УДК 343.988

Теоретические основы виктимологического воздействия на киберпреступность

Жмуров Дмитрий Витальевич

Кандидат юридических наук, доцент,
доцент кафедры уголовного права и криминологии,
институт юстиции,
Байкальский государственный университет
664003, Российская Федерация, Иркутск, ул. Ленина, 11;
e-mail: zdevraz@ya.ru

Аннотация

В статье исследуются концептуальные основы виктимологической профилактики и виктимологического воздействия на киберпреступность. Предлагается описание ключевых характеристик указанного воздействия, перечисляются условия его эффективности, кроме того, предлагаются дефиниции ряда отраслевых понятий, таких как объект и субъект виктимологической профилактики; её средства, в том числе, виктимологическое образование и просвещение, виктимологическое планирование, мониторинг, виктимологическая технология и проч. В заключении статьи показано, что главная цель виктимологической профилактики киберпреступности – это минимизация негативного воздействия отраслевых угроз на граждан, государственные институты и общество в целом. Среди задач этой деятельности видятся разработка и внедрение стратегий, направленных на девиктимизацию пользователей сети интернет, выявление и анализ уязвимостей в информационных системах, обеспечение информационной безопасности, обучение общества методам защиты от киберугроз.

Для цитирования в научных исследованиях

Жмуров Д.В. Теоретические основы виктимологического воздействия на киберпреступность // Вопросы российского и международного права. 2024. Том 14. № 4А. С. 539-545.

Ключевые слова

Кибервиктимология, виктимология, киберпреступление, кибержертва, профилактика киберпреступности.

Введение

Известно, что виктимологическая профилактика является одним из эффективных методов применения отраслевых знаний «науки о жертве преступления» в практической плоскости. Это социально необходимая деятельность [Титушкина, 2013], направленная на выявление и предотвращение условий, факторов и обстоятельств, способствующих формированию поведения жертвы, которое в свою очередь детерминирует совершение преступлений в её отношении. Это система мер, воздействующих на потенциальную жертву, её поведение в опасных предпреступных ситуациях [Рогова, 2011].

Виктимологическая профилактика также включает выявление групп риска и лиц, обладающих повышенной виктимностью; осуществление мер, направленных на восстановление или активизацию контркриминальных свойств личности [Васягина, 2015].

Для эффективного противодействия киберпреступности необходимо использовать широкий спектр социальных мер, которые способны оказывать воздействие на различные её детерминанты. Важно рассматривать преступность и связанные с ней явления как часть общественной системы. Преступность, будучи продуктом общества, имеет способность к саморазвитию и самоорганизации. Для эффективной борьбы с нею необходима профилактика, основанная на интегральных принципах.

Очевидность этого положения, к сожалению, нивелируется различиями в дефиниции и понимании системности, как фундаментального свойства материального мира, характеризующего его структурированность. И когда речь заходит о системном противодействии преступности, возникают несходные взгляды на предмет обсуждения: у одних - системность выступает проявлением многоуровневого порядка реализации профилактических мер на общесоциальном, специально-виктимологическом и индивидуальном уровнях [Кузнецова, 2011]; у других – выражена единством деятельности по прогнозированию, моделированию и практическому противодействию преступности [Васин, 2015]; третьи усматривают системность предупреждения преступности в специфике взаимодействия её субъектов (управляющей подсистемы) и объектов (управляемой подсистемы) [Щедрин, 1999], иные – констатируют системный характер в объединении усилий всех ветвей государственной власти и их межведомственном взаимодействии [Хан, 2019]. Очевидно, что указанные позиции по-своему разумны.

Основная часть

Используя в качестве основы настоящей статьи теоретические исследования Ю.А. Воронина и А.В. Майорова [Воронин,, Майоров, 2023], можно утверждать, что виктимологическое воздействие на киберпреступность имеет следующие особенности:

– это специализированная форма социального управления, описывающая организованный набор действий, а не случайное множество профилактических мер;
– ключевой его характеристикой является многоуровневый подход, который предполагает комплексное преодоление общих причин кибервиктимности, а также специфических форм виктимизации от различных видов киберпреступлений;
– работа по предотвращению киберпреступлений среди потенциальных потерпевших осуществляется как в рамках общего социального и экономического развития, так и посредством разработки специальных виктимологических программ;

– виктимологическая профилактика киберпреступлений является результатом сотрудничества различных субъектов, включая органы власти, правоохранительные органы, предприятия, общественные организации и частных лиц;
– главная цель виктимологической профилактики в области киберпреступности заключается в достижении эффектов раннего предупреждения. Они проявляют себя в предотвращении негативного воздействия на формирование личности потенциальной жертвы.

