Содержание

ВВЕДЕНИЕ

Актуальность исследования

Глобальные и локальные вычислительные сети проникли во все сферы человеческой жизни, от ведения предпринимательской деятельности до личной жизни. Вести переговоры и отправлять письмо по сети Интернет – легко и удобно.

Электронная почта - один из наиболее широко используемых видов сервиса, как в корпоративных сетях, так и в Интернет. Она является не просто способом доставки сообщений, а важнейшим средством коммуникации, распределения информации и управления различными процессами в бизнесе. Роль электронной почты становится очевидной, если рассмотреть функции, которые выполняет почта:

- обеспечивает внутренний и внешний информационный обмен;
- является компонентом системы документооборота;
- формирует транспортный протокол корпоративных приложений;
- является средством образования инфраструктуры электронной коммерции.

Благодаря выполнению этих функций электронная почта решает одну из важнейшихна настоящий момент задач - формирует единое информационное пространство**.** В первую очередь это касается создания общей коммуникационной инфраструктуры, которая упрощает обмен информацией между отдельными людьми, подразделениями одной компании и различными организациями.

Использование электронной почты для обмена информацией между людьми как внутри отдельно взятой организации, так и за ее пределами способно коренным образом изменить технологии и методы ведения дел. Переход к обмену документами в электронном виде открывает новые возможности для повышения эффективности труда и экономии средств и времени.

Электронная почта обладает многочисленными достоинствами, но именно из-за этих достоинств возникают основные риски, связанные с ее использованием. К примеру, доступность электронной почты превращается в недостаток, когда пользователи начинают применять почту для рассылки вредоносного программного обеспечения (ПО), спама, легкость в использовании и бесконтрольность приводит к

утечкам информации, возможность пересылки разных форматов документов и т.д.

В конечном итоге любой из этих рисков может привести к серьезным последствиям для компании. Это и потеря эффективности работы, и снижение качества услуг информационных систем, и разглашение конфиденциальной информации. Недостаточное внимание к данной проблеме грозит значительными потерями в бизнесе.

Вредоносные программы создаются специально для несанкционированного уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы и черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников (инструменты для взлома, конструкторы полиморфного вредоносного кода и т.д.)[10].

Сетевой червь - тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.В процессе размноженияпо каналам электронной почты червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе[10].

Особое место в списке сетевых неприятностей занимают так называемые «почтовые черви». По сути, эти программы ничем не отличаются от обычных вирусов, кроме способа распространения — через электронную почту. Червь располагается в прилагаемом к письму файле и активируется при его запуске[36].

А поскольку активное использование электронной почты в качестве инструмента предпринимательства стало неотъемлемым, возникает угроза проникновения почтового червя в систему.

Почтовый червь – это отдельная, самостоятельно размножающаяся компьютерная программа. Другими словами, это вирус, который не встраивается в заражаемые файлы. Вместо того чтобы передаваться от файла к файлу на одном

компьютере, червь использует для распространения своего кода интернет-соединение[16].

Существует несколько разновидностей почтовых червей. Одни распространяются в виде исполняемых файлов, другие – в виде скрипт-файлов, вложенных в почтовые сообщения, третьи – в виде скриптов, встроенных в HTML-сообщения. Общим для всех почтовых червей является то, что для их распространения используется электронная почта, обычно в сочетании с методами социальной инженерии, призванными убедить наивных пользователей запустить вредоносный код[26].

Социальная инженерия представляет собой комплекс нетехнических методов, применяемых с целью заставить пользователей пренебречь стандартными мерами безопасности. В контексте вирусов и червей это, как правило, означает прикрепление вредоносного кода к совершенно безобидному на первый взгляд почтовому сообщению.Кроме того, само электронное письмо может быть создано с таким расчетом, чтобы выглядеть не просто безвредным, но даже, несомненно, полезным[40].

Стоит отметить то, что на практике злоумышленники часто сочетают в одной и той же программе различные типы угроз. Например, некоторые почтовые черви способны маскироваться под троянские программы или подобно вирусам заражать исполняемые файлы на локальном диске [14].

