КОРНАУХОВА Н.Г.,
кандидат юридических наук, заместитель
начальника кафедры оперативно-разыскной
деятельности и специальной техники
Волгоградской академии МВД России
pongo_07@mail.ru

НОВИЧИХИН П.Г.,
кандидат юридических наук, старший преподаватель
кафедры конституционного и административного
права Волгоградской академии МВД России
p_chih@mail.ru

УДК 343.85+004

О НЕКОТОРЫХ ПРОБЛЕМАХ ПРЕДУПРЕЖДЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Киберпреступление, мошенничество, жертва киберпреступления, информационно-телекоммуникационные технологии, Интернет, информационная безопасность, латентность преступлений.

Преступления, совершаемые в киберпространстве, характеризуются высокой латентностью. Существует немало проблем, связанных с их предупреждением, выявлением, раскрытием. В связи с этим они создают серьезную угрозу для современного общества. В статье проанализированы статистические данные, свидетельствующие о динамике роста количества преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Констатируется, что система реализуемых в настоящее время превентивных мер не способна в достаточной степени эффективно воздействовать на киберпреступность. Авторами изучены причины, по которым часть преступлений, совершаемых в киберпространстве, остается вне поля зрения правоохранительных органов, сформулированы предложения, направленные на повышение эффективности предупреждения киберпреступности.

Цифровизация практически всех сфер жизни граждан, общества и государства изменила масштабы и само понимание преступности, актуализировала вопросы защиты информации. В нашей стране кибербезопасность включена в информационную безопасность, а информационная безопасность - в национальную [1, с. 21]. Защита информационных систем становится вопросом первостепенной важности. С ростом объема информации, попадающей в информационное пространство, возрастают риски посягательства на личность, собственность, а также на безопасность общества и государства [2, с. 27].

Киберпреступность является особой формой преступности. Она характеризуется использованием для совершения преступлений компьютерных сетей и технологий. К числу таких преступлений относятся хакерские атаки, мошенничество с использованием Интернета, кибертерроризм, производство и распространение детской порнографии, кражи данных и т.д. Киберпреступники могут находиться в любой части мира и быть труднодоступными для задержания, соответственно, таким преступлениям присуще отсутствие места преступления, поскольку само преступление совершается в виртуальном пространстве, где возникают различные виды общественных отношений, и его юридическая природа остается не совсем ясной. Киберпреступники часто используют технологии для маскировки своей деятельности и сокрытия своих персональных данных. Киберпреступность может иметь международный характер и затрагивать разные виды деятельности. Кроме прочего, киберпреступления совершаются в отношении объектов виртуальной собственности, статус которых в нашей стране все еще окончательно не определен. Организационные и процессуальные сложности связаны с высокой латентностью таких преступлений, затруднениями, возникающими в ходе их выявления и сбора доказательств [3, с. 98].

По мнению В.А. Номоконова и Т.Л. Тропиной, которое мы полностью разделяем, киберпреступность включает в себя преступления, совершаемые в киберпространстве с помощью компьютерных систем, компьютерных сетей и других средств доступа, а также преступления против компьютерных систем, компьютерных сетей и компьютерных данных [4, с. 48].

Развитие компьютерных и информационно-телекоммуникационных технологий, безусловно, влияет на трансформацию поведения преступников, они начинают совершать деяния с использова-

нием этих технологий. Согласно результатам анализа преступности, подготовленного МВД России, количество преступлений, связанных с использованием информационно-телекоммуникационных технологий или компьютерной информации, зарегистрированных за период с января по сентябрь 2023 года, достигало 489 тысяч, что на 29,2% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их доля увеличилась с 25,3% (в январе-сентябре 2022 года) до 33,3%. Практически все они были выявлены органами внутренних дел (98,8%)[1].

Причин, обусловливающих такое положение дел, на наш взгляд, несколько. Во-первых, это нежелание жертв преступлений рассматриваемого вида обращаться в правоохранительные органы. Не все жертвы преступлений, например, придают значение утрате электронных платежных средств, многие из них - ввиду заведомого нежелания становиться участником уголовного судопроизводства, объясняя это тем, что утерянная ими сумма денежных средств не стоит потраченного времени. Во-вторых, жертвами киберпреступлений могут быть лица, которые сами причастны к незаконным операциям с объектами, изъятыми из гражданского оборота (а это все виды оружия, боеприпасы, транспортные средства, взрывчатые, отравляющие, пожароопасные и радиоактивные вещества, деньги, ценные вещи, ценные бумаги, наркотические средства, психотропные вещества, прекурсоры, оружие, запрещенные компьютерные программы и т.д.). Они, конечно же, не станут информировать органы правопорядка о похищенных у них средствах. В-третьих, нельзя забывать о тех пострадавших в результате киберпреступлений, которые могут воспользоваться услугами деанонимизации[2], предоставляемыми на различных «теневых» интернет-форумах, и совершить своего рода самосуд над обидчиком. В-четвертых, иногда жертва злоумышленников, желая вернуть потерянные денежные средства, начинает искать схемы, способы и методику совершения аналогичных мошеннических действий в отношении уже других граждан. В этом случае преступление порождает преступника.

