УГОЛОВНО-ПРАВОВЫЕ НАУКИ

Научная статья
doi: 10.29039/2312-7937-2024-2-32-37

КЛЕЩИНА ЕЛЕНА НИКОЛАЕВНА
Московский государственный юридический университет
имени О.Е. Кутафина (МГЮА)
(Москва, Россия)

Elena-kleshchina@mail.ru

Киберпреступность на современном этапе и роль виктимологической профилактики в ее предупреждении

Аннотация. В статье рассмотрены состояние и тенденции киберпреступности на современном этапе. Подчеркивается, что с учетом роста и изменчивости киберпреступности важное значение имеет виктимологическая профилактика в ее предупреждении. Виктимологическая профилактика определяется в качестве комплекса социальных и правовых мер защиты лиц, которые с большей вероятностью, с учетом их индивидуальных качеств, могут стать жертвами противоправных посягательств. За последние годы, в период роста киберпреступности, накоплен значительный опыт проведения общей виктимологической профилактики, направленной на информирование населения страны о новых криминальных угрозах в информационном пространстве, способах совершения киберпреступлений. Вместе с тем существенное значение следует придавать не только общей, но и индивидуальной виктимологической профилактике, потенциал которой в полной мере не реализуется.

Ключевые слова и словосочетания: преступность, киберпреступность, детерминанты киберпреступности, виктимологическая профилактика, предупреждение киберпреступности.

Для цитирования: *Клещина Е.Н. Киберпреступность на современном этапе и роль виктимологической профилактики в ее предупреждении // Вестник ВИПК МВД России. – 2024. – № 2 (70). – С. 32-37; doi: 10.29039/2312-7937-2024-2-32-37.*

KLESCHINA ELENA N.
Moscow State Law University named after O.E. Kutafin (Moscow, Russia)

CYBERCRIME AT THE PRESENT STAGE AND THE ROLE OF VICTIMOLOGICAL PREVENTION IN HER WARNING

Annotation. The article examines the state and trends of cybercrime at the present stage. It is emphasized that, given the growth and variability of cybercrime, victimological prevention is important in its prevention. Victimological prevention is defined as a set of social and legal measures to protect individuals who are more likely to become victims of unlawful attacks. In recent years, during the period of the growth of cybercrime, significant experience has been accumulated in conducting general victimological prevention aimed at informing the population of the country about new

criminal threats in the information space, ways of committing cybercrimes. At the same time, significant importance should be attached not only to general, but also to individual victimological prevention, the potential of which is not fully realized.

Key words and word combinations: crime, cybercrime, determinants of cybercrime, victimological prevention, crime prevention.

For citation: *Kleschina E.N. Cybercrime at the present stage and the role of victimological prevention in her warning // Vestnik Advanced Training Institute of the MIA of Russia. – 2024. – № 2 (70). – P. 32-37; doi: 10.29039/2312-7937-2024-2-32-37.*

В современный период продолжается рост киберпреступлений. Этому способствует «повсеместное внедрение информационно-телекоммуникационных технологий во все сферы жизнедеятельности, что с неизбежностью влечет новые угрозы государственной и общественной безопасности» [1, с. 15]. При этом следует подчеркнуть приспосабливаемость преступников к новым событиям, происходящим в обществе, применяемым предупредительным мерам.

Экспертами Всемирного экономического форума «к основным мировым угрозам, как в краткосрочной, так и долгосрочной перспективе, отнесены киберпреступность и кибератаки на информационную инфраструктуру. Последние стали обычным явлением для таких секторов, как энергетика, здравоохранение и транспорт» [2].

По данным ГИАЦ МВД России, в 2023 году всего зарегистрировано 1 947,2 тыс. преступлений. Из них количество преступлений с использованием информационно-коммуникационных технологий составляет 677,0 тыс., что на 29,7% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5% в январе-декабре 2022 года до 34,8%. Практически все указанные преступления (98,8%) выявляются органами внутренних дел.

Больше половины таких преступлений (50,6%) относится к категориям тяжких и особо тяжких (342,6 тыс.; +25,9%), более чем три четверти (77,8%) совершается с использованием сети «Интернет» (526,8 тыс.; +38,2%), почти половина (44,7%) – с использованием средств мобильной связи (302,9 тыс.; +42,2%) [3].

В этой связи актуальной является проблема предупреждения киберпреступности.

