УДК 343.98
DOI https://doi.org/10.32849/2663-5313/2020.11.45

Григорий Третьяков,
канд. юрид. наук, доцент,
доцент кафедры уголовного права, уголовного процесса и криминалистики
Гродненского государственного университета имени Янки Купалы

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕНДЕНЦИЙ РАЗВИТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ ПУТЕМ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ, В РЕСПУБЛИКЕ БЕЛАРУСЬ И ЗА РУБЕЖОМ

Целью статьи является проведение сравнительного анализа общемировых тенденций развития преступлений, совершаемых с использованием компьютерной техники, и тенденций развития данного вида преступности в Республике Беларусь, необходимого для разработки соответствующих мер реагирования со стороны правоохранительных органов, осуществления эффективной профилактической деятельности. Отмечается, что активное распространение информационных технологий во всех сферах обуславливает значительный срез проблем, связанных с обеспечением их функционирования во благо развития общества. В первую очередь данные проблемы стоят перед правоохранительными органами и связаны с противодействием правонарушениям в рассматриваемой сфере. В статье приводятся статистические данные о состоянии преступности в сфере информационных технологий в Республике Беларусь, отмечается существенный рост количества зарегистрированных преступлений в течение последних нескольких лет. В то же время отмечается, что это не отражает всей динамики преступности в данной сфере, поскольку функциональный потенциал информационно-коммуникационных технологий позволяет использовать их в качестве орудий или средств совершения почти всех предусмотренных уголовным законом преступных посягательств. В статье проводится анализ наиболее распространённых видов преступлений, отраженных в ежегодном отчете Полицейской службы Европейского Союза (Europol) по оценке угроз развития организованной преступности в сети Интернет, выявленных и расследованных преступлений в данной сфере в Республике Беларусь. Проводится анализ таких групп преступлений, как киберзависимые преступления, объектом которых являются отношения в сфере информационной безопасности; посягательств против половой свободы и неприкосновенности несовершеннолетних; преступлений, связанных с использованием электронных платежных инструментов; преступлений в сфере незаконного оборота наркотических средств, психотропных веществ, их прекурсоров и аналогов. По итогам проведенного анализа, с учетом рассмотрения современных тенденций развития преступлений, совершаемых с использованием компьютерной техники и информационно-коммуникационных технологий, сформулирован комплекс практических рекомендаций, связанных с повышением эффективности противодействия данной категории преступлений.

Ключевые слова: противодействие преступности, информационная безопасность, киберпреступность, информационные технологии, расследование.

Постановка проблемы. Глобальный характер динамично развивающегося информационного общества представляет собой принципиально новый этап его развития, в котором информация и связанные с ней знания проникают во все сферы человеческой деятельности.

Информационная сфера сегодня приобретает ключевое значение и оказывает значительное влияние на современное общество, государство, на происходящие экономические, политические и социальные процессы.

Активное распространение информационных технологий во всех сферах обуславливает целый срез проблем, связанных обеспечением их функционирования во благо развития общества. Прежде всего данные проблемы стоят перед правоохранительными органами и связаны с противодействием правонарушениям в рассматриваемой сфере. Преступления, совершаемые с использованием информационно-коммуникационных технологий, сегодня прочно зарекомендовали себя как явление международного масштаба, носят ярко выраженный транснациональный характер. Повсеместное использование информационных технологий и сети Интернет во всех сферах, включая

экономическую, социальную деятельность, объективно влечет расширение интересов лиц, совершающих преступные действия, также и в данном направлении.

Преступления, совершаемые с использованием компьютерной техники, получили разностороннее освещение в юридической литературе. Исследованию данной проблемы посвящены работы многих ученых. Вместе с тем можно отметить, что проблема противодействия преступлениям данной категории требует дальнейшего изучения и исследования, систематизации различных аспектов и использования зарубежного опыта. Это обусловило выбор темы статьи.

Цель статьи – проведение сравнительного анализа общемировых тенденций развития преступлений, совершаемых с использованием компьютерной техники, и тенденций развития данного вида преступности в Республике Беларусь, необходимого для разработки соответствующих мер реагирования правоохранительными органами, осуществления эффективной профилактической деятельности.

