ВВЕДЕНИЕ

Актуальность темы исследования. Современное информационное пространство содержит большое количество рекламы. Самым дешевым способом ее распространения является спам-рассылка. По статистике, каждый тысячный адресат откликается на полученное спам-сообщение [1, 2]. В среднем, рассылка спам сообщений 100 млн. email-адресов обходится заказчику в сумму до 100$ [3]. Достаточно малая цена для распространения рекламы привлекает все больше клиентов, что является основной причиной для распространения спамерского бизнеса [4].

Можно отметить, что для распространения рассылок спамеру необходимы минимальные знания в области программирования и доступ в Интернет. Такие малые требования также привлекают людей, желающих подзаработать. Правда, более опытные организации подходят к работе намного серьезнее. Над реализацией атаки типа «СПАМ-рассылка» работают не только высококвалифицированные программисты, но и специалисты в области лингвистики, психологии и т.д. [2, 5 – 6].

Термин «спам» произошел от английского слова SPAM, которое расшифровывается как «Spicesham» (в переводе на русский «ветчина со специями») [1, 3, 7 – 13]. Термин «спам» появился в 1972 году после выхода в телеэфир английского шоу с группой MontyPythonFlyingCircus. В видео-ролике, посетители ресторана вынуждены слушать хор викингов, которые рекламировали консервы, потому что все блюда в меню этого ресторана состояли из содержимого консервов [4, 14 – 17]. Таким образом, реклама консервов SPAM стала ассоциироваться у потребителей с навязчивой нежелательной рекламой. На данный момент термин «СПАМ» обозначает нежелательное, навязанное, без согласия пользователя электронное сообщение.

В современном мире компьютерных технологий наибольший ущерб бизнесу, государству и пользователю приносят не целенаправленные атаки хакеров, а рассылаемая на электронную почту нежелательная реклама, которая является спамом [1, 7, 18 – 22].

Спам рассылка всегда несет ущерб не только программному обеспечению, но и экономике предприятия. По мнению экспертов, от 4 до 84 секунд затрачивает пользователь для определения и удаления спам-сообщения [5, 17, 23]. Компания AYAXI в рамках проекта Poll4Al провела опрос среди пользователей интернета в России. Опрос показал, что 61% пользователей получают СПАМ-сообщения чаще трех раз в неделю. Респонденты отметили, что подобные нежелательные письма являются причиной получения вирусов (около 61%) и приводят к трате личного времени (около 57%) [9].

Стоит отметить, что вред от СПАМ-сообщений получают не только пользователи сети, но также и крупнейшие компании. Так, более 75% входящей почты российского поставщика бесплатной почты MAIL.RU составляет спам. [3, 6]. Сотрудники предприятий затрачивает от 10 до 20 минут рабочего времени на проверку почты и удаление спам-сообщений. Для больших предприятий, где штат сотрудников больше 100 человек, ущерб экономике предприятия наносится значительный. По данным Российской консалтинговой компании ФБК, в России ущерб от спама составил почти два миллиарда долларов. Оценка, безусловно, спорная. Эта оценка основывается на исследовании количества человеко-часов, затраченных на просмотр и удаление спам-сообщений, приходящих на электронную почту сотрудников компаний [5].

Но кроме потери времени на удаление ненужной рассылки, основным ущербом от спам-рассылок является проникновение вредоносного программного обеспечения вместе с письмом, содержащим спам. Большое количество вирусов, троянских коней попадают к конечному пользователю благодаря спам-атаке [18]. Вредоносное ПО маскируется под файлы PDF, использует макросы документов MicrosoftWord [6], использует самораспаковывающиеся архивы ZIP [2] и т.д. Хакеры придумывают все более изощренные способы, чтобы обойти всевозможные антиспам-приложения и привлечь внимание пользователя.

Попадая на компьютер через электронную почту, вредоносные приложения специализируются на краже личной информации пользователя. Сканируя компьютер [11, 20, 34 – 39], вредоносное ПО может отправлять на удаленный сервер не только личные документы, но и собирать пароли, вводимые пользователем на

Объектом исследования является элемент взвешенной гетерогенной сети, подвергающийся деструктивному воздействию СПАМ-атак с вредоносными вложениями.

Предметом исследования является риск-анализ состояния элементов взвешенной гетерогенных сетей.

