ОТЗЫВ

официального оппонента на диссертацию

Тернового Олега Степановича на тему «Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности при DDoS-атаках», по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», на соискание ученой степени кандидата технических наук

1. Актуальность работы

Диссертация О.С. Тернового посвящена разработке методического, алгоритмического и программного обеспечения процесса своевременного обнаружения наиболее критичных компьютерных DDoS атак (Distributed Denial of Service - распределенный отказ в обслуживании). Обычно такие атаки осуществляются совместными усилиями множества программных компонентов, размещённых на скомпрометированных хостах в Интернете. Отметим, что DDoS атаки могут привести не только к выходу из строя конкретных серверов и/или служб (сервисов) и, следовательно, сделать невозможным предоставление тех или иных услуг легальным пользователям. Более того, с помощью DDoS атак возможна остановка работы корневых DNS-серверов, что способно вызвать частичное или полное прекращение функционирования сети Интернет. Поэтому разработка адекватных механизмов защиты от DDoS атак, а также формирование обоснованных рекомендаций по выбору механизмов, наиболее действенных в конкретных условиях является одной из актуальных задач в области защиты информации. Отметим, что для противодействия DDoS атакам важно именно своевременное обнаружение нелегитимного трафика, так как в дальнейшем, если такой трафик не остановлен, например, провайдером, то сделать что-то на входе будет невозможно, поскольку вся полоса пропускания будет занята. Именно разработка технологий своевременного обнаружения TCP SYN flood-атаки на сервер позволяют классифицировать тематику диссертационного исследования О.С. Тернового как **актуальную**.

2. Степень обоснованности научных положений и результатов

Обоснованность и достоверность представленных в диссертационной работе научных положений и результатов обеспечивается опорой на базовые положения защиты информации, корректной постановкой задачи, адекватным планированием и проведением экспериментов, а также реализацией алгоритмов, созданных на основе обработки полученных экспериментальных результатов, в авторском программном продукте.

3. Достоверность и новизна полученных результатов

Результатами диссертации, обладающими признаками научной новизны, являются:

1. Оригинальная методика описания сезонности сетевого трафика для различной его периодичности, учитывающая неопределенность начала и завершения периода.
2. Алгоритм раннего обнаружения начала распределенных TCP SYN flooding атак, направленных на отказ в обслуживании.

3. Оригинальное программное обеспечение для Web-серверов, позволяющее оперативно классифицировать легитимный и вредоносный трафики.

Основные результаты диссертационной работы получены автором самостоятельно и опубликованы в рецензируемых изданиях.

4. Теоретическая и практическая значимость результатов

В диссертационной работе получены результаты, имеющие практическую и теоретическую значимость, что подтверждается соответствующими актами внедрения и отзывами, полученными на специализированных научно-технических выставках, конкурсах и конференциях.

Теоретическая значимость результатов заключается в:

- выявлении сезонности в работе сетевых ресурсов, что позволяет более точно проводить оперативный анализ входящего трафика и при необходимости корректировать настройку средств безопасности;
- разработке методики раннего обнаружения начала DDoS–атаки, которая может быть использована для обеспечения безопасности конечного сетевого ресурса;
- определении критериев для разделения вредоносного и пользовательского трафика в реальном времени.

Практическая значимость работы О.С. Тернового заключается в разработке программного обеспечения и методических подходов, позволяющих повысить защищённость сетевых ресурсов от атак, направленных на отказ в обслуживании, без модификации аппаратного обеспечения сети и серверов.

5. Оценка структуры и содержания диссертации

Диссертационная работа выполнена на 130 листах машинописного текста, включает в себя 10 таблиц, 24 рисунка, 2 схемы, библиографический список, содержащий 96 ссылок, два приложения, включающие свидетельства о государственной регистрации программ для ЭВМ и копии актов внедрения результатов диссертации на предприятиях и в учебный процесс высших учебных заведений.

Во введении обоснована актуальность темы диссертационной работы, определены цель и задачи научного исследования, перечислены основные результаты, определена их научная новизна и практическая значимость.

Первая глава посвящена изучению текущего состояния проблемы. Сделан анализ зарубежных и российских печатных и Интернет источников в этой области. Рассмотрены принципы классификации DDoS–атак, существующие методы и инструменты для обнаружения атак, структуры и типы вредоносного трафика. По итогам анализа сформулированы выводы и в общих чертах определена область диссертационного исследования.

Вторая глава посвящена разработке методики обнаружения вредоносного трафика, поступающего в результате распределенных атак, направленных на отказ в обслуживании. Для снижения ошибки обнаружения вредоносного трафика автор предлагает использовать сезонный подход. Особое внимание уделяется обоснованию существования сезонности, в рамках этого анализируется посещаемость и нагрузка на сетевые ресурсы. Определяются факторы, влияющие на формирование сезонных периодов.

Третья глава посвящена разработке алгоритмов оперативного реагирования на DDoS атаки и их реализации в кроссплатформенном программном продукте, состоящем из трех модулей, которые позволяют обеспечивать безопасность ресурсов на различных уровнях.

Четвертая глава посвящена тестированию разработанного программного обеспечения. Автор описывает процедуру проведения экспериментов, уделяя внимание таким параметрам как характеристики клиентских компьютеров, установленное на них системное и пользовательское программное обеспечение. Эксперименты объединены в серии, по разному уровню сложности, начиная от простых нагрузочных тестов, генерирующих необходимый объем трафика, и заканчивая экспериментами с копиями реальных DDoS–атак. Приведены результаты сравнения результатов работы авторского ПО с результатами коммерческих и свободно распространяемых программных продуктов. Отдельно приведены результаты внедрения разработанного ПО.

