УДК 004

# РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ РИСКАМИ ДЛЯ КОРПОРАТИВНОЙ СЕТИ, АТАКУЕМОЙ ВРЕДОНОСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ТИПА СЕТЕВОЙ ЧЕРВЬ

***© 2020 Д. Д. Зеленин***

*Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный лингвистический университет» (г. Москва, Россия)*

*В работе представлено исследование атак вредоносного программного обеспечения типа Email-worm на корпоративные сети на основе моделирования процесса заражения отдельного компьютера сети, распространения в пределах всей системы, оценка и управление риском информационной безопасности распределенных компьютерных систем, в частности управление риском информационной безопасности распределенных компьютерных систем в условиях атаки типа Email-Worm.*

*Ключевые слова: вредоносное программное обеспечение, почтовый червь, сети Петри-Маркова, имитационное моделирование, корпоративная сеть, риск-модель, управление рисками ИБ.*

**Введение**

В условиях мировой глобализации все чаще встает угроза безопасности различных данных, в том числе и персональных. Вредоносному воздействию с помощью разнообразного программного обеспечения подвергаются как отдельные пользователи, так и крупные корпорации. [1]

Анализ актуальных проблем безопасности в компаниях показывает, что самой распространенной угрозой является вредоносное программное обеспечение (ВПО). Согласно данным «Positive technologies», 56 % всех атак в 2019 году было проведено именно так [1]. Сетевые черви являются одним из самых распространенных типов ВПО и по сей день.

Вред, который способны причинить почтовые черви, выражается не только в нарушении целостности информации, проявляющейся в ее уничтожении, похищении или искажении, а также выводе из строя программного обеспечения. Он также измеряется также в ощутимых временных затратах и силах обслуживающего персонала, затраченных на выявление и распознавание вредоносных атак, фильтрацию Интернет трафика, проверку и перезагрузку системы.

Зеленин Данила Денисович – Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный лингвистический университет» (ФГБОУ ВО МГЛУ), Институт информационных наук, Кафедра международной информационной безопасности, Студент ИИН 1-16-7, danilking32@mail.ru.

Современный бизнес базируется на информационных технологиях, обеспечивающих эффективную коммуникацию и обратную связь, нарушение или изменение которой может привести к значительным издержкам и, следовательно, убыткам. Именно поэтому важно обеспечить необходимую и надежную защиту всех каналов коммуникации, в том числе качественную почтовую связь, устойчивую к различным видам вредоносного программного обеспечения.

Таким образом, исследование управления информационными рисками информационных систем, атакуемых «червями», является актуальным.

В данной работе изучаются возможные способы проникновения вредоносного программного обеспечения типа почтовый червь в информационные системы, а также последствия заражения данным программным обеспечением.

Объектом исследования является корпоративная сеть, подвергаемая деструктивным воздействиям атак с использованием почтового червя.

Предметом исследования является риск-модель корпоративной сети под воздействием типа почтовый червь.

Целью работы является разработка риск-модели корпоративной сети, атакуемой вредоносным программным обеспечением типа почтовый червь, в целях обеспечения требуемого уровня защищенности и эффективности исследуемого объекта.

Для реализации данной цели решаются следующие задачи:

- дана общая характеристика исследуемому вредоносному программному обеспечению типа червь, а также способам заражения им компьютерных сетей, приведена классификация данного типа вредоносного воздействия;
- построена вероятностная модель успеха для известных разновидностей атак почтовых червей на компьютерные сети;
- дана аналитическая оценка ущербов для проникновения вышеуказанных разновидностей почтовых червей в
- построены аналитические риск-модели и даны рекомендации по управлению рисками в условиях атак почтовыми червями.

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

Для исследования воздействия червей типа почтовый червь на распределенные компьютерные сети проводилось математическое моделирование.

