victim behavior accounting standards); 3. Post-incident (development of standards for responding to cyber-victimization). Each of these levels is described in detail (including the rules of personal security in the pre-incident perspective; as well as scripts for responding to a virtual victim - at the post–incident stage). Each of these levels is a basic functional part of an individual psychological prevention in the information and telecommunications space.

Keywords: cybervictimization, victims on the Internet, cybervictimity, cybervictimology, Internet victim, victims of digital crimes, cyber victim, victim's identity in the virtual space.

Введение

Индивидуальная виктимологическая профилактика киберпреступности представляет собой превентивную деятельность, направленную на лиц, обладающих повышенной виктимностью в информационно-технологической среде

Разделяя мнение С. А. Невского и Е. Н. Клещиной относительно выделения двух типов виктимологической профилактики – общесоциального и индивидуального [5], последний желательно понимать как деятельность по недопущению кибервиктимизации среди отдельных групп населения и частных лиц (одновременно объединяющей признаки специальной и индивидуальной профилактики). Его суть, по мнению В. И. Полубинского, состоит в приобщении человека к социальному опыту, формировании у него положительных личностных качеств, поднятии уровня сознания до высоты общественного в целях уменьшения индивидуальной виктимности [6]. Целесообразность проведения виктимологической профилактики заключается в том, что данная политика социально необходима, экономически выгодна и не требует серьезных материальных затрат. В то же время, при условии качественного информационного и методического обеспечения, она вполне эффективна и рациональна [7].

Традиционно выделяются три подвида индивидуальной виктимологической профилактики: первичная, непосредственная и вторичная [4]. Первая касается раннего выявления признаков

повышенной виктимности, определения групп и лиц, подверженных криминальному воздействию в большей степени (носит предварительный характер). Вторая применима к субъектам, виктимизируемым в актуальный момент времени или тем, кто находится в предкриминальной ситуации (для текущих обстоятельств). Третья распространяет свое действие на состоявшихся жертв и предполагает оказание мер реабилитации-ресоциализации (на поствиктимном этапе).

Таким образом, можно отметить несколько отличительных особенностей индивидуальной виктимологической профилактики киберпреступности. Она:

– персонифицирована и направлена на ограниченный круг субъектов, являющихся потенциальными жертвами цифровых преступлений;

– представлена совокупностью мер разового характера, являющихся элементами единой системы и направленных на создание условий, при которых лицо (группа) не реализует свой виктимогенный потенциал;

– носит строго дифференцированный характер, реализуется в гармонии с личностными особенностями носителя виктимности и типизацией его поведения [3];

– оказывает локальное воздействие на группы риска кибервиктимизации.

К целевым установкам индивидуальной виктимологической профилактики можно отнести:

а) снижение рисков, располагающих лицо (группу) к тому, чтобы стать жертвой киберпреступления;

б) воздействие на причины и условия индивидуального поведения потенциальных жертв;

в) противодействие негативным факторам ближайшего социального окружения жертвы, т. е. виктимогенным особенностям ее микросреды;

г) прямое воздействие на личность, которая в силу индивидуальных характеристик способна оказаться жертвой киберпреступления.

Материалы и методы исследования

Для изучения проблемы использовался диалектический метод познания, позволяющий предметно и во всех отношениях проанализировать сущность виктимологической профилактики киберпреступности. В основу методологической базы положен ряд общенаучных приемов в их согласованности и взаимообусловленности. Указанные способы познания представлены как на теоретическом (сравнительный, системный, исторический методы), так и на эмпирическом уровнях (исследование документов, контент-анализ). Кроме того, учитывались современные методологические положения философии, социологии, криминологии, виктимологии, уголовного права, криминальной психологии и других гуманитарных наук.

Обзор литературы

Проблема, изучаемая в настоящей статье, находит свое фрагментарное отражение в работах отечественных и зарубежных исследователей.

Во-первых, это труды ученых, заложивших и разрабатывающих основы виктимологической профилактики как научной концепции (Ю. М. Антонян, Н. В. Исаев, В. И. Полубинский, А. В. Майоров, А. Л. Репецкая, Н. Е. Шинкевич, Д. В. Ривман и другие).

