УДК 343.98

КРИМИНАЛИСТИЧЕСКАЯ КЛАССИФИКАЦИЯ КИБЕРПРЕСТУПНОСТИ

студент магистратуры, группы Зсф18-г
Олейников Денис Юрьевич
Научный руководитель – кандидат юридических наук, доцент кафедры
«Криминалистики и судебных экспертиз»
Павлов Станислав Вячеславович
Донецкая академия внутренних дел

Киберпреступность в современном мире объявлена глобальной международной проблемой, о чём свидетельствуют принятые международные договорённости, предусматривающие совместные шаги по борьбе с этим высокотехнологичным злом. Опасность киберпреступности как для мирового сообщества в целом, так и для России признают и российские правоохранительные органы. Так, по данным Главного управления специальных технических мероприятий МВД России, киберпреступность (преступность в сфере высоких технологий) в настоящее время является одной из наиболее серьёзных угроз национальной безопасности Российской Федерации в информационной сфере. Масштабы киберпреступности возрастают пропорционально возрастающему числу пользователей Интернета. Наиболее часто совершаемыми правонарушениями этого рода, по данным БСТМ МВД России за 2013 – 2014 годы, отмечены: мошенничество (37 %), неправомерный доступ к компьютерной информации (19 %) и распространение детской порнографии (16 %). На нарушение авторских и смежных прав («компьютерное пиратство») и распространение вредоносных программ приходится 8 % от всех совершённых за указанный период киберпреступлений.

Раскрытие киберпреступлений остаётся достаточно сложной задачей для большинства сотрудников органов предварительного расследования, что обусловлено спецификой данного рода преступлений: трудностями с обобщением материалов следственной и судебной практики по каждому виду рассматриваемых правонарушений; отсутствием методических рекомендаций как по организации расследования преступных деяний, так и по тактике

производства следственных действий; недостаточной квалификацией следователей для работы со специфическими источниками доказательственной информации, оцифрованной в виде электронных сообщений, страниц, сайтов.

Киберпреступление – это действие, нарушающее закон, которое совершается с использованием информационно-коммуникационных технологий (ИКТ) и либо нацелено на сети, системы, данные, веб-сайты и/или технологии, либо способствует совершению преступления. Киберпреступление отличается от традиционного преступления тем, что оно «не признает физические или географические границы» и может совершаться с меньшими усилиями, большей легкостью и с большей скоростью, чем традиционное преступление.) Киберпреступления могут совершаться физическими лицами, группами лиц, коммерческими организациями и государствами. Хотя эти субъекты могут применять схожие тактические методы (например, использовать вредоносное программное обеспечение) и атаковать схожие цели (например, компьютерную систему), они имеют разные мотивы и намерения при совершении киберпреступлений.

Существует несколько технических причин, которые затрудняют борьбу с киберпреступностью.

Первая причина – атрибуция (для получения дополнительной информации. Любой компьютер, подключенный к Интернету, может взаимодействовать с любым другим компьютером, подключенным к Интернету. Обычно мы видим общедоступный IP-адрес компьютера, когда этот компьютер соединяется с нашим компьютером. IP-адрес – это, как правило, глобальный уникальный номер, который позволяет нам определить, из какой страны подключается этот компьютера, и к какому поставщику Интернет-услуг он подключен. Проблема состоит в том, что у злоумышленника есть много способов скрыть свой IP-адрес или даже притвориться, что он подключается с другого IP-адреса. Более того, преступники могут использовать различные инструменты, чтобы избежать

обнаружения правоохранительными органами, затруднить доступ и скрыть сайты.

Вторая техническая проблема связана с программным обеспечением. Компьютерные программы представляют собой программное обеспечение. Приложения на вашем телефоне или планшете являются программным обеспечением. Сервисы, к которым вы подключаетесь в Интернете, например, веб-сайт, также являются программным обеспечением. Очень часто программное обеспечение имеет уязвимости. Уязвимость может быть связана с проблемой в программе или неправильной конфигурацией, которая позволяет злоумышленникам делать то, что они не должны иметь возможность делать (например, загружать данные кредитной карточки клиента). Компаниям-разработчикам программного обеспечения бывает непросто обнаружить уязвимости, особенно те, которые связаны с крупными программными проектами, которые часто меняются. Иногда злоумышленники находят уязвимость раньше компании, производящей программное обеспечение. «пока уязвимость остается неизвестной, уязвимое программное обеспечение не может быть исправлено, а антивирусные программы не могут обнаружить атаку с помощью сканирования на основе сигнатур». Компании становится известно об уязвимости такого рода, когда она используется киберпреступниками для атаки на конфиденциальность, целостность или доступность программного обеспечения и пользователей программного обеспечения.