Цель исследования состоит в оценке и регулировании рисков, возникающих в взвешенных гетерогенных сетях, элементы которых подвергаются деструктивному воздействию атаки типа «СПАМ-рассылка». Для достижения цели представляется необходимым решить следующие **задачи**:

1. Классификация атак и исследование уязвимостей взвешенных гетерогенных сетей в контексте работы приложений при атаке на их элементы типа «СПАМ-рассылка» с вредоносными вложениями.
2. Построение риск-модели для пользователей гетерогенных сетей в условиях распространения атаки типа «СПАМ-рассылка» с вредоносными вложениями, основанной на ценностном подходе к оценке ресурса элементов взвешенной гетерогенной сети.
3. Разработка алгоритма и его численное моделирование для процесса управления информационными рисками в взвешенных гетерогенных сетях при деструктивном воздействии атаки типа «СПАМ-рассылка» с вредоносными вложениями.

На защиту выносятся:

1. Классификация атак и уязвимостей в взвешенных гетерогенных сетях при атаке типа «СПАМ-рассылка» с вредоносным вложением.
2. Риск-модель процесса деструктивного воздействия атаки типа «СПАМ-рассылка» с вредоносным вложением на элементы взвешенной гетерогенной сети.
3. Алгоритм управления информационными рисками в взвешенных гетерогенных сетях при деструктивном воздействии атаки типа «СПАМ-рассылка» с вредоносными вложениями.

Новизна результата:

1. Впервые проводится полный и комплексный риск-анализ атаки типа «СПАМ-рассылка» с вредоносным вложением во взвешенных гетерогенных сетях.

2. Алгоритм, в отличие от аналогов, впервые формализует процесс управления информационными рисками во взвешенных гетерогенных сетях при атаке «СПАМ-рассылка» с вредоносным вложением.

3. Впервые рассматривается риск-модель процесса деструктивного воздействия атаки типа «СПАМ-рассылка» с вредоносным вложением на элементы взвешенной гетерогенной сети.

Теоретическая значимость работы, состоит в том, что:

1. Доказаны положения, вносящие вклад в расширенное представление о явлении успешной реализации атаки типа «СПАМ-рассылка» на элементы взвешенной гетерогенной сети;

2. Применительно к проблематике работы, с получением обладающих новизной результатов, использован аппарат теории риск-анализа в отношении реализации атак типа «СПАМ-рассылка» с вредоносным вложением на элементы взвешенной гетерогенной сети;

3. Изложены положения и элементы теории для аналитической оценки ущерба, риска и эффективности защиты элементов взвешенных гетерогенных сетей, подвергающихся атаке типа «СПАМ-рассылка» с вредоносным вложением;

4. Проведена модернизация существующих математических моделей и алгоритмов, обеспечивающая возможность аналитической оценки и управления рисками, а также оценки эффективности защиты элементов взвешенных гетерогенных сетей, подвергающихся атаке типа «СПАМ-рассылка» с вредоносным вложением.

Практическая ценность работы заключается в том, что:

1. Классификация дает наиболее полную и логически взаимосвязанную картину процессов взаимодействия СПАМ-приложений во взвешенных гетерогенных сетях.

2. Модель, в силу своей аналитической природы, открывает практические перспективы оптимизации и регулирования информационных рисков в взвешенных гетерогенных сетях.

ЗАКЛЮЧЕНИЕ

В рамках работы были разработаны и дополнены методы регулирования СПАМ-рассылок с вредоносным вложением посредством ресурса взвешенной гетерогенной сети. Данные методы учитывают вероятности срабатывания СПАМ-фильтров, антивирусных систем, также данные методы нацелены на повышение СПАМ-грамотности пользователей сети Internet.

Также были предложены и реализованы имитационные модели СПАМ-атак с вредоносным вложением в гетерогенной сети. Результаты полученных моделей записали в сравнительную таблицу, и на основе полученных данных, был предложен оптимальный и наиболее эффективный метод реализации СПАМ-атаки во взвешенной гетерогенной сети. Рассчитаны значения ущерба и риска при реализации атаки СПАМ-рассылка.

Разработанная и реализованная имитационная модель подсистемы обнаружения и фильтрации СПАМ-злоумышленников была применена ко множеству взвешенной сети. Полученный результат был сравнен с реальными значениями, сделаны выводы об эффективности применения данной подсистемы обнаружения и блокирования СПАМ-сообщений.

Для анализа наполнителя сети e-mail рассылок был рассмотрены ресурс, потенциал, коэффициент баланса, показатель нормированной взвешенности сети, построена матрица ресурсов сети. Также предложена модель управления риском деструктивного воздействия атаки СПАМ-рассылка с вредоносным вложением.

В заключении работы можно сделать вывод о том, что на данный момент методов борьбы с атакой СПАМ-рассылка с вредоносным вложением большое количество. Наиболее эффективно методы борьбы срабатывают в комплексе. Поэтому для полноценной защиты пользователям от СПАМ-сообщений необходимо не только оценивать качество передаваемого наполнителя, но и объем этого наполнителя в единицу времени.

Полученные модели имеют гораздо более широкое применение, чем обеспечение вирусной защищенности ИТКС.