А.Е. Дёшина, М.В. Бурса, А.Г. Остапенко,
А.О. Калашников, Г.А. Остапенко

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ МУЛЬТИСЕРВЕРНЫХ СИСТЕМ ПРИ ВОЗДЕЙСТВИИ DDOS-АТАК

Монография

Под редакцией члена-корреспондента РАН
Д.А. Новикова

Воронеж
Издательство «Научная книга»
2014

УДК 004.056.5: 004.75
ББК 55.6
Д 39

Рецензенты:

Белоножкин В.И., д-р техн. наук (Аппарат уполномоченного представителя Президента по правам человека в Воронежской области);

Азизов Т.Я., д-р. физ.-мат. наук, профессор (Воронежский государственный университет)

Д 39 Дёшина, А.Е. Управление информационными рисками мультисерверных систем при воздействии DDoS-атак: Монография/ А.Е. Дёшина, М.В. Бурса, А.Г. Остапенко, А.О. Калашников, Г.А. Остапенко; под ред. чл.-корр. РАН Д.А. Новикова. – Воронеж: Издательство «Научная книга», 2014. – 160 с.

ISBN 978-5-98222-855-0

В монографии предлагается методика управления общим риском атакуемых мультисерверных систем на основе параметров рисков их элементов, намечен подход к параметрическому синтезу. Разработанное методическое обеспечение ориентировано на широкий спектр мультисерверных систем. Оно может использоваться в качестве базы для дальнейших исследований сетевых структур, подвергающихся разнообразным деструктивным воздействиям.

Табл. 3. Ил. 46. Библиогр.: 118 назв.

УДК 004.056.5: 004.75
ББК 55.6
Д 39

ISBN 978-5-98222-855-0

Введение

Инновационный тренд в развитии сетевых структур во многом заключается в распределении задач и ресурсов между серверами, множество которых весьма велико (мультисерверная система), что открывает широкие перспективы для различных атак злоумышленников [90,106,110], в том числе и для DDoS-атак, способных причинить значительный вред технологическим и функциональным процессам [35] и обусловить серьёзную угрозу экономической безопасности любого государства, в том числе и России [34].

Объектами подобных деструктивных воздействий являются, прежде всего, сетевые структуры [47, 67, 70, 73, 84, 86] распределенного характера, в том числе широко распространенные мультисерверные системы (МСС) [25, 92], которые успешно используются для реализации способности системы стабильно функционировать при росте нагрузки, например, при значительном увеличении числа пользователей или объема используемых данных. Построение системы на основе распределенной компонентной архитектуры, позволяет разъединить компоненты и расположить их на различных физических серверах [110, 111].

Мультисерверная работа становится всё более важным ресурсом в условиях развития современных корпоративных технологий. Расширяется круг компаний, внедряющих их в своей практической деятельности. Вместе с тем из-за того, что операционные системы позволяют исполнять некоторые виды скриптов (например, Java Script), легко могут быть внедрены эксплойты пользователей [7, 31] с правами записи инструкций для сервера, приложений, а также критерии, по которым определяется их работоспособность. Таким образом, аспекты повышения безопасности при проведении DDoS-атак на МСС выходят на первое место. Интенсивное развитие таких систем ведет к увеличению интереса к ним со стороны нарушителей [110], поэтому следует возрастание количества атак.

В связи с этим представляется актуальным изучение угроз, возникающих при проведении DDoS-атак на МСС и связанных с ними рисков, как с точки зрения их оценки, так и возможности управления ими с использованием элементов параметрического синтеза.

Наиболее уязвимыми элементами МСС, чаще всего подвергающимися DDoS-атакам, являются: связанные между собой серверы, балансировщик загрузки серверов, межсетевой экран.

Методология риск-анализа [1, 2, 10-16, 23-70] предусматривает исследование динамики риска [23-26, 53, 59, 67, 68], что необходимо для управления этим параметром [23, 25, 47, 48, 66, 58, 59, 64, 65] в целях обеспечения требуемого уровня защищенности и эффективности исследуемого объекта [46, 52, 55, 63].