Во-вторых, источники, посвященные вопросам виктимологической профилактики киберпреступности и ее частных проявлений. Последние в основном представлены на уровне тезисов выступлений или научных статей. Например, общим вопросам виктимологической превенции в виртуальной среде посвящены работы Т. М. Лопатиной (2006), И. Н Заварыкина (2021), Е. А. Родиной (2022), Г. Ф. Биктагировой, Р. А. Валеевой, А. Р. Дроздиковой-Зариповой, Н. Н. Калацкой, Н. Ю. Костюниной (2019) и др. Частные аспекты виктимологической профилактики в интернете представлены в исследованиях Я. С. Киракосяна, Е. А. Колотухиной, А. А. Смирнова, Н. А. Коротковой, Л. В. Ушаковой, О. В. Мицука, Я. С. Горбатюка, О. С. Березиной, Т. В. Шинкевича, Е. К. Погодиной, О. А. Старостенко, С. А. Стяжкиной, А. А. Комарова и других авторов. Среди ключевых тем указанных публикаций можно отметить предупредительную работу с потенциальными жертвами сексуальных деликтов; преступлений, связанных с вовлечением в незаконный оборот наркотиков; кибермошенничества, кибербуллинга и проч.

Результаты исследования

Индивидуальная виктимологическая профилактика киберпреступности сводится к адаптации, аксикреации, девиктимизации отдельных категорий субъектов. Главная ее задача – усилить личную безопасность потенциальных жертв интернет-преступлений, повысить степень их защищенности и выработать основы социального иммунитета (антикриминальных защитных реакций).

Упомянутые выше тезисы позволяют сформулировать ключевые уровни индивидуальной виктимологической профилактики:

1. *Доинцидентный* (разработка моделей раннего противодействия киберпреступности) – заключается во внедрении значительного числа стандартов и шаблонов, снижающих виктимность в цифровом пространстве и не до-

пускающих ее реализации. Они формируются на *индивидуально-поведенческом уровне* (путем воспитательных или образовательных мероприятий, сертификации персонала, повышения квалификации, предустановки на устройства комплекса обучающих и защитных программ) или *нормативном* – в виде национальных стандартов информационной безопасности, которых на сегодня насчитывается уже более десятка.

Например, для физических лиц можно выделить несколько эталонов доинцидентной виктимологической безопасности:

– *безопасное использование гаджетов и персонального компьютера*. Установка лицензионного программного обеспечения и его регулярные обновления; загрузка приложений только из официальных источников; установка платной антивирусной защиты; осторожность и аккуратность при опубликовании личной информации или ее пересылке; установка ПИН-кода на сим-карту; систематическая очистка средств отслеживания – cookie-файлов, временных файлов браузера, журнала посещений; разделение доступа к данным в многопользовательском режиме; периодическая проверка состояния платных услуг и подписок; проверка сторонних подключений, например, по Bluetooth; хранение конфиденциальной информации в автономном режиме; настройка оповещений о выпуске электронной подписи на портале госуслуг; оформление в Росреестре запрета на сделки с недвижимостью без личного присутствия с использованием электронной подписи; подключение оповещений банков через push, а не СМС; отключение прав на просмотр СМС, звонков, записной или адресной книги у приложений, которые вызывают сомнения; блокировка удаленных соединений, удаленного восстановления доступа и закрытие внешних портов;

– *безопасный серфинг в виртуальном пространстве*. Проверка надежности сайтов и защищенности соединения; осознание того, что в интернете нет ничего бесплатного; отказ от публичных торрент-трекеров; опросов, розыгрышей, кешбэк-сервисов, особенно их браузерных расширений; проявление осторожности в выборе круга общения и демонстрации интимных сторон жизни; использование двухфакторной аутентификации и сложных ключей генерации; двойная проверка достоверности информации, обнаруженной в Сети; защита доступа через отпечаток пальца, FACE ID, подтверждение на третьем устройстве; практика обязательного разлогинивания на чужих ПК, использование защищенных и анонимных сетей VPN, шифрование собственного интернет-трафика; удаление метаданных из публикуемого контента, к примеру имени автора, меток геолокации, даты создания файлов; грамотное генерирование паролей в соответствии с правилами безопасности; использование настроек приватности в виде отказа от передачи телеметрии, избыточных данных, рекламных идентификаторов;

