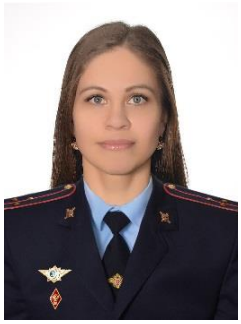
Научная статья
doi: 10.29039/2312-7937-2024-1-107-111



СИДОРОВА ЕКАТЕРИНА ЗАКАРИЕВНА
Восточно-Сибирский институт МВД России (Иркутск, Россия)

ketrik6@mail.ru

ORCID.ORG/0000-0001-5045-2054

УСОВ ЕВГЕНИЙ ГЕННАДЬЕВИЧ
Байкальский институт БРИКС ИРНИТУ (Иркутск, Россия)

usov.evgeniy@list.ru

ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ (ЦИФРОВЫХ) ТЕХНОЛОГИЙ

Аннотация. В статье представлена общая характеристика виктимологической профилактики преступлений, совершенных с использованием информационных (цифровых) технологий. Авторы подчеркивают, что изучение уголовно-правовых и криминологических особенностей цифровой преступности является обоснованным и необходимым на современном этапе развития общества и государства. Актуальность исследования обусловлена тем, что современный мир в большей степени ориентирован на переход в цифровое пространство. И поскольку современная преступность активно использует в своих криминальных целях информационные (цифровые) технологии, правоприменитель, занимающийся борьбой с цифровыми преступлениями, нуждается в теоретически обоснованных исследованиях по данной тематике.

Целью настоящей работы является раскрытие виктимологических особенностей профилактики некоторых составов цифровых преступлений, а также исследование криминологически значимых характеристик современной цифровой преступности и разработка на данной основе ключевых мер, направленных на предупреждение преступлений, совершаемых в информационном пространстве.

В настоящем исследовании авторы делают акцент на основах виктимологической профилактики цифровой преступности. В статье идет речь о том, какие основные меры должны быть приняты гражданами, чтобы обезопасить себя от становления жертвой цифрового (кибер) преступления. Распространенность использования современных цифровых технологий не вызывает сомнений, и человек, использующий ИТТ, может с легкостью стать жертвой киберпреступления либо просто пострадать из-за отсутствия у него базисных правил цифровой безопасности. В этой связи основы виктимологической профилактики представляют собой важную составляющую превенции цифровой преступности.

Настоящее исследование предназначено для лиц, интересующихся вопросами уголовно-правового противодействия преступлениям, совершенным с использованием информационных (цифровых) технологий.

Ключевые слова и словосочетания: цифровая преступность, киберпреступления, виктимология, криминологическое предупреждение, жертва преступления, виктимологическая профилактика.

Для цитирования: *Сидорова Е.З., Усов Е.Г. Виктимологическая профилактика преступлений, совершенных с использованием информационных (цифровых) технологий // Вестник ВИПК МВД России. – 2024. – № 1 (69). – С. 107-111; doi: 10.29039/2312-7937-2024-1-107-111*

SIDOROVA EKATERINA Z.
East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation (Irkutsk, Russia)
USOV EVGENIJ G.
Baikal Institute of BRICS IRNTU (Irkutsk, Russia)

VICTIMOLOGICAL PREVENTION OF CRIMES COMMITTED WITH THE USE OF INFORMATION (DIGITAL) TECHNOLOGIES

Annotation. The article presents the general characteristics of victimological prevention of crimes committed using information (digital) technologies. The authors emphasize that the study of criminal law and criminological features of digital crime is justified and necessary at the present stage of development of society and the state. The relevance of the research is due to the fact that the modern world is more focused on the transition to the digital space. And since modern crime actively uses information (digital) technologies for its criminal purposes, a law enforcement officer engaged in combating digital crimes needs theoretically grounded research on this topic.

The purpose of this work is to reveal the victimological features of the prevention of certain types of digital crimes, as well as the study of criminologically significant characteristics of modern digital crime and the development on this basis of key measures aimed at preventing crimes committed in the information space.

