Наталья Александровна ГРИШКО,
доцент кафедры уголовного права, уголовного процесса и правоохранительной деятельности Российского университета транспорта (МИИТ), кандидат юридических наук
grish.nat88@yandex.ru
127055, Россия, г. Москва, ул. Образцова, д. 9, стр. 9

Защита потенциальных жертв киберпреступлений: виктимологический подход

Аннотация. *В статье анализируется природа кибервиктимности, выделяются ключевые категории риска и основные формы виктимного поведения в киберсреде. Особое внимание уделяется профилактическим стратегиям, направленным на снижение виктимного потенциала личности, а также возможностям правового и социального реагирования. Предложены рекомендации по развитию системы виктимологической помощи, просветительских программ и межведомственного взаимодействия. Подчеркивается необходимость формирования культуры цифровой безопасности как элемента общей профилактики киберпреступности. Предлагаются рекомендации по совершенствованию системы защиты жертв в рамках виктимологической парадигмы. Важное значение отводится индивидуальной виктимологической профилактике. Отмечаются сущностные особенности процесса кибервиктимизации как части общей виктимологической теории. Рассматриваются проблемы, возникающие при расследовании киберпреступлений, оказывающие, в свою очередь, влияние на виктимологическую составляющую киберпреступлений. Выделены и охарактеризованы ключевые компоненты поведенческой модели жертвы киберпреступлений: когнитивный, эмоциональный и поведенческий. Приведены типовые модели поведения, предрасполагающие к виктимизации в киберпространстве.*

В работе приведены зарубежный и отечественный опыт реализации программ и проектов, направленных на виктимологическую профилактику в цифровом пространстве, так как международный опыт представляет ценность для формирования эффективной системы виктимологической профилактики в России и может служить основой для сравнительно-правового анализа.

Ключевые слова: *киберпреступность, кибервиктимизация, модель поведения жертвы, индивидуальная виктимологическая профилактика*

DOI: 10.17803/2311-5998.2025.129.5.234-243

Natalia A. GRISHKO,
Associate Professor of the Department of Criminal Law,
Criminal Procedure and Law Enforcement
at the Russian University of Transport (MIIT),
Cand. Sci. (Law)
grish.nat88@yandex.ru
9/9, ul. Obraztsova, Moscow, Russia, 127055

Protecting Potential Victims of Cybercrime: a Victimological Approach

Abstract. *The article analyzes the nature of digital victimization, identifies key risk categories and the main forms of victim behavior in the cyber environment. Special attention is paid to preventive strategies aimed at reducing the victim potential of the individual, as well as the possibilities of legal and social response. Recommendations on the development of a system of victimological assistance, educational programs and interdepartmental cooperation are proposed. The need for the formation of a digital security culture as an element of the general prevention of cybercrime is emphasized. Recommendations for improving the victim protection system within the victimological paradigm are proposed. Individual victimological prevention is of great importance. The essential features of the process of cyber-victimization as part of the general victimological theory are noted. The problems that arise in the investigation of cybercrimes, which, in turn, have an impact on the victimological component of cybercrime, are considered. The problems that arise in the investigation of cybercrimes are considered, which, in turn, have an impact on the victimological component of cybercrimes. The key components of the behavioral model of a victim of cybercrime are identified and characterized: cognitive, emotional and behavioral. Typical patterns of behavior predisposing to victimization in cyberspace are given.*
The paper presents foreign and domestic experience in the implementation of programs and projects aimed at victimological prevention in the digital space, as international experience is valuable for the formation of an effective system of victimological prevention in Russia and can serve as a basis for comparative legal analysis.
Keywords: *cybercrime, cyber-victimization, victim's behavioral model, individual victimological prevention*

Современная виктимология, ориентированная на анализ причин, способствующих становлению личности жертвой преступления, в условиях цифровизации сталкивается с новыми формами виктимности. Киберпреступность характеризуется высокой анонимностью, трансграничностью и социальной инженерией, что создает качественно иные условия для формирования виктимного поведения. Эффективная защита жертв невозможна без глубокого понимания виктимологических закономерностей цифрового пространства.