– *навыки защиты от вредоносных программ*. Использование операционных систем последней версии; автообновление браузера; использование системных решений в области безопасности, включающих не только антивирус и файрволл, но и антиспам, антифишинг и проч.; установка патчей для рабочих программ; использование компьютера в статусе пользователя, а не администратора; отказ от установки неизвестных программ и приложений, неиспользование файлов, происхождение которых сомнительно; систематические проверки внешних носителей и внутреннего дискового пространства; отказ от передачи собственных устройств третьим лицам и применения чужих гаджетов;

– *безопасная эксплуатация сетей Wi-Fi*. Приоритет использования запароленных сетей; запрет на передачу конфиденциальных данных и платежной информации через публичный доступ; обязательное использование файрволла, зашифрованных соединений, VPN; использование специальных браузерных расширений, усиливающих безопасность, например HTTPS Everywhere; включение передачи данных в защищенном режиме для ресурсов, автоматически не поддерживающих эту опцию; дезактивация функций «подключение к Wi-Fi автоматически» и «общий доступ к файлам и принтерам»;

– *безопасная активность в социальных сетях*. Тщательное отношение к кандидатам в друзья; удаление неиспользуемых аккаунтов; проверка подлинности профилей, входящих в круг общения; самоограничения на публикацию конфиденциальных сведений, геоданных, информации о родственниках; использование закрытого профиля и систем усиленной защиты авторизации; верификация при помощи дополнительного e-mail; периодическая смена паролей; проверка достоверности информации от друзей по телефону, вне сети или других мессенджерах, особенно когда речь о денежных переводах и т. п.; осторожность при информировании аудитории о дорогих покупках, поездках, состоянии здоровья, сделках, детях, маршрутах передвижения, планах на ближайшее будущее; осмотрительность при встрече с новыми друзьями офлайн, желательно в людных местах и с извещением близких; вежливое и корректное поведение; ограничение запросов со стороны

социальной сети и связанных с ней приложений на сканирование адресной книги; осторожность при инсталляции дополнений и приложений для социальной сети; фиксация в настройках видимости пункта «показывать только друзьям»; благоразумие при использовании чужих сведений для регистрации фейковых аккаунтов;

– *безопасное использование электронной почты*. Выбор зарекомендовавшего себя почтового сервиса с адекватным уровнем защиты; создание нескольких почтовых ящиков – для официальной и частной переписки; установка дополнительного пароля на папку «исходящие письма»; отказ от хранения на почте сканированных документов и паролей; обязательность выхода из аккаунта в случае просмотра корреспонденции в местах публичного пользования; использование ЭПЦ для важной переписки; активное использование спам-фильтрации; хранение адресов корреспондентов в поле «скрытая копия» (blind carbon copy, BCC), избегание неизвестной корреспонденции и ссылок, содержащихся в ней; отказ от самостоятельного удаления очевидного спама (требуется добавление его в «черный список»), а также некритичного аннулирования подписок, на которые пользователь не давал согласия; использование почтовых антивирусов; осторожность при вводе защитных паролей или кодов для разархивирования вложений, запуска макросов, активного содержимого или Active X в прикрепленных почтовых файлах; верификация и проверка отправителей сомнительных писем; требования к паролям и VPN аналогичны указанным выше;

– *безопасная игровая деятельность онлайн*. Отказ от внесения персональных данных в игровой профиль; от использования анонимных и пиратских серверов с низким рейтингом; разрешение конфликтов и спорных ситуаций через администрацию сайта; блокирование подозрительных (агрессивных) игроков; использование «белого списка» игроков; неприменение читерских программ, неофициальных патчей, а также сторонних обновлений; вежливое общение в игровых чатах; сдержанность и недоверие к различного рода «выгодным предложениям», например раздаче игрового инвентаря, продаже внутриигровых товаров по сниженным ценам, организации договорных сражений или «виртуальных банд»; осторожность при покупке-продаже высокоуровневых персонажей; использование антигриферских плагинов для резервного копирования игрового мира, борьбы с массовым спауном мобов, флудом чата, для записи информации о взаимодействии игроков с хранилищами предметов и т. п.; скрин-фиксация коммуникаций или разрушений в игре для предъявления в качестве возможных доказательств; бережное хранение игрового имущества, в реализуемых случаях – анонимность и неприметность игровой жизни;

