злоумышленниками), Rilide копирует конфиденциальную информацию. Расширение также содержит код, который позволяет генерировать поддельную страницу для ввода кода подтверждения криптовалютной транзакции (что позволяет злоумышленникам обойти двухфакторную аутентификацию). При этом кошелек получателя криптовалюты подменяется кошельком мошенников. Благодаря украденному коду-подтверждению оператор расширения Rilide может подтвердить транзакцию от имени пользователя. Также зловред способен вмешиваться в работу электронного ящика жертвы, скрывая оповещение по e-mail о выводе средств.

Кроме того, указанное расширение собирает и отправляет оператору историю браузера (включая куки-файлы), а также (по команде злоумышленников) может сделать и отправить снимки экрана.

Вредоносное расширение маскируется под обычное браузерное расширение для Google-диска и может быть встроено в браузеры Opera, Edge, Chrome и Brave.

Способов распространения этого опасного расширения обнаружено достаточно много – от вредоносных сайтов и электронных писем до зараженных установщиков криптоигр. Одним из наиболее интересных является распространение поддельной PowerPoint-презентации, созданной для сотрудников Zendesk. Презентация представляла собой предупреждение о безопасности, но на самом деле являлась пошаговой инструкцией по установке браузерного расширения Rilide.

Также в прошлом году стало известно об опасном расширении для браузеров Google Chrome, Microsoft Edge, а также южнокорейского браузера Naver Whale, позволяющего злоумышленникам читать переписку пользователей почтовой службы Gmail[1].

Все это говорит о том, что даже официальные площадки не являются абсолютно надежными. Для того чтобы модераторы заметили опасные расширения и убрали их из магазина, как правило, не достаточно отзывов пользователей. Чаще всего необходимы публикации исследователей безопасности, и лучше на крупном медиаресурсе.

Для того чтобы не попасться на уловку мошенников, не спешите устанавливать новые плагины. Если все же решили установить, то делайте это с официального сайта (там хотя бы есть служба безопасности), предварительно прочитав отзывы (бдительные граждане могут вас предупредить, что с плагином что-то не так). Хоть иногда просматривайте список установленных расширений и удаляйте ненужные (особенно если не можете вспомнить, что его устанавливали). И обязательно используйте надежную защиту на всех ваших устройствах.

Ущекин С.Н.

Академия управления МВД России (г. Москва)

Виды виктимности жертв хищений, совершаемых с использованием электронных средств платежа

В настоящее время, в период активного развития современного общества, отмечается явная тенденция к цифровизации экономических отношений. Этот процесс привлекает особое внимание научного сообщества, которое придает большую значимость изучению и анализу данной тенденции. В связи с этим возрастает интерес к проблеме роста качественных и количественных показателей преступности, связанной с использованием информационных технологий.

Исследователи обращают внимание на появление новых разновидностей средств платежа, которые, в свою очередь, становятся потенциальной угрозой для совершения хищения чужого имущества. Это вызы-

[1] Joint Cyber Security Advisory // The German domestic in-tel-li-gence ser-vices : сайт. URL: https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/prevention/2023-03-20-joint-cyber-security-advisory-korean.html (дата обращения: 03.01.2024).

вает необходимость более глубокого изучения данной проблемы и разработки соответствующих мер по ее предотвращению[1].

Научное сообщество активно занимается анализом и классификацией новых разновидностей средств платежа, а также изучением мотивов и психологических характеристик как преступников, совершающих хищения с использованием электронных средств платежа (далее – ЭСП), так и потерпевших от рассматриваемых преступлений. Это позволяет более глубоко понять сущность данной проблемы и разработать эффективные стратегии по ее преодолению.

На сегодняшний день особую актуальность приобретает изучение виктимности потерпевших от рассматриваемых преступлений в контексте цифровой среды, в которой осуществляется преступная деятельность. За период с января по ноябрь 2023 года было зарегистрировано значительное количество информационно-телекоммуникационно-обособленных преступлений, их число составило 614,8 тыс. случаев. Особенно важным является тот факт, что около 70,6% этих преступлений связаны с кражей или мошенничеством, и общее количество таких случаев составляет 433,8 тыс., что на 29% больше, чем в предыдущем году[2].

Статистические данные свидетельствуют о значительном увеличении числа преступлений, связанных с кражей и мошенничеством в цифровой среде. Это требует проведения более глубокого исследования, чтобы понять особенности и характеристики виктимности потерпевших, а также разработать соответствующие стратегии и меры для защиты от таких преступлений.

На современном этапе уголовно-правовой охраны собственности, когда речь заходит о преступлениях, связанных с хищениями и осуществляемых с использованием ЭСП, мы рассматриваем деяния, которые закреплены в п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 УК РФ. Тем не менее необходимо отметить, что несовершенство правил квалификации приводит к применению ст. 159 УК РФ, что, по нашему мнению, противоречит сущности данного криминального акта и искажает представление о рассматриваемом социально-негативном явлении[3].