Виктимологический подход позволяет рассматривать защиту жертв киберпреступлений не как эпизодическую реакцию, а как системную превентивную деятельность. Цифровая виктимность — это новое явление, требующее мультидисциплинарного подхода. Важнейшим направлением становится формирование *цифровой культуры виктимологической осведомленности*, где каждый субъект понимает собственную уязвимость и знает способы ее снижения.

Уголовное законодательство РФ сегодня не предлагает легального определения киберпреступления, что непосредственно оказывает влияние на понятие «жертва киберпреступления». Чаще всего под киберпреступлением понимается деяние, совершенное с использованием информационных технологий или направленное на объекты информационной инфраструктуры[1].

Важно определить в этой связи ключевые признаки киберпреступлений:
— использование компьютерных технологий как инструмента совершения преступления;
— объект посягательства — информация, данные, системы и сети;
— сложность установления личности правонарушителя;
— часто носит трансграничный характер[2].

Расследование киберпреступлений представляет собой одно из самых сложных направлений в деятельности правоохранительных органов, поскольку такие деяния совершаются в условиях высокой технологической динамики, трансграничности и анонимности субъектов. При расследовании данного вида преступлений возникает множество препятствий: от пробелов в правовом регулировании и дефицита специалистов до международных барьеров и недостаточной технологической базы. Эффективное преодоление этих проблем требует:
— совершенствования уголовного и уголовно-процессуального законодательства;
— создания специализированных подразделений с технической экспертизой;
— расширения международной кооперации;
— внедрения современных методов цифровой криминалистики.

Процесс кибервиктимизации сегодня вовлекает все большее количество участников, а сам процесс становления жертвы киберпреступлений отличается следующими признаками:
— «коллективность» жертв;
— анонимность «преступника»;
— скоростной режим преступного воздействия;
— низкий уровень правосознания;
— доступность киберпространства;
— киберзависимость;
— психологические проблемы;
— разнообразие форм и методов киберпреступлений;
— нормативно-правовая ограниченность;
— удаленный режим воздействия преступника на жертву и др.

---

[1] *Яковлев А. Ф.* Преступления в киберпространстве: правовые аспекты // Уголовное право. 2022. № 5. С. 34—38.

[2] *Соловьев Д. П.* Киберугрозы и уголовная ответственность // Вестник Московского университета. Серия 11 : Право. 2021. № 6. С. 72—78.

Обозначенные причины оставляют небольшие шансы участнику киберпространства обеспечить свою безопасность от преступного посягательства. При этом гибкость «преступных возможностей» своевременно подстраивается под современные реалии практически всех сфер жизнедеятельности людей.

Кибервиктимизацию рассматривают сегодня многие научные междисциплинарные направления, среди которых: социология Интернета, киберпсихология, цифровая криминология, кибервиктимология, технические науки, опосредующие процесс взаимодействия операторов и машин в виртуальной среде[3]. Кибервиктимизация — сложный и многогранный феномен, сочетающий в себе как индивидуальные поведенческие установки жертвы, так и социальные и технологические риски.

Одним из ключевых механизмов кибервиктимизации является поведенческая модель личности, определяющая способ ее присутствия и взаимодействия в цифровом пространстве. В отличие от классических форм виктимного поведения, поведенческие и коммуникативные установки в Интернете приобретают новые характеристики, связанные с особенностями виртуальной среды: иллюзией анонимности, стремлением к самопрезентации, доступностью и быстротой коммуникаций. В отличие от традиционных форм виктимного поведения, поведенческая модель жертв киберпреступлений формируется под влиянием особых условий цифровой среды, в которой отсутствует физический контакт, преобладают дистанционные коммуникации и наблюдается смещение границ частного и публичного.

