Влияние DDoS-атак на финансово-экономические результаты деятельности компаний

Influence of DDoS-Attacks on Companies' Performance

DOI 10.12737/article_59393ce8a306c5.84631716 Получено: 21 марта 2017 г. / Одобрено: 10 мая 2017 г. / Опубликовано: 16 июня 2017 г.

Дацко Т.Г.
Студентка 1 курса магистратуры
факультета математической экономики,
статистики и информатики
Российского экономического университета
имени Г.В. Плеханова
Россия, 117997, г. Москва, Стремянный пер., д. 36
e-mail: tanya-datsko@mail.ru

Алёшина И.Ф.
Канд. экон. наук, доцент
кафедры математических методов в экономике
Российского экономического университета
имени Г.В. Плеханова
Россия, 117997, г. Москва, Стремянный пер., д. 36
e-mail: ifaleshina@mail.ru

Datsko T.G.
1st-year Master Degree Student,
Faculty of Mathematical Economics,
Statistics and Informatics,
Russian Plekhanov University of Economics
36 Stremyanniy Pereulok, Moscow, 117997, Russia
e-mail: tanya-datsko@mail.ru

Aleshina I.F.
Candidate of Economic Sciences, Associate Professor,
Mathematical Methods in Economy Department,
Plekhanov Russian University of Economics
36 Stremyanniy Pereulok, Moscow, 117997, Russia
e-mail: ifaleshina@mail.ru

Аннотация

Данная статья посвящена рассмотрению актуальных вопросов обеспечения информационной безопасности в бизнес-среде. Раскрыта сущность понятия «информационные риски» и представлена характеристика отдельных составляющих экономического ущерба от реализации кибератак на бизнес. Особое внимание сконцентрировано на анализе динамики DDoS-атак как одной из мощнейших информационных атак, связанных со значительными убытками для компаний. Представленные аналитические выводы позволили выявить основные инструменты и каналы воздействия, используемые злоумышленниками (факторы риска), а также дать экономическую оценку уязвимостям компонентов информационной инфраструктуры организаций (последствия риска). В заключение отмечены приоритетные направления обеспечения информационной безопасности компаний ввиду угроз DDoS-атак. Основной акцент сделан на необходимости интенсификации превентивных мер, и, прежде всего, установке специализированных пакетов защиты и реализации эффективной политики в отношении конфиденциальной информации.

Ключевые слова: DDoS-атака, информационные риски, информационная безопасность, киберпреступления.

Abstract

The article is devoted to topical issues of information security in the business environment. The essence of the concept of «information risks» has been presented as well as the main characteristics of the individual components of the economic cost of cyber-attacks have been considered. Particular attention has been focused on the analysis of DDoS-attacks as one of the most powerful information attacks, involving large losses for companies. Presented analytical findings have helped to identify the main tools and channels of influence used by attackers (risk factors), and also give an economic assessment of the vulnerabilities of the information infrastructure of the organizations (risk consequences). In conclusion, the priority directions of ensuring information security of the companies due to threats of DDoS-attacks have been noted. The main emphasis is on the need to intensify preventive measures, and, above all, the installation of specialized security packages and the implementation of the effective policy in relation to the confidential information.

Keywords: DDoS-attack, information risks, information security, cybercrime.

Повсеместное внедрение новейших информационных технологий во внутреннюю инфраструктуру организаций различных сфер деятельности давно перестало быть формальной целевой установкой развития и стало объективной реальностью. Подобные нововведения открыли широкие возможности для расширения коммуникационных взаимосвязей на всех управленческих уровнях — локальные сети департаментов объединяются в офисные многоярусные структуры, подключаются к глобальной сети Internet, в результате разрастаются до уровня распределенных корпоративных сетей.

Внедрение популярных сегодня автоматизированных систем управленческого учета и планирования — это, безусловно, прогрессивные процессы. Однако зачастую неизбежным следствием такого прогресса выступает неструктурированный гетерогенный характер организации информационной инфраструктуры. В свою очередь, это приводит к неконтролируемому росту уязвимостей системы, а также облегчению доступа к управленческой, коммерческой и производственной информации со стороны злоумышленников. Перечисленные уязвимости могут быть объединены емким понятием «информационные риски», под которыми понимают опасность возникновения ущерба или убытка в результате использования компанией в своей повседневной деятельности различных информационных технологий. Прежде всего, информационные риски связаны с созданием, передачей, хранением и использованием значимой для компании информации при помощи электронных носителей и иных средств связи.