Изложение основного материала. Республика Беларусь не стоит в стороне от происходящих глобальных процессов развития киберпреступности. Так, по данным Министерства внутренних дел Республики Беларусь, за последние годы отмечается существенный рост количества преступлений в исследуемой сфере. За 2019 г. было зарегистрировано 10 567 преступлений в сфере высоких технологий. Рост по сравнению с 2018 г. составил 121,6% (4 769 преступлений в 2018 г.). В 2018 г. по сравнению с 2017 г. количество выявленных преступлений также возросло на 53%. Вместе с тем увеличивается и удельный вес преступлений данной категории от общего количества регистрируемых в стране преступлений (в 2015 г. – 2,5%, в 2016 г. – 2,7%, в 2017 г. – 3,6%, в 2018 г. – 5,7%).

Подавляющее число преступлений (2019 г. – 76,4%; 2018 г. – 75,6%), выявленных в сфере высоких технологий, относятся к хищениям путем использования компьютерной техники (ст. 212 Уголовного кодекса Республики Беларусь). Число таких преступлений, относящихся к категориям особо тяжких и тяжких, увеличилось в 2019 г. в 3 раза (с 44 до 130).

В 2019 г. было установлено 1 859 лиц (2018 г. – 1 283), совершивших преступления в сфере высоких технологий [1].

Следует отметить, что представленные статистические сведения включают лишь преступления, предусмотренные гл. 31 Уголовного кодекса (далее – УК) Республики Беларусь (ст. ст. 349–355), – преступления против информационной безопасности, и ст. 212 УК Республики Беларусь – хищение путем использования компьютерной техники.

В то же время, как отмечают многие отечественные и зарубежные исследователи, а также практические работники, эволюционирование киберпреступности привело к интеграции киберкомпонента в почти все формы традиционной преступности. Значительное количество преступлений, совершаемых в данной сфере, имеет своей целью посягательство не отношения в сфере информационной безопасности, а другие объекты – право собственности, тайна личной жизни, здоровье населения. Функциональный потенциал информационно-коммуникационных технологий позволяет использовать их в качестве орудий или средств совершения почти всех предусмотренных уголовным законом преступлений.

Анализ судебно-следственной практики позволяет говорить о том, что сегодня тенденции развития киберпреступности в Республике Беларусь в целом совпадают с основными мировыми тенденциями развития преступности в исследуемой сфере.

В зарубежных странах в силу отличий национального законодательства существуют различные подходы к оценке показателей преступности. В ежегодном отчете Европола по оценке угроз преступности в сети Интернет на сегодняшний день в качестве наиболее опасных выделяют следующие типы преступных посягательств [2], которые характерны также и для Республики Беларусь:

1. Киберзависимые преступления. В данную категорию включаются преступления, объектом которых являются отношения в сфере информационной безопасности.

Одной из ключевых угроз является все большее распространение специализированных программ-вымогателей, которые наносят ущерб как государственному, так и частному сектору. Сложность противодействия данной категории преступлений обусловлена также их высокой латентностью, высокой степенью конфиденциальности, частым нежеланием жертв по различным причинам обращаться в правоохранительные органы.

Так, неустановленными лицами предположительно с территории иностранного государства на нескольких сайтах белорусского сегмента сети Интернет была размещена вредоносная программа, которая при попадании в персональные компьютеры пользователей блокировала работу и выводила на экран сообщение о том, что их компьютер заблокирован за просмотр в сети Интернет

видеоматериалов, содержащих элементы порнографии с участием несовершеннолетних. Им предлагалось во избежание уголовной ответственности в течение нескольких часов оплатить «штраф» на указанные на экране расчетные счета.

Программы-вымогатели становятся ориентированными на все более целевую аудиторию, что влечет более целенаправленное влияние на потенциальную жертву и, соответственно, повышение эффективности преступной деятельности.