Современные криминологи и виктимологи выделяют три ключевых компонента поведенческой модели жертвы киберпреступлений:

— когнитивный компонент — уровень знаний о цифровых рисках, правовом регулировании онлайн-деятельности, принципах кибергигиены. Низкая информированность и отсутствие критического мышления повышают вероятность попадания в опасные ситуации;
— эмоциональный компонент — эмоциональное состояние личности, ее склонность к доверчивости, тревожности, одиночеству. Люди, испытывающие потребность в общении или признании, чаще вовлекаются в манипулятивные взаимодействия (например, скамеры, груминг, шантаж);
— поведенческий компонент — конкретные действия и практики пользователя в сети: размещение персональной информации, участие в онлайн-конфликтах, переход по сомнительным ссылкам, отсутствие защиты аккаунтов[4].

Поведенческая модель жертвы киберпреступления — это результат взаимосвязи индивидуальных психологических характеристик, уровня цифровой культуры и особенностей онлайн-коммуникации. Поведенческая модель жертвы киберпреступления не является статичной — она может меняться под влиянием внешних обстоятельств (кризисы, изоляция, эмоциональные потрясения), что повышает вероятность вовлечения в преступную ситуацию. Более того, многие

[3] *Жмуров Д. В.* Кибервиктимизация. Исследовательская матрица // Пролог: журнал о праве. 2021. № 3. С. 109—121.

[4] *Назаров Д. В.* Киберповедение личности: между безопасностью и риском // Социальная психология и общество. 2021. № 3. С. 59—64.

пользователи одновременно могут выступать и жертвами, и участниками виктимогенных ситуаций, особенно в условиях массовой цифровой коммуникации.

Для части пользователей Интернет становится основным каналом общения, источником признания и самооценки. Это особенно характерно для подростков и представителей маргинализированных групп. Такое стремление к социальной валидации делает их восприимчивыми к манипуляциям и втягиванию в опасные отношения.

Анализ правоприменительной и эмпирической практики позволяет выделить *типовые модели поведения*, предрасполагающие к виктимизации в цифровой среде:

— наивно-доверчивый тип — характеризуется отсутствием осторожности, открытостью к незнакомцам, некритичным восприятием информации (часто — пожилые люди и подростки);
— самопрезентативный тип — склонен к демонстрации личной жизни в соцсетях, что делает жертву уязвимой к шантажу, буллингу и манипуляциям;
— рисково-экспериментальный тип — участвует в опасных интернет-активностях (хакерские игры, флешмобы, подпольные чаты), часто не осознавая последствий;
— правонеосведомленный тип — не знает или игнорирует механизмы защиты своих прав в сети, не обращается в правоохранительные органы при столкновении с преступлением[5].

Киберпреступность представляет собой многоплановую угрозу, требующую адаптивных и комплексных решений. Защита потенциальных жертв — это не только задача правоохранительных органов, но и приоритетное направление государственной политики в области цифрового развития и безопасности. В современных условиях необходим переход от реактивного подхода к проактивной модели, основанной на профилактике, просвещении и межсекторальном сотрудничестве.

В условиях цифровой среды особенно возрастает значение индивидуальной виктимологической профилактики, поскольку киберугрозы обладают высокой адаптивностью, а потенциальные жертвы все чаще становятся объектами *персонализированных атак*.

В отличие от групповой или массовой профилактики (например, информационных кампаний), *индивидуальная профилактика* позволяет учитывать личностные, психологические, социальные и технические особенности человека. Это особенно важно в киберпространстве, где один пользователь может быть защищен, а другой — в силу возраста, состояния здоровья или стиля поведения — оставаться крайне уязвимым.

Индивидуальный подход позволяет:

— выявлять скрытые формы виктимности, которые не видны в рамках общей статистики;
— адаптировать методы профилактики к уровню цифровой грамотности и психологической устойчивости субъекта;

[5] *Соколова И. А.* Виктимологический анализ интернет-преступлений: поведенческий аспект // Криминология: научные труды. 2022. № 2. С. 42—47.

— снижать риск вторичной виктимизации, особенно у лиц, уже переживших киберпосягательство.

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[6].