В настоящее время, когда геополитическое и социально-экономическое напряжение на мировой арене

нарастает, информационная война развернулась и идет полным ходом на просторах сети Internet, и одним из основных, широко используемых «оружий» в этой войне выступают хорошо известные DDoS-атаки.

Цель данной статьи заключается в том, чтобы на основе анализа статистики реализации DDoS-атак в различных сегментах бизнес-среды и финансовой оценки основных компонентов ущерба от подобного рискового инцидента обосновать необходимость инвестирования в эффективную систему защиты информационного пространства компании.

DDoS-атака (от англ. *Distributed Denial of Service* — распределенная атака типа «отказ в обслуживании»), — один из самых распространенных и излюбленных сервисов киберпреступников. Атаки, запускаемые с его помощью, беспрецедентны по масштабам и технологической сложности. Задача подобной кибератаки заключается в том, чтобы довести атакуемую информационную систему (как правило, сайт, сервер или хост, подключенный к сети Internet) до такого состояния, при котором легитимные пользователи не могут получить доступ к ней [1, с. 123]. Инициаторами DDoS-атак выступают различные субъекты, которые преследуют личные своеобразные цели, — некоторые таким образом противостоят правительственному режиму, другие препятствуют развитию конкурирующих фирм или мотивированы идеологическими разногласиями с новостными порталами и общественными организациями.

Упрощенно описать процесс реализации DDoS-атаки можно следующим образом: киберпреступники направляют множество бессмысленных запросов в таком объеме, что атакуемый сервер занят исключительно только обработкой этих запросов. Таким образом, времени на обработку запросов легитимных, т.е. реальных, посетителей не остается, а зачастую сервер, переполненный искусственно созданными заявками, вовсе перестает функционировать. В этот период киберпреступники реализуют свои незаконные замыслы. Уже беспрепятственно внедряясь во внутреннюю информационную систему атакуемой компании, они изменяют, искажают и крадут важнейшие конфиденциальные данные. В настоящее время один из самых популярных сценариев DDoS — это атака с помощью ботнетов — сети вирусных программ, активизирующихся по сигналу киберпреступников и наносящих нацеленные атаки на критический узел информационной системы компании-жертвы.

Доступность и простота использования инструментов для проведения DDoS-атак приводит к ускоренному расширению диапазона атакуемых целей. Общепринято утверждение, что DDoS-атакам подвергаются преимущественно государственные учреждения, финансовые организации, коммерческие компании наиболее конкурентных сфер деятельности и средства массовой информации [2, с. 501]. Однако практика показала, что мишенью DDoS-атаки может стать любой информационный ресурс, вызвавший недовольство отдельных пользователей, — даже образовательный портал.

В качестве информационной базы для анализа тенденций развития и структурных изменений DDoS-атак нами были использованы данные, опубликованные в официальных статистических исследованиях Лаборатории Касперского [3] — компании, которая предоставляет широкий спектр услуг по защите от киберугроз и является ключевым игроком на этом рынке. Будем считать, что полученные результаты анализа являются обоснованным индикатором сложившейся в настоящий момент ситуации в сфере DDoS-атак и могут быть распространены на всю совокупность объектов, когда-либо подвергшихся подобной киберугрозе.

Статистика количества DDoS-атак демонстрирует устоявшийся тренд. На диаграмме (см. рис. 1) представлена подневная динамика с IV квартала 2015 г. по III квартал 2016 г. За рассматриваемый период количество атак в отдельные дни превышало 1750, особенно заметно такие пиковые периоды стали проявляться во втором полугодии 2016 г.

В глобальном масштабе оценить объем киберпреступности в этой сфере позволяет статистика специализированного сервиса KasperskyDDoSIntelligence. Так, в 2016 г. было зафиксировано свыше 120 тыс. атак на 68 тыс. информационных ресурсов, расположенных в 96 странах мира. При этом более половины атак пришлось на долю компаний, имеющих хостинги своих серверов и сайтов в Китае и США — 41,1 и 16,9% соответственно. Россия в географическом разрезе по количеству DDoS-атак на ресурсы, расположенные на ее территории, занимает пятую строчку с показателем 3,6%.

Мощность угрозы (фактор риска) при реализации DDoS-атаки зависит от множества ее характеристик. Поясним данное утверждение, основываясь на анализе статистических данных об общей динамике количества DDoS-атак и их распределении по уровням, продолжительности и используемых типов ботнетов.