На расширенной коллегии Генеральной прокуратуры Российской Федерации по итогам 2023 года Генеральный прокурор И. Краснов отметил, что «вновь зафиксирован рост киберпреступлений, а их доля в общем количестве криминальных деяний впервые достигла 35%. Раскрывается лишь четверть из них, а размер возмещенного ущерба критически мал. Утратившие человеческий облик преступники выбирают жертв из уязвимых слоев общества, пенсионеров и даже детей. Пользуясь их доверчивостью, обманывая и запугивая, отнимают порой последние деньги. Причем для обхода принимаемых мер по предотвращению киберпреступлений применяют все новые способы их совершения» [4].

Важнейшим направлением в предупреждении киберпреступности является виктимологическая профилактика.

Как отмечается в научной литературе, «виктимологическая профилактика – это комплекс социальных и правовых мер защиты лиц, которые с большей вероятностью могут стать жертвами противоправных посягательств. Этот вид профилактики складывается из деятельности правоохранительных органов, общественных организаций, отдельных лиц, направленной на выявление формирования предкриминальных ситуаций, а также лиц, склонных в силу своих ролевых функций и индивидуальных особенностей становиться жертвами противоправных посягательств, и на разработку мер по устранению таких причин и снижению риска формирования опасных для человека ролевых функций» [5, с. 120].

Для реализации мер виктимологической профилактики киберпреступности и их совершенствования важное значение имеет изучение виктимных качеств жертв, а также процессов виктимизации, т.е. процессов превращения лиц в жертв киберпреступлений.

Приведем примеры судебной практики.

Так, приговором Железнодорожного районного суда г. Орла от 21 марта 2024 г. по уголовному делу № 1-98/2024 признана

виновной С. в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ. Установлено, что 09.10.2023 С., находясь в квартире у ее знакомой П., решила тайно похитить с банковского счета последней денежные средства посредством входа в ее личный кабинет ПАО «Сбербанк». Реализуя преступный умысел, попросила у П. ее мобильный телефон якобы для обновления настроек. Взяв данный телефон, посмотрела входящие сообщения с номера «900» и получила полный доступ к банковскому счету П. Затем осуществила четыре перевода с ее банковской карты, привязанной к счету. Своими действиями С. причинила значительный материальный ущерб потерпевшей.

Из показаний потерпевшей П. следует, что к ней пришла в гости С., в ходе разговора предложила обновить установки на телефоне, она согласилась и передала свой мобильный телефон. Что конкретно делала в телефоне подсудимая, она не заметила, потом С. быстро собралась и ушла. После ее ухода она заметила, что на кухонном столе лежали две ее банковские карты банка «Сбербанк», которые она достала по просьбе подсудимой. После этого она пошла в магазин за продуктами и при оплате товаров банковской картой на кассе обнаружила, что на ней недостаточно средств. Позже через приложение «СберБанк Онлайн» установила, что без ее ведома с кредитной карты списаны деньги.

В приведенном примере судебной практики очевидны виктимные качества жертвы, в частности неосмотрительность, доверчивость, а также непосредственно процесс виктимизации.

Приведем пример процесса превращения в жертву юридического лица.

Так, приговором Армавирского городского суда Краснодарского края от 5 февраля 2024 г. по уголовному делу № 1-82/2024 установлено, что К., работая в ПАО «ВымпелКом» в должности директора офиса, осуществлял организационно-распорядительные функции по принятию решений, имеющих юридическое значение и влекущих юридические последствия, а именно: заключение договоров на предоставление услуг связи; обеспечение обработки персональных данных физических лиц, с которыми связана работа сотрудника; соблюдение мер безопасности, разработанных в компании и направленных на защиту персональных данных; обеспечение конфиденциальности обрабатываемых персональных данных.

Для выполнения процедуры регистрации сим-карт от имени ПАО «ВымпелКом» при трудоустройстве на К. была оформлена учетная запись, с помощью которой он получал доступ к служебной информации, содержащейся в АИС, и смог вносить изменения в указанную систему.

У К. из корыстной заинтересованности с целью повышения статистических показателей своей работы, а также получения в связи с этим стимулирующих надбавок и выплат возник преступный умысел, направленный на нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, правил доступа к указанной информации, информационным системам, с использованием своего служебного положения. В результате внес в программный модуль «1с-Retail», который в дальнейшем перенес указанные данные в автоматизированную информационную систему «Amdocs Ensemble», сведения о регистрации сим-карт с абонентскими номерами на вымышленные, т.е. фиктивные анкетные данные «А, С». В дальнейшем вышеуказанными сим-картами, оформленными с указанием фиктивных анкетных данных с нарушением действующего законодательства в сфере связи, К. распорядился по собственному усмотрению.