– *безопасное осуществление онлайн-покупок*. Использование в интернете виртуальной (кредитной, дебетовой) карты, специально выпущенной для этих целей; хранение ограниченной суммы денег на счету либо выставление лимитов по проводимым операциям; оплата на защищенных сайтах с сертификатом, подписанным доверенными центром (желательно уровня OV – Organization Validation, EV – Extended Validation); своевременное информирование банка о смене номера телефона или утрате платежной карты; отказ от использования публичных прокси-серверов, анонимайзеров, общих точек доступа при проведении финансовых операций; отключение автозаполнения платежных форм в браузере; детальная проверка контрагентов, с которыми намечается проведение сделок; поиск отзывов о качестве работы площадок (магазинов), предоставляющих услугу; перед осуществлением покупок проверка наличия разнообразных чек-боксов, навязывающих подписки, взносы или страховки; хранение платежных реквизитов и данных карт в строжайшей конфиденциальности; использование приложений из официальных магазинов; ввод веб-адресов непосредственно от руки в адресной строке; периодическое ознакомление с выписками по кредитной карте на наличие несанкционированных транзакций; бойкотирование предварительной оплаты покупок; мониторинг цен товаров, при этом их низкая стоимость должна вызывать подозрения; приоритетный выбор самовывоза или курьерской доставки товара с оплатой на месте;

– *доведение уровня индивидуальных технико-виктимологических стандартов до приемлемого*. Заключается во внедрении комплексных решений, направленных на персональную девиктимизацию и предназначенных для пользователей информационно-телекоммуникационных систем.

Предпочтительными выглядят системные технические решения, во-первых, оценивающие степень виктимности пользователя; во-вторых, препятствующие ее возможной реализации. Оценка виктимности может осуществляться по формализованным критериям (наличие фейковых профилей в списках друзей из социальных сетей; степень открытости личного аккаунта; использование или отказ от программ безопасности, характер посещаемых интернет-ресурсов; время, проведенное в Мировой сети, наличие

и частота спама на персональных устройствах и проч.). Воспрепятствование реализации виктимного потенциала представляется более сложной задачей. На автоматизированном уровне оно может быть воплощено в функциональном комплексе ассистирующих программ, которые включают в себя несколько традиционных и новых компонентов. Среди них:

– антивирусная защита и сетевой экран;

– блокировка спама, антифишинговые инструменты, антишпион, защита от перехвата, контроль программ и устройств, родительский контроль;

– защищенный канал (VPN), резервное копирование, менеджер паролей, шифрование информации, безопасные платежи;

– менеджер обновления программ, фоновое удаление следов активности, отслеживание потенциально опасных и нежелательных утилит;

– защита конфиденциальных данных и настоящей личности пользователя, ограничение времени пребывания в интернете;

– эвристический анализ потенциальной виктимности действий пользователя с отправкой ему соответствующих предупреждений (например, касающихся текста получаемых или отправляемых сообщений; загружаемых сканов документов; оформляемых покупок и проводимых транзакций, регистрации на низкорейтинговых или недавно появившихся сайтах);

– автоматический анализ политик конфиденциальности используемых ресурсов с предоставлением пользователю конспективного изложения их основных условий и индикацией опасных параметров (когда, к примеру, сайт получает право распоряжаться личными данными клиента);

– антифейк – субкомпонент, позволяющий верифицировать качество получаемой информации. Ее анализ может быть основан на сверке источников данных, оценке их авторитетности, обнаружении плагиата в посторонних материалах, нахождении признаков монтажа в фотоснимках (технологии уже существующих сервисов, например Forensically и Ghiro).