К настоящему времени киберпреступники, организующие DDoS-атаки, значительно расширили арсенал используемых сервисов. Они не ограничиваются ставшими классическими ботнетами, состоящими из персональных компьютеров и рабочих

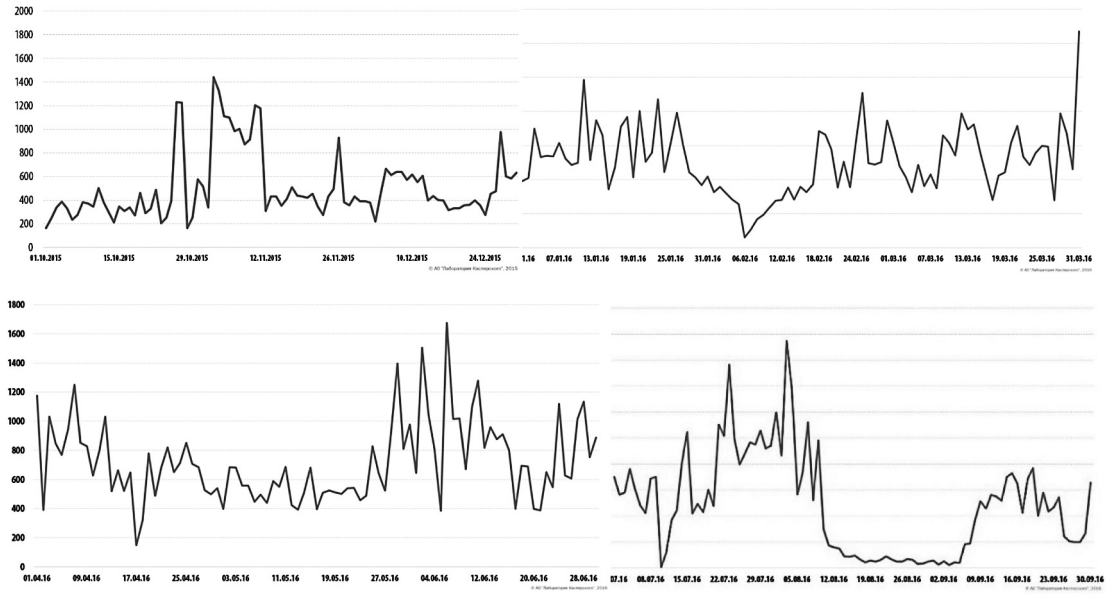

Рис. 1. Динамика количества DDoS-атак [3]

станций, а используют все доступные уязвимые информационные ресурсы, в том числе web-приложения, серверы, IoT-устройства (Internet of things).

Как правило, выделяют два уровня DDoS-атак — атаки на уровне приложений и атаки сетевого уровня. Разделение на указанные группы осуществляется в соответствии со способом осуществления атаки, учитывающего отдельные слабости серверного программного обеспечения и операционных систем. Ниже представлена динамика изменения количества атак для обоих уровней.

В рассматриваемый период преобладающая доля атак осуществлялась на уровне приложений — порядка 60%. В то же время более заметно увеличение доли атак сетевого уровня — за прошедшие два года рост составил 5,2 п.п. — с 36,7% до 41,9%. Если сформировавшийся тренд будет продолжаться, то к 2018 г. атаки сетевого уровня, представляющие значительно большую угрозу информационным ресурсам организаций, станут настолько же распространены, как и атаки уровня приложений.

Основной метрикой DDoS-атаки является ее мощность, которая, как правило, определяется в гигабитах в секунду или количестве запросов в секунду (Gbps и RPS). За последние несколько лет было предотвращено множество атак мощностью более 200 Gpbs. На графике (см. рис. 3) представлены наиболее мощные DDoS-атаки, осуществленные на сетевом уровне и уровне приложения.

Новая особенность, которая начинает укрепляться в большинстве реализуемых DDoS-атак, заключается в использовании небольших сетевых пакетов, о которых речь пойдет ниже, в сочетании с высокой пропускной способностью. Полагаясь на высокую скорость отправки пакетов, киберпреступники используют недоработки существующих устройств подавления атак, не способных справиться с такими высокими нагрузками. Справедливо предположение, что количество таких атак будет возрастать в дальнейшем.

Среди наиболее важных характеристик DDoS-атаки следует также выделить ее продолжительность и сценарий реализации, так как именно от них зависит величина ущерба для защищающейся стороны.

