ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРЕДУПРЕЖДЕНИЯ КРИМИНОГЕННОЙ ВИКТИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ «ИНТЕРНЕТ» В КИБЕРПРОСТРАНСТВЕ

Кашликова Полина Алексеевна

студент, Ростовский институт (филиал,) Всероссийский государственный университет юстиции (РПА Минюста России), РФ, г. Ростов-на-Дону

Воропаева Елена Валерьевна

преподаватель, Ростовский институт (филиал,) Всероссийский государственный университет юстиции (РПА Минюста России), РФ, г. Ростов-на-Дону

KEY DIRECTIONS FOR PREVENTING CRIMINOGENIC VICTIMIZATION OF INTERNET USERS IN CYBERSPACE

Polina Kashlikova

student, Rostov Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Russia, Rostov-on-Don

Elena Voropaeva

Teacher, Rostov Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Russia, Rostov-on-Don

Аннотация. В статье автор рассматривает существующие меры, как основные направления предупредительного воздействия на криминогенную виктимизацию пользователей сети «Интернет» в киберпространстве. Анализирует официальные статистические данные по совершенным преступлением с использованием современных информационных технологий, влияние на безопасность как отдельной личности, так и на экономическую безопасность страны.

Сопоставляет ключевые факторы криминальной виктимизации пользователей сети «Интернет» в киберпространстве с индивидуальной поведенческой профилактики, а так же делает выводы по безопасному использованию сетевых ресурсов и использованию привентивных мер.

Abstract. In the article, the author examines existing measures as the main directions of preventive impact on criminogenic victimization of Internet users in cyberspace. Analyzes official statistics on crimes committed using modern information technologies, the impact on the security of both an individual and the economic security of the country. Compares key factors of criminal victimization of Internet users in cyberspace with individual behavioral prevention, and also draws conclusions on the safe use of network resources and the use of preventive measures.

Ключевые слова: криминогенная виктимизация, кибервиктимизация, кибервиктив-ность,

киберпространство, киберпреступление, кибержертва, несовершеннолетние, предупреждение виктимизации, виктимологическая профилактика, индивидуальная профилактика, общесоциальная профилактика.

Keywords: criminogenic victimization, cyber victimization, cyber victimhood, cyberspace, cyber crime, cyber victim, minors, victimization prevention, victimological prevention, individual prevention, general social prevention.

В современном мире уровень криминогенной виктимизации остается высоким, несмотря на осведомленность большинства пользователей сети «Интернет» в киберпространстве.

Согласно результатам национального виктимологического обзора кибержертв в Российской Федерации за 2024 год, полученных кандидатом юридических наук Д. В. Жмуровым из 127,6 млн. пользователей российского Интернета, 78,7 млн. считают себя жертвами киберпреступлений. Общий коэффициент виктимизации на 1 млн. населения составил 537 394 человека. Этот показатель свидетельствует о чрезвычайной напряженности данной сферы общественных отношений: глобальных масштабах проблемы; высокой динамике криминализации и виктимизации в информационно-телекоммуникационной области [4, с. 535-537].

Наиболее распространенными преступлениями за прошедший год о которых упоминали опрашиваемые оказались деяния по статьям 272 УК РФ «Неправомерный доступ к компьютерной информации» (27,1 % пострадавших).

Особую тревогу вызывает виктимизация несовершеннолетних, поскольку с помощью виртуальной реальности преступники могут подавить желания несовершеннолетнего, ввести в тяжелое эмоциональное состояние и убедить в необходимости суицида [2, с. 108].

В погоне за лайками подростки готовы раздеться, выставить напоказ интимные части своего тела, принять участие в любых аморальных и противоправных действиях, совершить суицидальную попытку [3, с. 86].

Важнейшей составляющей предупреждения киберпреступлений является виктимологическая профилактика киберпреступности, а ее прогрессивным направлением выступает кибервиктимология - отрасль научного знания, исследующая виктимность (виктимизацию) пользователей в виртуальном пространстве объединенных компьютерных сетей» [7, с. 542].

Доктор юридических наук А. В. Майоров отмечает, что одним из способов предотвращения негативных последствий в информационной среде является цифровая гигиена (кибергигиена), которая входит в систему виктимологической профилактики как пассивный метод обеспечения безопасности цифрового профиля личности. Цифровая гигиена - это формирование полезных привычек в отношении кибербезопасности, позволяющих не стать жертвой киберугроз и избегать проблем сетевой безопасности. Развитие критического мышления и осознанности помогают личности не поддаваться на манипуляции и принимать взвешенные решения, противодействуя методам социальной инженерии и дистанционным мошенничествам [9, с. 84].