In this study, the authors focus on the basics of victimological prevention of digital crime. The article discusses what basic measures should be taken by citizens to protect themselves from becoming a victim of a digital (cyber) crime. The prevalence of the use of modern digital technologies is beyond doubt, and a person using ITT can easily become a victim of cybercrime or simply suffer due to the lack of basic rules of digital security. In this regard, the basics of victimological prevention are an important component of the prevention of digital crime.

This study is intended for researchers interested in the issues of criminal law counteraction to crimes committed using information (digital) technologies.

Key words and word combinations: digital crime, cybercrime, victimology, criminological prevention, victim of crime, victimological prevention.

For citation: *Sidorova E.Z., Usov E.G. Victimological prevention of crimes committed with the use of information (digital) technologies // Vestnik Advanced Training Institute of MIA of Russia. – 2024. – № 1 (69). – P. 107-111; doi: 10.29039/2312-7937-2024-1-107-111*

Начиная изучение темы, связанной с особенностями виктимологического предупреждения преступлений, совершаемых с использованием информационных (цифровых) технологий, необходимо отметить следующее.

В современных реалиях защита цифрового пространства является одной из актуальных задач государственных и правоохранительных структур. Рост современных технологий не останавливается [1, с. 33]. Новые общественные отношения в данной области возникают столь стремительно, что нормативно-правовое регулирование не успевает за этими процессами. При этом Российская Федерация столкнулась с цифровой преступностью только в 90-е годы XX века. В связи с тем, что цифровая (кибер) преступность выделяется в самостоятельный вид преступной деятельности, возможно детальное изучение ее особенностей, специфики детерминации, причинности, а также выработка дифференцированных мер по борьбе с ней. При этом подчеркнем, что современная судебная практика и статистика по делам о цифровых преступлениях на современном этапе достаточно разнообразна, и пока, к сожалению, не выработаны единые

подходы к квалификации преступлений в данной сфере, что предполагает необходимость внесения отдельных законодательных изменений либо урегулирования спорных вопросов в актах Верховного Суда Российской Федерации.

В связи с актуальностью и распространенностью цифровых отношений, а также проблем, возникающих с их появлением и развитием, достаточно большое количество исследователей уже обратились к изучению обозначенной проблематики. Например, это работы В.М. Быкова, О.С. Гузеевой, О.С. Капинус, В.В. Крылова, Е.А. Русскевича, А.В. Суслопарова, Л.Г. Устьева, В.Н. Черкасова, А.Е. Шаркова, Н.А. Шведа и многих других исследователей.

Объектом нашего исследования выступили цифровые преступления, цифровая преступность, криминологические и виктимологические особенности и способы борьбы с ней.

Подчеркнем, что настоящая работа опирается на действующие нормативные правовые акты, регламентирующие ответственность за цифровые преступления, а также на материалы актуальной судебной практики. При этом методология исследования основана на общенаучном диалектическом методе познания. Нашли также применение общенаучные методы, такие как анализ, формально-логический метод и др., а также использованы частнонаучные методы: сравнительный, системный, метод обобщения правоприменительной практики и др.

По нашему мнению, настоящая работа имеет практическое назначение, которое заключается в том, что представленные выводы и результаты исследования могут использоваться в дальнейшем в учебном процессе по таким дисциплинам и отраслям права, как «Информационное право», «Правовые вопросы функционирования информационных систем», «Правозащитная деятельность и права человека» и пр., а также могут выступить в качестве учебного материала для разработки исследовательских работ по смежной или аналогичной тематике.

Новизна данного исследования состоит в том, что в данной работе путем всестороннего исследования научно-юридической литературы, а также правоприменительной практики освещены ключевые аспекты виктимологической профилактики с цифровыми преступлениями.

В общем смысле понимания слова под киберпреступлением (или цифровым преступлением) подразумевается любое виновное общественно опасное посягательство, совершенное за счет использования IT-технологий или в самом информационном пространстве.

В то же время информационными технологиями именуются как сами технические устройства с выходом в сеть Интернет, к числу которых следует отнести, например, персональные компьютеры, ноутбуки, гаджеты, так и сама информация с ее материальными носителями.