Как видим, проблемы выявления преступлений, совершаемых в сфере оборота электронных платежных средств, зачастую связаны с нежеланием жертвы преступления сообщать о его совершении. Это обстоятельство дает нам основание утверждать, что одним из путей решения этих проблем в первую очередь может быть предупреждение преступлений рассматриваемого вида.

Ощущение своей безнаказанности у киберпреступников основывается, на наш взгляд, на представлении о том, что разработанные ими схемы и методы преступной деятельности предполагают полную цифровую защиту интернет-мошенника, или кардера[3], от правоохранителей. В связи с этим одним из наиболее эффективных способов предупреждения преступлений в киберпространстве можно считать публикацию в средствах массовой информации материалов об уже раскрытых преступлениях такого вида, особое внимание авторов которых уделяется объяснению механизмов осуществления преступных замыслов. Использование данного способа позволяет ставить под сомнение конфиденциальность и защищенность преступной деятельности в киберпространстве и способствует в той или иной мере предотвращению совершения в нем новых преступлений.

Киберпреступники, устанавливая контакт с потенциальными жертвами своих преступлений, зачастую пользуются методом социальной инженерии[4]. Тем самым они добиваются того, что в результате общения потенциальные жертвы проникаются доверием к преступнику. Причем оказывается, что они верят ему больше, чем профилактическим листовкам и оповещениям о мошеннической деятельности, с помощью которых правоохранительные органы стараются убедить население не попадаться на уловки злоумышленников.

Говоря о социальной инженерии необходимо понимать, действительно ли преступники, действующие в киберпространстве, имеют психологическое образование, как утверждают некоторые исследователи, или же так или иначе связаны с такой наукой, как психология? Думается, это вовсе не обязательно. Многие интернет-преступники по итогам своей деятельности, принесшей им криминальный доход, разрабатывают собственные программы обучения (кейсы), для того чтобы впоследствии их продать и получить дополнительную выгоду. В таких кейсах их пользователям предлагаются шаблоны общения с потенциальными жертвами преступных действий. Найти такие программы не составляет труда для обычного пользователя Интернета: их размещают на общедоступных каналах в социальных сетях или на «теневых» форумах, которые для обхода блокировки со стороны правоохранительных органов просто меняют домен. Таким образом, очевидно, что у потенциального или действующего киберпреступника может и не быть преступного прошлого, его половые и возрастные характеристики могут сильно варьироваться, для него не обязательно наличие профессионального образования, специальных знаний и т.д. Обучающие кейсы подробно описывают каждый шаг: как общаться с потенциальной жертвой, где такую жертву найти, как получить доход от такого рода деятельности и пр.

Высокий уровень латентности преступлений данного вида, а следовательно, и проблемы, касающиеся возможностей повышения эффективности их предупреждения, обусловлены не только тем,

[1] Краткая характеристика состояния преступности в Российской Федерации за январь-сентябрь 2023 года // Официальный сайт МВД России. 26.10.2023 // URL: https://мвд.рф/reports/item/42989123/ (дата обращения: 11.11.2023).

[2] Доксинг (деанон, деанонимизация, пробив) (англ. «doxing» или «doxxing», от сокр. «docs» - документы) - поиск и публикация персональной или конфиденциальной информации о человеке без его согласия.

[3] Кардер - преступник, занимающийся мошенничеством с платежными картами.

[4] Социальная инженерия - это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании человеческих слабостей.

что жертвы киберпреступлений далеко не всегда обращаются за помощью в правоохранительные органы. Одной из причиной латентности может быть то, что часть киберпреступников, ранее такой деятельностью не занимавшихся, после приобретения описанного выше обучающего кейса осуществляют посягательство на совершение преступления или как минимум формируют соответствующий умысел, но остаются вне поля зрения правоохранительных органов из-за того, что по разным причинам не получают от этой деятельности какого-либо дохода. Вместе с тем необходимо все-таки признать, что киберпреступники постоянно повышают уровень своей криминальной квалификации, укрепляют свою защищенность, обновляют схемы и методы преступной деятельности. И следует констатировать, что их количество стремительно растет.

Министерство внутренних дел Российской Федерации столкнулось с проблемой нехватки сотрудников, обладающих специальными знаниями, необходимыми для выявления преступников в интернет-пространстве и пресечения их противоправной деятельности. Лица, у которых такие знания и опыт их применения есть, не соглашаются на предлагаемые им в правоохранительных органах условия работы и размер дохода. Скорее, наоборот, таким профессионалам проще и прибыльнее «играть за другую сторону», где нет графиков и режимов работы, обязанностей и обязательств, фиксированной заработной платы. То же самое касается и возможностей. Если в киберпреступном мире так называемый доксер[1] может за короткий промежуток времени отыскать любое лицо, какими бы оно средствами защиты не пользовалось, то у сотрудника оперативного подразделения правоохранительных органов, использующего законные методы проведения поиска, на это могут уйти месяцы, а то и годы. За такое время злоумышленник успеет совершить еще немало преступлений.