Для реализации такого подхода в МСС можно использовать управление рисками за счет выбора параметров функций риска компонентов на основе аналитических выражений, а также на основе положений теории чувствительности [23-26, 45, 47, 67-70, 74, 78].

В настоящее время оценка, анализ и управление рисками в области информационной безопасности рассматривается как обязательная составляющая процесса формирования защиты мультисерверных систем [16,17]. Все сказанное выше делает актуальным исследование информационных рисков, возникающих в результате успешной реализации DDoS-атак на МСС, а также разработки математических методов для анализа и количественной оценки рисков, позволяющих управлять риском всей системы через параметры функций рисков ее компонентов на основе полученных аналитических выражений.

Сейчас, когда время проведения и интенсивность DDoS-атак на МСС увеличиваются, необходимо скорректировать подходы к формированию их защиты, включая управление рисками.

Целью исследования является повышение защищенности МСС при проведении на них DDoS-атак.

Для достижения указанной цели необходимо решить следующие задачи:

1. Развитие методологии анализа и регулирования рисков МСС с использованием предельно допустимых значений для числа открытых соединений и предельно допустимое значение коэффициента загрузки центрального процессора отдельных компонентов, позволяющей настроить параметры защиты системы таким образом, чтобы суммарный риск находился в заданной полосе неравномерности, включая поиск:

– аналитических выражений для предельно допустимых значений для числа открытых соединений и предельно допустимое значение коэффициента загрузки центрального процессора компонент системы, обеспечивающих заданное поведение общей функции риска, в случае асинхронных атак на серверы;

– аналитических выражений на основе предельно допустимых значений числа открытых соединений и предельно допустимых значений коэффициентов загрузки центральных процессоров компонент системы для оценки чувствительности риска всей МСС, позволяющие управлять общим риском, как при асинхронных атаках, так и при синхронных DDoS-атаках на ее компоненты.

2. Разработка методики управления общим риском МСС, как при асинхронных, так и при синхронных DDoS-атаках на ее компоненты, которая на основе параметров рисков компонент системы позволит заранее оценивать риски и ущербы от нахождения системы в режиме отказа в обслуживании и принимать эффективные управленческие решения по оптимизации риска МСС.

3. Реализация подхода к параметрическому синтезу МСС с заданным диапазоном неравномерности риска, позволяющего по виду задан-

ной общей функции риска МСС, а, следовательно, и максимально допустимому диапазону ущербов, получать аналитические выражения для нахождения риск-параметров.

Практическая значимость результатов видится в том, что разрабатываемое методическое обеспечение ориентировано на широкий спектр МСС и может быть адаптировано к конкретным типам МСС, характер которых изменяется при каждом практическом применении. Оно может использоваться в качестве базы для дальнейших исследований разнообразных сетевых структур, подвергающихся самым разнообразным деструктивным воздействиям.

Содержание

Научное издание

ДЁШИНА Анна Евгеньевна
БУРСА Максим Васильевич
ОСТАПЕНКО Александр Григорьевич
КАЛАШНИКОВ Андрей Олегович
ОСТАПЕНКО Григорий Александрович

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ МУЛЬТИСЕРВЕРНЫХ СИСТЕМ ПРИ ВОЗДЕЙСТВИИ DDOS-АТАК

Монография

Под ред. чл.-корр. РАН Д.А. Новикова

Издание публикуется в авторской редакции

Дизайн обложки С.А.Кравец

Подписано в печать 18.08.2014. Формат 60x84 1/16.
Усл. печ.л. 10,0. Заказ 000. Тираж 500 экз.

ООО Издательство «Научная книга»
394077, Россия, г.Воронеж, ул. 60-й Армии, 25-120
http://www.sbook.ru/

Отпечатано с готового оригинал-макета
в ООО «Цифровая полиграфия»
394036, г. Воронеж, ул. Ф. Энгельса, 52.
Тел.: (473)261-03-61