Важно отметить, что виктимологическая профилактика не является единственной или достаточной целью. Поскольку киберпреступность оценивается как системная угроза, задача предупреждения которой не может быть решена исключительно с помощью инициатив в области кибербезопасности или правовой фиксации [Manmeet Mahinderjit Singh, Anizah Abu Bakar, 2019], виктимологическая профилактика выступает важной дополнительной мерой, необходимой для контроля её показателей.

Попытки применения системного подхода в кибервиктимологии уже имели место, причем отражены они не только в научной, но и в нормативной литературе.

Научные изыскания, связанные с попытками внедрения системного подхода в кибервиктимологию, уже имели место не только в исследованиях коллективов ученых, но и в нормативных документах. Иллюстрацией данной тенденции является, к примеру, предложенная малазийскими авторами «архитектурная модель интересантов киберпреступности», которая включает четыре основных компонента этих социальных взаимодействий, потенциально восприимчивых к превентивному влиянию (правонарушитель; объект или жертва; технология и социальное окружение&закон&юрисдикция). Лишь целостное воздействие на указанные элементы по мнению авторов позволит обеспечить результативность профилактического процесса. Близким по духу к системному подходу является закрепление в нормативных актах различных государств т.н. условно-синонимичных понятий «стратегия кибербезопасности» (cybersecurity strategies) и «стратегия киберпреступности» (cybercrime strategies). Первые акцентируют внимание на усилиях по прямому и косвенному противодействию киберпреступности, например, на мерах реагирования правоохранительных органов и содействия национальному/международному сотрудничеству между правительством, предприятиями, академическими учреждениями, организациями и общественностью, с целью контроля над киберпреступностью. Вторые предполагают выработку рекомендаций в области кибербезопасности (включая предотвращение киберпреступности).

Разработка основ воздействия на жертв киберпреступности включает в себя выполнение следующих необходимых процедур:
– получение качественных и количественных сведений о пострадавших от киберпреступлений;
– анализ различных типов киберпреступлений и эффектов их воздействия на пострадавших;
– разработка программ и стратегий, направленных на предотвращение киберпреступности с использованием знаний в области виктимологии;
– определение признаков и факторов, влияющих на уязвимость потенциальных жертв;
– создание методов прогнозирования киберпреступности с учетом виктимологического аспекта;
– обучение населения методам виктимологического предотвращения киберпреступлений;
– оптимизация законодательства и разработка политик для защиты жертв киберпреступности;

– совершенствование системы раннего обнаружения и реагирования на случаи киберпреступлений;
– сотрудничество с различными организациями для эффективного предотвращения и противодействия киберпреступности;
– оценка эффективности контрмер, направленных на предотвращение киберпреступности.

Формирование теоретических основ виктимологического воздействия на киберпреступность требует введения основополагающих понятий в данной сфере.

К таковым традиционно относятся объект и субъект; средства виктимологической профилактики и проч.

Виктимологическое предупреждение имеет сложную структуру, идентичную структуре общей предупредительной деятельности. Оно включает в себя следующие элементы: объект предупредительного воздействия; субъекты, осуществляющие предупредительную работу; а также меры виктимологического предупреждения [Мироненко, 2021] (иногда именуются методами или средствами). Применительно к целям и задачам настоящего исследования целесообразно предложить следующий вариант их интерпретации.

Объект виктимологической профилактики киберпреступности - это явления или группы явлений, обусловливающие виктимизацию индивида в киберпространстве. Речь может идти об уязвимостях информационных систем, недостатках в обеспечении кибербезопасности, низкой информационной грамотности пользователей, неэффективных мерах предупреждения и защиты населения в интернете, социально-экономических, психологических факторах, которые мотивируют поведение будущих жертв и проч.

