ВВЕДЕНИЕ

Актуальность исследования

В современном мире от информационных технологий зависит успех деятельности организаций разных уровней: от небольших фирм до градообразующих предприятий и государственных структур. С появлением сети Интернет стал возможен мгновенный обмен информацией, новостями, мультимедийным контентом. Непрерывно растèт популярность средств электронных коммуникаций, в том числе и электронной почты. Большинство организаций регистрирует электронные почтовые ящики на каждого сотрудника, практически все пользователи всемирной паутины имеют свой электронный почтовый ящик, притом зачастую несколько. Поток электронных сообщений постоянно увеличивается, этому способствует простота использования электронной почты, мгновенная доставка писем и бесплатность. [4,10]

Преимущества электронной почты сделали возможным рассылку нежелательных электронных сообщений (спама). Доля спама в потоке электронной почты составила 80,26%.[99, 103, 104] С помощью несанкционированных рассылок может осуществляться реклама или антиреклама организации, вымогательство денег, хищение данных или паролей, внедрение вредоносных программ. [8]

Спам в современном Интернете является неправомерным занятием, и в законодательстве ряда стран предусмотрены различные виды ответственности за такую деятельность. Например, в США один из крупнейших провайдеров Интернет AOL (AmericaOnline) ежемесячно выдвигает по несколько судебных исков к злоумышленникам, которые занимаются систематической рассылкой несанкционированных электронных сообщений по адресам еè клиентов.[30]

Нежелательные сообщения пользователь удаляет, зачастую даже не просматривая. Проведенный эксперимент исследователей университета Калифорнии показал, что из 12,5 миллионов разосланных сообщений со спамом только одно находит отклик у адресата и приводит к покупке рекламируемого товара, то есть эффективность спам рекламы 0,000008%.[102] Несмотря на столь

низкие показатели эффективности, услуги по рассылке спама пользуются популярностью, а, как известно, где есть спрос – есть и предложение.

По оценкам различных компаний, занимающихся проблемами информационной безопасности, основная доля спама рассылается с использованием сетей компьютеров обычных пользователей, превращенных в компьютеры – зомби при помощи уязвимости в ПО или использования вирусных технологий. Такие сети называют ботнетами, доля спам сообщений, разосланных при помощи сетей компьютеров-зомби, превышает 70% (по данным компании SophosLabs).[8]Ботнеты позволяют злоумышленникам не только рассылать огромное количество писем, но и оставаться безнаказанными, скрывая истинные источники рассылок. [1]

Пагубность спама том, что для злоумышленника отправка спам сообщения практически ничего стоит, но дорого обходится как получателю, так и провайдеру. Большое количество рекламной корреспонденции может привести к излишней нагрузке на серверы и провайдера, замедляя доставку электронных писем обычных пользователей.[5] Получатель спама тратит своѐ время, время в сети Интернет, затрачиваемое на получение незапрошенной корреспонденции. Помимо этого, открытие ссылки в спам письме может обернуться для получателя потерей денег с электронных кошельков или банковских карт, заражением компьютера вирусом или троянской программой, утратой паролей от популярных сервисов.

Резюмируя вышесказанное, можно сделать вывод о важности исследований в области несанкционированных массовых рассылок. Ведущие компании в области информационной безопасности постоянно ведут разработку новых алгоритмов, методов, средств и систем защиты пользователей отспам сообщений.

Пожалуй, особый интерес имеют риск-модели, учитывающие не только вероятность наступления ущерба, но и его величину в случае успешного проникновения спама в автоматизированную систему. Данное направление исследования представляется весьма актуальным и слабо проработанным.

Степень научной разработанности

В настоящее время активно ведутся исследования в области подсчета риска проникновения спама в автоматизированную систему.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

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

Научная новизна ожидаемых результатов заключается в следующем:

1 В отличие от аналогов, процесс исследования не запрошенных массовых рассылок в распределенных автоматизированных системах учитывал результаты их количественного и качественного развития, а также особенности реализации при различных условиях и типах объектов.

2 В отличие от аналогичных, полученная риск-модель спам-атак на распределенные автоматизированные системы включает в себя выражения для экстремумов интегрального риска распределенных автоматизированных систем.

3 В отличие от аналогов, алгоритм регулирования интегрального риска реализации асинхронных спам-атак на распределенные автоматизированные системы отличается особенностью управления общего риска с помощью регулирования среднего значения ущерба и среднеквадратического отклонения в компонентах системы, с учетом распределения риска в них.

На защиту выносятся следующие основные положения работы:

1 Понятие спам-атак в распределенных автоматизированных системах, основные виды спама, способы рассылки и маскировки спам-сообщений;

2 Риск-модель спам-атак в распределенных автоматизированных системах;

3 Алгоритм регулирования рисков в распределенных автоматизированных системах, подверженных угрозамспам-атак.

Практическая ценность работы заключается в том, что:

1 Классификация основных видов спам-атак в распределенных автоматизированных системах позволяет выявить наиболее опасные их виды в

ЗАКЛЮЧЕНИЕ

Работа посвящена исследованию распределенных автоматизированных систем и риск-анализу воздействия на них спам-атак. Основные научные и практические результаты, полученные в ходе выполнения работы:

1. На основании проведенных исследований предложена новая экспериментальная методика регулирования риска реализации спам-атак на распределенные автоматизированные системы.

2. Предложены оригинальные суждения по оценке суммарного риска для случая спам-атак на распределенные автоматизированные системы, у которых плотность вероятности наступления ущерба в компонентах имеет бета-распределение второго рода.

3. Возможностью применения построенной риск-модели для оценки рисков спам-атак в РАС доказана перспективность и состоятельность использования полученных выражений для экстремумов интегрального риска, с целью его анализа в распределенных автоматизированных системах, выявления уязвимых компонент, защите которых необходимо уделить особое внимание, а также для построения защищенных РАС.

5. Исследованы аналитические риск-модели распределенных автоматизированных систем, подвергающихся синхронному или асинхронному воздействию дестабилизирующих факторов, а также проведена оценка и регулирование общего риска системы при данных воздействиях.

6. При решении задач, применительно к проблематике работы, эффективно использован комплекс базовых методов исследования, таких как метод системного анализа, теории риска, теории вероятности, математической статистики.

7. В работе изложены подходы к оценке и регулированию риска в распределенных автоматизированных системах, на основании которых разработана методика обработки риска реализации спам-атак на компоненты РАС, плотность вероятности наступления ущерба в которых имеет бета-распределение.