УДК 343.988

**Олег Александрович СТАРОСТЕНКО,**
адъюнкт
Краснодарского университета МВД России
*olegstaros94@gmail.com*

# ВИКТИМОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛИЧНОСТИ В СЕТИ ИНТЕРНЕТ

# VICTIMOLOGICAL PROBLEMS OF ENSURING PERSONAL SECURITY ON THE INTERNET

В статье рассмотрено понятие виктимологической безопасности личности, произведен анализ жертв, пострадавших от хищений в сети Интернет. В ходе анализа установлено, что поведение жертвы складывается из психологической и технической составляющих. Кроме того, выделены основные насущные проблемы обеспечения безопасности личности в сети Интернет: несовершенство действующего законодательства, отсутствие механизмов выявления правонарушителей по электронно-цифровому следу, анонимность цифрового пространства, экстерриториальность, отсутствие цифровой культуры; приводятся рекомендации для пользователей сети, как не стать жертвой хищений в сети Интернет.

The article considers the concept of victimological security of a person, analyzes the victims who suffered from theft on the Internet. The analysis found that the behavior of the victim consists of psychological and technical components. In addition, the main pressing problems of ensuring the security of the person on the Internet are revealed: imperfection of the current legislation; lack of mechanisms for identifying offenders on an electronic digital trace; anonymity of digital space; extraterritoriality; lack of digital culture; the instructions for network users how not to become a victim of theft on the Internet are given.

**Ключевые слова:** виктимологическая безопасность, жертва, Интернет, хищения, профилактика.
**Keywords:** *victimological safety, victim, Internet, theft, prevention.*

Исследователи в области психологии, социологии и криминологии на протяжении длительного времени пытаются понять радикальное развитие новой парадигмы отношений, возникшей в результате распространения информационно-телекоммуникационных технологий. Использование сети Интернет и осуществление профессиональной деятельности в режиме «онлайн» становятся повседневным явлением. Однако стоит отметить, что на фоне масштабного развития кибертехнологий развиваются тенденции использования их возможностей против личности. В связи с этим изучение проблем виктимологического обеспечения личности в киберпространстве становится актуальным направлением науки криминологии.

Определение виктимологической безопасности личности впервые было введено в научный оборот В.И. Задорожным. Он считал, что содержание виктимологической безопасности составляет «защищенность граж-

дан от реализации присущих им виктимных свойств и качеств, при которой будут созданы условия, дающие возможность выявлять, устранять или нейтрализовать факторы, способствующие совершению преступлений в отношении конкретного лица, а также выявлять группы риска или конкретных лиц с повышенной степенью виктимности, воздействовать на них с целью восстановления их защитных свойств» [2, с. 38].

В виктимологическом словаре под исследуемым термином понимается «уровень защищенности лиц и их виктимных категорий от внешних и внутренних угроз, в том числе экстремальных, криминальных, возникающих в конфликтных ситуациях, обеспечиваемый государством и его субъектами посредством снижения виктимности этих лиц. Кроме того, снижение уровня негативного влияния виктимогенных факторов достигается с помощью активного внедрения мер, которые вырабатывает криминальная виктимология»[1].

В.И. Полубинский утверждает, что безопасность личности является неотъемлемым качеством конкретного индивида и обуславливается совокупностью психологических, социальных и физических свойств, а также в зависимости от возникшей жизненной ситуации способствует формированию обстоятельств, при которых реализовывается возможность причинения вреда [4, с. 24].

Несмотря на комплексные научные разработки криминальной виктимологии, проблемам обеспечения безопасности жертв в сети Интернет уделяется меньше внимания. По данным официальной статистики Генпрокуратуры России, в 2020 г. правоохранительные органы зарегистрировали 510,4 тыс. киберпреступлений – это седьмая часть от общего количества уголовных дел. Прирост по сравнению с 2019 г. составил 70,1%. Расследованы менее 50 тысяч. Речь идет о нарушениях Уголовного кодекса Российской Федерации, которые совершаются с помощью Интернета, мобильной связи и использования банковских карт[2].