В распределении атак по длительности с большим отрывом традиционно лидируют непродолжительные атаки менее суток. Тем не менее, как свидетельствует статистика, даже кратковременная разовая атака спо-

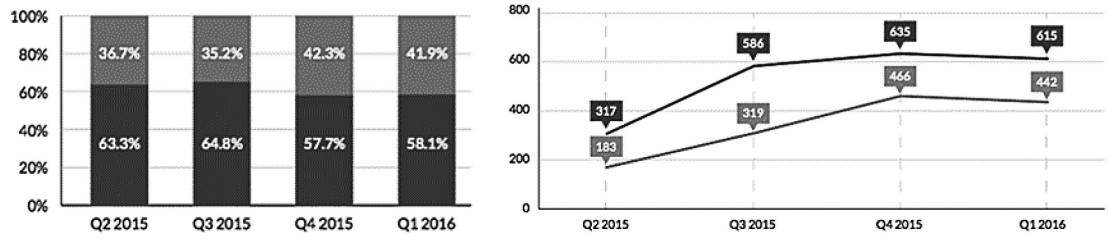

Рис. 2. Распределение DDoS-атак по уровням (уровень приложений — черный цвет, сетевой уровень — серый цвет) [3]

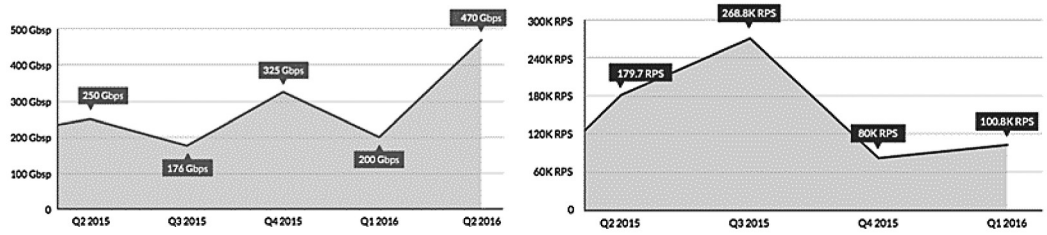

Рис. 3. Динамика мощности реализуемых DDoS-атак
(уровень приложений — черный цвет, сетевой уровень — серый цвет) [3]

собна существенно нарушить нормальную работоспособность незащищенного информационного ресурса.

Киберпреступники остаются весьма настойчивыми. Так, в отдельные периоды встречались единичные случаи DDoS-атак длительностью свыше двух недель. Например, самая продолжительная атака, зафиксированная во втором квартале 2016 г., составила 291 час или более 12 дней, а самый атакуемый ресурс выдержал 33 атаки.

Ярким недавним примером массированных DDoS-атак является волна атак на несколько крупнейших российских банков, которая была зафиксирована в период с 8 по 14 ноября 2016 г. [4]. Киберпреступники атаковали веб-ресурсы пяти известных финансовых организаций, в том числе ПАО Сбербанк, ПАО РОСБАНК, АО Альфа-банк, ПАО Банк ВТБ (Банк Москвы), Московская биржа и др. Особенностью этой серии DDoS-атак стало комбинирование методов ее совершения. Злоумышленники использовали многовекторные атаки двух типов — SYN-flood, ориентированные на истощение ресурсов операционной системы компании, и HTTP-flood, перегружающие атакуемый веб-сервер.

Самая продолжительная атака этой кампании длилась 102 часа (более четырех дней), а пиковая мощность атаки составила 660 тыс. запросов в секунду. Следует пояснить, что средняя нагрузка на веб-сайт крупной финансовой организации в рабочее время крайне редко превышает одну тысячу запросов в секунду.

Последующий анализ трафика данной серии DDoS-атак показал, что в ней принимали участие порядка 24 тыс. уникальных ботнетов (атакующих зараженных устройств), расположенных в 30 различных странах.

Что касается последствий произошедшего инцидента, то здесь следует отметить следующее. Российские банки сталкиваются с DDoS-атаками регулярно, предыдущая масштабная серия атак была зафиксирована в октябре 2015 г., а всего с октября 2015 г. по март 2016 г. Банк России диагностировал 21 кибератаку на платежные системы и иные информационные ресурсы российских финансовых организаций. Подобные инциденты привели к возникновению серьезных трудностей у клиентов при совершении операций в системах онлайн-банкинга, являющихся одним из основных каналов получения доходов для банка. Помимо прочего, снижение доступности услуг банка негативно сказалось на репутационной составляющей его деятельности.