Ключевые уровни индивидуальной виктимологической профилактики можно представить в следующей классификации:

1. Доинцидентный уровень (разработка моделей раннего противодействия киберпреступности) заключается во внедрении значительного числа стандартов и шаблонов, снижающих виктимность в цифровом пространстве и не допускающих ее реализации. Они формируются на индивидуально-поведенческом (путем воспитательных или образовательных мероприятий, сертификации персонала, повышения квалификации, предустановки на устройства комплекса обучающих и защитных программ) или нормативном уровне в виде национальных стандартов информационной безопасности, которых на сегодня насчитывается уже более десятка. Среди них можно выделить:

а) безопасное использование гаджетов и персонального компьютера (установка лицензионного программного обеспечения, антивирусная защита; проверка сторонних подключений, очистка средств отслеживания, блокировка удаленных соединений и др.);

б) безопасный серфинг в виртуальном пространстве (использование двухфакторной аутентификации и сложных ключей генерации, практика обязательного разлогинивания на чужих ПК, использование настроек приватности в виде отказа от передачи телеметрии, избыточных данных, рекламных идентификаторов и др.);

в) навыки защиты от вредоносных программ (отказ от установки неизвестных программ и приложений, отказ от передачи собственных устройств третьим лицам, автообновление браузера, использование системных решений в области безопасности и др.);

г) безопасная эксплуатация сетей Wi-Fi (запрет на передачу конфиденциальных данных и платежной информации через публичный доступ, использование специальных браузерных расширений, усиливающих безопасность, дезактивация функций «подключение к Wi-Fi автоматически» и др.);

д) безопасная активность в социальных сетях (проверка подлинности профилей, периодическая смена паролей, осторожность при инсталляции дополнений и приложений для социальной сети др.);

[6] *Жмуров Д. В.* Индивидуальная виктимологическая профилактика киберпреступности // Сибирский юридический вестник. 2023. № 1. С. 52—59.

е) безопасное использование электронной почты (избегание неизвестной корреспонденции и ссылок, верификация и проверка отправителей сомнительных писем, использование почтовых антивирусов, использование ЭПЦ для важной переписки, активное использование спам-фильтрации и др.);

ж) безопасная игровая деятельность онлайн (использование антигриферских плагинов для резервного копирования игрового мира, скрин-фиксация коммуникаций и др.);

и) безопасное осуществление онлайн-покупок (хранение ограниченной суммы денег на счету, отключение автозаполнения платежных форм в браузере, проверка наличия разнообразных чек-боксов, периодическое ознакомление с выписками по кредитной карте на наличие несанкционированных транзакций)[7].

2. Инцидентный уровень (разработка стандартов учета виктимного поведения) предполагает концентрацию внимания на выявлении, фиксации, подсчете и статистическом отображении группы виктимизированных лиц в Интернете.

3. Постинцидентный уровень (разработка стандартов реагирования на кибервиктимизацию) относится к преодолению ближайших и отдаленных последствий киберпреступности. К нему относятся: организация работы по приему заявлений о киберпреступлениях; формирование институтов поддержки жертв киберпреступлений — создание структур, призванных оказывать содействие виктимизированным лицам (консультационная, правовая, психологическая помощь); обучение сценариям реагирования.

Разработка системы эффективной защиты жертвы киберпреступлений не может отвечать практико-ориентированности без таких важных звеньевых элементов, как виктимное профилирование и прогноз.

Виктимное профилирование должно разработать наиболее четкий и полный профиль жертвы в киберпространстве на основе классификационных типологий с определением индивидуальных особенностей психолого-поведенческого свойства.

Виктимологический прогноз должен основываться на критериях обусловленности, распространенности и эпидемичности[8].

Обусловленность строится на дифференциальном подходе — выявлении зависимости кибервиктимных тенденций от гендерных, возрастных, поведенческих, личностных условий или причин. Как статистический показатель распространенность определяет интенсивность кибервиктимных актов и число лиц, потерпевших от них. Эпидемичность в данном вопросе оценивает способность актов кибервиктимизации причинять вред в плане социального и физического здоровья, негативно воздействовать на популяцию.