Преступные действия К. нанесли вред критической информационной инфраструктуре, а именно «ABS Amdocs Ensemble», принадлежащей на праве собственности ПАО «ВымпелКом», который выразился в модификации информации, содержащейся в указанной базе данных, внесении в нее недостоверной информации, что нарушило целостность системы. При этом действия К. повлекли за собой необходимость проведения внеплановых проверок по оценке защищенности автоматизированной системы и актуализации циркулирующей в ней информации.

В приведенном примере можно выделить недостатки контроля за деятельностью сотрудника организации, тем более что его деятельность связана с информа-

ционной системой ПАО «ВымпелКом», являющегося субъектом критической информационной инфраструктуры.

С учетом отмеченного важное значение имеет проведение общей и индивидуальной виктимологической профилактики.

За последние годы, в период роста киберпреступности накоплен значительный опыт проведения общей виктимологической профилактики, направленной на информирование населения страны о новых криминальных угрозах в информационном пространстве, способах совершения киберпреступлений. При этом информирование осуществлялось в различных формах, в том числе путем: демонстрации роликов, слайдов в общественном транспорте, на стендах различных организаций; опубликования новостей в средствах массовой информации о совершенных киберпреступлениях и новых киберугрозах, мерах защиты от киберпреступников и др.

Соответственно, общая виктимологическая профилактика направлена на предотвращение виктимизации граждан от киберпреступлений. При этом необходимо и далее активно применять и совершенствовать меры общей виктимологической профилактики, что обуславливается ростом киберпреступлений, приспосабливаемостью преступников к различным событиям, происходящим в обществе, принимаемым мерам противодействия данным преступлениям.

Приведем примеры приспосабливаемости киберпреступников к различным событиям и способам совершения преступлений. Так, например, в 2024 году мошенники разработали и использовали новую схему обмана пользователей. Они рассылали письма с предупреждением о списании средств для уплаты якобы налога на специальную военную операцию. По электронной почте клиентам банков приходили сообщения о том, что якобы со счета будут каждый месяц списывать средства. При этом указывалось на то, что можно подписать отказ, пройдя по ссылке в этом письме, которая направляла на поддельный сайт банка. Далее преступники получали данные в личный кабинет плательщика и похищали денежные средства с реального счета жертвы» [6].

По мнению экспертов, в ближайшие годы киберпреступники будут активно применять искусственный интеллект в области социальной инженерии для убедительного взаимодействия с жертвами. Эти системы позволят им также более эффективно и результативно распространять программы-вымогатели, «прячущиеся в фишинговых письмах», которые, как правило, направлены на кражу данных или доставку вредоносного программного обеспечения [7].

По нашему мнению, существенное значение необходимо придавать не только общей, но и индивидуальной виктимологической профилактике, потенциал которой в полной мере не использован.

Индивидуальная виктимологическая профилактика заключается в выявлении лиц с повышенной виктимностью и проведении с ними профилактических (воспитательных) мероприятий.

Как справедливо отмечается в научной литературе, «приемы и методы индивидуальной виктимологической профилактики, как правило, сводятся лишь к защитно-воспитательной работе с гражданами, уже ставшими потерпевшими. Работа по выявлению лиц с повышенной виктимностью практически не ведется. Такая односторонность в индивидуальной виктимологической профилактике обусловлена главным образом отсутствием специальных методик по выявлению лиц с повышенной виктимностью и субъектов, осуществляющих этот специфический вид профилактики» [8, с. 189-190].

Индивидуальная виктимологическая профилактика киберпреступлений возможна в следующих формах, например: 1) работник банка, взаимодействуя с клиентом, разъясняет ему правила пользования онлайн-банком, перевода денежных средств с одной карты на другую, дает разъяснения о средствах защиты (защищенные ключевые носители, генераторы одноразовых ключей, многофакторный анализ платежей и др.); 2) следователь или дознаватель при производстве предварительного расследования, доказывая обстоятельства, способствовавшие преступлению, выявляет, что тому способствовали виктимные качества потерпевшего. В этом случае необходимо провести индивидуальную профилактическую беседу с потерпевшим, разъяснив суть механизма данного преступления и роли в нем поведения жертвы.

Обратим внимание на положения приказа МВД России от 17.01.2006 № 19 (ред.