Научная новизна исследования:

– построены вероятностные модели успеха для всех известных разновидностей атак почтовых червей на ИС;

– проведена аналитическая оценка ущербов для проникновения рассматриваемых разновидностей почтовых червей в ИС;

– построены аналитические риск-модели ИС, и выработаны рекомендации по управлению рисками в условиях атак почтовыми червями.

**Оценка и управление риском информационной безопасности распределенных компьютерных систем**

«Оценкой рисков называют оценку угроз для информации и средств ее обработки, возможного ущерба для них в случае нарушения безопасности, их уязвимостей, а также возможности их возникновения. Посредством методической оценки рисков происходит определение требований к безопасности. Методы оценки рисков могут применяться ко всей организации или только к ее отдельным частям, а также к отдельным информационным системам, системным компонентам и сервисам – в зависимости оттого, что окажется наиболее практичным, реалистичным и полезным» [14].

Оценка рисков состоит из систематического анализа следующих показателей:

– ущерб для системы, который может возникнуть при нарушении безопасности. При этом следует учитывать возможные последствия утраты целостности, конфиденциальности или доступности информации и других ресурсов;

– оценка вероятности такого нарушения безопасности с учетом известных угроз, уязвимостей и реализованных средств защиты от них.

Результаты такой оценки помогают определить необходимые действия и приоритеты для управления рисками, связанными с информационной безопасностью, а также для реализации выбранных средств защиты от этих рисков.

Для того чтобы охватить различные части организации или отдельные информационные системы, может потребоваться выполнить процесс оценки рисков и выбора средств защиты несколько раз [15].

Управлением рисками называют процесс определения, контроля и уменьшения или полного устранения рисков для информационной безопасности, которые могут повлиять на информационные системы.

Основной замысел мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и рациональные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки и остаются таковыми. Таким образом, управление рисками включает в себя два вида деятельности, которые чередуются в виде цикла:

– (пере)оценка или первичное измерение рисков;

– выбор эффективных и рациональных защитных средств (нейтрализация рисков).

По отношению к найденным рискам возможны следующие действия:

– ликвидация риска (в случае устранения причины);

– уменьшение риска (использования дополнительных защитных средств);

– принятие риска, а также последующая выработка плана действия в соответствующих условиях;

– переадресация риска.

Весь процесс управления рисками можно разделить на несколько этапов:

– выбор объектов, подвергающихся анализу, а также уровня детализации их рассмотрения;

– выбор методологии оценки рисков;

– идентификация активов;

– анализ угроз и их последствий, выявление уязвимых мест в защите;

– оценка рисков;

– выбор возможных защитных мер;

– реализация и контроль эффективности выбранных мер;

– оценка остаточного риска [15].

К выбору защитных средств (нейтрализации рисков) относятся этапы: выбор возможных защитных мер, а также реализация и контроль эффективности выбранных мер, все остальные этапы относятся к оценке рисков. Становится очевидным, что управление рисками - процесс циклический. В целом же можно сказать, что последний этап - это оператор конца цикла, предписывающий вернуться к его началу. Риски необходимо контролировать постоянно, периодически проводя их переоценку. Важен также и тот факт, что качественно выполненная и детально оформленная первоначальная оценка рисков способна существенно упростить последующую деятельность.

Необходимо интегрировать в жизненный цикл информационной системы (ИС) управление рисками – как и любую другую деятельность в области информационной безопасности. В таком случае эффект окажется наибольшим, а затраты – минимальными. Управление рисками в жизненном цикле ИС включает в себя несколько этапов: этап инициации – следует учесть известные риски при выработке требований к системе в целом и средствам безопасности в частности; этап закупки (разработки) – знание рисков поможет выбрать соответствующие архитектурные решения, играющие ключевую роль в обеспечении безопасности; этап установки – следует учитывать выявленные риски при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию; этап эксплуатации – управление рисками должно сопровождать все ключевые изменения в системе; этап вывода системы из эксплуатации - управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

**Предварительные результаты**

На подготовительном этапе были рассчитаны дифференциальные и относительные коэффициенты чувствительности риска для отдельных компонентов распределенных компьютерных систем при реализации атак вредоносного программного обеспечения типа Email-worm или почтовый червь. С помощью данных коэффициентов становится возможным построение соответствующих матриц чувствительности риска.