В глобальном плане наблюдается широкий диапазон киберпреступлений, которые включают преступления, совершаемые в целях получения финансовой выгоды, преступления, связанные с использованием информации, которая содержится в компьютере, а также преступления, направленные против конфиденциальности, целостности и доступности компьютер Будапештская Конвенция, как основополагающий документ в сфере борьбы с киберпреступностью, предоставляет следующую классификацию киберпреступлений:

1) правонарушения против конфиденциальности, целостности и доступности компьютерных данных и систем, в частности: незаконный доступ, например, путем взлома, обмана и другими средствами; нелегальный перехват компьютерных данных; вмешательства в данные, включая умышленно повреждение, уничтожение, ухудшение, изменение или сокрытие компьютерной информации без права на это; вмешательства в систему, включая умышленное создание серьезных помех функционированию компьютерной системы, например, путем распределенных атак на ключевую информационную инфраструктуру; злоупотребления устройствами, то есть изготовление, продажа, приобретение для использования, распространения устройств, компьютерных программ, компьютерных паролей или кодов доступа с целью осуществления киберпреступлений;

2) правонарушения, связанные с компьютерами, включая подделку и мошенничество, совершенные с использованием компьютеров;

3) правонарушения, связанные с содержанием информации, в частности, детская порнография, расизм и ксенофобия;

4) правонарушения, связанные с нарушением авторских и смежных прав, например, незаконное воспроизведение и использование компьютерных программ, аудио/видео и других видов цифровой продукции, а также баз данных и книг.

Наиболее распространенными являются следующие виды преступлений:

1) мошенничество в сети Интернет, в частности: создание «финансовых пирамид» в сети Интернет; мошенничество при продаже товаров (услуг) через Интернет или на Интернет-аукционах; деятельность по созданию программных средств с целью хищения финансовой, коммерческой или персональной информации (создание фиктивных WEB-сайтов, распространение компьютерных вирусов и троянских программ, перехват трафика и т.п.);

2) мошенничество в системах дистанционного банковского обслуживания (далее – ДБО), в частности: создание компьютерных вирусов и троянских программ для скрытого перехвата управления компьютером клиента с установленным программным обеспечением ДБО; открытие счетов, проведение несанкционированных операций и получения наличных средств в результате несанкционированных операций в системах ДБО; получение платежей от иностранных отправителей через международную систему SWIFT вследствие вмешательства в работу компьютеров и систем ДБО клиентов иностранных банковских учреждений.

3) подделка платежных карт и банкоматное мошенничество, в частности: использование утраченных/похищенных/поддельных платежных карт; похищение реквизитов платежных карт, в том числе с применением технических средств их «клонирования»;

Подводя итог всему вышесказанному можно сделать вывод, что киберпреступелния по своей сути относятся к преступлениям высокого интеллектуального уровня, следовательно, и борьба с ним должна осуществляться квалифицированными специалистами в сфере информационных технологий. Поэтому важной задачей является повышение уровня специальной криминалистической подготовки следователей, проводящих расследование данного рода преступлений. Необходимо учитывать особенности тактики производства следственных действий, направленных на получение виртуальной информации, поскольку виртуальные следы, зачастую не подлежат непосредственному восприятию человеком, и для обнаружения требуется специальное аппаратное обеспечение. Следовательно, работники органов предварительного расследования и привлекаемые специалисты должны иметь высокий уровень материально-технического оборудования для грамотного выявления и пресечения киберпреступлей. Также при производстве следственных действий необходим подбор понятых, обладающих навыками работы в компьютерной сфере. Можно сделать вывод о том, что при

расследовании киберпреступлений необходимо использовать специальные знания и привлекать соответствующих специалистов в области компьютерной криминалистики, информатики и других.

Список использованной литературы

Нормативные правовые акты

«Конвенция о преступности в сфере компьютерной информации» (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) [Электронный ресурс]. // URL: http://uristu.com/library/konventsii/konvenciy_773/ (дата обращения: 19.10.2016)

Литература

Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов. – М.: Юрлитинформ, 2012. – 182 с.

Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь, 2004. – № 7.

Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. 2007. № 2. С. 17 - 25.

Илюшин, Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: Дис. … канд. юрид. наук: 12.00.09 / Илюшин Денис Анатольевич. – Волгоград, 2008. – 233 с.

Ищенко Е.П. Новые информационные технологии обеспечения раскрытия и расследования преступлений [Электронный ресурс]. // URL: http://www.studfiles.ru/preview/2801191/page6/3 (дата обращения: 10.10.2016)

Косынкин А. А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования / А. А. Косынкин // Российский следователь. – 2012. – № 2