В Министерстве внутренних дел Российской Федерации данную тенденцию подтверждают. За 2020 г. «число противоправных деяний, совершенных с применением информационных технологий», увеличилось почти на 72%[3].

Аналитики организации «Интернет-розыск» прогнозируют к 2023 г. рост доли хищений, совершаемых с использованием информационно-телекоммуникационных технологий, с 14 до 30%. Связано это со сложностью идентификации IT-злоумышленников[4].

Анализ полученных в ходе нашего исследования данных (был произведен контент-анализ информационных ресурсов, изучены более 210 приговоров суда по ст. 158, 159, 159.6 УК РФ, произведен анонимный интернет-опрос 412 пользователей IT-технологий, 276 из которых становились жертвами IT-хищений) свидетельствует о том, что жертв, пострадавших от IT-хищений, можно разделить на две группы:

1) жертвы хищений, совершенных путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет (необходимо квалифицировать по ст. 158, 159; 159;3 УК РФ). Данные преступления включают в себя сокрытие информации или предоставление неверной информации с целью вымогательства или кражи у жертв денег, имущества или наследства (механизм воздействия: человек-человек);

2) жертвы хищений, совершенных в сфере компьютерной информации (необходимо квалифицировать по ст. 159.6 УК РФ) – целенаправленное вмешательство в работу программ и баз данных (воздействие на технику), которое нарушает процесс обработки, хра-

1 Словарь виктимологических терминов. URL https://slovar.cc/rus/tolk/12772.html (дата обращения: 07.10.2021).

2 Статистические данные о зарегистрированных преступлениях на территории Российской Федерации за период 2020 года. Генеральная прокуратура Российской Федерации. URL: http://genproc.gov.ru (дата обращения: 01.05.2021).

3 Официальный сайт МВД России. URL https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 01.05.2021).

4 Официальный сайт журнала «Известия». URL: https://iz.ru/962966 (дата обращения: 07.10.2021).

нения, передачи компьютерной информации и позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него[5].

Ввиду того, что при хищениях в сфере компьютерной информации зачастую наблюдается «размывание» субъекта индивидуальной виктимизации, т.е. физического лица, непосредственной жертвы преступления [1, с. 116] (виктимогенным фактором выступает техническая незащищенность пользователя, а не личность потерпевшего), обратимся к анализу жертв хищений первой группы.

Согласно позиции науки виктимологии, жертву хищений, совершенных путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, можно охарактеризовать как виновную жертву.

При рассмотрении случаев виновного поведения жертв в сети Интернет самую серьезную группу составляют провокации, которые чаще всего происходят при высокой активности пользователя в социальных сетях, желании приобрести какой-либо товар по наиболее выгодной цене на электронных торговых площадках, таких как «Авито», «Юла», «Дром» и др., найти доступный способ удаленного заработка. Кроме того, виновное поведение жертв зачастую проявляется в неосмотрительности, легкомысленности и неосторожности. Выражается это, к примеру, в отказе от конфиденциальных настроек при использовании социальных сетей, принятии запросов о добавлении в друзья от незнакомых лиц, переходе по потенциально опасным ссылкам.

Основной причиной такого рода виктимности будут выступать отсутствие у большей части граждан общих навыков использования информационно-телекоммуникационных технологий в домашних и рабочих условиях, низкая просвещенность о способах совершения IT-мошеннических действий и способах защиты от них, а также легкомысленное отношение к ним.

Таким образом, действия преступника зачастую зависят не только от его личностных качеств, мотивов, наклонностей, но и от поведения жертвы, которая своими действиями и поступками создает необходимые условия для совершения в отношении себя преступления (стремится обогатиться, получить платное бесплатно, приобрести редкие предметы и вещи, принять участие в благотворительности и др., чаще всего используя при этом систему быстрого обмена сообщениями посредством электронной почты и социальных сетей) [подр.: 7, с. 104].