Виктимологическая профилактика киберпреступности представляет собой совокупность мероприятий, направленных на недопущение кибервикитимизации отдельных социальных групп или частных лиц [6, с. 37].

В данном случае речь идет об индивидуальной виктимологической профилактике киберпреступности, которая представляет собой превентивную деятельность, направленную на лиц, обладающих повышенной виктимностью в информационно-технологической среде. Главная ее задача - услить личную безопасность потенциальных жертв интернет-преступлений, повысить степень их защищенности и выработать основы социального иммунитета [5, с. 52-57].

Индивидуальная виктимологическая профилактика имеет следующие ключевые уровни:

1. Доинцидентный, разработка моделей раннего противодействия киберпреступности - заключается во внедрении значительного числа стандартов и шаблонов, снижающих виктимность в цифровом пространстве и не допускающих ее реализации.

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);

- безопасный серфинг в виртуальном пространстве (проверка надежности сайтов и защищенности соединения; отказ от публичных опросов, розыгрышей, кешбэк-сервисов);

- навыки защиты от вредоносных программ (использование операционных систем последней версии; автообновление браузера);

- безопасная эксплуатация сетей Wi-Fi (приоритет использования запароленных сетей; запрет на передачу конфиденциальных данных и платежной информации через публичный доступ);

- безопасная активность в социальных сетях (тщательное отношение к кандидатам в друзья; удаление неиспользуемых аккаунтов);

- безопасное использование электронной почты (использование почтовых антивиру-сов);

- безопасная игровая деятельность онлайн (отказ от внесения персональных данных в игровой профиль; от использования анонимных и пиратских серверов с низким рейтингом);

- безопасное осуществление онлайн-покупок (хранение ограниченной суммы денег на счету, либо выставление лимитов по проводимым операциям).

2. Инцидентный уровень (разработка стандартов учета виктимного поведения) предполагает концентрацию внимания на выявлении, фиксации, подсчете и статистическом отображении группы виктимизированных лиц в интернете. В США, например, функционирует Internet Crime Complaint Center (IC3), центр приема сообщений о преступлениях в интернете, в России эти функции мог бы выполнять Единый центр кибервиктимизации (ЕЦК).

3. Постинцидентный уровень (разработка стандартов реагирования на кибервиктимизацию) относится к преодолению ближайших и отдаленных последствий киберпреступнос-ти, например, для пострадавших от кибербуллинга открыты интернет-программы «Травли.net», сервис «Маяк» проекта «Добро.mail.ru»

Кандидат юридических наук Е. А.Родина в своем диссертационном исследовании «Противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве» отмечает, что снижению виктимизации пользователей сети Интернет могут служить следующие меры общесоциального характера [10, с. 11-12]:

- формирование полноценного цифрового суверенитета Российской Федерации, то есть способности государства реализовывать и контролировать весь спектр технологий и программного обеспечения, лежащих в основе функционирования киберпространства, для чего необходимо построение современной национальной полупроводниковой индустрии и переход на национальное программное обеспечение, начиная с государственных учреждений, и переноса деятельности всех цифровых компаний отечественного происхождения в отечественную юрисдикцию;

- разработка отечественной цифровой валюты;

- поддержка государственным финансированием наиболее успешных информацион-ных проектов патриотической, образовательной, энциклопедической и культурной

направленности, формирующих общее культурное пространство страны, повышающих уровень грамотности населения и снижающих тем самым риски виктимизации пользователей с условием бесплатного доступа для всех желающих либо радикального снижения расценок на такой доступ;

- министерствам просвещения, образования и науки, министерствам образования субъектов РФ необходимо стимулировать перенос обучающих видеоматериалов, которые готовятся преподавателями учебных заведений, на российские аналоги западных видеосервисов;

- органы государственной власти должны обязать подчиненные им подразделения переносить проведение дистанционных мероприятий на российские программные платформы, запретить использование иностранных мессенджеров и обеспечить переход на российские программные продукты аналогичной функциональности.

Кандидатом юридических наук Е. В Кузнецовой в своем диссертационном исследовании «Предупреждение делинкветного поведения несовершеннолетних, провоцируемого контентом сети Интернет» предложены направления по совершенствованию предупреждения делинквентного воздействия контента и асоциального поведения в сети Интернет на несовершеннолетних, которые включают [8, с. 10-11]:

- закрепление прав и обязанностей субъектов предупреждения преступлений, установление перечня, содержания и порядка проведения профилактических мероприятий в сети Интернет;

- разработку холдингами Яндекс, Mail.RuGroup, Google*, Rambler&Co и др. системы маркировки, позволяющей лицам, размещающим информационную продукцию, самостоятельно определять возрастную классификацию пользователей, на которых она ориентирована;

- введение возрастной маркировки абонентов мобильной связи (до 18 лет и старше) с целью ограничения доступа несовершеннолетних к контенту сети Интернет;

- создание на базе образовательных организаций системы МВД России и высших образовательных организаций юридической направленности групп из числа наиболее подготовленных обучающихся, осуществляющих профилактическую деятельность в общеобразовательных учреждениях;

- проведение просветительских программ и производство фильмов и мультфильмов для детей, сюжетная линия которых будет содержать информацию о рисках и угрозах, связанных с использованием сети Интернет, и мероприятиях, направленных на их профилактику.