В Заключении приведены результаты, полученные в процессе выполнения диссертационного исследования.

В Приложениях представлены документы, свидетельствующие о внедрении результатов работы в учебный процесс и на предприятиях, а также свидетельства о государственной регистрации программ для электронных вычислительных машин.

6. Замечания к работе

Раздел с обзором технологий защиты от DDoS атак содержит слишком много описаний технологий и решений, направленных на сети и атаки принципиально различного типа (в том числе, далекие от технологий, применимых в контексте решаемой автором задачи). Это может говорить о попытке собрать как можно больше информации по ключевому слову «DDoS» без учета автором того, в каком направлении именно он ведет исследование.

Поэтому в работе не сформулирована *гипотеза о том*, при каких конкретных ограничениях на типы атак (реально автор детально исследовал только TCP SYN-flooding, а не весь арсенал DDoS атак) и ее мощности (измеряемой, например, в процентной доле полосы пропускания канала, занимаемой вредоносным трафиком, или отношением числа SYN пакетов к числу ACK пакетов, или интенсивностью атаки, т.е., количеством вредоносных и легальных пакетов в секунду), возможны определенные методы раннего обнаружения и противодействия этим атакам. А далее из *гипотезы* можно было бы четко определить и *конкретную цель* работы, и необходимые для ее достижения задачи.

При таком подходе не пришлось бы использовать такие условные понятия как *«атака регионального уровня», «приемлемая точность», «мощные корпорации», «огромные ресурсы»* и т.п. Не стоило также приводить на стр. 63 формулы (4) и (5) из работы А. С. Родионова, В. В. Шахова, не упомянув, что они выведены в предположении, что очередь полуоткрытых соединений сервера при атаке TCP SYN-flooding может быть описана Марковской цепью с конечным числом состояний и соответствует процессам гибели и размножения. Это и позволило автором оценить метрику живучести и вероятность блокировки SYN пакета. Но такой результат справедлив только для этого типа DDoS атак.

В тексте работы везде упоминается конкретный класс DOS атак - HTTP Flood, однако теме исследования заявлены методы защиты от DDOS атак в общем смысле.

В работе отсутствует наглядное представление экспериментальных данных или ссылки на работы, объясняющие то, откуда эти данные взяты. На стр. 56 приведены невразумительные таблицы (2) и некий график без ссылок, но утверждается, что вычислен показатель Херста H= 0,63. На этом основании делается вывод о сезонных периодах. Но в диссертации отсутствует проверка или ссылка на проверку на значимость полученного значения показателя H. Более того, на этой же странице величина H определяется уже как множество вредоносных клиентских запросов.

Выбор метод кластеризации K-means не выглядит достаточно убедительно. Надо исходить не из того, что заранее известно число кластеров, а из формы данных. K-means будет плохо работать с близкими и вытянутыми кластерами. Вообще идея, что должно быть только два кластера, и весь неблагонадёжный трафик будет в одном из них, довольно оригинальна. Но почему так должно происходить не пояснено.

Автор отмечает, что WaveCluster работает хорошо с кластерами произвольной формы, но результаты ухудшаются при увеличении размерности. Но далее использует метод главных компонент для снижения размерности. А снижение размерности даст потерю информации. Эта потеря не оценена.

Список литературы следует приводить не в порядке цитирования, а по алфавиту, разделив на русскоязычные источники и иностранные, причем для Интернет источников следует указывать дату обращения к ресурсу.

Данные замечания не снижают общей положительной оценки диссертационной работы, значимости полученных научно-практических результатов.

7. Соответствие автореферата основному содержанию диссертации

Текст автореферата достаточно полно и точно отражает содержание диссертации. В нем раскрывается актуальность работы, обозначаются цель, объект и предмет исследования, обосновывается новизна и достоверность полученных результатов, приводится основное содержание и выводы исследования.

8. Соответствие содержания диссертации содержанию опубликованных работ

По теме диссертационной работы издано 15 научных публикаций, в том числе: 5 публикаций в ведущих рецензируемых журналах, рекомендованных для публикации результатов кандидатских и докторских работ ВАК; два свидетельства о государственной регистрации программы для ЭВМ; глава в рецензируемой коллективной монографии, посвященной региональным аспектам технической и правовой защиты информации. В указанных публикациях отражены все основные положения, выводы и результаты диссертации.

9. Соответствие темы диссертации заявленной научной специальности

Тема диссертационной работы соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по следующим пунктам:

Пункт 2. (Методы, аппаратно-программные и организационные средства

защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.)

Пункт 5. (Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.)

Пункт 14. (Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.)

11. Заключение

Диссертация Тернового Олега Степановича на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой содержится решение задачи обнаружения и противодействия распределенным атакам, направленным на отказ в обслуживании, изложены научно обоснованные методические и программно-алгоритмические решения и разработки, имеющие существенное значение для развития технологий защиты информации от атак типа «отказ в обслуживании», что соответствует требованиям п. 9 «Положения о порядке присуждения ученых степеней» ВАК России, утвержденного постановлением Правительства РФ № 842 от 24.09.2013 г., а ее автор, Терновой Олег Степанович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (технические науки).

Официальный оппонент —
Захаров Александр Анатольевич
д.т.н., профессор,
заведующий кафедрой информационной безопасности
Федерального государственного автономного
образовательного учреждение высшего образования
"Тюменский государственный университет"

А.А. Захаров

почтовый адрес – 625003 г. Тюмень, ул. Володарского, 6;
телефон - 8(3452)297637;
электронная почта - azaharov@utmn.ru

ПОДПИСЬ ЗАВЕРЯЮ:
Ученый секретарь Ученого совета
01.03.2017
ТюмГУ Э.М. Лимонова