7. Аршинский, Л.В., Жигалов, Н.Ю., Мункожаргалов, Ц.Б. Проблемы применения информационного и логико-математического моделирования в судебной экспертизе и криминалистике // Российский следователь. - 2013. - № 3. - С. 6 - 10.

8. Сушина, Т.Е., Собенин, А.А. Перспективы и риски использования искусственного интеллекта в уголовном судопроизводстве // Российский следователь. - 2020. - № 6. - С. 21 - 25.

9. Лаптев, В.А. Ответственность «будущего»: правовое существо и вопрос оценки доказательств // Гражданское право. - 2017. - № 3. - С. 32 - 35.

ТЕНДЕНЦИИ РАЗВИТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Г.М. Третьяков
доцент кафедры уголовного права,
уголовного процесса и криминалистики
УО «Гродненский государственный университет им. Янки Купалы»,
кандидат юридических наук, доцент

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

Активное распространение информационных технологий во всех сферах обуславливает срез определенных проблем. В том числе 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.

В Республике Беларусь за последние годы отмечается существенный рост количества преступлений в сфере высоких технологий. Так, за 2019 год было зарегистрировано 10 567 преступлений в сфере высоких технологий. Рост по сравнению с 2018 годом составил 121,6% (4769 преступлений в 2018 году). В 2018 по сравнению с 2017 годом 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%, 2016 г. – 2,7%, 2017 г. – 3,6%, 2018 г. – 5,7%).

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

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

Следует отметить, что представленные статистические сведения включают лишь преступления, предусмотренные главой 31 УК Республики Беларусь (стст. 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 том, что функциональный потенциал информационно-коммуникационных технологий позволяет использовать их в качестве орудий или средствсовершения 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.

За рубежом 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.

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

В числе ключевых угроз присутствует все большее распространениеспециализированных 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.

Используемое программное обеспечение может быть предназначено не только для персональных компьютеров, но и также 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 году 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, совершаемых с различной мотивацией от простого любопытства и «пробы» собственных сил, до вымогательства и совершения тщательно спланированных преступных действийза вознаграждение.

Посягательства против половой свободы и неприкосновенности несовершеннолетних. Практика правоохранительных органов ЕС 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 отчетеЕвропола в 2020 году отмечено несколько причин этому, в том числе популярность порнографических материалов, ростколичества материалов собственного производстванесовершеннолетними, 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 также отличается латентностью, поскольку жертвы могут быть не осведомлены, что интимная информация получила распространение или предпочитают скрывать обстоятельства совершения преступления в отношении них.

В Республике Беларусь также выявляются преступления, связанные с изготовлением порнографии с участием несовершеннолетних в целях ее дальнейшего коммерческого распространения.

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) – получение доступа к корпоративным учетным записям электронной почты, чтобы при помощи методов социальной инженерии обмануть получателей, вынудив их осуществить перевод денежных средств, переслать конфиденциальную информациюлибо совершить иные действия.

Также по прежнему распространенным способом мошенничества является создание различных онлайн платформ, обещающих быстрый стабильно высокий заработок путем инвестиций и др.

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

Распространенными остаются преступления в сфере незаконного оборота наркотических средств, психотропныхвеществ, их прекурсоров и аналогов, совершаемы с использованием сети Интернет Правоохранители отмечают, что сегодня практически при совершении каждого преступления в этой сфере используются информационно-коммуникационные технологии.

Подводя итог рассмотренному, можно сформулировать направления совершенствования противодействия преступлениям, совершаемым с использованием компьютерной техники:

Совершенствование механизмов международного сотрудничества в сфере противодействия киберпреступности.

Совершенствование правового регулирования ответственности за преступления, совершаемые с использованием компьютерной техники, гармонизация законодательства, выработка единообразных подходов к квалификации и расследованию преступных действий на международном уровне.

Совершенствование правового механизма проведения оперативно-розыскных мероприятий в сети Интернет, в том числе также и механизмов оперативного обмена информацией с зарубежными органами

Совершенствование профилактических мер, направленных на предупреждение преступности, повышение уровня осведомленности населения о распространенных угрозах и способах совершения преступных действий.

Повышение качества и специализированная подготовка сотрудников правоохранительных органов в области информационных технологий, экономики и др.

Библиографический список

1. Статистика управления по раскрытию преступлений в сфере высоких технологий [Электронный ресурс] / Министерство внутренних дел Республики Беларусь. – Режим доступа: https://www.mvd.gov.by/ru/page/ upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/statistika-urpsvt. – Дата доступа: 30.03.2020.

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