Общие тенденции изменения продолжительности DDoS-атак можно свести к следующему утверждению: на фоне постепенного повышения длительности DDoS-атак общая структура распределения по времени остается неизменной при подавляющем преобладании многократных непродолжительных

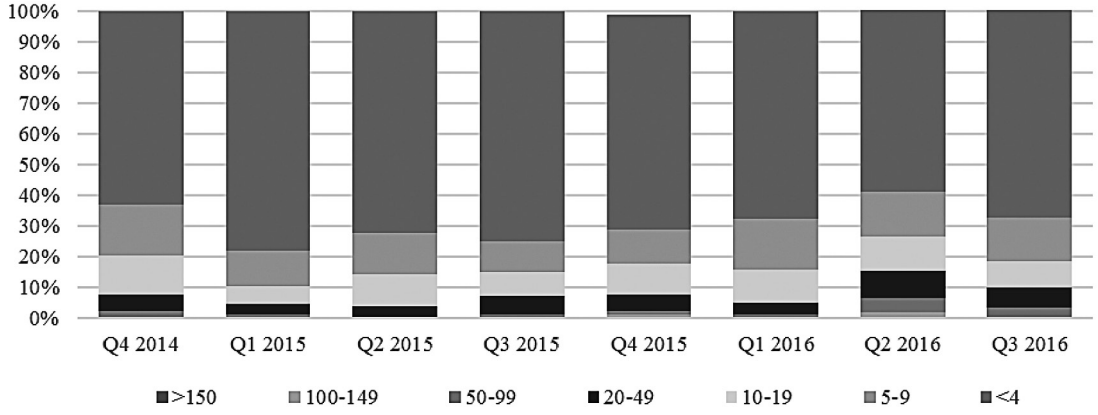

Рис. 3. Распределение DDoS-атак по продолжительности [3]

атак. Так, доля кратковременных атак, продолжительностью менее 4 часов, за три года увеличилась на 5,7 п.п., достигнув 69% по итогам 2016 г. DDoS-атаки, продолжающиеся от 5 до 9 часов, сохранили свои позиции на уровне 14,5%. Доля долговременных атак продолжительностью более 50 часов приближается к 5%-ной отметке.

Существует немало сценариев реализации DDoS-атак, у каждой — свой почерк и свои способы преодоления. Более того, следует отметить, что не все атаки можно ослабить или побороть, а в некоторых случаях проще и дешевле переждать подобный инцидент. Сценарий реализации DDoS-атаки представляет собой сочетание метода, инструментов и каналов отправки ложных запросов на целевой информационный ресурс. Тип DDoS-атаки определяется форматом упомянутых «мусорных» запросов.

Обобщенно можно выделить пять основных методов реализации DDoS-атак:

1. SYN-DDoS — отправка в открытый порт атакуемого сервера массы SYN-пакетов, где место отправителя занимает произвольный или же вовсе несуществующий IP-адрес. SYN-пакеты не приводят к установке реального соединения, что влечет за собой создание мнимых полуоткрытых соединений, переполняющих очередь подключений, вынуждая сервер отказывать в обслуживании легитимным пользователям.

2. TCP-DDoS — атака на транспортный протокол, отвечающий за передачу данных по сети Internet между локальными компьютерами. Принцип реализации схож с описанной выше.

3. HTTP-DDoS — отправка в порт атакуемого сервера небольшого по объему, но достаточного по мощности для насыщения полосы пропускания HTTP-пакета. В результате переполнения ресурсов сервера происходит аварийная остановка его работы.

4. ICMP-DDoS — один из самых опасных типов атак. Злоумышленник осуществляет отправку подельного ICMP-пакета через усиливающую сеть, подменяя в дальнейшем IP-адрес на адрес целевого устройства атаки. В результате на фоне формального сохранения небольшого трафика возникает перегрузка с последующей потерей соединения с легитимными пользователями.

5. UDP-DDoS — отправка множества UDP-пакетов большого объема на определенные или произвольные номера портов удаленного хоста, который после проверки активности соответствующего приложения отправляет ответное сообщение о недоступности адресата. В итоге система оказывается перегруженной.

Наглядно доли каждого типа DDoS-атак представлены на рис. 5.

Пять наиболее используемых злоумышленниками сценариев DDoS-атак практически не изменяется из квартала в квартал уже на протяжении трех лет. Все также наиболее часто применяемым методам остается SYN-DDoS, чья доля стремительно увеличилась за прошедший год и достигла 80%. Далее по частоте применения следует TCP-DDoS, имеющий долю 8,2%, что почти на три четверти ниже в сравнении с началом 2014 г. Резко сократилась частота реализации HTTP-DDoS — с 30,2% в начале 2015 г. до 7,6% по итогам 2016 г. Аналогичная тенденция характерна для UDP-DDoS и ICMP-DDoS, чья суммарная доля уменьшилась с 5,5 до 3%. Однако общую расстановку сценариев атак перечисленные тенденции не изменили. В результате равноправно предположение, что в сочетании с появлением и закреплением новых векторов для реализации DDoS-атак в ближайшем будущем следует ожидать дальнейшего увеличения их мощностей и частоты, а также появления ботнетов, состоящих из уязвимых устройств качественно нового типа.