С помощью полученных выражений движения риска возможно рассмотрение влияния параметров вероятностного распределения на функцию риска, а также минимизация величины риска не только для значений ущерба.

**Управление риском информационной безопасности распределенных компьютерных систем в условиях атаки типа Email-Worm**

Для того чтобы снизить уровень риска системы возможно применение стратегии изменения параметров плотности вероятности наступления ущерба в её составных частях. Решение данной задачи требует использования функций чувствительности риска к изменению параметров, которые его определяют.

Основная цель анализа чувствительности состоит в сравнительном анализе влияния различных параметров на изменение общего уровня риска информационной безопасности. Стадии проведения анализа чувствительности: первая – выбор допустимого уровня риска; вторая - выбор относительного параметра, предположив, что именно этот параметр влияет на величину ущерба, а соответственно и на риск относительной информационной безопасности.

Для атаки вредоносного программного обеспечения типа Email-Worm такими параметрами могут являться:

– распространенность почтового червя, т. е. какое количество потенциально зараженных писем уже находится в системе;

– момент времени, в который произошла атака данным вредоносным программным обеспечением, т.к. попадание почтового червя может произойти в различные периоды жизни системы - начальный момент жизни системы, когда ущерб от реализации будет минимальный, и момент максимальной полезности системы, когда ущерб, нанесенный вредоносным ПО, будет наиболее значительным;

– период действия атаки почтового червя;

– длительность периода прохождения почтового червя через установленные меры защиты.

Алгоритм управления рисками на основе анализа параметров (чувствительности включает в себя несколько этапов:

– расчет функции чувствительности по каждому из параметров отдельно, затем построение графика полученной функции, позволяющего сделать вывод о наиболее критическом параметре, влияющего на уровень ущерба;

– расчет величины коэффициентов чувствительности риска для выбранных параметров, а также их ранжирование от наибольшего значения коэффициента чувствительности к наименьшему;

– выбор параметра, для которого значение коэффициента чувствительности максимально и дальнейший расчет значения риска с учетом изменения выбранного параметра;

– сравнение допустимого риска системы с полученным на предыдущем этапе – если риск приемлем, алгоритм заканчивается (т.к. определен параметр, влияющий на уровень риска), в противном случае переходим к расчету следующего коэффициента чувствительности.

Данный алгоритм в упрощенном виде представлен на рисунке.