Данное программное обеспечение может быть предназначено не только для персональных компьютеров, но и для иных устройств. В особой зоне риска находятся мобильные телефоны, которые все чаще используются для осуществления мобильных платежей, являются средством хранения либо обеспечения доступа к конфиденциальной информации.

Отмечено также, что в 2020 г. пандемия COVID-19 и переход многих компаний на дистанционные формы работы привели к существенному снижению обеспечения безопасности данных и компьютерных сетей и, как следствие, увеличению количества преступных посягательств.

Как отмечается в указанном выше отчете Европола, по-прежнему не теряют актуальности угрозы DDoS-атак, как целенаправленных, так и автоматизированных.

Данные атаки могут совершаться с различной мотивацией от простого любопытства и «пробы» собственных сил, до вымогательства и совершения тщательно спланированных преступных действий за вознаграждение.

В ходе проведения комплекса оперативно-разыскных мероприятий были установлены двое 24-летних граждан, которые в период с 2018 г. по ноябрь 2019 г. совершали DDos-атаки на вебсайты предприятий, торговых центров, учреждений образования и здравоохранения, интернет-магазинов в Республике Беларусь, а также различные интернет-ресурсы других государств. По показаниям обвиняемых, основной их мотивацией была проверка своих способностей и навыков, а также уязвимости определенных ресурсов в сети Интернет. При этом один из них размещал на специализированных форумах объявления о возможности осуществления им DDos-атак за денежное вознаграждение.

2. Посягательства против половой свободы и неприкосновенности несовершеннолетних. Практика правоохранительных органов Европейского Союза отмечает постоянное увеличение количества материалов сексуального характера с участием несовершеннолетних, размещаемых в сети Интернет, и связанных с ними преступлений, таких как распространение данных материалов, сексуальное насилие, сексуальное принуждение, вымогательство. В отчете Европола в 2020 г. отмечено несколько причин этому, в том числе популярность порнографических материалов, рост количества материалов собственного производства несовершеннолетними, совершенствование механизмов выявления данных правонарушений, расширение времени досуга несовершеннолетних в сети Интернет, связанного с противоэпидемиологическими мероприятиями.

Индивидуальное распространение и обмен между пользователями обычно происходят в социальных сетях, сетевых платформах и широко используемых зашифрованных мессенджерах.

Данная категория преступных посягательств отличается наибольшей латентностью, поскольку жертвы зачастую не осведомлены о том, что интимная информация получила распространение, или предпочитают скрывать обстоятельства совершения преступления в отношении них.

Судом вынесен приговор в отношении 26-летнего гражданина К. по ч. 2 ст. 343. УК Республики Беларусь (изготовление и распространение порнографических материалов или предметов порнографического характера). К. в течение года лет встречался с потерпевшей, 17-летней С., имел с ней интимные отношения. В этот период К. были изготовлены интимные фотографии С., которые он хранил у себя в мобильном телефоне. После разрыва взаимоотношений К. требовал их продолжения, угрожая распространить данные фотографии. После получения отказа К. создал в социальной сети страницу от имени С., разместил там фотографии, разослал приглашения посетить страницу общим знакомым.

Отчет Евпропола отмечает такие негативные факторы, связанные с материалами сексуального характера в отношении несовершеннолетних, как использование DarkWeb-сообществ для обмена информацией преступными группами, распространение прямых интернет-трансляций с демонстрацией сексуальных сцен с несовершеннолетними, растущей коммерциализацией распространения детской порнографии.

В Республике Беларусь также отмечаются случаи изготовления детской порнографии в целях ее дальнейшего коммерческого распространения.

Так, судом был вынесен приговор в отношении мужчины и двух женщин. Обвиняемый познакомился с двумя женщинами, являвшихся сестрами, каждая из кото-

рых воспитывала дочь двух и четырех лет сответственно. Вскоре обвиняемый стал сожительствовать с одной из женщин. Впоследствии отношения привели к тому, что мужчина стал систематически совершать действия сексуального характера в отношении ее дочери, а также племянницы. Свои действия снимал на видео и продавал ролики в закрытых сетях. Матери были в курсе происходящего и получали за это деньги.