Методы, применяемые в индивидуальной профилактике кибержертв, имеют важное значение и могут варьироваться в зависимости от характеристик потенциальной жертвы. К ним можно отнести:

— консультирование — индивидуальные беседы с психологами, педагогами или специалистами по информационной безопасности;

---

[7] *Жмуров Д. В.* Индивидуальная виктимологическая профилактика киберпреступности.

[8] *Жмуров Д. В.* Кибервиктимизация. Исследовательская матрица.

— обучение на примерах — разбор конкретных случаев кибермошенничества, имитация фишинговых атак в контролируемой среде;
— психологическая поддержка — оказание помощи лицам, уже ставшим жертвами, с целью предотвращения повторной виктимизации;
— настройка технических средств защиты — помощь в установке и правильной конфигурации антивирусов, систем двухфакторной аутентификации и родительского контроля;
— медико-социальное сопровождение для лиц с психоневрологическими расстройствами или когнитивными нарушениями.

Индивидуальная виктимологическая профилактика в условиях киберугроз становится необходимым элементом национальной политики в сфере безопасности. Она позволяет не только снижать риск виктимизации конкретных лиц, но и формировать культуру цифровой самозащиты, опирающуюся на осознанность, компетентность и психологическую готовность, что делает ее стратегическим инструментом в борьбе с современной, все более сложной и персонализированной киберпреступностью.

В зарубежной криминологической и виктимологической практике особое внимание уделяется снижению уровня виктимности посредством комплексных мер, включающих правовое просвещение, технические инструменты защиты и институциональные гарантии.

В Великобритании функции по защите населения от киберугроз возложены на Национальный центр кибербезопасности (NCSC)[9], действующий при разведывательном агентстве GCHQ. Центр активно взаимодействует с бизнесом, образовательными учреждениями и гражданским обществом. Одним из ключевых направлений работы является программа Cyber Aware, ориентированная на формирование цифровой грамотности населения. В рамках инициативы распространяются рекомендации по настройке учетных записей, использованию двухфакторной аутентификации, защите данных. Дополнительно функционирует сервис Suspicious Email Reporting Service (SERS), позволяющий оперативно реагировать на фишинговые атаки и обучать население их распознаванию.

Германия делает акцент на формировании цифровой ответственности и превенции виктимизации на ранних этапах социализации. Проект Klicksafe, реализуемый при поддержке Европейской комиссии, предоставляет платформу для обучения школьников, учителей и родителей основам цифровой безопасности[10]; активно развиваются направления поведенческой аналитики и индивидуальной оценки киберрисков, что позволяет предсказывать вероятность виктимизации определенных категорий пользователей и адаптировать меры защиты.

Сингапур демонстрирует пример системного стратегического подхода к снижению киберрисков. Государственное агентство Cyber Security Agency of Singapore

[9] National Cyber Security Centre. Cyber Aware // URL: https://www.ncsc.gov.uk/cyberaware (дата обращения: 20.03.2025).

[10] U.S. Department of Homeland Security. Stop.Think.Connect. Campaign // URL: https://www.dhs.gov/stopthinkconnect (дата обращения: 22.03.2025).

(CSA)[11] разработало национальную стратегию кибербезопасности, в которую включен отдельный блок, посвященный защите населения. Программа Go Safe Online охватывает не только обучающие кампании, но и разработку пользовательских приложений для мониторинга подозрительных действий в сети, а также поддерживает «кибердобровольчество» — инициативу вовлечения молодежи в просветительскую деятельность.

Изучение зарубежного опыта защиты потенциальных жертв киберпреступлений позволяет выделить ряд эффективных подходов:

— превенция через образование и цифровую грамотность;
— широкое межведомственное и общественно-государственное сотрудничество;
— индивидуализация профилактики с учетом уязвимости пользователя;
— активное вовлечение частного сектора и гражданских инициатив.

