УДК 343

DOS-АТАКИ В СВЕТЕ СОВРЕМЕННОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ

А. М. Кузенная, Д. А. Комаров

В данной работе проведено исследование современного правового регулирования DoS-атак в Уголовном Кодексе Российской Федерации и британском Законе о судопроизводстве и полиции 2006 года. Рассмотрены статьи, которые могут быть применимы к таким преступлениям, исследована их применимость к реальным условиям. Приведены примеры недавних DoS-атак, показан ущерб, нанесённый пострадавшим сторонам. Проведено сравнение с зарубежным законодательством, найдены соответствия и различия в настоящих Законах. Обосновано утверждение о применимости законов в Российской Федерации и других странах. Сделан вывод о необходимости внесения поправок в существующие правовые документы, что позволит конкретизировать определения и повысить качество судопроизводства и следствия.

Ключевые слова: Уголовный Кодекс РФ, информационно-телекоммуникационные сети, компьютерная преступность, киберпреступления, неправомерный доступ к компьютерной информации.

Характерной чертой современного мира является стремительное развитие электронно-вычислительной техники. Повсеместное использование компьютерных вычислений порождает собой множество правовых проблем, таких как: компьютерное хулиганство (то есть несанкционированное проникновение с помощью персональных компьютеров в чужие информационные сети; нарушение функционирования компьютерных систем посредством выведения из строя программного обеспечения и другое); борьба с так называемой компьютерной преступностью, включающей хищение информации, в том числе конфиденциального или секретного характера, а также хищение денежных сумм, хранящихся в банках, путём изменения программы ЭВМ, мошенничества или подлога.

Всеобщая информатизация различных банковских услуг порождает серьёзную проблему безопасности. Часто при разработке программного обеспечения банковских систем невозможно предусмотреть защиту от мошенничества, так как пользователи самостоятельно предоставляют преступникам (мошенникам) доступ к данным.

Рассмотрим несколько нарушений закона в компьютерной сфере.

1. **Мошенничество** путём обмана и злоупотребления доверием пользователя. Этот способ распространён среди пользователей банковских приложений. Мошенник получает пароль или код для входа в систему или для подтверждения перевода от самого пользователя, представляясь сотрудником банка или любым другим способом обмана. При этом данная ситуация подпадает под статью 159 УК РФ (мошенничество) и наказывается лишением свободы до 10 лет и (или) штрафом до 1 миллиона рублей.

2. **Снятие денег** с предварительно похищенной банковской карты. В такой ситуации при потере или краже платёжной карты и отсутствии её блокировки в течение некоторого времени возможно снятие или перевод денежных средств. Действует статья 159.3 УК РФ (мошенничество с использованием платёжных карт), наказывается лишением свободы до 10 лет и (или) штрафом до 1 миллиона рублей.

3. **Подмена страницы сайта** для изъятия учётных данных пользователя. Мошенник размещает на домене со схожим названием сайт идентичного дизайна, при этом в случае ввода учётных данных они фиксиру-

Кузенная Анастасия Михайловна,
(4ervya4-ok@mail.ru),
студент IV курса факультета информатики;
Комаров Дмитрий Александрович,
(ehpgms@gmail.com),
студент IV курса факультета информатики
Самарского университета,
443086, Россия, г. Самара, Московское шоссе, 34.

ются, а затем используются заинтересованными лицами в незаконных целях. Статьи 159.6 (мошенничество в сфере компьютерной информации), 273 (создание, использование и распространение вредоносных компьютерных программ) УК РФ.

4. **Атака на банковский сервер**. При таком развитии событий преступник может неправомерно завладеть информацией о чужих лицевых счетах, модифицировать их в свою пользу, при этом страдает не только конечный пользователь, то есть клиент банка, но и сам банк. Обычно банковские сервера обладают довольно высоким уровнем защиты, однако они защищены лишь от взлома и копирования информации с них и практически беззащитны перед DoS-атаками (англ. Denial of Service). В случае если происходит кража информации у банка, рассматривается статья 272 УК РФ (неправомерный доступ к компьютерной информации).

5. **DoS-атака** – это хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён [1]. **DDoS-атаки** (англ. Distributed Denial of Service) отличаются своей распределённостью как по месту, так и по кругу лиц, совершающих такую атаку. В данный момент DDoS- и DoS-атаки в зависимости от их мотива относят к статьям 272–274 УК РФ, что, на наш взгляд, не совсем соответствует действительности. Рассмотрим эти статьи подробнее.

Статья 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации <...> [2].

При DDoS- или DoS-атаке обычно не совершается неправомерного доступа к информации, а сама информация не представляет никакого интереса для злоумышленника. Поэтому эта статья кажется не совсем подходящей для такого преступления.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации <...> [2].

Эта статья может применяться только в случае, если хакер, осуществлявший попытку атаки, преследовал при этом цель «уничтожения, блокирования, модификации, копирования» *информации*, и при этом использовал программы или информацию для той же цели, а не для выведения из строя конкретного оборудования потерпевшей стороны.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб <...> [2].

Эта статья применима только к *нарушениям правил эксплуатации и правил доступа,* а DDoS-атаки отнести к ним можно с большой натяжкой, так как они лишь превышают ограничение использования имеющихся ресурсов сети. При этом такое ограничение нельзя назвать правилом, скорее, оно является технической характеристикой сети. Более того, правовая система не имеет определения правил эксплуатации, и, исходя из этого, не совсем понятно, что именно следует использовать в их качестве.

Стоит рассмотреть также статью 213 (хулиганство).

Хулиганство, то есть грубое нарушение общественного порядка, выражающее явное неуважение к обществу, совершённое:

а) с применением оружия или предметов, используемых в качестве оружия;

б) по мотивам политической, идеологической, расовой, национальной или рели-

гиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы <...> [2].

