УДК 343.9.018

ПРОБЛЕМЫ ОРГАНИЗАЦИИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

© 2021 А. А. Душкин, И. В. Потанина

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (г. Воронеж, Россия)

В представленной статье предпринята попытка рассмотреть некоторые особенности расследования преступлений, совершённых с использованием современных компьютерных технологий. Проанализированы способы совершения преступлений данной категории, рассмотрены проблемы их раскрытия.

Ключевые слова: преступления, компьютерные технологии, киберпреступления, компьютерная информация, вредоносные компьютерные программы.

В условиях современной действительности вопросы об особенностях расследований преступлений, совершаемых в сфере компьютерных технологий, являются достаточно актуальными. В последние годы именно в данной сфере совершается самое большое количество преступлений в России, ущерб от них превысил десятки миллионов долларов, что, безусловно, является достаточно значимой цифрой для нашего государства. Вследствие этого борьба с преступлениями, совершёнными с использованием компьютерных технологий, является одним из приоритетных направлений правоохранительной деятельности в Российской Федерации.

Особенностью современности является появление новых, ранее неизвестных форм преступности, в которых средствами совершения преступлений выступают компьютеры, аппаратное обеспечение и различные компьютерные программы, в том числе и вредоносные. Такие формы преступности образуют новый вид преступлений – киберпреступления, т. е. преступления, совершаемые с помощью или посредством компьютерных систем или компьютерных сетей, в рамках компьютерных систем и сетей, и против компьютерных систем и компьютерных данных [1].

Необходимо заметить, что в последнее время появилось достаточно много способов совершения киберпреступлений: программы-взломщики, вирусы, контенты различного содержания, распространяющиеся через мобильную связь, электронную почту, так называемые веб-доски объявлений, различные чаты и группы в социальных сетях, NFC-приёмники и многие другие. Вместе с тем появилось огромное количество новых преступных киберпрофессий: вирусописатели, кардеры, фишеры, заливщики, а вместе с ними и много новых видов преступлений, которые совершаются с помощью компьютерных технологий: взлом компьютерной сети, хищение денег с банковских карт, вирусные атаки, компьютерное пиратство, торговля порнографической продукцией, перехват трафика, фишинг, кибершпионаж и кибертерроризм. Сегодня в России существуют целый подпольный рынок киберпреступности – даркнет, в котором практически можно купить любое оружие, наркотики, личные персональные данные любого пользователя сети интернет, а также сделать заказ на убийство и даже теракт. Безусловно, даркнет представляет серьёзную опасность для всех граждан страны.

Заметим также, что достаточно серьёзную проблему представляют собой и атаки на различные объекты инфраструктуры, которые вместе с финансовым ущербом, могут привести к серьёзным последствиям, угрожающим безопасности государства.

Стоит также обратить внимание на то, что некоторые реально совершённые преступления остаются в тени: например, когда в онлайн-игре «World of Tanks» преступники крадут у пользователя игры танк ценой в несколько тысяч долларов или же, используя компьютерные вирусы, похищают личные

Душкин Алексей Александрович – Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, студент, alekskrok48@yandex.ru.

Потанина Ирина Витальевна – Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, канд. юрид. наук, доцент, irina-potanina@yandex.ru.

пароли от криптокошельков, с помощью которых крадут криптовалюту Bitcoin. О таких преступлениях люди чаще всего не заявляют, и по ним соответственно никто не возбуждает уголовные дела.

Согласно официальным данным Генпрокуратуры раскрываемость преступлений, совершённых с использованием компьютерных технологий, составляет в настоящее время всего лишь 41,3 % [2]. Итак, киберпреступлений с каждым годом становится всё больше, а их раскрываемость оставляет желать лучшего.

К наиболее распространённым преступлениям с использованием новейших компьютерных технологий сегодня относятся: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), а также мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) [3].

Что касается ст. 272 УК РФ, неправомерный доступ к компьютерной информации – стоит заметить, что сегодня с помощью вредоносных компьютерных программ рассылки различного вида спамов преступники взламывают компьютерные системы и похищают много различной конфиденциальной информации. Однако, в законе нет понятия вредоносной программы, поэтому для возбуждения уголовного дела по ст. 273 УК РФ необходимо указать объективную сторону. Если не получается доказать, что программа – вредоносная, дело будет обоснованно прекращено.

В отношении ст. 159.3 УК РФ стоит отметить, что с 2018 г. наказуемы любые мошеннические действия с использованием электронных средств платежа. В этих случаях наряду с классическими доказательствами (показаниями потерпевшего) со стороны обвинения могут быть использованы: приобщённые к материалам дела справки о результатах расследования, устанавливающие факт взлома сети компании; проведение компьютерной экспертизы, в заключении которой отражено, что были обнаружены следы функционирования хакеров.

