НЕКОТОРЫЕ СПОСОБЫ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

А.В. Ширяев, Вит.В. Поляков
Алтайский государственный университет, г. Барнаул

Быстрое развитие сети Интернет открыло новые возможности для преступной деятельности. Согласно исследованию компании «Juniper Research», при сохранении текущего уровня кибератак общие убытки мировой экономики от их осуществления составят к 2019 году 2,1 триллиона долларов [1]. Киберпреступность осваивает новые способы совершения преступлений, активно используя возможности сети Интернет [2]. Перед криминалистикой стоит сложная задача исследования непрерывно изменяющейся компьютерной преступности и выработке соответствующих методик расследования [3]. Анализ имеющейся судебно-следственной практики позволяет изучить основные способы совершения компьютерных преступлений, осуществляемые удаленным образом с помощью сети Интернет. Рассмотрим на конкретных примерах некоторые из этих способов.

1. Незаконные действия, направленные на неправомерный доступ к компьютерной информации [4], могут являться подготовкой к совершению других, более серьезных преступлений. К ним относится, например, создание «подставных» веб-сайтов для получения паролей у пользователей или применение программных методов, регистрирующих каждое нажатие клавиш на клавиатуре для получения паролей. Неправомерная деятельность в сфере компьютерных преступлений может включать в себя взлом защищенных паролями веб-сайтов, обход защитных паролей компьютерной системы, создание вирусных программ, создание «ботнетов» и т.д. Так, в 2014 г. гражданка О. в своей квартире, имея умысел, направленный на неправомерный доступ к охраняемой законом информации и изменение такой информации, с личного персонального компьютера при помощи провайдера ОАО «Ростелеком» осуществила доступ в генератор испытательных телевизионных сигналов (ГИТС). Продолжая свои действия, О. осуществила вход в не принадлежащий ей электронный почтовый ящик и умышленно сменила на нем пароль, тем самым заблокировав к нему доступ. Затем она удалила содержащуюся в нем компьютерную информацию. Кроме того, О. ознакомилась с сообщениями, содержащимися в электронном почтовом ящике, нарушив конституционное право потерпевшей И. на тайну почтовых

и иных сообщений. По данному факту правоохранительными органами г. Омска было возбуждено уголовное дело по признакам преступлений, предусмотренных статьями 138 и 272 УК РФ [5].

2) Незаконное получение данных, модификация компьютерной информации или компьютерных систем, которое представляет собой изменение, блокирование или удаление содержащихся в компьютере данных, в информационных системах, подключенных к сети Интернет, осуществлятся из любой точки мира. Система кибербезопасности включает в себя многообразные компоненты, в том числе повышение уровня цифровой грамотности населения, содействие в продвижении индивидуальных способов защиты личной информации, механизмы по противодействию и профилактике киберугроз [6]. Для совершения таких преступлений, как правило, используются программы для сканирования незащищенных портов и обхода средств его защиты, а также может применяться психологическое воздействие на пользователя (социальный инжиниринг). Нередко используются программные инструменты, установленные на компьютерах потерпевших, или вредоносные программы для передачи данных, также могут использоваться аппаратные устройства, например, «клавиатурные шпионы», которые устанавливаются при физическом доступе к компьютерной системе. Так, 16 ноября 2015 г. Сызранским городским судом Самарской области был вынесен приговор гражданину К.. Согласно приговору, К., имея в личном пользовании персональный компьютер, изучив предварительно специализированную литературу, самостоятельно освоив навыки работы с персональным компьютером, изучив возможности ЭВМ, правила и порядок установки программного обеспечения, в целях создания и использования вредоносных компьютерных программ, обладая достаточными знаниями в области пользования компьютерной техники и опытом работы в глобальной сети, создал собственное приложение, предназначенное для несанкционированных модификаций и копирования компьютерной информации. Это приложение обладало следующими функциями: перехват смс-сообщений пользователя операционной системы, сокрытие входящих сообщений от всех отправителей; блокировка информации в мобильных устройствах (смартфонах, планшетах), выражающаяся в сокрытии получения, отправления и удаления СМС - сообщений; истребование, то есть копирование данных с лицевого счета банковской карты (ее номер, срок действия, CVV-код) путем отображения сообщения о подтверждении платежных данных для

сервиса с последующей модификацией, выраженной в изменении первоначальных данных по движению денежных средств по счету, отправки смс-сообщений в скрытом от пользователя операционной системы режиме [7].

3. В отличие от несанкционированного доступа к компьютерной информации незаконный перехват данных осуществляется при их загрузке на веб-серверы, а также при передаче их на внешние средства хранения информации на базе «облачных» технологий и иных действий, связанных с перемещением информации в дистанционные хранилища. Такие способы являются сложными, так как в большинстве случаев передаваемые через провайдеров данные перехватить достаточно трудно. Более уязвимыми являются данные, переданные с помощью беспроводных технологий, которые обширно используют отели, кафе, рестораны. Беспроводные точки доступа передают сигнал электронному устройству, поддерживающему стандарты беспроводной передачи данных, в радиусе в среднем около 100 м.[2], соответствующее оборудование для перехвата данных, находится примерно в этих же пределах. Так, в 2015 г. Первомайским районным судом г. Омска был вынесен приговор гражданину, который с личного мобильного телефона, где были установлены специализированные программы, предназначенные для сканирования и перехвата данных через беспроводную сеть, проигнорировав предупреждение об уголовной ответственности, осуществил сканирование трафика и перехватил сессию пользователя социальной сети [8].