3. Преступления, связанные с использованием электронных платежных инструментов.

Отмечается увеличение преступлений, связанных с изготовлением дубликатов сим-карт мобильной связи в целях получения доступа к сервисам, защищенным двухфакторной аутентификацией на основе SMS-сообщений. Поскольку для этого требуются профессиональные навыки и подробная информация об объекте, действия, связанные с изготовлением дубликатов сим-карт, являются хорошо спланированными и целенаправленными.

Отмечается стабильно высокий уровень преступности, связанной с компрометацией электронной почты (BEC-атака) – получением доступа к корпоративным учетным записям электронной почты, чтобы при помощи методов социальной инженерии обмануть получателей, вынудив их осуществить перевод денежных средств, переслать конфиденциальную информацию либо совершить иные действия.

Также популярным способом интернет-мошенничества является создание различных инвестиционных онлайн-платформ, обещающих быстрый стабильно высокий заработок.

Возбуждено уголовной дело в отношении неустановленного лицо, создавшего в Интернете сайт, представленный как инвестиционная платформа. Сайт предлагал зачислять денежные средства на счет, после чего с помощью брокеров осуществлять игру на онлайн-бирже с целью получения прибыли. Так, одна из потерпевших перечислила на счет данной организации 250 долларов США. В последующем с ней неоднократно связывались различные представители данной платформы, которые сообщали, что сумма на ее счету многократно увеличивается, и, чтобы обналичить данные средства, необходимо перечислять дополнительные суммы денег – налоговые сборы и за услуги курьера. Таким образом под вышеуказанными предлогами в течение полугода неустановленное лицо завладело ее денежными средствами на общую сумму более 82 тысяч долларов США.

Отмечается увеличение количества преступлений, связанных с использованием похищенных данных о банковских картах при покупке товаров и услуг и электронным перехватом платежных данных с использованием вредоносных программ.

Также по-прежнему распространен так называемый джекпоттинг – взлом банкоматов. Распространены как способы удаленного взлома, так и путем непосредственного подключения оборудования к банкомату. Доступность специального оборудования и программного обеспечения привлекает в данную сферу и непрофессиональных правонарушителей.

4. Широко распространенными посредством использования сети Интернет остаются преступления в сфере незаконного оборота наркотических средств, психотропных веществ, их прекурсоров и аналогов. Правоохранители отмечают, что сегодня практически при совершении каждого преступления в этой сфере используются информационно-коммуникационные технологии.

Выводы

Подводя итог рассмотренному, с учетом изучения современных тенденций развития преступлений, совершаемых с использованием компьютерной техники и информационно-коммуникационных технологий, можно сформулировать следующие комплексы действий, связанных с повышением качества противодействия данной категории преступлений:

1. Повышение эффективности международного сотрудничества в сфере информационной безопасности, включая оперативный обмен информацией, совершенствование механизмов оказания правовой помощи с учетом тенденций развития преступности.

2. Совершенствование правового регулирования ответственности за преступления, совершаемые с использованием компьютерной техники и информационно-коммуникационных технологий, гармонизация законодательства, выработка единообразных подходов к квалификации и расследованию преступных действий.

3. Совершенствование правового механизма проведения оперативно-разыскных мероприятий в сети Интернет.

4. Совершенствование профилактически мер, направленных на предупреждение преступности в исследуемой сфере, повышение уровня осведомленности населения о возможных угрозах.

5. Совершенствование качества подготовки сотрудников правоохранительных органов, получение комплексных знаний в области информационных технологий, экономики и др.

Список использованных источников:

1. Статистика управления по раскрытию преступлений в сфере высоких технологий. *Министерство внутренних дел Республики Беларусь*. URL: https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/statistika-urpsvt (дата обращения: 30.03.2020).

2. Internet Organised Crime Threat Assessment. European Union Agency for Law Enforcement Cooperation (Europol), 2019. 63 p.