Решение проблем, связанных с описанными обстоятельствами, «требует как постоянно интегрируемого и автоматизируемого подхода к кибербезопасности, так и адаптации законодательства к этим угрозам» [3, с. 145]. Один из путей решения этих проблемы обозначен в Федеральном законе от 20 октября 2022 г. № 408-ФЗ «О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе»». До 21 октября 2023 года для установления дальнейшего движения похищенных денежных средств необходимо было отправлять запросы банкам и электронным кошелькам и в течение длительного времени ждать ответы, что, несомненно, затягивало процесс выявления и раскрытия фактов совершения мошенничества при осуществлении денежных переводов. Названный выше нормативный правовой акт создал условия для быстрого обмена значимой для осуществления противодействия киберпреступности информацией между Банком России и МВД России. В частности, закон предусматривает подключение МВД России к автоматизированной системе «ФинЦЕРТ» Банка России, в которой содержится информация об операциях, проведенных без согласия клиентов. Благодаря этому правоохранительные органы могут практически в онлайн-режиме получать сведения о мошеннических операциях, в том числе о получателях похищенных денег. МВД России, в свою очередь, должно передавать в базу данных «ФинЦЕРТ» сведения о совершенных противоправных действиях. Такие сведения банки учитывают в своей работе, корректируя бизнес-процессы так, чтобы обеспечить безопасность переводов[2].

Научно-технический прогресс внес значительные изменения в современную жизнь человечества, предоставив компьютерные

[1] Доксер - человек, который совершает доксинг.

[2] Подписан закон о взаимодействии Банка России и МВД России по фактам мошенничества при осуществлении переводов денежных средств // СПС «Гарант» // URL: https://www.garant.ru/news/1581261/ (дата обращения: 11.11.2023).

KORNAUKHOVA N.G.,
PhD in Juridical Sciences,
Deputy Head of the Department of Operational Investigative Activities and Special Equipment of the Volgograd Academy of the Ministry of Interior of Russia

NOVICHIKHIN P.G.,
PhD in Juridical Sciences, Senior Lecturer of the Department of Constitutional and Administrative Law of the Volgograd Academy of the Ministry of Interior of Russia

ON SOME PROBLEMS OF PREVENTING CYBERCRIMES IN MODERN SOCIETY

Cybercrime, fraud, victim of cybercrime, information and telecommunication technologies, Internet, information security, crime latency.

Crimes committed in cyberspace are characterized by high latency. There are many problems associated with their prevention, identification, and disclosure. In this regard, they pose a serious threat to modern society. The article analyzes statistical data indicating the dynamics of growth in the number of crimes committed using information and telecommunication technologies. It is stated that the system of currently implemented preventive measures is not capable of sufficiently effectively influencing cybercrime. The authors studied the reasons why some crimes committed in cyberspace remain beyond the sight of law enforcement agencies, and formulated proposals aimed at increasing the effectiveness of cybercrime prevention.

и информационно-телекоммуникационные технологии. Эти технологии не только привели к возникновению новых информационных ресурсов, но и спровоцировали развитие новых видов преступности. Важной составляющей этих процессов являются компьютерные сети, разрастание которых привело к резкому увеличению числа компьютерных преступлений, совершаемых с использованием возможностей глобальной информационной сет. Для обеспечения кибербезопасности общества и государства необходимо решить проблемы, которые мешают эффективному выявлению, предупреждению и расследованию преступлений, связанных с применением новых достижений в области компьютерных технологий. Требуется разработка стратегии, реализация которой позволит оперативным подразделениям опережать преступников в развитии и использовании интернет-пространства. Только таким образом можно обеспечить эффективное противодействие киберпреступлениям. Важно принять меры, чтобы оперативные службы обладали знаниями и навыками, необходимыми для борьбы с киберпреступниками [5, с. 185]. Нивелировать недостаток сил и средств для предупреждения преступлений рассматриваемого вида можно с помощью грамотного подбора кадров (это должны быть специалисты, которые понимают, как киберпреступления совершаются, и могут найти пути их выявления и раскрытия), а также постоянного обновления программного обеспечения, помогающего оперативным сотрудникам быстрее устанавливать лиц, совершивших преступления и киберпространстве. ■

Библиографический список:

1. Диденко К.В. Некоторые проблемы выявления и предупреждения киберпреступлений // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2020. № 3. С. 20-24.

2. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25-33.

3. Никульченкова Е.В. Трансформация киберпреступности: современные угрозы и их предупреждение // Вестник Омского университета. Серия «Право». 2023. Т. 20. № 3. С. 96-105.

4. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 45-55.

5. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. Б.П. Смагоринского. М.: Право и закон, 2019. 200 с.