Доинцидентный уровень виктимологической профилактики, таким образом, исходит из нескольких существенных положений, несмотря на разнообразие и содержательную специфику частных предписаний. Укажем их тезисно:

а) *максимальная персонализация*, т. е. привязка устройств и профилей к личности пользователя, его индивидуальным характеристикам, позволяющим отличить от других объектов идентификации (цифровые ключи и подписи, объемно-пространственная форма лица, следы пальцев рук, голосовая биометрия, подтверждение через другие персональные устройства);

б) *индивидуализация использования*, когда цифровые устройства приравнены к средствам персональной гигиены, при этом постулируется их единоличное применение; этикетно подразумевается непередаваемость (нетранзакционность) третьим лицам ввиду интимности и важности содержащегося контента;

в) *минимизация цифрового следа* – настроенность оставлять как можно меньше информации о своей личности, отдельных сторонах частной жизни, а также информационных отпечатков, если в этом нет определенной необходимости;

г) *нулевое доверие* к происходящим в виртуальной жизни событиям: требование постоянных сомнений, уточнения, перепроверки и верификации получаемых сведений;

д) *использование актуальных систем и инструментов цифрового мира* означает требование к постоянному обновлению рабочих программ и элементов. В диалектической борьбе создателей программного обеспечения и хакеров, пытающихся обнаружить в нем уязвимости, техническая платформа виртуального пространства быстро устаревает и становится податливой для компрометации. Перспективным является не только обучение виктимологической безопасности, но и создание комплексного технического инструментария ее поддержки;

е) *мотивированность на контрвиктимные репутационные и поведенческие стратегии* означает приоритет правил и норм бесконфликтного взаимодействия в интернете, ограничение импульсивных финансового, коммуникативного, стратификационного и иных форм поведения.

2. *Инцидентный* уровень (разработка стандартов учета виктимного поведения) предполагает концентрацию внимания на выявлении, фиксации, подсчете и статистическом отображении группы виктимизированных лиц в интернете. Сегодня уже существует практика создания специальных институтов, выполняющих указанные задачи. Конечно, проблема может быть решена общепринятым форматом приема заявлений граждан о киберпреступлениях. Однако такой подход не исключает субъективизма представителей правоохранительных органов на местах: их нежелания реагировать на сложные, не имеющие следственной перспективы инциденты; отсутствия в локальных подразделениях квалифицированных кадров, способных оказать профессиональную помощь и т. п. Эти трудности отчасти преодолимы за счет учреждения специальных органов интернет-монито-

ринга. Они могут быть как государственными, так и общественными (частными).

В США, например, функционирует Internet Crime Complaint Center (IC3), центр приема сообщений о преступлениях в интернете [2]. Он является подразделением Федерального бюро расследований (ФБР) и осуществляет целенаправленную деятельность в отношении подозреваемых в киберпреступлениях. Центр информирует органы власти, правоохранительные органы разных уровней (от местного до международного), составляет ежегодные аналитические доклады и рассматривает обращения граждан. Обратиться с заявлением может либо пострадавший, либо третья сторона в его интересах. При этом бюрократические процедуры сведены к минимуму: подача заявления осуществляется онлайн, для его рассмотрения достаточно указать имя, адрес, телефон, электронную почту жертвы и обстоятельства произошедшего. Аналогичными или близкими по смыслу являются службы Action Fraud (при генеральной прокуратуре Великобритании); Melani (учрежденное Федеральной службой разведки и Федеральным стратегическим подразделением по информационным технологиям Швейцарии); онлайн-система приема сообщений об интернет-преступлениях ICROS в системе Европола и проч. В России эти функции мог бы выполнять Единый центр кибервиктимизации (ЕЦК).

Каждая из названных выше организаций аффилирована с государственными службами, хотя имеются прецеденты, когда инициатива исходит от частных лиц. Например, государственно-частное партнерство Signal Spam (Франция), целью которого является систематизация данных о спам-потоках и их организаторах, которые впоследствии могут быть использованы при расследовании уголовных или административных дел. Схожей инициативой стали Cyberbullying Research Center (Центр изучения кибербуллинга), Национальный центр по предотвращению издевательств PACER и проч. В этом ракурсе важной задачей властей выступает поддержка НКО, развитие общественных организаций, связанных с отслеживанием и оценкой случаев виктимизации в виртуальном пространстве. Немаловажное значение имеет международное сотрудничество в вопросах регистрации и расследования киберпреступлений.