Стоит обратить внимание на тот факт, что, прежде всего, трудности в расследовании киберпреступлений, а, следовательно, и существующая на данный момент их низкая раскрываемость, обусловлены:

- во-первых, несовершенством действующего уголовного законодательства (существующие статьи УК РФ не включают в себя составы некоторых современных компьютерных преступлений, таких как: майнинг и DDoS атаки);

- во-вторых, расследованием компьютерных преступлений занимаются юристы, а не технические эксперты с юридическим образованием [4].

Отметим также, в качестве отрицательных факторов длительность проведения компьютерных экспертиз (в среднем около полугода) и нехватку квалифицированных специалистов.

В этой связи стоит заметить, что часть компьютерных преступлений, таких, как: взлом социальных сетей и вирусные атаки на домашние компьютеры очень часто нигде не фиксируется, так как потерпевшая сторона предпочитает не сообщать о таких преступлениях правоохранительным органам, в первую очередь, не надеясь на быстрое решение проблемы.

Сегодня распространённым и популярным у преступников способом хищения в киберпространстве становится фишинг, который заключается в рассылке электронных писем владельцам денежных средств, с помощью которых все их денежные средства перемещаются на счета хакеров. Стоит отметить, что такой фишинг может расследоваться достаточно долго, так как следствию необходимо: получить показания потерпевшего и сотрудников интернет-провайдера; провести оперативно-розыскные мероприятия, установить похитителя; получить ответ от банка о снятии денежных средств со счёта потерпевшего; произвести задержание, изъять компьютерную технику и т. д. Также заметим, что следователи часто заходят в тупик при расследовании таких преступлений, когда непосредственно отсутствуют как таковые место преступления в классическом понимании.

В настоящее время трудности в расследовании компьютерных преступлений обусловлены нехваткой высококлассных специалистов и отсутствием современных инструментов для анализа цифровых доказательств, а также слабыми возможностями по идентификации онлайн-злоумышленников. Современные киберпреступники применяют такие средства, которые скрывают реальную личность (VPN/VPS-сервисы для анонимизации интернет-трафика, виртуальные номера мобильных телефонов и т. д.), что усложняет идентификацию личности [5].

Согласно верному замечанию А. П. Суходулова, «электронная среда существенно затрудняет идентификацию правонарушителя, а значит, его изобличение и уголовное преследование, что влечёт появление одной из характерных черт преступности … – многоэпизодность криминальной активности» [6].

Обратим внимание также на то, что следователи и дознаватели при производстве следственных действий, связанных с обнаружением, исследованием и изъятием электронных носителей информации, сталкиваются с рядом трудностей, обусловленных разнообразием подлежащих исследованию объектов, недостатком применяемых технико-криминалистических средств, необходимых для обнаружения и изъятия объектов информационных технологий, отсутствием достаточного количества методической литературы по возникающим проблемам. Трудности вызывают и риск случайной утраты информации в результате неквалифицированных действий участников следственного действия [7].

Таким образом, на данный момент расследование киберпреступлений представляется достаточно сложной задачей для правоохранительных органов России.

ЛИТЕРАТУРА

1. Нестерович С. А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов / С. А. Нестерович // Вестник науки и образования. – 2018. – № 8 (44). – Т. 2. – С. 46-50.

2. Официальный сайт Генеральной прокуратуры Российской Федерации. – URL: http: //www.genproc.gov.ru (дата обращения: 31.05.2021).

3. Уголовный кодекс Российской Федерации: федеральный закон Рос. Федерации от 13 июня 1996 года № 63-ФЗ (ред. от 05.04. 2021 г.) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

4. Никеров Д. М. Преступления в сфере высоких технологий в современной России / Д. М. Никеров, О. М. Хохлова // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2 (89). – С. 82-93.

5. Официальный сайт компании кибербезопасности «Интернет-розыск». – URL: https://интернет-розыск.рф (дата обращения: 02.06.2021).

6. Суходолов А. П. Проблемы противодействия преступности в сфере цифровой экономики / А. П. Суходолов, Л. А. Колпакова, Б. А. Спасенников // Всероссийский криминологический журнал. – 2017. – Т. 11. – № 2. – С. 258-267.

7. Гайдин А. И., Потанина И. В. Тактические особенности изъятия электронных носителей информации при производстве следственных действий / А. И. Гайдин, И. В. Потанина. – Воронеж: Воронежский институт МВД России, 2015. – 62 с.

PROBLEMS OF ORGANIZATION OF INVESTIGATION OF CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

© 2021 A. A. Dushkin, I. V. Potanina

Russian Presidential Academy of National Economy and Public Administration (Voronezh, Russia)

This article attempts to consider some features of the investigation of crimes committed using modern computer technologies. The methods of committing crimes of this category are analyzed, and the problems of their disclosure are considered.

Keywords: crimes, computer technologies, cybercrime, computer information, malicious computer programs.