Могилевский институт МВД

УДК 343

***М. В. Рудик***

*старший преподаватель кафедры уголовного права*
*и криминологии Крымского филиала*
*Краснодарского университета внутренних дел МВД России,*
*кандидат юридических наук, доцент*

***Р. С. Федорский***

*курсант 3 курса Крымского филиала*
*Краснодарского университета внутренних дел МВД России*

# ОТКАЗ В ОБСЛУЖИВАНИИ КОМПЬЮТЕРНЫХ СИСТЕМ КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 272 УК РФ

DoS (от англ. *Denial of Service* — отказ в обслуживании) — хакерская атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен [1].

Однако большинство специалистов в области обеспечения компьютерной безопасности сходятся во мнении о том, что Ddos-атака — это лишь начало, первый шаг на пути к неправомерному доступу и попросту к овладению системой. Поэтому обозначенная киберугроза несет в себе повышенную опасность для неограниченного количества пользователей информационных ресурсов [2, с. 330].

Кто же может стать наиболее вероятной жертвой таких атак? По мнению специалистов, чаще всего страдают от этого коммерческие и информационные сайты. Но для чего злоумышленники направляют Ddos-атаки на указанные ресурсы? Ответ на этот вопрос кроется в экономическом факторе, а точнее в возможности незаконного обогащения или, проще сказать, вымогательстве, при этом денежные средства выступают своеобразным способом прекращения атаки и блокирования системы.

Известны примеры хорошо спланированных Ddos-атак на такие известные информационные сервисы, как Amazon, Yahoo, CNN, eBay, E-Trade и другие [3].

Как же такие действия становятся возможными? Алгоритм запуска Ddos-атак состоит в следущем: на слабозащищенные компьютеры интересующей компании или сети устанавливаются хорошо скрытые троянские программы. При этом данные вредные программы долгое время вообще могут никак себя не проявлять на зараженном компьютере, ожидая команды от своего хозяина. Компьютер может подвергнуться такой атаке при посещении различных зараженных сайтов, при получении почты или при установке нелицензионного программного обеспечения. И только после соответствующей команды, которая исходит от преступника, данная программа начинает свое деструктивное действие и все ранее зараженные компьютеры начинают одновременно слать запросы на сайт-жертву, что приводит к блокированию канала доступа к интернет ресурсам данной компании или целого региона.

Противодействие таким преступным действиям может заключаться в фильтрации и блэкхолинге интернет-ресурсов, в устранении уязвимостей сервера, наращивании ресурсов, рассредоточении (построении распределенных и продублированных систем, которые продолжат обслуживать пользователей, маскировке IP-адреса) [3]. С юридической стороны противодействие данному общественно опасному действию можно обеспечить при помощи ст. 272 УК РФ. Однако судебная практика не содержит большого количества судебных решений по причине неслаженности в работе закона и отдельных технических аспектов рассматриваемого явления. В то же время существуют многочисленные примеры Ddos-атак на различные организации и ведомства.

Так, информационное агентство «Интерфакс» сообщает, что официальный сайт Росгвардии стал жертвой хакеров. Сбои в работе ресурса начались 25 января 2017 г. около 17:00. Сотрудники Главного управления связи Росгвардии обнаружили, что причиной сбоев является массированная DDos-атака [2], вследствие того что большое количество сетевых запросов перегрузило сервер и парализовало работу сайта. 26 января в 02:00 сотрудникам управления связи удалось отследить и заблокировать 450 IP-адресов, с которых поступали запросы. Однако впоследствии число адресов увеличи-

лось сначала до 7,8 тыс., а потом достигло 160 тыс. В настоящий момент все адреса удалось отследить, их блокировка продолжается, работа сайта восстановлена.

В сентябре 2016 г. компания IDC обнародовала отчет о первом в России исследовании рынка услуг по защите от DDoS-атак. Объем этого рынка в 2015 г. составил $16,34 млн, продемонстрировав рост по сравнению с 2014 г. на 25,4 % в долларах и на 34,7 % в рублях. По данным IDC, во II квартале 2016 г. Россия заняла шестое место в мире как объект атак этого типа — в ней было зарегистрировано 0,6 % всех случаев на планете. По количеству командных серверов, с которых производятся DDoS-атаки, Россия заняла четвертое место — на ее территории находится 4,5 % таких серверов [2].

Подытожив вышесказанное, можно сделать вывод о том, что для улучшения взаимодействия технической стороны вопроса и буквы закона предлагаем создать на базе правоохранительных органов мощной системы аналитических подразделений по противодействию киберугрозам и обеспечения безопасности информации. Данные подразделения будут призваны не просто выявлять такие угрозы, но и проводить постоянный мониторинг Интернет-пространства с целью предупреждения возможных Ddos-атак.

**Список основных источников**

1. Википедия — свободная энциклопедия [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0. — Дата доступа: 02.08.2017.

2. Росгвардию атаковали хакеры со 160 тыс. IP-адресов [Электронный ресурс] / CNews. — Режим доступа: http://safe.cnews.ru/news/top/2017-01-26_rosgvardiya_stala_zhertvoj_masshtabnoj_ddosataki. — Дата доступа: 12.09.2017.

3. Что такое DDoS-атака и с какой целью их осуществляют? [Электронный ресурс]. — Режим доступа: http://www.aif.ru/dontknows/eternal/1149114. — Дата доступа: 02.08.2017.