Субъект виктимологической профилактики киберпреступности представляет собой организацию, учреждение или индивида, которые принимают участие в предотвращении киберпреступлений и защите их потенциальных жертв.

Субъектами виктимологического предупреждения выступают:
– государство в лице законодательных, исполнительных и судебных органов;
– информационно-технические компании, IB-проекты, антивирусные вендоры, образовательные учреждения, неправительственные организации, коммерческие предприятия, проявляющие интерес к вопросам кибербезопасности и вносящие свой вклад в снижение уровня интернет-виктимизации;
– должностные лица и граждане, осуществляющие предупреждение преступности, в т.ч. в цифровом поле.

Виктимологическое предупреждение осуществляется путем применения определенных способов, приемов, влияющих на виктимогенный объект, то есть с помощью специальных методов [Белякова, Дробот, 2022] или средств.

К средствам виктимологической профилактики киберпреступности относятся инструменты, используемые для предотвращения киберпреступлений и снижения уровня виктимизации в киберсреде. Они включают:
– виктимологическое образование и просвещение (проведение семинаров, тренингов и конференций, разработка информационных ресурсов для широкой аудитории с целью повышения информационной грамотности и приобретения навыков кибербезопасности, внедрение учебных программ в ВУЗы и школы и т.п.);
– виктимологическое планирование включает разработку и организацию предварительно обдуманных действий, мероприятий, объединённых целью предотвращения киберпреступлений, путем воздействия на их потенциальных жертв. Указанная деятельность включает анализ и оценку рисков виктимного поведения, разработку

стратегий по обеспечению кибербезопасности, определение приоритетов и целей профилактических программ, определение эффективных методов обучения и информирования и проч.;

– виктимологический мониторинг (систематическое и непрерывное наблюдение за состоянием виктимизации общества от разнообразных проявлений киберпреступности);
– виктимологическая пропаганда представляет информационную кампанию, направленную на осведомление общественности о рисках и последствиях киберпреступлений с целью предотвращения подобных инцидентов в будущем;
– виктимологическая реклама подразумевает маркетинговую акцию или обнародование материалов, которые разрабатываются и используются для привлечения внимания и инициации осознания опасностей киберпреступности;
– виктимологическая технология — это методологический подход, который предполагает использование (внедрение) технических мер и инструментов с целью защиты жертв киберпреступлений (как потенциальных, так и состоявшихся). Сюда входят разработка и осуществление необходимых процедур цифровой безопасности, обеспечение защиты систем обработки информации и пользовательских данных, использование шифрования и аутентификации, разработка специализированного программного обеспечения и т.п.

Заключение

Таким образом, виктимологическая профилактика киберпреступности является неотъемлемой частью обеспечения безопасности в цифровой среде. Она направлена на снижение показателей киберпреступности посредством воздействия на её реальных или потенциальных жертв.

Главная цель виктимологической профилактики киберпреступности – это минимизация негативного воздействия отраслевых угроз на граждан, государственные институты и общество в целом. Среди задач этой деятельности видятся разработка и внедрение стратегий, направленных на девиктимизацию пользователей сети интернет, выявление и анализ уязвимостей в информационных системах, обеспечение информационной безопасности, обучение общества методам защиты от киберугроз.

Библиография

1. Cybersecurity Strategies: Basic Features. URL: https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/cybersecurity-strategies---basic-features.html (дата обращения 30.08.2023).
2. Manmeet Mahinderjit Singh, Anizah Abu Bakar. A Systemic Cybercrime Stakeholders Architectural Model // Procedia Computer Science. 2019. № 161. Pp. 1147–1155
3. Белякова В.И., Дробот С.А. Виктимология в структуре криминологического предупреждения преступлений // Юридический факт. 2022. № 184. С. 3-7.
4. Васин А.Г. Борьба с организованной преступностью: опыт теоретического моделирования. М: Институт государства и права РАН. 2015, 291 с.
5. Васягина М.М. Теоретические аспекты виктимологической профилактики // Инновационная наука. 2015. № 3. С. 212-215.
6. Воронин Ю.А., Майоров А.В. Теоретические основы формирования системы противодействия преступности в России // Всероссийский криминологический журнал. 2013. № 1. С. 7-16.
7. Кузнецова А.В. О системном подходе в профилактике преступности несовершеннолетних // Право и образование. 2011. № 2. С. 145-150
8. Мироненко С.Ю. Понятие и методы виктимологического предупреждения преступности // Виктимология. 2021. № 2 (8). С. 149-155.
9. Рогова Е.В. Роль виктимного поведения потерпевших в механизме совершения преступлений // Baikal Research