Рассмотрев основные тенденции развития DDoS-атак, вернемся к оценке последствий от реализации подобных киберинцидентов.

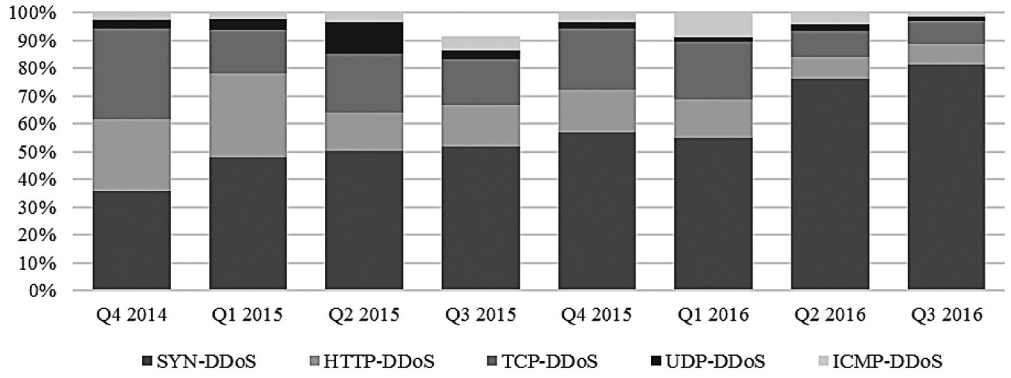

Рис. 5. Распределение DDoS-атак по сценариям реализации [3]

Укрупненно потери можно разделить на две категории [5, с. 124]:

- ущерб, вызванный утечкой ценной для компании информации и ее использованием злоумышленниками в целях, которые могут повредить бизнесу;
- ущерб, вызванный техническими сбоями в работе основных каналов передачи информации и взаимодействия с контрагентами.

Утечки данных в крупных компаниях всегда оказываются в первых строках новостных лент, поскольку в таких случаях похищенная конфиденциальная информация зачастую передается в руки киберпреступников или конкурентов, выступающих в качестве заказчиков атак. Ущерб от утечки информации очевиден и крайне болезнен. Как правило, он охватывает прямой финансово-экономический ущерб, проявляющийся в потере денег, прибыли, юридических и финансовых санкциях регулирующих органов, штрафах в результате судебных разбирательств и пр., и нематериальные потери, включающие утрату доверия и лояльности пользователей, клиентов, партнеров и конкурентного преимущества (например, за счет утраты интеллектуальной собственности). Компании, пострадавшие от утечек конфиденциальных данных, затрачивают непропорционально большой объем средств и времени на обнаружение и техническое устранение вторжений злоумышленников, выявляя и блокируя DDoS-атаки и реализуя меры по повышению безопасности информационной инфраструктуры.

Как отмечалось выше, последствия DDoS-атак схожи с последствиями иных информационных: утечка критически важных данных и отказ в обслуживании. В связи с этим наиболее серьезные виды ущерба охватывают потери прибыли, снижение продуктивности пользователей, проблемы технической поддержки, порчу ИТ-ресурсов и др. На рис. 6 приведена диаграмма, на которой представлены риски, связанные с реализацией DDoS-атак, проранжированные по мере убывания ущерба.

Как следует из представленных данных, для большинства компаний основу ущерба составляет потеря гарантированных доходов и контрактов — 26% компаний отнесли данный тип потерь в разряд первичных рисков.

Репутационные риски указали 23% компаний. Этот вид риска особенно проблемный для полностью веб-зависимых организаций, чьи услуги должны быть доступны 24 часа в сутки и семь дней в неделю. Потеря легитимных клиентов, которые не смогли получить доступ к нужному веб-сервису, оказалась на третьем месте — 19%. Далее следуют технические сбои — 17% компаний отметили необходимость развертывания резервных информационных систем, которые позволяют поддерживать онлайн-операции. Обеспокоены расходами на непосредственное отражение DDoS-атаки и восстановление работы веб-ресурса в нормальном рабочем режиме 14% компаний.

Основной целью DDoS-атаки является снижение производительности информационной системы (рабочей станции, веб-сервера, приложения и пр.) или же приостановка ее функционирования. В результате успешной реализации DDoS-атаки киберпреступникам удается спровоцировать падение темпов развития производства или продаж атакованной компании, что оказывает негативное влияние на финансовую устойчивость и рентабельность компании.