Можно было бы описать DoS-атаку этой статьей, если бы не расшифровка термина «хулиганство». Из неё видно, что такая атака не подпадает ни под один пункт настоящей статьи и не может расцениваться как хулиганство.

Таким образом, как же расценивать DDoS- и DoS-атаки? Законодательство не предусматривает их, а между тем, они стали очень популярны. Так, например, совсем недавно, 21 октября 2016 года, в США произошла массивная DDoS-атака на сервера Twitter, Sound Cloud, Spotify, Shopify, а также Ebay и Netflix, Vox, Airbnb [3]. Кибератаки нанесли огромный ущерб российской экономике, который оценивается суммой более 200 млрд. руб. только за 2016 год [4]. Тем не менее, многие считают атаки законным способом граждан проводить «виртуальные митинги» и согласны с узакониванием таких актов выражения своего мнения. Так, известная группа хакеров Anonymous в начале 2013 года собирала подписи на сайте белого дома с целью признать DDoS-атаки защищённой формой выражения свободы слова [5]. Кеес Верховен считает, что такая легализация возможна, если обязать протестующих согласовывать время и сроки проведения онлайн-акции протеста заранее, как это делается в случае традиционных протестных действий [6]. Таким образом, преследуется цель отделить «мирные» атаки протеста от атак в связи с личной неприязнью, конкуренцией, развлечением или вымогательством и шантажом.

Наказание зачинщиков DDoS-атак усложняется в связи с распространённым характером последних, который достигается путём использования ботнетов. *Ботнет* (англ. botnet) – компьютерная сеть, состоящая из некоторого количества узлов, с запущенным автономным программным обеспечением (ботов). Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера [7]. Использование ботнетов усложняет поиск компьютеров, с которых проводилась атака, и процесс доказывания факта совершения преступления.

Зарубежное законодательство имеет более развитые перспективы для достижения законного регулирования DDoS-атак и других киберпреступлений в сравнении с российским. Так, британский Закон о судопроизводстве и полиции 2006 года [8] предусматривает до 10 лет лишения свободы за действия, повлёкшие за собой нарушение работы сети, совершённые с преступным умыслом или вследствие небрежности. Интересно, что даже сам факт использования программного обеспечения, предназначенного для совершения кибератак, в рамках Закона является преступлением. В 36-й статье этого закона учитывается распределённость атак и их временный эффект. Законодатель даёт определение DoS-атаке как однократному или многократному действию, совершённому лицом или группой лиц с целью ограничения доступа к некоторой информации или программам, хранимых на одном или нескольких компьютерах. Статья достаточно полно отражает суть атак, что позволяет с долей успеха применять Закон в судебной практике.

Таким образом, анализ российских нормативных документов в сфере киберпреступлений показал, что оценить существующим законодательством кибератаку не представляется возможным, что показывает необходимость внесения поправок в главу 28 УК РФ «Преступления в сфере компьютерной информации», касающихся DoS-атак. Вместе с правками в законодательстве необходимо внести изменения в процесс следствия таких дел, а также повысить уровень компетенции сотрудников правоохранительных органов. Вместе с тем, и в зарубежном законодательстве до сих пор нет чёткого мнения насчёт такого типа атак, что говорит о том, что судебные системы всего мира оказались не готовы к резкому развитию киберпреступности.

Литература

1. DoS-атаки // Википедия – свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/DoS-атака (дата обращения: 10.10.2016).

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 06.07.2016) [Электронный ресурс]. Доступ из справочно-правовой системы «КонсультантПлюс».

3. Many sites including twitter and Spotify suffering outage. URL: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/ (дата обращения: 10.10.2016).

4. Подсчитан ущерб российской экономики от киберпреступлений. URL: http://www.rbc.ru/technology_and_media/13/04/2016/570e1d9c9a794753f73b8fde (дата обращения: 10.10.2016).

5. DDoS-атаки признают мирными. URL: https://habrahabr.ru/post/165605/ (дата обращения: 10.10.2016).

6. Anonymous wants ddos attacks to be protected under free speech. URL: http://www.theverge.com/2013/1/9/3856202/anonymous-wants-ddos-attacks-to-be-protected-under-free-speech (дата обращения: 10.10.2016).

7. Ботнет // Википедия – свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Ботнет (дата обращения: 10.10.2016).

8. Police and Justice Act 2006. URL: http://www.legislation.gov.uk/ukpga/2006/48 (дата обращения: 10.10.2016).

THE DOS-ATTACKS IN MODERN LEGAL REGULATION

A. M. Kuzennaya, D. A. Komarov

In this article there are a study of modern legal regulation of DoS-attacks in the Criminal Code of the Russian Federation and the British Police and Justice Act 2006. Many articles, which may be applicable to such crimes, was considered, and their applicability to real conditions was investigated. Examples of recent DoS-attacks are showing the damage caused by the affected parties. A comparison with foreign legislation was conducted, similarities and differences in this laws was found. Statement about the applicability of the laws of the Russian Federation and other countries was justified. The conclusion about the need to amend the existing legal instruments, which will specify the definitions and improve the quality of legal proceedings and investigations was made.

Key words: Criminal Code, Police and Justice Act, Anonymous, cybercrimes, unauthorized access.

Статья поступила в редакцию 04.11.2016 г.

Kuzennaya Anastasia Michailovna,
(4ervya4-ok@mail.ru),
student IV course of the faculty of Informatics;
Komarov Dmitriy Alexandrovich,
(ehpgms@gmail.com),
student IV course of the faculty of Informatics
of the Samara University,
443086, Russia, Samara, Moskovskoye shosse, 34.