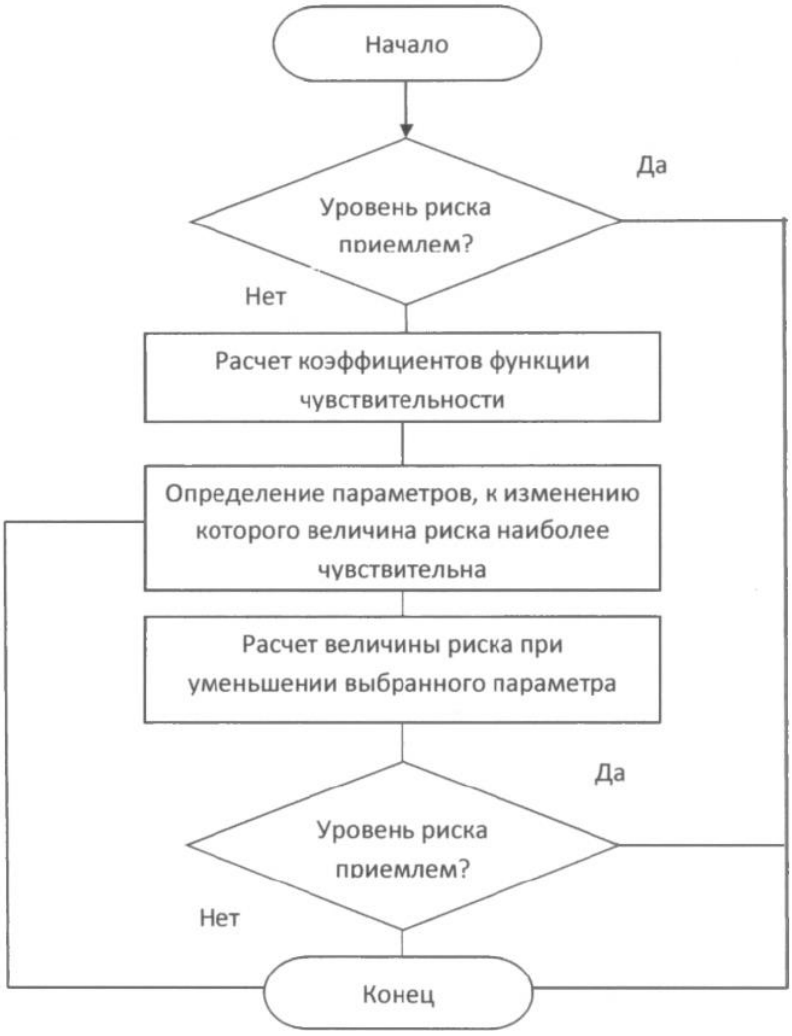


Рисунок. Алгоритм управления рисками на основе анализа параметров чувствительности.

Описанный метод является хорошим примером влияния отдельных исходных параметров на общий риск информационной системы.

Основным недостатком данного метода является то, что изменение одного фактора рассматривается изолированно, в то время как на практике многие параметры могут влиять на уровень риска отдельно и в совокупности друг с другом.

**Выводы**

В работе представлено исследование атак вредоносного программного обеспечения типа Email-worm на корпоративные сети на основе моделирования процесса заражения отдельного компьютера сети, распространения в пределах всей системы, а также анализа рисков. В ходе ее выполнения были получены следующие основные результаты:

На основании проведенных исследований была разработана аналитическая модель процесса проникновения вредоносного программного обеспечения типа Email-worm дополняющая концепцию моделирования процессов распространения данного типа сетевых атак, заключающаяся в адаптации математических графовых моделей.

Также была применена имитационная эпидемиологическая SIS модель в контексте распространения почтового червя в системе, что позволяет в большей мере проследить поведение данного класса вредоносного программного обеспечения, выявить закономерности его распространения в компьютерной сети, рассчитанные с помощью данной модели переходные состояния и вероятности заражения при нахождении почтового червя в системе, могут служить для предотвращения возможных ущербов.

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 компьютерные сети почтовым червем.

Проведенное моделирование атак вредоносного программного обеспечения класса почтовый червь. для различных его видов доказывает состоятельность в применении изучения подобных сетевых атак с помощью метода имитационного моделирования.

Для обоснования выбора функции ущерба проведена параметрическая аппроксимация статистических данные распространения вредоносного программного обеспечения типа Email- Worm с целью выбора аналитической функции ущерба, с использованием в качестве метода аппроксимации – алгоритма Левенберга-Марквардта, а в качестве инструмента – набора пользовательских графических интерфейсов Curve Fitting Toolbox созданных в вычислительной среде MATLAB®.

Разработана аналитическая модель процесса реализации атаки вредоносного программного обеспечения типа Email-worm.

Выявлены проблемы защиты компьютерной сети от сетевых атак типа почтовый червь, связанные с использованием электронной почты. Решением этой проблемы является: выявление способов проникновения в систему, построение риск-моделей, способных выявить уязвимые компоненты систем и снизить риски реализаций атак типа Email-worm.

Получены аналитические выражения функций чувствительности по всем параметрам, описывающим риск-модели для данной атаки.

Идея работы в целом базируется на разбиении целого класса вредоносного программного обеспечения типа Email-worm на отдельные виды с целью более детального рассмотрения его деструктивных действий в зависимости от вида.