В табл. 1 представлены ключевые характеристики DDoS-атак в различных секторах экономики России. Приведенные цифры получены в результаты усреднения интервальных оценок, публикуемых в ежегодном отчете Лабораторией Касперского [3].

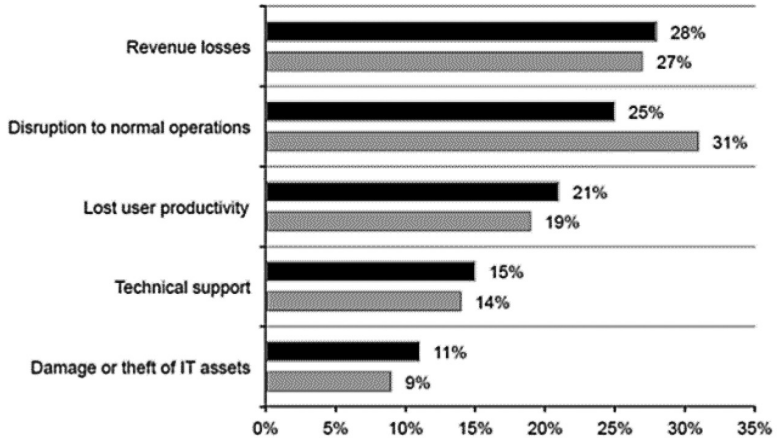

Рис. 6. Основные компоненты ущерба от реализации DDoS-атаки [3]

Таблица 1

Количественные характеристики DDoS-атак в различных секторах экономики России

Сектор / Индикатор	Количество атак на 1 компанию из сектора за год	Продолжительность атаки, ч	Средняя оценка ущерба, долл. США
Строительство	5,3	4,2	17 656,71
Государственный сектор	2,1	1,6	11 203,63
Розничные продажи	3,2	0,1	4298,58
Образование	1,8	6,8	975,50
СМИ	6,5	1,5	19 500,50
Финансовый сектор	2,5	7,8	1125,50
Здравоохранение и фармацевтика	2,3	4,1	2375,50
ИТ и телеком	4,2	14,8	23 757,82
Производственный сектор	2,5	6,7	13875,50
Профессиональные бизнес-услуги	2,7	3,0	6469,25
Транспорт и инфраструктура	4,0	2,7	32 518,36
Прочие	18,3	17,1	1406,75

Для количественной оценки информационных рисков необходимо оценить частотность возникновения атак и стоимость вызванных ими потерь, зависящую от стоимости информационных активов организаций. Однако сама стоимость активов не ограничивается стоимостью замены программного обеспечения, ИТ-оборудования и иных аппаратных средств. При оценке величины потерь необходимо иметь в виду и величину ущерба, нанесенного бизнес-процессам компании. Кроме того, более отдаленное от основных факторов риска по причинно-следственной цепочке, в то же время более сильное по воздействию последствие — это ущерб деловой репутации компании и ослабление конкурентных позиций [6, с. 49]. Представим обобщенные числовые характеристики перечисленных составляющих информационного риска, используя данные совместного исследования Лаборатории Касперского и B2BInternational [3]. Исходя из результатов опроса представителей IT-департаментов организаций различных сфер деятельности, можно заключить, что средняя величина ущерба от DDoS-атаки составляет порядка 15,5 тыс. долл. США на одну атаку. Наибольший ущерб характерен для компаний, работающих в транспортной отрасли, его величина может достигать 32,5 тыс. долл. США. Менее масштабный, но ощутимый ущерб возможен у компаний телекоммуникационной сферы и представителей СМИ — 23,7 и 19,5 тыс. долл. США соответственно.

Финансовые и коммерческие потери в результате успешной реализации DDoS-атаки, которые помимо оттока клиентов и упущенного дохода охватывают также снижение производительности труда и ухудшение репутации, имеют долговременное влияние и значительно превышают операционные убытки. Согласно усредненной оценке респондентов, доля финансовых и коммерческих потерь в общей величине ущерба от DDoS-атаки достигает 86%.

Работа по минимизации информационных рисков делится на организационную и техническую составляющие. Организационные меры связаны с непосредственным ограничением доступа к критически важным данным компании. С этой целью вся информация классифицируется на общедоступную, для служебного пользования и секретную (конфиденциальную). В дополнение, содержание информационных потоков компании можно разделить по назначению: для рабочей группы проекта, для исполнителей и руководителей финансовых подразделений и департаментов по работе с клиентами и партнерами, для топ-менеджмента организации и т.д. В итоге формируется матрица информационных потоков, каждому уровню которой соответствует определенный уровень доступа, связанный со степенью уязвимости информации и оценкой от ее возможной потери в результате реализации DDoS-атаки или иного инцидента нарушения информационного пространства компании.