Journal. 2011. № 2. С. 50.
10. Титушкина Е.Ю. Правовые основы профилактики преступности: пути совершенствования // Всероссийский криминологический журнал. 2013. № 1. С. 59-62.
11. Хан В.Ю. О системе предупреждения преступности // Известия ВУЗов Кыргыстана. 2019. № 7. С. 134-139
12. Щедрин Н.В. Основы общей теории предупреждения преступности: Учеб. пособие / Краснояр. гос. ун-т, 1999. 58 с.

Theoretical bases of victimological impact on cybercrime

Dmitrii V. Zhmurov

PhD in law, associate professor,
Associate Professor of the Department of Criminal Law and Criminology,
Institute of Justice,
Baikal State University,
664003, 11, Lenina str., Irkutsk, Russian Federation;
e-mail: zdevraz@ya.ru

Abstract

The article examines the conceptual foundations of victimological prevention and victimological impact on cybercrime. A description of the key characteristics of this impact is proposed, the conditions for its effectiveness are listed, in addition, definitions of a number of industry concepts are proposed, such as the object and subject of victimological prevention; its means, including victimological education and awareness, victimological planning, monitoring, victimological technology, etc. In conclusion, the article shows that the main goal of victimological prevention of cybercrime is to minimize the negative impact of industry threats on citizens, government institutions and society as a whole. Among the tasks of this activity are the development and implementation of strategies aimed at victimizing Internet users, identifying and analyzing vulnerabilities in information systems, ensuring information security, and training society in methods of protection against cyber threats.

For citation

Zhmurov D.V. (2024) Teoreticheskie osnovy viktimologicheskogo vozdeistviya na kiberprestupnost' [Theoretical bases of victimological impact on cybercrime]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (4A), pp. 539-545.

Keywords

Cybervictimology, victimology, cybercrime, cybervictimisation, cybercrime prevention.

References

1. Cybersecurity Strategies: Basic Features. URL: https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/cybersecurity-strategies---basic-features.html (accessed 08/30/2023).
2. Manmeet Mahinderjit Singh, Anizah Abu Bakar. A Systemic Cybercrime Stakeholders Architectural Model // Procedia Computer Science. 2019. No. 161. Pp. 1147–1155
3. Belyakova V.I., Drobot S.A. Victimology in the structure of criminological crime prevention // Legal fact. 2022. No. 184. pp. 3-7.

4. Vasin A.G. The fight against organized crime: experience of theoretical modeling. M: Institute of State and Law of the Russian Academy of Sciences. 2015, 291 p.
5. Vasyagina M.M. Theoretical aspects of victimological prevention // Innovative science. 2015. No. 3. P. 212-215.
6. Voronin Yu.A., Mayorov A.V. Theoretical foundations of the formation of a system for combating crime in Russia // All-Russian Journal of Criminology. 2013. No. 1. P. 7-16.
7. Kuznetsova A.V. On a systematic approach to the prevention of juvenile delinquency // Law and Education. 2011. No. 2. P. 145-150
8. Mironenko S.Yu. Concept and methods of victimological crime prevention // Victimology. 2021. No. 2 (8). pp. 149-155.
9. Rogova E.V. The role of victim behavior of victims in the mechanism of crime // Baikal Research Journal. 2011. No. 2. P. 50.
10. Titushkina E.Yu. Legal foundations of crime prevention: ways of improvement // All-Russian Criminological Journal. 2013. No. 1. P. 59-62.
11. Khan V.Yu. On the crime prevention system // News of Universities of Kyrgyzstan. 2019. No. 7. P. 134-139
12. Shchedrin N.V. Fundamentals of the general theory of crime prevention: Textbook. allowance / Krasnoyarsk. state Univ., 1999. 58 p.