4. Незаконные действия, направленные на вывод из строя информационных ресурсов либо ограничение возможности доступа к ним, осуществляются в основном при помощи «компьютерных червей» (подгруппа вредоносного ПО) и DDoS-атак [6]. При этом «компьютерные черви» чаще всего заражают всю сеть, не нацеливаясь на конкретную компьютерную систему, в отличие от DDoS и APT-атак, которые дезорганизуют работу конкретного ресурса, направляя огромное количество запросов, с которыми крайне сложно справиться, вследствие чего происходит аварийное завершение работы. Атака APT превосходит обычные киберугрозы, так как она готовится на основе заранее собранной информации о цели, осуществляя взлом целевой инфраструктуры посредством эксплуатации программных уязвимостей. Перечисленные выше действия, согласно Конвенции Совета Европы о компьютерных преступлениях, возможно объединить в группу преступлений против

конфиденциальности, целостности и доступности компьютерных данных и систем [10].

5. Отдельно выделим незаконные действия, совершаемые в файлообменных сетях или виртуальном хостинге. Файлообменная система первого поколения представляет собой одноранговую компьютерную сеть для совместного использования файлов, каждый ее участник является и клиентом и сервером, для нее необходима инфраструктура, объединяющая разрозненных клиентов между собой в определенное сообщество. При этом файлообменные системы первого поколения типа «Napster» зависели от центрального сервера, что позволяло правоохранительным органам их блокировать. Файлообменные системы второго поколения частично децентрализованы, например, «eDonkey2000», «OpenNap», «Kazaa», имеющие независимые индексационные серверы, постоянно синхронизирующие информацию между собой, вместо центрального сервера, что позволяло отследить пользователя сети по IP-адресу и определить местоположение веб-узла. Последние версии файлообменных систем типа «FreeNet», «GNUnet» используют специальные приемы анонимизации, существенно затрудняющие расследование, так как сложно определить лицо, чей компьютер хранит необходимую информацию, так как содержимое каждого файла зашифровано и может быть разбито на части, которые распределяются между множеством различных компьютеров.

Следует отметить, что общественно-опасные и противоправные посягательства, имеющие своим предметом не компьютерную информацию, а электронно-вычислительную технику, объединяются в совершенно другую группу преступлений, нарушающую охраняемые законом отношения собственности [11].

Таким образом, способы совершения компьютерных преступлений, основанные на новых сервисах сети Интернет, меняют облик современной киберпреступности [12].. Эффективное расследование и предупреждение таких преступлений требует совместных действий государства, институтов гражданского общества, органов местного самоуправления, образовательных и научных учреждений, средств массовой информации.

Публикация подготовлена в рамках поддержанного РФФИ научного проекта 16-33-01160-ОГН.

Библиографический список

1. Общемировые убытки от киберпреступности // securitylab.ru: информационный сайт 14.05.2015. URL: https://

http://www.securitylab.ru/news/472924.php. (дата обращения 21.11.2018).
2. Поляков, В.В. О высокотехнологичных способах совершения преступлений в сфере компьютерной информации : матер. ежег. Всеросс. науч.-практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета «Уголовно-процессуальные и криминалистические чтения на Алтае». – Барнаул : Изд-во Алт. ун-та, 2012. – Вып. 11-12. – С.123 - 126.
3. Ширяев, А.В. Поводы, основания и особенности возбуждения уголовных дел по компьютерным преступлениям / А.В. Ширяев // Проблемы правовой и технической защиты информации. Выпуск IV: сб. науч. статей. – Барнаул : Изд- во Алт. ун-та, 2016. – С. 296.
4. Поляков, В.В. Типичные способы совершения преступлений, связанных с неправомерным доступом к компьютерной информации / В.В. Поляков // Сборник материалов криминалистических чтений 2005-2006 гг. / под ред. Ю.Л. Бойко. – Барнаул : Изд-во БЮИ МВД России, 2006. – С. 96 - 97.
5. Архив Октябрьского районного суда г. Омска. Уголовное дело № 3245/14.
6. Поляков, В.В. Классификация способов совершения преступлений в сфере компьютерной информации / В.В. Поляков, Е.Г. Смирнов // V Пленум СибРОУМО (Сибирского регионального отделения учебно-методического объединения) вузов России по образованию в области информационной безопасности. XIII Всерос. конф. «Проблемы информационной безопасности государства, общества и личности»: 5-9 июня 2012г. : Томск-Новосибирск. – Томск : Изд-во «В-Спектр», 2012. – С. 108 - 109.
7. Архив Сызранского городского суда Самарской области. Уголовное дело № 579/15.
8. Архив Первомайского районного суда г. Омска. Уголовное дело №454/15.
9. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. № 8, 2014 г., С. 46–50.
10. Конвенция Совета Европы о компьютерных преступлениях от 23.11.2001 года – www.polis.osce.org/library (дата обращения 21.03.2016 г.)
11. Ширяев, А.В. Объект и предмет неправомерного доступа к компьютерной информации / А.В. Ширяев // Информационное противодействие экстремизму и терроризму. Сборник трудов II

всероссийской научно-практической конференции: Изд-во Краснодарского университета МВД РФ, 2015. – С.108-109.
12. Пархоменко С.В. Предупреждение компьютерной преступности в Российской федерации: интегративный и комплексный подходы / С.В. Пархоменко, К.Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. № 2, 2015 г., С. 265 – 276.