Необходимо понимать, что цифровые преступления всегда взаимодействуют с информационным пространством. Информационное пространство – это, прежде всего, информационно-телекоммуникационная сеть. Например, к таковым стоит отнести сеть Интернет, локальную компьютерную сеть и т.д. При этом главной особенностью совершения вышеуказанной разновидности противоправных посягательств является место совершения уголовно наказуемого деяния.

Среди факторов, способствующих совершению цифровых преступлений, следует отметить высокий уровень правового нигилизма в нашем государстве. Большинство граждан не знают о том, какие именно преступления следует относить к цифровым и каким образом обезопасить себя от становления жертвой от их совершения.

При этом предупреждение преступности является важнейшей составляющей государственной политики [4, с. 21]. В свою очередь, предупреждение именно цифровой преступности – это многоплановая задача, в решении которой принимают участие многие субъекты и заинтересованные лица. Одними из таких лиц выступают потенциальные жертвы киберпреступлений. Иными словами, виктимологическая профилактика цифровой преступности есть нечто иное, как основа предупреждения преступлений, совершаемых в сфере информационных (цифровых) технологий.

Выступая на расширенном заседании коллегии МВД России 17 февраля 2022 г., Президент Российской Федерации В.В. Путин подчеркнул, что в результате действий кибермошенников урон несут

отечественные компании, и, кроме того, жертвами преступников становятся пенсионеры, многодетные семьи, люди с ограниченными возможностями по здоровью [3].

В свою очередь, Министр внутренних дел В.А. Колокольцев указал, что «на 70% увеличилась штатная численность подразделений по противодействию преступлениям, совершённым с использованием ИТТ, однако успешная борьба с IT-преступностью возможна только при консолидации усилий правоохранительных органов, соответствующих регуляторов, а также с участием операторов связи и интернет-провайдеров» [3].

В научной литературе отмечается, что под киберпреступлением можно понимать акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет [10, с. 33].

Жертвами киберпреступлений могут стать различные категории граждан. Статистические показатели о числе лиц, официально признанных жертвами цифровых преступлений, заставляют снова и снова обращаться к вопросам необходимости повышения уровня защищенности граждан от киберпреступности. Кроме того, ущерб мировой экономики от киберпреступлений растет в геометрической прогрессии [10, с. 34].

В основе борьбы с цифровой преступностью (как и с любым иным видом преступности) должна лежать деятельность, направленная на нейтрализацию негативного воздействия криминогенных факторов, способствующих развитию данного вида преступности. Кроме того, большим потенциалом обладает виктимологическая профилактика. Для того чтобы эффективно противодействовать цифровым преступлениям, необходимо пресекать негативные проявления таких факторов, как несоразмерность роста цифровизации общества и цифровой грамотности населения РФ [2], увеличение аудитории социальных сетей и мессенджеров [8], активный рост применения электронных средств платежей [6].

В данном случае можно заключить, что распространенность использования современных цифровых технологий не вызывает сомнений [7]. Человек, использующий ИТТ, может с легкостью стать жертвой киберпреступления либо просто пострадать из-за отсутствия у него базисных правил цифровой безопасности, таких как:

– не переходить по ссылкам, отправленным ему через личные сообщения мессенджеров или социальных сетей, поскольку пользователь, отправивший их, может быть взломан, вследствие чего другому пришла ссылка на фишинговый сайт; в данном случае пользователь может получить материальный вред от кражи конфиденциальной информации или же искомых данных банковских карт;

– при покупке на интернет-ресурсах, какой бы ни была привлекательной цена того или иного товара, не следует переводить предоплату, поскольку злоумышленники часто пользуются наивностью людей, это один из основных механизмов социальной инженерии;

– не стоит ставить один и тот же пароль на все свои интернет-ресурсы, будь то электронная почта или аккаунт от социальных сетей, не следует также хранить пароли в любом электронном виде из-за возможности дистанционного взлома телефона, целесообразнее всего свои пароли хранить на бумажных носителях или в голове;