В работе С.Г. Войтенко была проведена глубокая аналитика концепции виктимности, которая представляет собой комплекс социально-психологических и физиологических характеристик личности, оказывающих влияние на ее склонность стать жертвой преступления под воздействием внешних факторов[4]. Это исследование также выявило особое свойство личности, которое определяет степень ее уязвимости перед общественно опасными посягательствами.

Подобные взгляды разделяет и К.В. Вишневецкий, который вкладывает в понятие «виктимность» определенную предрасположенность (способность) индивида стать объектом преступления в определенных обстоятельствах или его неспособность противостоять криминальному поведению[5].

Ф.С. Сафуановым было выявлено два основных типа виктимного поведения, характерных для жертв интернет-мошенничества:

– активное поведение, которое провоцирует преступление своими действиями, такими как просьбы или обращения;

– агрессивное поведение, которое провоцирует преступные действия через оскорбления, клевету, издевательства и другие подобные действия[6].

Поведение жертвы в контексте рассматриваемых преступлений является проявлением виктимогенной деформации личности, которая выражается в неправомерных дей-

[1] Подр.: Ущекин С.Н. Характеристика электронных средств платежа как средства совершения хищений // Закон и право. 2023. № 4. С. 258-260.

[2] Краткая характеристика состояния преступности в Российской Федерации за январь – ноябрь 2023 года. URL: https://xn--b1aew.xn--p1ai/reports/item/45293174/ (дата обращения: 10.01.2024).

[3] Подр.: Ущекин С.Н. Уголовно-правовые аспекты противодействия хищениям, совершенным с использованием электронных платежных средств // Вестник Уфимского юридического института МВД России. 2023. № 3(101). С. 118-125.

[4] Войтенко С.Г. Криминологическое исследование виктимности потерпевших. Белгород: Белгор. юрид ин-т, 2000. 164 с.

[5] Вишневецкий К.В. Криминогенная виктимизация социальных групп в современном обществе : дис. ... докт. юрид. наук. М.: МУ МВД России, 2008. 399 с.

[6] Сафуанов Ф.С., Докучаева Н.В. Особенности личности жертв противоправных посягательств в Интернете // Психология и право. 2015. Т. 5. № 4. С. 80-93.

ствиях. Это означает, что жертва, подвергшись мошенничеству, может изменить свои нормы и ценности, а также приобрести негативные черты характера, которые приводят к неправомерным действиям.

По-видимому, большинство исследователей сосредоточено на личностной виктимности, которая тесно связана с ситуационной виктимностью. В таком случае возникает необходимость разделения этих видов виктимности с целью разработки наиболее точной теоретической системы виктимологической профилактики хищений, осуществляемых с использованием ЭСП.

Резюмируя представленное, мы выделяем две основные формы виктимности: личностную виктимность и ситуационно-личностную виктимность:

Личностная виктимность характеризуется следующими характеристиками потенциальных жертв:

– определенный возраст или наличие заболеваний;

– антиобщественный образ жизни;

– значительные финансовые средства и инвестиции в системах дистанционного банковского обслуживания.

– активное использование услуг дистанционного банковского обслуживания в повседневной жизни.

– поиск выгоды через оформление дистанционных банковских услуг.

Таким образом, мы имеем дело с различными категориями граждан, которые отличаются по социально-экономическому положению, уровню финансовой грамотности и информационно-телекоммуникационной грамотности. Представленные характеристики по отдельности описывают конкретную личность в конкретной ситуации.

Ситуационно-личностная виктимность, в свою очередь, связана с конкретными ситуациями, в которых потенциальная жертва может стать реальной жертвой. В контексте взаимосвязи этих форм виктимности мы можем выделить основные ситуации, характерные для хищений, совершаемых с использованием ЭСП.

Злоумышленник целенаправленно осуществляет действия, направленные на создание фиктивных ситуаций у потенциальной жертвы, используя следующие убеждения и состояния:

– убеждения, связанные с трагическими ситуациями, требующими немедленных реакций и действий;

– состояние доверия и ощущения безопасности, которые могут быть нарушены совершением криминальных актов;

– убеждения, связанные с экономически выгодными ситуациями.

Байкалов В.А.

Сибирский юридический институт МВД России (г. Красноярск)

Подростковая преступность: современные угрозы и пути их устранения

С 2015 года по 2022 год наблюдается тенденция к снижению числа выявленных несовершеннолетних лиц, совершивших преступления. По состоянию на декабрь 2022 года их число составило 26305 человек, по сравнению с аналогичным периодом прошлого года их было выявлено незначительно больше – на 9,7%, что составило 29126 лиц[1].

Если проанализировать ситуацию в отдельных регионах страны, то весьма высока криминогенность несовершеннолетних в Иркутской области, Кемеровской области – Кузбассе, а также в Свердловской и Челябинской областях, Краснодарском и Красноярском крае и некоторых других.

К признакам преступности несовершеннолетних следует отнести специфический возраст преступника, совокупность совершаемых преступлений, а также психологические особенности личности преступника[2].

[1] Официальный сайт-портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/offenses_chart (дата обращения: 10.02.2024).

[2] Мальков С.М. Криминология и предупреждение преступлений : курс лекций. Красноярск: СибЮИ МВД России, 2020. С. 172.