В заключение можно отметить, что DDoS-атаки, оставаясь одним из наиболее эффективных инструментов нанесения экономического ущерба в результате отказа в обслуживании и простоя информационных сервисов, в ближайшем будущем не утратят свои позиции в киберпространстве, а, вероятнее, перейдут на новый уровень и станут более масштабными и сложными с точки зрения их предотвращения. Данные атаки получили особый инкремент развития при нарастании геополитического напряжения и экономической конкуренции в мире, что делает их более изощренными и непредсказуемыми. В настоящее время информация перестала играть роль вспомогательного средства производства и давно стала одним из наиболее ценных активов любой современной организации. В связи с этим информационная безопасность и, в частности, надежная защита от DDoS-атак выходят на передний план и требует пристального внимания со стороны руководства. Но защита информации — это сложная и затратная задача. Помимо высоких инвестиций в средства защиты, необходимо разрешить противоречие между доступностью информационных ресурсов и необходимой степенью их конфиденциальности.

Литература

1. *Терновой О.С.* Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности в результате ddos атак [Текст] / О.С. Терновой // Известия АлтГУ. — 2013. — № 1 (77). — С. 123–125.
2. *Лисенкова В.С.* Проблема защиты информации как элемента экономической безопасности на примере борьбы с DDoS-атаками [Текст] / В.С. Лисенкова, А.Г. Резникова // Сборник научных трудов и результатов совместных научно-исследовательских проектов РЭУ им. Г.В. Плеханова. — 2016. — С. 500–503.
3. Квартальные отчеты об угрозах [Электронный ресурс] // URL: https://securelist.ru/all/?category=390 (дата обращения: 17.02.2017).
4. DDoS на российские банки. Хронология атаки [Электронный ресурс] // URL: https://habrahabr.ru/company/jetinfosystems/blog/315226/ (дата обращения: 21.02.2017).
5. *Марков А.А.* Понятие и характеристика информационных рисков, опасностей и угроз в современном постиндустриальном обществе [Текст] / А.А. Марков // Вестник ВолГУ. — Серия 7: Философия. Социология и социальные технологии. — 2010. — № 1. — С. 123–129.
6. *Зинкевич В.* Информационные риски: анализ и количественная оценка [Текст] / В. Зинкевич, Д. Штатов // Бухгалтерия и банки. — 2007. — № 2. — С. 50–53.

References

1. Ternovoy O.S. Metodika i sredstva rannego vyyavleniya i protivodeystviya ugrozam narusheniya informatsionnoy bezopasnosti v rezul'tate ddos atak [Methods and Means for Early Detecting and Countering Threats to Information Security Breaches as a Result of DdosAttacs]. *Izvestija AltGU* [Bulletin of AltGU]. 2013, I. 1 (77), pp. 123–125. (in Russian)
2. Lisenkova V.S., Reznikova A.G. Problema zashchity informatsii kak elementa ekonomicheskoy bezopasnosti na primere bor'by s DDoS-atakami [The problem of information security as an element of economic security on the example of DDoS attacks]. *Sbornik nauchnyh trudov I rezul'tatov sovmestnyh nauchno-issledovatel'skih proektov RJeU im. G.V. Plehanova* [Collection of scientific papers and the results of joint research projects of the Russian Academy of Sciences. G.V. Plekhanova]. 2016, pp. 500–503. (in Russian)
3. *Kvartal'nye otchjoty ob ugrozah* [Quarterly threat reports]. Available at: https://securelist.ru/all/?category=390 (accessed 17 February 2017).
4. *DDoS na rossijskie banki. Hronologija ataki* [DDoS on Russian banks. Timeline of events]. Available at: https://securelist.ru/all/?category=390 (accessed 21 February 2017).
5. Markov A.A. Ponyatie i kharakteristika informatsionnykh riskov, opasnostey i ugroz v sovremennom postindustrial'nom obshchestve [The notion and characteristics of inrormation risks, dangers and threats in the modern post0industrial society]. *VestnikVolGU* [Bulletin of VolGU]. 2010, I. 1, pp. 123–129. (in Russian)
6. Zinkevich V., Shtatov D. Informatsionnye riski: analiz i kolichestvennaya otsenka [Information risks: analysis and quantification]. *Buhgalterija I banki* [Accounting and banking]. 2007, I. 2, pp. 50–53. (in Russian)