Ущерб, наносимый вредоносными программами, как почтовый червь, может выражаться не только в уничтожении, искажении или похищении информации, приведении в нерабочее состояние программного обеспечения, а значит, компьютера и системы в целом, но и в значительных затратах времени и сил администраторов на обнаружение и распознавание атак, фильтрацию внешних сообщений, тестирование и перезагрузку систем [36].

Успешность современного предприятия зависит от различных информационных систем, обеспечивающих его жизнедеятельность. Нарушение функционирования любой из них может нанести значительный ущерб, вплоть до банкротства компании.

Поэтому тема диплома, направленная на исследование, защиту, предотвращению минимизацию ущерба информационно-телекоммуникационной системы, атакуемой вредоносным программным обеспечением, является актуальной.

Соответствие темы диплома специальности.

Данная работа посвящена изучению последствий проникновения в информационно-телекоммуникационные системы вредоносного программного обеспечения - почтовых червей, предотвращения нанесения ими ущерба ИТКС, иначе говоря, обеспечению безопасности ИТКС. Поэтому тема данной работы соответствует специальности «Безопасность телекоммуникаций».

Объектом исследования являются информационно-телекоммуникационные системы подвергающиеся воздействиям вредоносного программного обеспечения типа «почтовый червь».

Предметом исследования является риск-оценка информационной устойчивости информационно-телекоммуникационных системв условиях реализации воздействия типа «почтовый червь».

Цель и задачи исследования.

Целью настоящей работы является исследование ИТКС, атакуемых сетевым вредоносным программным обеспечением типа «E-mail-Worm (почтовые черви)».

Для реализации данной цели необходимо решить следующие задачи:

1. Провести сравнительную характристику различных модификаций исследуемого вредоносного программного обеспечения «E-mail-Worm (почтовые черви)» и способы проникновения в информационную систему.
2. Разработать модель процесса атаки и распространения вредоносного ПО класса «E-mail-Worm (почтовые черви)» на ИТКС.
3. Разработатьриск-модели ИТКС, подвергающейся атаке программы класса «E-mail-Worm (почтовые черви)», описать еепараметры.

4. Сравнить результаты прогнозирования, полученные с помощьюмодели, со статистическими данными о распространении вредоносного программного обеспечения класса E-mail-Worm.

5. Провести оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования.

Методы исследования

Для решения поставленных задач необходимо использовать следующие методы: теории вероятности, теории риска, теории чувствительности, теории управления, элементы теории сложных систем, элементы теории экономического планирования.

Обоснование математической модели

Для исследования воздействия почтовых червей типа «E-mail-Worm» на ИТКС в дипломном проекте будет проводиться математическое моделирование, которое представлен в виде сетей Петри-Маркова, так как данный математический аппарат в наибольшей степени отражает процесс распространения во времени почтового червя, так же для описания механизма заражения системы представлена детерминированная эпидемиологическая SEIS модель.

На защиту выносятся следующие основные положения работы:

1. Классификация вредоносного программного обеспечения типа «E-mail-Worm (почтовые черви)», способов их проникновения на компьютеры пользователей;

2. Вероятностная модель процесса атакивредоносного ПО класса «E-mail-Worm (почтовые черви)» на ИТКС;

3. Риск-модельИТКС, подвергающейся атаке программы класса «E-mail-Worm (почтовые черви)»;

4. Оценка экономической эффективности,а также расчет сметной стоимости и договорной цены проведенного исследования.

Научная новизна исследования

1. В дипломной работе было проведеноразбиение целого классавредоносного программного обеспечения типа «E-mail-Worm (почтовые черви)» на отдельные его виды, описаны способы их проникновения на компьютеры пользователей, выработанаих обобщенная структура.

2. Проведено моделирование процесса заражения отдельного элемента ИТКС с помощью сетей Петри-Маркова на отдельные виды «почтового червя», что отличается своей детальность рассмотрения деструктивных воздействий данного вредоносного ПО.

3. Применение эпидемиологической SEIS модели для изучения распространения такого вредоносного ПО, как почтовый червь при попадании в информационную систему, а также для возможности определения ущерба, наносимого системе при реализации данной атаки.