В ходе сбора и анализа эмпирического материала выявлены следующие основные проблемы обеспечения безопасности личности в сети Интернет:

1) несовершенство действующего законодательства, информационно-аналитической работы, планирования и прогнозирования, организации взаимодействия субъектов, обеспечения должного контроля в данной сфере. Данные пробелы не позволяют в полной мере включить виктимологическую профилактику в арсенал правоохранительной деятельности;

2) отсутствие механизмов выявления правонарушителей по электронно-цифровому следу [6, с. 303];

3) анонимность цифрового пространства. Если в физическом мире злоумышленник осуществляет какие-либо действия для сокрытия своей личности, то в мире цифровых технологий за него это уже сделано. Все пользователи сайтов, форумов или социальных сетей в цифровом пространстве изначально не имеют ни имен, ни внешнего вида – они эфемерны, и нередко информационные ресурсы сами присваивают таким пользователям имя «anonymous», то есть аноним;

4) экстерриториальность. Хищения, совершаемые с использованием глобальной сети Интернет, во многих случаях подпадают под несколько юрисдикций ввиду сложности установления места преступления [2, с. 178];

5) отсутствие цифровой культуры. В киберпространстве отсутствуют законодательно закрепленные правила поведения, что заставляет администраторов сайтов раз-

5 О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 29.06.2021).

рабатывать собственные стандарты. Такие стандарты поведения являются малоэффективными, поскольку в случае блокировки пользователя на одном сайте ему не составит сложности найти сходный сайт. Кроме того, отсутствие закрепленных правил поведения в сети Интернет породило такие организованные преступные сообщества, как хакеры, киберпираты, «яхубои» и т.д.

Таким образом, противодействие киберпреступности требует всестороннего подхода, включающего в себя активизацию виктимологической профилактики.

На основе собранного и проанализированного эмпирического материала нами была разработана инструкция для пользователей сети Интернет «Как не стать жертвой хищений в сети Интернет» [подр.: 8, с. 377].

1. Персональные данные можно вводить только на государственных сайтах либо на сайтах покупки билетов (в том случае, когда соединение устанавливается по протоколу https). Слева от адреса веб-сайта должен появиться значок в виде зеленого замка, означающий, что соединение защищено. Если же пользователем принято решение осуществить покупку на другом сайте, то перед отправкой персональной или конфиденциальной информации необходимо проявлять осмотрительность и изучать сторонний интернет-сайт, анализировать отзывы, активность, контент, контактную информацию.

2. При обнаружении подозрительных действий необходимо сообщить об этом администратору веб-сайта, на котором был размещен «фиктивный листинг», кликнув на панель «онлайн-консультант» или позвонив по номеру телефона технической поддержки, указанной на сайте.

3. Необходимо защитить свою личность и финансы. В случаях денежного перевода в пользу мошенников необходимо срочно уведомить компанию, через которую был произведен платеж, с целью отслеживания и возврата денежных средств. Кредитные и дебетовые карты имеют право на возврат платежа, а средства, отправленные с помощью подарочных карт или банковского перевода, могут быть заблокированы. Также периодически следует проверять выписки из банка и кредитной карты на предмет любых мошеннических списаний денежных средств.

4. Очень желательно предупредить других. Если лицо подверглось преступному воздействию, следует произвести обмен опытом и предупредить близких как посредством социальных сетей и телекоммуникационной связи, так и на чат-форумах, оставив негативные отзывы.

5. Важно использовать надежные технические средства защиты: антиспам-фильтры (антискамминг-технологии, фильтрации технического спама и др.); непрерывную аутенфикацию с целью анализа событий, происходящих на протяжении всего сеанса при использовании цифрового сервиса (например, Advanced Authentication by Kaspersky[6] и др. ); программы, анализирующие устройства и окружения (для идентификации «правомерных» устройств на основе поведенческого анализа пользователя и поведенческой биометрии – анализа взаимодействий клиента с устройством путем отслеживания движений мыши, кликов, касаний и др.), например Avast Fraud Prevention[7] и др., антивирусное программное обеспечение и т.д.

