ОГЛАВЛЕНИЕ

8 (952) 106-88-60 vk.com/a.projectit a.projectit

8 (952) 106-88-60 vk.com/a.projectit a.projectit

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, за 2008 год 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

различных сайтах, делать скриншоты рабочей области экрана через заданный промежуток времени, собирать информацию о всех действиях пользователя [14, 21, 25]. Данная информация помогает не только получить доступ к личным аккаунтам пользователя, но и собрать статистическую информацию для дальнейшей атаки на данный компьютер. Так же, от имени пользователя вредоносное ПО может инициировать рассылку спам-сообщений на найденные на компьютере адреса электронной почты.

Согласно статистическим данным из «Лаборатории Касперского», установлено, что значительная часть атаки типа «СПАМ-рассылка» была разослана из России. За 2015 год из России было успешно реализовано более шести процентов спам-атак от общего количества мирового спама [8, 18]. Что обеспечило России вторую строчку в списке стран-источников спама. Лидером же по этому показателю оказались Соединенные Штаты Америки, у которых данный показатель превышал 15 % от общего количества спам-рассылок.

Россия попала в первую тройку стран по количеству пользователей, столкнувшихся с вредоносными вложениями в сообщениях. По подсчетам специалистов, на долю России пришлось более 6 % от всех вредоносных писем, разосланных по миру [8].

Поскольку злоумышленникам становится сложнее обходить спам-фильтры, они постоянно изобретают новые приемы. Например, во многих спам-сообщениях могут встречаться не классические ссылки URL, которые легко распознаются фильтрами, а QR-коды, помещенные непосредственно в теле письма. Кроме того, латинские буквы и цифры в доменах и IP-адресах часто заменяются спамерами на символы, которые похожи по виду, но взяты из других алфавитов и символьных систем. Для скрытия вредоносных вложений в сообщениях, спамеры используют архивы не самых популярных форматов – .cab, .ace.7z.z, .gz [6]. Это помогает им не только отвлекать внимание пользователей, знакомых в основном с широко распространенными расширениями .zip и .rar, но также и позволяет максимально сжимать файл и уменьшать таким образом размер письма.

Также, для привлечения внимания пользователя, злоумышленники в теле письма и в заголовках используют громкие мировые события. Например,

Олимпийские Игры, которые будут проведены в Бразилии только в 2016, однако уже в 2015 году встречаются упоминания об этих играх в спам сообщениях. "Нигерийские" спамеры активно "работают" с политическими событиями на Украине, войной в Сирии [18], выборами президента Нигерии и землетрясением в Непале, чтобы убедить получатели писем в правдивости историй, которую они придумали с целью выманивания денег [6].

В настоящее время большинство исследований спам-атак сфокусировано на содержании спама или на его источнике. Эти исследования плохо описывают поведенческую характеристику атак типа «СПАМ-рассылка». Именно анализ и классификация поведения спама помогает не только идентифицировать хакеров, но и предотвратить массовые спам-рассылки. Особенно актуальным является исследование спам-атак в гетерогенных сетях. Гетерогенная сеть – это сеть, которая образуется в результате соединения линиями точек (вершин), произвольно расположенных в пространстве. Такая сеть представляет собой некую геометрическую фигуру – каркас (пространственный граф), состоящий из вершин (v) и ребер(e). В некоторых случаях ребра образуют замкнутые контуры [45]. С другой стороны, «гетерогенная сеть» определяется как вычислительная сеть, соединяющая персональные компьютеры и другие устройства с различными операционными системами или протоколами передачи данных. Например, локальная вычислительная сеть (ЛВС), которая соединяет компьютеры под управлением операционных систем MicrosoftWindows, Linux и MacOS, является гетерогенной [46]. Термин «гетерогенные сети» также употребляется в беспроводных вычислительных сетях, где используются различные технологии для подключения. Например, беспроводная сеть, которая обеспечивает доступ через беспроводную локальную сеть и способна обеспечивать доступ, переключаясь на сотовую связь, также называется гетерогенной сетью.

В современных сетях большое значение имеют веса вершин и дуг сети. Включенные в метрику сети, эти показатели позволяют дать более качественную оценку. Такие сети, учитывающие веса вершин и дуг, носят название взвешенные, когда каждому элементу сети ставится в соответствие некоторый собственный вес. Исследование подобных сетей в контексте обеспечения их безопасности требует

проведения риск-анализа, для которого необходимо оценить возможный ущерб. Возможный ущерб может быть оценен как количество пораженных атакой вершин и дуг. Но, так как современные сети неоднозначны, то веса вершин существенно отличаются друг от друга в зависимости от их степени. Наполнитель больше концентрируется в вершинах с высокой степенью, и через них в единицу времени проходят наибольшие объемы наполнителя [1]. Таким образом, вершины с высокой степенью не сопоставимы с вершинами, имеющими значительно меньшую степень. Подобный факт заставляет отказаться от традиционных метрик и проводить риск-анализ только взвешенных гетерогенных сетей.