3) *Постинцидентный* уровень (разработка стандартов реагирования на кибервиктимизацию) относится к преодолению ближайших и отдаленных последствий киберпреступности. Виктимологическое наполнение этого направления деятельности сводится к следующим аспектам:

– *качественным изменениям индивидуального сознания* в части восприятия процессуального правосудия как доверенного института [9], куда можно *сообщать об опыте виктимизации в Сети*. Иными словами, недостаточно организации работы по приему заявлений о киберпреступлениях (на общем уровне виктимологической профилактики), необходима также мотивация со стороны потерпевших уведомлять компетентные органы о подобных случаях. Именно заявления жертв позволят выявлять отдельные категории киберпреступлений и охарактеризовать modus operandi виртуального делинквента [1]. Известно, что искажения статистики и высокая латентность киберпреступлений вызваны не только их сложным техническим характером, но и нежеланием кибержертв делиться опытом виктимизации с семьей, друзьями или правоохранительными органами [10]. Для применения протекционных мер со стороны государства требуется «сигнал о необходимости» этих действий – заявление защищаемого или уполномоченного лица [8];

– *формированию институтов поддержки жертв киберпреступлений* – созданию структур, призванных оказывать содействие виктимизированным лицам (консультационная, правовая, психологическая помощь). В России сегодня действуют НКО и волонтерские проекты, направленные на решение указанной задачи, но этой работе не хватает системности и масштабирования. Например, для пострадавших от кибербуллинга открыты интернет-программы «Травли.net», сервис «Маяк» проекта «Добро.mail.ru», горячая линия «Дети онлайн» и проч. Для пострадавших от иных киберпреступлений подобных инициатив, к сожалению, обнаружить не удалось.

Обучение частным сценариям реагирования на отдельные преступления также является эффективной составляющей постинцидентной профилактики. Следует указать на несколько направлений подобной работы:

– обучение *сценариям реагирования на кибербуллинг*. Асимметричная и, как правило, неагрессивная реакция; по возможности отстраненное восприятие происходящего; игнорирование разовых попыток киберпреследования или запугивания; блокировка комментариев и установка запрета отмечать себя в записях (на фото); бан агрессора, сообщение администрации сайта; фото- и видеофиксация переписки, сохранение аудиосообщений; если игнорирование неэффективно, целесообразно использовать гибкие сценарии ответа на активность буллера (требование деанонимизации, обсуждение его

поведения с наблюдателем, использование понижающих словосочетаний и фраз, публичное информирование о предпринятых формальных мерах, попытка войти в доверие и проч.); закрытие профиля, а в наиболее серьезных ситуациях – удаление своего аккаунта для пресечения дальнейших попыток дискриминации; смена электронных контактов; для несовершеннолетних – обращение к педагогам и родителям; заявление в правоохранительные органы – в случае угроз жизни и здоровью;

– обучение *сценариям реагирования на интернет-мошенничество.* Блокировка карты, аккаунтов и номеров, привязанных к платежным идентификаторам; сообщение на горячие линии банка, мобильного оператора, платежной системы о произошедшем инциденте, оповещение друзей и близких о факте мошенничества, если имеется угроза дальнейших вредоносных действий; смена паролей на всех устройствах; сообщение о правонарушении в поддержку «Яндекса» и «Гугла», Роспотребнадзор; сохранение скриншотов транзакций, переговоров с преступниками, детализации телефонных звонков, помимо этого, получение в банке выписки с отраженной криминальной операцией и заявление в полицию; проверка устройства на вирусы и вредоносные программы; в других случаях эксперты рекомендуют полное отключение смартфона или ПК для того, чтобы обеспечить сохранность цифровых следов для полицейских экспертов; использование механизмов чарджбэка или опротестования платежа в течение определенного периода;

– обучение *сценариям реагирования на несанкционированный доступ к почте и аккаунтам.* Восстановление доступа и смена паролей; удаление подозрительных устройств и сессий; проверка настроек переадресации почты на ящик преступника; уведомление всех заинтересованных лиц, в том числе администрации ресурса; проверка других своих аккаунтов на предмет действий, которые не совершались, а именно отправки сообщений с просьбами финансового характера, подачи заявлений на портале госуслуг, оформления электронной подписи и т. д.;