– при совершении покупок в Интернете следует завести дополнительную банковскую карту для переводов определенных сумм денежных средств, что позволит в случае утечки банковских данных, то есть номера карты или трехзначного кода на обратной стороне, сохранить денежные средства владельца;

– не спешить заполнять анкеты, приходящие из неизвестных спам-рассылок; свои персональные данные следует вводить только на проверенных сайтах, поскольку в противном случае данное заполнение может быть использовано не по назначению указанной анкеты;

– помнить о том, что киберзлоумышленники – хорошие манипуляторы, искусно пользующиеся приемами социальной инженерии, они могут вызвать у потерпевшего чувство тревожности и стресса путем сообщения информации о чрезвычайном положении

близких и родных или иных ситуаций, которые могут дестабилизировать жертву преступления;

– внимательно следить за файлами, которые скачиваются из неизвестных источников, при этом на том или ином устройстве обязательно должно быть установлено антивирусное программное обеспечение;

– проверять условия и права доступа при скачивании программ и файлов из неизвестных источников;

– своевременно обновлять антивирус, что предотвратит возможное установление вредоносного программного обеспечения.

Из вышесказанного следует, что всю входящую информацию следует пропускать через призму скептицизма. Не стоит доверять любой входящей информации, ведь впоследствии она может принести как материальный, так моральный вред.

В завершение еще раз подчеркнем, насколько важно проявлять основы виктимологической профилактики гражданам, если они не хотят стать жертвами цифрового (кибер) преступления. В этой связи, на наш взгляд, основы виктимологической профилактики представляют собой важную составляющую превенции цифровой преступности в целом [5, с. 72].

1. Гришина Е.П. Цифровые технологии правосудия: международный опыт и российские перспективы защиты бизнеса // Безопасность бизнеса. 2023. № 1.

2. Информационное общество в Российской Федерации – 2019: стат. сборник / М.А. Сабельникова, Г.И. Абдрахманова, Л.М. Гохберг [и др.] // URL: https://rosstat.gov.ru/storage/mediabank/info-ob2019.pdf (дата обращения: 05.10.2023).

3. Расширенное заседание коллегии Министерства внутренних дел. 2022 г.: офиц. сайт // URL: http://kremlin.ru/events/president/news/67795 (дата обращения: 24.10.2023).

4. Сидорова Е.З. Современная уголовная политика в области предупреждения преступности в сфере образования, реализуемая на международном уровне // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2021. № 1 (57).

5. Сидорова Е.З. Современные криминологические характеристики цифровой преступности (цифровой преступник и его жертва) // Сибирский юридический вестник. 2023. № 3 (102).

6. Социальные сети в России: цифры и тренды, осень 2022 // Brand Analytics: сайт // URL: https://br-analytics.ru/blog/social-media-russia-2022/ (дата обращения: 05.10.2023).

7. Статистика национальной платежной системы // Банк России: сайт. // URL: https://cbr.ru/statistics/nps/psrf/ (дата обращения: 05.10.2023).

8. Цифровая грамотность россиян: исследование 2020 // НАФИ. Аналитический центр: сайт // URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ (дата обращения: 05.10.2023).

9. Численность населения Российской Федерации по полу и возрасту на 1 января 2022 года: стат. бюллетень // Федеральная служба государственной статистики (Росстат): сайт // URL: https://rosstat.gov.ru/storage/mediabank/Bul_chislen_nasel-pv_01-01-2022.pdf (дата обращения: 05.10.2023).

10. Швед Н.А. Неправомерный доступ к компьютерной информации: уголовно-правовая защита в Российской Федерации и Республике Беларусь // Информационное право. 2016. № 2.

Информация об авторах:

Е.З. Сидорова, *заместитель начальника кафедры уголовного права и криминологии, кандидат юридических наук*

Е.Г. Усов, *доцент, кандидат юридических наук*

About the authors:

E.Z. Sidorova*, Deputy Head of the Department of Criminal Law and Criminology, PhD in Law*

E.G. Usov, *associate professor, candidate of law*

Статья поступила в редакцию 30.10.2023