Так как наполнителем в подобных сетях является информация, то для определения ценности вершин необходимо применять один из методов определения ценности информации. Если объем информации – величина объективная, то ценность информации – субъективна для вершин сети и обусловлена ее функциональным назначением и стоящими перед ней целями и задачами. Отсюда, для принятия решения, необходима информация определенного потенциала. Увеличение объема информации и снижение ценности контента, принятого во внимание при принятии решения, снижает правильность этого решения в вершине сети. Этому негативному явлению способствует СПАМ. СПАМ-сообщение представляет собой контент, сокращающий потенциал сети и ее вершин [47]. Поэтому, качественная фильтрация информации, поступающей в вершины, и уничтожение СПАМ-сообщений напрямую влияют на эффективность функционирования вершины сети в отдельности, а с учетом веса вершин – и на всю сеть в целом.

По причине того, что элементы гетерогенной сети являются разнообразными как платформенно, так и программно, их рассмотрение позволит разработать более универсальный подход для оценки такого явления как СПАМ-атаки с вредоносными вложениями на взвешенные гетерогенные сети.

Актуальность исследования обусловлена следующим:

- злоумышленники постоянно изобретают новые приемы для реализации атаки спам-рассылка с вредоносным вложением, усложняется маскировка

вредоносного вложения в спам-сообщениях, усложняется определение адреса отправителя спам-сообщения;

- в России растет доля злоумышленников, реализующих атаки типа «СПАМ-рассылка» с вредоносным вложением от общего мирового числа спам-атак.
- с развитием новых уловок спамеров, для предотвращения подобных атак необходимо построение риск-модели для пользователей взвешенных гетерогенных сетей в условиях распространения атаки типа «СПАМ-рассылка» с вредоносными вложениями.

В связи с этим представляется актуальным развитие научно-методического обеспечения в данной области, включая изучение угроз, возникающих при проведении атак типа «СПАМ-рассылка» с вредоносным вложением, и связанных с ней рисков с точки зрения оценки и управления этими рисками с целью повышения защищенности как элементов, так и всей гетерогенной сети в целом.

Степень разработанности темы исследования. Касательно вопросов обеспечения информационной безопасности [15, 38–39, 48–59] опубликовано достаточно большое количество материалов на тему атак типа «СПАМ-рассылка» [7, 57]. В данных материалах опубликованы не только основные типы спам-сообщений с вредоносным вложением [16, 65], алгоритмы реализации атаки [40, 51, 52], этапы развития спам-рассылок [13, 43, 66], анализ поведения спам-рассылок [11, 67], подробный анализ основных методов реализации атаки [10, 16, 20, 37, 68], но и основные виды спам-фильтров, средств методов защиты и противоборства [7, 31, 57, 69, 70]. Также рассматривались вопросы управления рисками [11, 36, 38 – 39, 57–58] и оценки живучести систем [38, 54–56, 58]. Но в тоже время совсем не уделено внимание проблеме риск-анализа атаки типа «СПАМ-рассылка» во взвешенных гетерогенных сетях, отсутствует риск-модель по рассматриваемой атаке, по которой можно определить основные показатели системы, такие как ущерб, живучесть, эпистойкость и другие. Совершенствование методологии риск-анализа с целью повышения защищенности гетерогенных сетей от атаки типа «СПАМ-рассылка» представляется актуальным.

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.

3. Алгоритм предлагает практический инструмент программного управления информационными рисками атаки типа «СПАМ-рассылка» на элементы в взвешенных гетерогенных сетях.

Методы исследования. В исследовании используются методы теории вероятностей и математической статистики, методы системного анализа. Также применяется теория вероятности и математической статистики, используется математический анализ, применяются методы теории рисков и теории чувствительности функций.

Ожидаемые результаты и их новизна. В качестве ожидаемых результатов исследования можно выделить: анализ основных параметров атаки СПАМ-рассылка с вредоносным вложением; разработка методов регулирования ресурса атаки СПАМ-рассылка с вредоносным вложением во взвешенных гетерогенных сетях; математическое и имитационное моделирование алгоритма противоборства атаке СПАМ-рассылка с вредоносным вложением во взвешенной гетерогенной сети.

Достоверность и обоснованность результатов и выводов обусловлены корректным построением и применением моделей, соответствующим реальным механизмам реализации СПАМ-атаки с вредоносным вложением во взвешенных гетерогенных сетях, а также обобщением и доработкой существующих алгоритмов и методов противоборств других авторов.

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.

На данный момент существует большое количество методов управления рисками деструктивного воздействия СПАМ-атак с вредоносным вложением. Каждый из методов управления заслуживает отдельного подробного анализа и моделирования. Для дальнейшей разработки дополнительных методов противодействия СПАМ-атакам в гетерогенных взвешенных сетях необходимо выделить основные направления исследований:

– Учет взвешенности дуг и токсичности распространяемого контента в гетерогенной взвешенной сети обмена e-mail сообщениями с учетом типа СПАМ-сообщения;

– Риск-анализ СПАМ-атак на дуги сети с высокой центральностью в контексте блокирования связей;

– Управление эпистойкостью взвешенной сети, подвергающейся СПАМ-атакам с вредоносным вложением;

– Построение обобщенной имитационной модели комплексного противодействия основным видам СПАМ-атак;

– Построение риск-моделей деструктивного воздействия основных видов СПАМ-атак на пользователей взвешенной гетерогенной сети обмена e-mail сообщений.