– обучение *сценариям реагирования на кибервымогательство*. Откат устройства к заводским настройкам, если информация на нем не представляет особой ценности; загрузка устройства в безопасном режиме и использование различных утилит для поиска вредоносных программ или дешифровки данных (проект nomoreransom.org); перепрошивка устройства в сервисном центре; использование программ-дешифраторов или деблокировщиков операционной системы, а также специальных защит от программ-вымогателей, например Kaspersky Anti-Ransomware Tool; тщательное документирование непрограммных вымогательств и заявление о них в полицию.

Итак, постинцидентный уровень виктимологического реагирования построен на таких важнейших максимах, как:

а) *инициативность жертвы*, т. е. осознание необходимости противодействия киберпреступникам, а также личной ответственности за разрешение этой конфронтации;

б) *формирование виктимологических скриптов реагирования* на эпизоды дискриминации, т. е. закрепление в информационной культуре стереотипов ответа кибержертвы на действия преступника, применение ей фактических и процессуальных мер защиты;

в) *создание ассистирующей инфраструктуры,* посредством которой должна реализоваться организационная и психологическая поддержка жертв киберпреступлений.

Обсуждения и заключения

Безусловно, индивидуальная виктимологическая профилактика киберпреступности не ограничивается перечисленными мерами. Особый интерес вызывает выстраивание системы прогнозирования кибервиктимизации и оценки ее последствий, использование методов неотложной виктимологической профилактики замышляемых и подготавливаемых киберпреступлений и т. п. Наиважнейшими задачами представленных мер являются формирование у виртуальной личности установок на индивидуальную безопасность, снижение склонности к цифровым рискам, а также выработка контрвиктимных компетенций. Указанные меры окажутся малоэффективными без коррелирующей связи с элементами общей виктимологической профилактики, которым суждено составить концептуальную суть превентивной политики в виртуальной среде.

СПИСОК ЛИТЕРАТУРЫ

1. Кириленко В. П., Алексеев Г. В. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. 2020. Т. 14, № 6. С. 898–913. https://doi.org/10.17150/2500-4255.2020.14(6).898-913.

2. Комаров А. А. Исследование виктимологических рисков интернет-мошенничества в зависимости от возраста пользователей глобальной сети // Всероссийский криминологический журнал. 2012. № 1. С. 65–68.

3. Коновалова И. А. Виктимологические аспекты предупреждения корыстных преступлений, совершаемые несовершеннолетними // Право и жизнь. 2013. № 5 (179). С. 256–281.

4. Мумаев С. С. Понятие, типология и профилактика криминальной виктимности // Аспирант и соискатель. 2004. № 5. С. 325–326

5. Невский С. А. Клещина Е. Н. О современных проблемах профилактики преступлений // Историческая и социально-образовательная мысль. 2010. № 2. С. 19–24.

6. Полубинский В. И. Виктимологические аспекты профилактики преступлений. М. : Акад. МВД СССР, 1980. 77 с.

7. Титушкина Е. Ю. Правовые основы профилактики преступности: пути совершенствования // Всероссийский криминологический журнал. 2013. № 1. С. 59–62.

8. Щедрин Н. В. Введение в правовую теорию мер безопасности: монография. Красноярск : Краснояр. гос. ун-т, 1999. 184 с.

9. Enzmann D., Lukash A. Виктимизация, обращение в полицию и понимание термина «процедурная справедливость» в межнациональном аспекте // International Scientific Conference «Contemporary Criminology: Achievements, Problems, Perspectives». At: Kharkiv, Ukraine.

10. Jansen J., Leukfeldt E. R. Coping with cybercrime victimization: An exploratory study into impact and change // Journal of Qualitative Criminal Justice and Criminology. 2018. Vol. 6, iss. 2. P. 205–228.