Необходимо отметить, что использование автоматизированных средств противодействия IT-мошенничеству не позволит искоренить проблему полностью: «Первичная виктимизация пользователей зачастую связана с низким уровнем их правовой грамотности» [5, с. 112]. Это свидетельствует о необходимости непрерывного повышения уровня правовой и финансовой грамотности личности.

Повысить уровень осведомленности личности можно путем проведения лекций, профессиональных бесед, собраний с трудовыми коллективами, учащимися в школах, колледжах, университетах, пенсионерами по месту

6 Новейшие технологии на основе экспертных знаний // Официальный сайт Лаборатории Касперского. Защита от кибермошенничества. URL: https://www.kaspersky.ru/enterprise-security/fraud-prevention (дата обращения: 19.10.2021).

7 Официальный сайт Avast. Защита от мошенничества. URL: https://www.avast.ru/c-scam (дата обращения: 19.10.2021).

проживания. Представляется достаточно важным, помимо проведения бесед виктимологического профиля, поручить основным субъектам профилактической работы вести специализированный учет лиц, пострадавших от сетевых мошеннических деяний. На каждое указанное лицо должна быть заведена виктимологическая карта, в которой отражалась бы информация о совершенных противоправных действиях, их причинах и последствиях. Виктимологические карты могли бы послужить основой при определении направлений индивидуальной профилактической работы.

Таким образом, дальнейшее развитие и совершенствование системы виктимологической профилактики во многом будет зависеть от комплексности принимаемых мер, а также поддержки общества и государства.

**Библиографический список**

1. Жмуров, Д.В. Кибервиктимология как новая учебная дисциплина: методическая разработка / Д. В. Жмуров // Baikal Research Journal. – 2021. – Т. 12. – N 3. – DOI 10.17150/2411-6262.2021.12(3).25.

2. Задорожный, В.И. Виктимологическая безопасность и ее обеспечение мерами виктимологической профилактики : монография / В.И. Задорожный. – Тамбов: Першина, 2005. – 161 с.

3. Ищук, Я.Г. Цифровая криминология : учебное пособие / Я.Г. Ищук, Т.В. Пинкевич, Е.С. Смольянинов. – М.: Академия управления МВД России, 2021. – 244 с.

4. Полубинский, В.И. Правовые основы учения о жертве преступления / В.И. Полубинский. – Горький, 1979. – 83 с.

5. Профилактика и коррекция виктимного поведения студенческой молодежи в Глобальной сети Интернет: теория, практика / Г.Ф. Биктагирова, Р.А. Валеева, А.Р. Дроздикова-Зарипова [и др.]. – Казань: Издательство «Отечество», 2019. – 320 с.

6. Старостенко, Н.И. Механизм следообразования вишинга / Н.И. Старостенко // Теория и практика расследования преступлений : материалы IX международной научно-практической конференции (Краснодар, 15 апреля 2021 г.) / редкол.: Э.С. Данильян [и др.]. – Краснодар: Краснодарский университет Министерства внутренних дел Российской Федерации, 2021. – С. 301-306.

7. Старостенко, О.А. О необходимости теоретических знаний в исследовании феномена IT-мошенничества / О.А. Старостенко // Правовая культура в современном обществе : сборник научных статей IV международной научно-практической конференции (Могилев, 14 мая 2021 г.). – Могилев: Могилевский институт Министерства внутренних дел Республики Беларусь, 2021. – С. 103-105.

8. Старостенко, О.А. Об особенностях дифференциации способов совершения информационно-телекоммуникационного мошенничества в период пандемии COVID-19 и основных мерах безопасности в киберпространстве / О.А. Старостенко // Уголовная политика и культура противодействия преступности : материалы международной научно-практической конференции (Краснодар, 11 сентября 2020 г.). – Краснодар: Краснодарский университет Министерства внутренних дел Российской Федерации, 2020. – С. 375-378.