от 29.09.2022) «О деятельности органов внутренних дел по предупреждению преступлений». Согласно пункту 18.6 сотрудники следственных подразделений осуществляют профилактическую деятельность среди лиц, потерпевших от преступных посягательств, в целях изменения их виктимного поведения. Аналогичное положение содержится в пункте 14.4, касающееся деятельности сотрудников подразделений дознания.

Вместе с тем согласимся с обозначенным в научной литературе суждением, что «ресурсы индивидуальной виктимологической профилактики не используются в полной мере, поскольку работа по выявлению лиц с повышенной виктимностью практически не ведется.

В этой связи возможно использование двух взаимосвязанных программ, действующих в рамках индивидуальной виктимологической профилактики: программы выявления лиц с повышенной виктимностью и программы коррекции виктимности у отдельных граждан» [9].

По нашему мнению, на современном этапе определилась необходимость создания в научно-исследовательских институтах правоохранительных органов, в высших учебных заведениях ведущих вузов страны научных центров, направленных на проведение виктимологических исследований.

Кроме того, как представляется, необходима активизация деятельности в части проведения виктимологической профилактики в различных сферах общественными организациями, общественными движениями. Такая практика в стране имеется. Приведем пример. Молодежным отделением Международной общественной организации «Союз криминалистов и криминологов» были подготовлены просветительские материалы, посвященные основным правилам того, как не стать жертвами мошенников, и направлены в Правительство г. Москвы, откуда получен положительный ответ по вопросу содействия распространению просветительских листовок [10].

Поскольку значительное количество киберпреступлений совершается в отношении различных организаций, необходимы эффективные меры кибербезопасности, предпринимаемые именно этими организациями. Стратегические решения по кибербезопасности должны быть исключительно в ведении руководства организации.

Таким образом, совершенно очевидно, что киберпреступность является глобальным вызовом обществу, поскольку наблюдается ее рост, изменчивость, быстрая приспосабливаемость к новым событиям. В этой связи важное значение в противодействии киберпреступности имеет виктимологическая профилактика. За последние годы, в период роста киберпреступности накоплен значительный опыт проведения общей виктимологической профилактики, направленной на информирование населения страны о новых криминальных угрозах в информационном пространстве, способах совершения киберпреступлений. Вместе с тем существенное значение следует придавать не только общей, но и индивидуальной виктимологической профилактике, потенциал которой в полной мере не реализован.

1. Прокурорский надзор за исполнением законов при выявлении, расследовании и предупреждении преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации: монография. – М., 2022.

2. The Global Risks Report 2020.15.01. Wold Economic Forum.

3. Состояние преступности в Российской Федерации за 2023 год. Главный информационно-аналитический центр МВД России.

4. Краснов заявил, что киберпреступления составляют уже треть всех преступлений в стране. Тасс. 2024. 26 марта // URL: https://tass.ru/obschestvo/20361331/amp (дата обращения: 30.04.2024).

5. Криминология: учебник / отв. ред. И.М. Мацкевич. – М., 2023.

6. Россиян предупредили о схеме мошенников со списанием «налога на СВО» // Известия. 2024. 28 февр. // URL: https://iz.ru/1656952/2024-02-28/rossiian-predupredili-o-skheme-moshennikov-so-spisaniem-naloga-na-svo (дата обращения: 22.04.2024).

7. В ближайшие годы Искусственный интеллект увеличит количество хакерских атак // Рос. газ. 2024. 29 янв. // URL: https://rg.ru/2024/01/29/v-blizhajshie-gody-ii-uvelichit-kolichestvo-hakerskih-atak.html (дата обращения: 30.04.2024).

8. Криминология: учебник для вузов / под ред. В.Д. Малкова. – М., 2008.
9. Там же.
10. Получены ответы на обращения Союза криминалистов и криминологов по вопросам содействия распространению просветительских листовок // URL: http://crimescience.ru/news/polucheny-otvety-na-obrashheniya-soyuza-kriminalistov-i-kriminologov-po-voprosu-sodejstviya-rasprostraneniyu-prosvetitelskix-listovok.html. (дата обращения: 30.04.2024).

Информация об авторе:

Е.Н. Клещина,
профессор кафедры криминологии
и уголовно-исполнительного права,
доктор юридических наук, профессор

About the author:

E.N. Kleschina,
professor of the department of criminology
and criminal executive law,
doctor of law, professor

Статья поступила в редакцию 15.05.2024