В настоящее время во всем мире, в том числе и России, стремительный рост набирает игровая индустрия, которая подталкивает людей искать новые способы развлечений и общения.

Для того, чтобы не стать жертвой незаконной азартной деятельности, совершаемой в телекоммуникационной системе сети «Интернет», следует соблюдать определенные превентивные меры [1, с. 98]:

1. На электронном ресурсе, где предлагают вести платёжную информацию, проверять наличие SSL-сертификата, а также его тип: DV - с проверкой по домену, OV - с проверкой по организации, EV - с расширенной проверкой организации;

2. Осуществлять проверку на отсутствие опечаток в наименовании доменного имени;

3. Читать отзывы о сайте сети и проверять наличие контактных данных, оферт, информацию о предоставляющей услуги организации на данном сайте;

4. При регистрации аккаунта использовать сложные пароли;

5. Использовать дополнительные средства защиты online банка путём ограничения на online покупки и установления двойной аутентификации;

6. Применять лицензионное и общепризнанные средства защиты компьютерной информации, такие как антивирусы, фаерволы и адблок.

Несомненно, что в условиях стремительного развития компьютерных технологий, пользователи будут сталкиваться с новыми видами угроз их законным правам и интересам, однако, как представляется, предложенные в настоящей статье комплексные меры профилактики при их реализации создадут фундамент для надежной системы обеспечения безопасности в киберпространстве.

Список литературы:

1. Агаян В. А., Вавилова А.А. Государственное регулирование азартных игр в сети Интернет // Актуальные вопросы обеспечения прав и свобод человека и гражданина: Региональный вектор: Материалы IV Всероссийской научно-практической конференции, Хабаровск, 07 декабря 2021 года. - Ростов-на-Дону: Ростовский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Всероссйский государственый университет юстиции (РПА Минюста России) в г. Ростове-на-Дону, 2022. - С. 96 - 99.

2. Агаян В. А., Пичугина И.Ю. Цифровые средства совершения преступлений или искуственный интеллект, виртуальная реальность, Darknet в преступной деятельности // Актуальные вопросы обеспечения прав и свобод человека и гражданина: Региональный вектор: Материалы IV Всероссийской научно-практической конференции, Хабаровск, 07 декабря 2021 года. - Ростов-на-Дону: Ростовский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Всероссйский государственый университет юстиции (РПА Минюста России) в г. Ростове-на-Дону, 2022. - С. 106 - 109.

3. Алтухов С. А. Проблемы борьбы с преступностью в условиях изменения формата медиапространства // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции: Сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 года. - Ростов-на-Дону: Ростовский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Всероссйский государственый университет юстиции (РПА Минюста России) в г. Ростове-на-Дону, 2021. - С. 82-87.

4. Жмуров Д. В. Виктимологическая характеристика жертв киберпреступлений России // Вопросы российского и международного права. 2024. Том 14, № 4А. С. 532-538.

5. Жмуров Д. В. Индивидуальная виктимологическая профилактика киберпреступности // Сибирский юридический вестник. 2023. №1 (100). С. 52-59.

6. Изосимов В. С., Габова А. П. Виктимологическая профилактика киберпреступности // Вестник Пермского института Федеральной службы исполнения наказаний. 2024. № 3 (54). С. 35-41.

7. Кабанов П. А. Рецензия на книгу Д. В. Жмурова «Кибервиктимология // Виктимология. 2023. Т. 10, №4. С. 538-559.

8. Кузнецова Е. В. Предупреждение делинкветного поведения несовершеннолетних, провоцируемого контентом сети Интернет: Автореф. дис. … канд. юрид. наук - Курск, 2019. - 25 с.

9. Майоров А. В. Виктимологическое обеспечение информационной безопасности личности // Правопорядок: история, теория, практика. 2024. № 3 (42). С. 80-88.

10. Родина Е. А. Противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве: дис. … канд. юрид. наук. - Саратов, 2022. - 217 с.

[*] По требованию Роскомнадзора информируем, что иностранное лицо, владеющее информационными ресурсами Google является нарушителем законодательства Российской Федерации – прим. ред.