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.

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

Полученные в данной работе результаты являются актуальными для предотвращения распространения вредоносного программного обеспечения типа Email-worm в существующих компьютерных системах.

**ЛИТЕРАТУРА**

1. Positive Technologies. Актуальные киберугрозы. Электронное издание 2019//URL [https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/] Дата обращения 12.03.2020

2. Код безопасности. Защита информации на рабочих станциях и серверах [Электронный ресурс] URL: https://www.securitycode.ru/upload/iblock/7f2/zaschita_informacii_rabochih_stanciy.pdf Дата обращения 04.04.2020

3. Brad Duncan. MyDoom Still Active in 2019.// PaloAlto Networks Электронное издание URL [https://unit42.paloaltonetworks.com/

mydoom-still-active-in-2019/] Дата обращения 04.04.2020

4. Мальков М. В. Сети Петри и моделирование / М. В. Мальков, С. Н. Малыгина // Труды Кольского научного центра РАН. – 2010. – № 3.

5. Вероятностные аналитические модели сетевой атаки с внедрением вредоносного программного обеспечения / В. И. Борисов [и др.] // Информация и безопасность. – 2013. – Т. 16. – № 1. – С. 5-30.

6. Моделирование компьютерных атак на распределенную информационную систему / Корниенко А. А. [и др.] // Известия Петербургского университета путей сообщения. – 2018.

7. Котенко И. В. Аналитические модели распространения сетевых червей / И. В.Котенко, В. В. Воронцов // Труды СПИИРАН. Вып. 4. – СПб.: Наука, 2007.

8. Бутузов В. В. К вопросу обоснования функции ущерба атакуемых систем / В. В.Бутузов, А. В. Заряев // Информация и безопасность. – 2013. – Т. 16. – № 1. – С. 47-54.

9. Canadian Institute for Cybersecurity NSL-
KDD dataset. // URL:https://www.unb.ca/cic/datasets/nsl.html Дата обращения 08.04.2020.

10. GitHub. NSL-KDD dataset https://github.com/defcom17/NSL_KDD. Дата обращения 08.04.2020

11. Вуколов Э. А. Основы статистического анализа. Практикум по статистическим методам и исследованию операций с использованием пакетов statistica и excel / Э. А. Вуколов; изд. 2. – М.: Инфра-М, 2015.

12. Радько Н. М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н. М. Радько, И. О. Скобелев. – М. : Радио Софт, 2010.

13. Радько Н. М. Аналитическое моделирование процессов реализации удаленных атак при помощи аппарата теории сетей Петри-Маркова: сниффинг пакетов в сети без коммутаторов / доступа / Н. М. Радько, И. О. Скобелев // Информация и безопасность: Регион, науч.-техн. журнал. – 2008. – № 4. – С. 585-588.

14. Скрыль С. В. Информационная безопасность телекоммуникационных систем (технические вопросы) / С. В. Скрыль. – М.: Радио и связь, 2004.

15. Скрыль С. В. Показатель эффективности защиты информации в автоматизированных системах / С. В. Скрыль // Материалы Международной конференции. Информатизация правоохранительных систем. – 1997. – № 3. – С. 36-38.

## DEVELOPMENT OF A RISK MANAGEMENT MODEL FOR A CORPORATE NETWORK ATTACKED BY MALICIOUS SOFTWARE SUCH AS A NETWORK WORM

***© 2020 D. D. Zelenin***

*Federal State Budgetary Educational Institution of Higher Education*
*«Moscow State Linguistic University» (Moscow, Russia)*

*The paper presents a study of malicious software attacks such as Email-worm on corporate networks based on modeling the process of infection of an individual computer in the network, spreading throughout the entire system, assessing and managing the information security risk of distributed computer systems, in particular, managing the information security risk of distributed computer systems in Email-Worm attack conditions.*

*Keywords: malicious software, email worm, Petri-Markov networks, simulation, corporate network, risk model, information security risk management.*