Анализируется значение виктимологической профилактики преступлений в условиях цифровизации общества. Исследуется трансформация виктимного поведения в цифровом пространстве, обусловленная как ростом цифровых угроз, так и изменением структуры коммуникаций. Рассматриваются ключевые группы риска, механизмы воздействия на потенциальных жертв со стороны преступников, а также типовые модели виктимизации.

В России активно развиваются проекты и программы, направленные на виктимологическую профилактику в цифровом пространстве. Такие инициативы реализуются на государственном, региональном и общественном уровнях. В ряде регионов реализуются пилотные проекты, направленные на виктимологическую профилактику, например:

— программа «Цифровой иммунитет» для школьников и студентов;
— интерактивный портал МВД России по кибербезопасности;
— инициативы по цифровому просвещению от «Сбербанка», «Яндекса», Лаборатории Касперского и др.

Особое внимание в системе виктимологической профилактики уделяется просветительским и образовательным проектам. Так, в рамках национального проекта «Цифровая экономика» реализуется программа повышения цифровой грамотности, направленная на формирование устойчивого защитного поведения в сети. Аналогичную цель преследует инициатива «Цифровой диктант», ориентированная на диагностику и развитие навыков безопасного поведения у широкого круга пользователей.

В последние годы активно развиваются федеральные, региональные и частные инициативы, направленные на формирование культуры безопасного поведения в цифровой среде и снижение виктимности различных социальных групп, они включают как образовательные, так и информационно-просветительские компоненты и реализуются при сотрудничестве государственных структур, IT-компаний и образовательных учреждений.

Цифровизация различных сфер общественной жизни привела к трансформации традиционных форм преступности и появлению новых угроз. Одновременно с этим изменяется и профиль потенциальной жертвы. Виктимологическая

[11] Cyber Security Agency of Singapore. Go Safe Online // URL: https://www.csa.gov.sg/gosafeonline (дата обращения: 12.03.2025).

профилактика приобретает особую актуальность в условиях стремительного роста количества киберпреступлений и повышения уязвимости граждан в цифровой среде.

Киберпреступность порождает особую форму виктимности, требующую специализированных подходов к защите. Виктимологическая профилактика в цифровом пространстве должна сочетать правовые, образовательные и психологические меры, а также учитывать специфику уязвимых групп. Только системное внедрение моделей цифровой самозащиты и широкая виктимологическая просветительская работа способны эффективно снизить уровень виктимизации и укрепить личную и общественную безопасность в киберпространстве.

БИБЛИОГРАФИЯ

1. *Жмуров Д. В.* Индивидуальная виктимологическая профилактика киберпреступности // Сибирский юридический вестник. — 2023. — № 1. — С. 52—59.
2. *Жмуров Д. В.* Кибервиктимизация. Исследовательская матрица // Пролог: журнал о праве. — 2021. — № 3. — С. 109—121.
3. *Назаров Д. В.* Киберповедение личности: между безопасностью и риском // Социальная психология и общество. — 2021. — № 3. — С. 59—64.
4. *Соколова И. А.* Виктимологический анализ интернет-преступлений: поведенческий аспект // Криминология: научные труды. — 2022. — № 2. — С. 42—47.
5. *Соловьев Д. П.* Киберугрозы и уголовная ответственность // Вестник Московского университета. — Серия 11 : Право. — 2021. — № 6. — С. 72—78.
6. *Яковлев А. Ф.* Преступления в киберпространстве: правовые аспекты // Уголовное право. — 2022. — № 5. — С. 34—38.
7. Cyber Security Agency of Singapore. Go Safe Online // URL: https://www.csa.gov.sg/gosafeonline (дата обращения: 12.03.2025).
8. National Cyber Security Centre. Cyber Aware // URL: https://www.ncsc.gov.uk/cyberaware (дата обращения: 20.03.2025).
9. U.S. Department of Homeland Security. Stop.Think.Connect. Campaign // URL: https://www.dhs.gov/stopthinkconnect (дата обращения: 22.03.2025).