ВВЕДЕНИЕ

Актуальность исследования

С развитием в России информационных технологий широкое распространение получила всемирная сеть - интернет, зарекомендовавшая себя в качестве удобного информационного источника. В стране с каждым днем увеличивается количество пользователей интернета, в любых организациях и предприятиях присутствует доступ во всемирную сеть[1,3,7].

Однако ситуация связанная с распространенностью сети интернет характеризуется и рядом негативных признаков. Наряду с информатизацией наблюдается и возрастание интереса к сети со стороны криминальных кругов[34]. По мере увеличения количества пользователей интернета и все большей циркуляции информации в сети возникает опасность хищения этой информации заинтересованными лицами. Анализ динамики видов преступлений позволяет сделать вывод о росте числа правонарушений в сфере компьютерной информации, который идет не менее быстрыми темпами, чем компьютеризация в России. Одновременно непрекращающееся увеличение числа пользователей персональных компьютеров и сети интернет в последние годы породило множество незаконных явлений, атаки хакеров на web-рессурсы, распространение программно-математических средств, «троянских» программ, интернет-мошенничество, спам, распространение детской порнографии, и кибертерроизм.

В современном обществе роль глобальной информационной сети интернет - немаловажна. Для многих людей пользование интернетом стало привычным делом, наряду с чтением газет, просмотром телевизионных передач. Многие уже не могут представить свою жизнь без социальных сетей, веб-форумов, новостных лент, различных сайтов «тумблеров», содержащих фото и видео подборки тематического материала[1-7]. Популярность и доступность интернета приводит к тому, что с каждым днем все большее и большее количество пользователей привязываются к данному источнику информации. Внимание огромнейшей массы людей приковано к относительно небольшому количеству веб-ресурсов, которые они посещают

регулярно. Для поддержки такого рода ресурсов используют специальное оборудование, позволяющее сразу обслуживать множество пользователей. Остальные редко посещаемые или узкоспециализированные ресурсы не нуждаются в таком дорогостоящем оборудовании, ведь работают одновременно с небольшим количеством пользователей. Случается такие события, что популярные ресурсы размещают в своих новостных лентах ссылки на другие сайты, которые не рассчитаны на столь множественные запросы, и это приводит к перегрузке последних[3, 5-9]. Работа сервера становится невозможной, все запросы пользователей не выполняются. Собственник сайта при этом терпит ущерб от упущенной прибыли, затраты на восстановление нормальной работы сайта и ликвидации последствий атаки, но с другой стороны это является своеобразной рекламой сайта, и повышение его рейтинга в поисковых системах. Эта ситуация аналогична атаке в отказе в обслуживании, только без участия злоумышленников, она называется слэшдот-эффект[1, 3-7]. Это проблема особенно актуальна в развитых странах Европы и Америки, где процент пользователей сети интернет от общего числа населения велик. На данный момент населением России все еще происходит освоение всемирной паутины. В России около 43% от общего числа людей имеют доступ к сети, когда в большинстве развитых стран эта цифра приближается к 80%, а в наиболее развитых более 90% (данные веб-ресурса wikipedia.org).Отсюда следует, что для Российских веб-ресурсов проблема слэшдот-эффекта вскоре также станет актуальна[6].

В связи с этим, рассмотрение риск-анализаслэшдот атак – крайне актуальная задача. Она является сложной и многогранной, так как требует исследования множества факторов. Одним из таких факторов является математическое моделирование атак, которое позволит оценить, во-первых, возможный ущерб от успешной атаки на заданную автоматизированную систему, во-вторых - эффективность используемых средств защиты.

В данном случае под математическим моделированием понимается построение риск-моделейслэшдот атак на автоматизированные системы.

слэшдот-эффект. Для достижения поставленной цели необходимо решить следующие задачи:

1. Произвести анализ, рассмотреть сущность, условие возникновения и деструктивное воздействие атаки слэшдот-эффект, на высоконагруженные автоматизированные системы общего доступа, имеющие подключение к сети интернет, собрать статистику для данных атак и найти закономерности которым она подчиняется.

2. Построение риск-модели, на основе закономерностей справедливых для атак слэшдот эффект, которая позволит рассчитать риски для деструктивных воздействий на высоконагруженные автоматизированные системы общего доступа, имеющие подключение к сети интернет, оценить условия при которых возможно регулирование рисков.

3. Произвести изучение распределенных атак типа слэшдот эффект, на высоконагруженные автоматизированные системы общего доступа, имеющие подключение к сети интернет, рассмотреть управление рисками предложить инновационное эффективное решение.

Объектом исследования являются высоконагруженные автоматизированные систем общего доступа, имеющие подключение к сети интернет, подверженные атаке слэшдот эффект.

Предметом исследования являются риски реализации деструктивных воздействий в сетях общего пользования, и явления в автоматизированных системах при реализации информационных атак.

В исследовании используются методы теории графов, системного анализа, методы экспертных оценок и математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики, системного анализа, интегральных оценок, применения функций чувствительности.

Научная новизна. В данной работеиспользована теория оценки рисков для высоконагруженных систем общего доступ имеющих подключение к сети интернет, обусловленных атакой слэшдот эффект. Ранее данный вопрос не был должным образом рассмотрен в теории оценки рисков для

Заключение

Работа посвящена оцениванию рисков высоконагруженных автоматизированных систем общего доступа, обусловленных атакой слэшдот-эффект. В ходе еѐ выполнения были получены следующие основные результаты:

1. В проделанной работе изучен процесс осуществления атаки, изучены существующие научные исследования и экспериментально наработанные данные в представленной проблеме.Приведено описание протекания атаки, причины ее возникновения, построена математическая описательная риск-модель приведены и возможные способы уменьшения ущерба от ее негативных последствий.

2. Разработана методика оценивание рисков, с помощью интегральных оценок риска, рассмотрен вариант ассинхронной распределенной атаки на высоконагруженные автоматизированные системы общего доступа, обусловленных атакой слэшдот-эффект.

3. В работе был использован подход который ранее применялся к данной проблеме не достаточно эффективно, при этом выдвинуты гипотезы о корреляции времени отклика с ущербом от атаки и равномерное распределение коэффициентов распределения при реальной атаке. Данный подход, а именно – интегральная оценка рисков и управление рисками является нестандартной для данной проблемы – атак слэшдот эффект.

4. В работе выявлена закономерность изменения рисков от регулирования внешних параметров, наибольшей эфффективностью в регулировании является параметр q, что дает возможность широкого применения, а также перспективность данного подхода. В ходе работы был использован ранее введенный понятийные аппарат.

5. В ходе исследований была сопоставлена статистика времени отклика сервера и ущерба от проведения атаки, и определена их корреляция