Структура и объем работы.Работа состоит из введения, пяти глав, заключения и списка литературы, включающего 112 наименований.

Содержание работы изложено на 170 странице машинописного текста, проиллюстрировано 36 рисунками и 27 таблицами.

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

projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT

ЗАКЛЮЧЕНИЕ

Данная дипломная работа посвящена исследованию атак вредоносного программного обеспечения типа «E-mailworm» на информационно-телекоммуникационные системы на основе моделирования процесса заражения отдельного элемента системы, распространения в пределах системы, а так же анализа рисков. В ходе ее выполнения были получены следующие основные результаты:

1. На основании выполненных исследований была разработана аналитическая модель процесса проникновения вредоносного программного обеспечения типа «E-mailworm», дополняющая концепцию моделирования процессов распространения данного типа сетевых атак, заключающаяся в адаптации математических графовых моделей.

2. Была применена имитационная эпидемиологическая SEIS модель в контексте распространения почтового червя в системе, что позволяет в большей мере проследить поведение данного класса вредоносного ПО, выявить закономерности его распространения, рассчитанные с помощью данной модели переходные состояния и вероятности заражения при нахождении почтового червя в системе, могут служить для предотвращения возможных ущербов.

3. При приведении исследований был применен комплекс методов, таких как теории случайных графов, имитационного моделирования, математической статистики и системного анализа, что позволило получить адекватную модель атаки на ИТКС почтовым червем.

4. Проведенное моделирование атак вредоносного ПО класса «почтовый червь» для различных его видов доказывает состоятельность в применении изучения подобных сетевых атак методов имитационного моделирования.

5. Путем математического моделирования была обоснована применимость эпидемиологической SEISмодели для нахождения ущерба информационно-телекоммуникационной системы.

6. Разработана аналитическая модель процесса реализации атаки вредоносного ПО класса «почтовый червь». Разработаны аналитическая риск - модель для компонент информационных систем, риск - модели для систем, которых подвергаются совместному воздействию соответствующих дестабилизирующих факторов, а так же для систем, компоненты, компоненты которых подвергаются несовместному воздействию соответствующих дестабилизирующих факторов.

7. Выявлены проблемы защиты ИТКС от сетевых атак типа «почтовый червь», связанные с использованием электронной почты. Решением этой проблемы является выявление способов попадания в систему, построение риск-модели, способных выявить уязвимые компоненты систем и снизить риски реализаций атак типа «почтовый червь».

8. Получены аналитические выражения функций чувствительности по всем параметрам, описывающим риск – модели для данной атаки. Данные выражения получены для отдельных компонент системы, компоненты которых подвергаются несовместному воздействию дестабилизирующих факторов, а так же для систем, компоненты которых подвергаются совместному воздействию дестабилизирующих факторов. Построены соответствующие уравнения движения риска.

9. Идея работы базируется на разбиении целого класса вредоносного программного обеспечения типа «почтовый червь» для более детального рассмотрения его деструктивных действий в зависимости от вида.

10. В процессе работе использованы результаты применения современных систем сбора и обработки исходной информации, таких как статистические данные. Для этого применялись методы их анализа и предварительной обработки. Путем такого научного метода, как аппроксимация было обосновано применение имитационного подхода для определения выражения ущерба.

11. В ходе исследования изучены причинно-следственные связи возникновения рисков при атаках почтовыми червями. Это осуществлено при построении сетей Петри-Маркова.

12. Результаты работы внедрены в технологию разработки средств автоматизации в ОАО "Концерн "Созвездие" и были изложены на научно-техническом совещании.

13. Полученные в данной работе результаты являются актуальными для предотвращения распространения вредоносного программного обеспечения - почтовый червь в уже существующих информационных системах.

14. Проведена оценка экономических показателей эффективности разработанной математической модели защиты информации в информационно-телекоммуникационной системе.

15. Личный вклад автора состоит в сборе информации об исследуемой задаче, в обработке и интерпретации экспериментальных данных, синтезе по ним математической модели и ее исследовании.

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