REFERENCES

1. Kirilenko V.P., Alekseev G.V. Garmonizaciya rossijskogo ugolovnogo zakonoda-tel'stva o protivodejstvii kiberprestupnosti s pravovymi standartami Soveta Evropy [The harmonization of Russian criminal legislation on counteracting cybercrime with the legal standards of the Council of Europe]. *Vserossijskij kriminologicheskij zhurnal* [Russian Journal of Criminology], 2020, Vol. 14, no. 6, pp. 898-913. https://doi.org/10.17150/2500-4255.2020.14(6).898-913 (in Russian)

2. Komarov A.A. Issledovanie viktimologicheskih riskov internet-moshennichestva v zavisimosti ot vozrasta pol'zovatelej global'noj seti [A study of victimological risks of the internet fraud depending on the age of the internet users]. *Vserossijskij kriminologicheskij zhurnal* [Russian Journal of Criminology], 2012, no. 1, pp. 65-68. (in Russian)

3. Konovalova I.A. Viktimologicheskie aspekty preduprezhdeniya korystnyh prestuplenij, sovershaemye nesovershennoletnimi [Victimological aspects of the prevention of acquisitive crimes committed by minors]. *Pravo i zhizn'* [Law and Life], 2013, no. 5 (179), pp. 256-281. (in Russian)

4. Mumaev S.S. Ponyatie, tipologiya i profilaktika kriminal'noj viktimnosti [The concept, typology and prevention of criminal victimization]. *Aspirant i soiskatel'* [PhD student and applicant], 2004, no. 5, pp. 325-326. (in Russian)

5. Nevskij S.A., Kleshchina E.N. O sovremennyh problemah profilaktiki prestuplenij [On the current problems of crime prevention]. *Istoricheskaya i social'no-obrazovatel'naya mysl'* [Historical and Social-Educational Idea], 2010, no. 2, pp. 19-24. (in Russian)

6. Polubinskij V.I. *Viktimologicheskie aspekty profilaktiki prestuplenij* [Victimological aspects of crime prevention]. Moscow, SSSR MIA Academy Publ., 1980, 77 p. (in Russian)

7. Titushkina E.Yu. Pravovye osnovy profilaktiki prestupnosti: puti sovershenstvovaniya [Legal fundamentals of crime prevention: ways of improvement]. *Vserossijskij kriminologicheskij zhurnal* [Russian Journal of Criminology], 2013, no. 1, pp. 59-62. (in Russian)

8. Shchedrin N.V. *Vvedenie v pravovuyu teoriyu mer bezopasnosti: monografiya* [Introduction to the legal theory of security measures: monograph]. Krasnoyarsk, Krasnoyar. gos. un-t Publ., 1999, 180 p. (in Russian)

9. Enzmann D., Lukash A. *Viktimizaciya, obrashchenie v policiyu i ponimanie termina «procedurnaya spravedlivost'» v mezhnacional'nom aspekte* [Victimization, appeal to the police and understanding of the term «procedural justice» in the international aspect]. International Scientific Conference "Contemporary Criminology: Achievements, Problems, Perspectives". Kharkiv, Ukraine. (in Russian)

10. Jansen J., Leukfeldt E.R. *Coping with cybercrime victimization: An exploratory study into impact and change*. Journal of Qualitative Criminal Jus-tice and Criminology. 2018, vol. 6, iss. 2, pp. 205-228.

Статья поступила в редакцию 24.03.2022; одобрена после рецензирования 15.05.2022; принята к публикации 08.02.2023

Received on 24.03.2022; approved on 15.05.2022; accepted for publication on 08.02.2023

Жмуров Дмитрий Витальевич – кандидат юридических наук, доцент кафедры уголовного права и криминологии, Институт юстиции, Байкальский государственный университет (Россия, 664003, г. Иркутск, ул. Ленина, 11), ORCID: 0000-0003-0493-265X, ResearcherID: ABH-8471-2020, e-mail: zdevraz@ya.ru

Zhmurov Dmitry Vitalievich – Candidate of Juridical Sciences, Associate Professor of the Department of Criminal Law and Criminology, Institute of Justice, Baikal State University (11, Lenina st., Irkutsk, 664003, Russian Federation), ORCID: 0000-0003-0493-265X, ResearcherID: ABH-8471-2020, e-mail: zdevraz@ya.ru