Григорій Третьяков. Порівняльний аналіз тенденцій розвитку злочинів, скоєних шляхом використання комп'ютерної техніки, у Республіці Білорусь та за кордоном

Метою статті є проведення порівняльного аналізу загальносвітових тенденцій розвитку злочинів, скоєних із використанням комп'ютерної техніки, і тенденцій розвитку даного виду злочинності в Республіці Білорусь, необхідного для розроблення відповідних заходів реагування з боку правоохоронних органів, здійснення ефективної профілактичної діяльності. Відзначається, що активне поширення інформаційних технологій у всіх сферах обумовлює значний зріз проблем, пов'язаних із забезпеченням їх функціонування на благо розвитку суспільства. Передусім дані проблеми стоять перед правоохоронними органами та пов'язані із протидією правопорушенням у даній сфері. У статті наводяться статистичні дані про стан злочинності у сфері інформаційних технологій у Республіці Білорусь, відзначається суттєве зростання кількості зареєстрованих злочинів протягом останніх кількох років. Водночас відзначається, що це не відображає всієї динаміки злочинності в даній сфері, оскільки функціональний потенціал інформаційно-комунікаційних технологій дозволяє використовувати їх як знаряддя або засоби вчинення майже всіх передбачених кримінальним законом злочинних зазіхань. У статті проводиться аналіз найбільш поширених видів злочинів, відображених у щорічному звіті Поліцейської служби Європейського Союзу (Europol), за оцінкою загроз розвитку організованої злочинності в мережі Інтернет та виявлених і розслідуваних злочинів у даній сфері в Республіці Білорусь. Проводиться аналіз таких груп злочинів, як кіберзалежність злочину, об'єктом яких є відносини у сфері інформаційної безпеки; посягань проти статевої свободи та недоторканості неповнолітніх; злочинів, пов'язаних із використанням електронних платіжних інструментів; злочинів у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх прекурсорів і аналогів. За підсумками проведеного аналізу, з урахуванням розгляду сучасних тенденцій розвитку злочинів, скоєних із використанням комп'ютерної техніки й інформаційно-комунікаційних технологій, сформульований комплекс практичних рекомендацій, пов'язаних із підвищенням ефективності протидії злочинам даної категорії.

Ключові слова: протидія злочинності, інформаційна безпека, кіберзлочинність, інформаційні технології, розслідування.

Hryhoryi Tretiakov. Comparative analysis of trends in the development of crimes committed by the use of computer technologies in the Republic of Belarus and abroad

The purpose of the article is to conduct a comparative analysis of global trends in the development of crimes committed with the use of computer technologies, and trends in the development of this type of crime in the Republic of Belarus, which is necessary for the development of appropriate response measures for law enforcement agencies, for the implementation of effective preventive activities. It is noted that the active dissemination of information technologies in all spheres causes a significant number of problems associated with ensuring their functioning for the benefit of the development of society. First of all, these problems are faced by law enforcement agencies and are associated with countering offenses in this area. The article provides statistical data on the state of crime in the field of information technology in the Republic of Belarus, a significant increase in the number of registered crimes over the past few years is noted. At the same time, it is noted that this does not reflect the entire dynamics of crime in this area, since the functional potential of information and communication technologies allows them to be used as instruments or means of committing almost all criminal offenses provided for by the criminal law. The article analyzes the most common types of criminal offenses, reflected in the report of the European Union's law enforcement agency (Europol) on the Internet organized crime threat assessment and identified and investigated crimes in this area in the Republic of Belarus. The analysis of such groups of crimes as cyber-dependent crimes, the object of which is relations in the field of information security; attacks against sexual freedom and inviolability of minors; crimes related to the use of electronic payment instruments; crimes in the sphere of illegal traffic in narcotic drugs, psychotropic substances, their precursors and analogues is conducted. Based on the results of the analysis, taking into account the consideration of modern trends in the development of crimes committed with the use of computer technology and information and communication technologies, a set of practical recommendations related to improving the quality of countering this category of crimes was formulated.

Key words: crime prevention, information security, cybercrime, information technology, investigation.