DOI 10.36622/VSTU.2023.26.3.013
УДК 004.056.57

ПОЛИГОННЫЕ КИБЕРУЧЕНИЯ НА ПРИМЕРЕ МОДЕЛИРОВАНИЯ КОМПЬЮТЕРНЫХ ЭПИДЕМИЙ СЕТЕЙ

Е.А. Москалева, А.И. Шеншин, И.А. Каданцев

В настоящее время повсеместное применение киберполигонов продолжает набирать обороты, расширяя возможности и повышая эффективность информационной защиты систем. Количество и качество преднамеренных информационных угроз, неуклонно растет, включая атаки с применением вредоносного программного обеспечения. Значительную угрозу представляют вредоносы, способные порождать масштабные сетевые эпидемии, поскольку их деструктивное воздействие позволяет быстро и эффективно наносить значительный финансовый и репутационный ущерб организациям и частным лицам. Несмотря на значительный прогресс в исследовании в области сетевой эпидемиологии, актуальным остается вопрос эффективной оценки и регулирования рисков возникновения компьютерных эпидемий в сетях. В статье обсуждается методика моделирования эпидемии сети, учитывающая диффузию вирусного программного обеспечения. Рассматриваемая методика предусматривает программную реализацию моделирования процессов размножения и диффузии вирусного программного обеспечения в атакуемой телекоммуникационной сети. На основе методики проводились киберучения на базе киберполигона кафедры систем информационной безопасности Воронежского государственного университета.

Ключевые слова: киберполигон, эпидемический процесс, компьютерная эпидемия, вредоносное программное обеспечение, дискретное моделирование, информационная безопасность.

Введение

По итогам 2022 года [1] более половины успешных атак на телекоммуникационные сети была организована с применением вирусного программного обеспечения (ВПО). При этом общее количество инцидентов в сравнении с 2021 годом увеличилось на 20,8%. Основными целями атак выступают государственные, медицинские организации и промышленные предприятия. Наибольшая доля атак ожидаемо приходится на государственные организации. При этом стоит отметить существенные изменения в характере ущерба, наносимого с помощью ВПО в прошлом году. Значительно увеличилась доля межотраслевого ущерба, наносимого в результате целенаправленных атак на информационную инфраструктуру IT-компаний. Отмечаются сбои работы сервисов, взломы инфраструктуры клиентов. Вторым значимым фактором в данном контексте является активизация распространения вирусов-вайперов, основной механизм поражения которых заключается в безвозвратном удалении данных с зараженного оборудования. Данные изменения можно связать с падением доходов киберпреступников-вымогателей по сравнению с 2021 годом на 40%, связанной с отказами жертв выплачивать крупные суммы выкупа после атак вирусов-шифровальщиков. Таким образом, злоумышленники применяют своеобразную тактику «кибер-террора», стремясь наносить наибольший прямой ущерб из-за невозможности получать прежние доходы от выкупа данных.

При этом на первый план выходит обеспечение безопасности отечественного киберпространства, что требует учитывать и более значительные угрозы, связанные с враждебными действиями недружественных государств в киберпространстве по отношению к РФ на фоне проведения специальной военной операции. С целью точечного поражения (что снижает риск обнаружения) конкретных информационных систем, как правило, государственных и банковской сферы, создаются специализированные экземпляры вирусного программного обеспечения. Кроме того, проводятся целенаправленные атаки на

граждан РФ, например, летом 2022 года распространение получил экземпляр ВПО, замаскированный под приложение российского банка «ВТБ» для мобильной платформы Android [1].

В связи с этим актуальной остается разработка и модернизация инструментария сетевой эпидемиологии в аспектах оценки и регулирования рисков возникновения эпидемических процессов в телекоммуникационных сетях [2, 3]. Наиболее целесообразным соответствующее исследование видится в контексте работы с актуальным методическим обеспечением моделирования эпидемических процессов, разработанным в результате научно-исследовательских работ кафедры систем информационной безопасности Воронежского государственного технического университета (далее – кафедра СИБ) [например, 2-5].

В настоящее время на кафедре СИБ создана основа киберполигона [6], предназначенного для тренинга тестируемых систем. Киберполигон представляет собой программно-технический комплекс, эмулирующий поведение исследуемой киберсистемы в условиях воздействия киберугроз и предоставляет инструментарий для оценки рисков, ущербов, шансов атакуемых систем.

Рассмотрим далее актуальные разработки, предполагающие моделирование атаки вирусного программного обеспечения на телекоммуникационную сеть, их перспективу и результаты моделирования на базе киберполигона кафедры.

Программный модуль моделирования сетевых эпидемий «Epidemics on Networks (EoN)»

«Epidemics on Networks (EoN)» представляет собой специализированный программный модуль, предназначенный для моделирования сетевых эпидемических процессов. Основой данного модуля является популярная библиотека «NetworkX», которая повсеместно применяется для моделирования и визуализации различных сетей и протекающих в них процессов, включая сетевые эпидемии [7].

«Epidemics on Networks» использует расширенную и оптимизированную реализацию эпидемических моделей SIS и SIR (включая дискретные и аналоговые варианты), а также отдельный подмодуль с аналитическим блоком, включающим в себя реализации алгоритмов для анализа результатов моделирования [7].

Данное решение успешно применяется для моделирования сетевых эпидемий в рамках классической эпидемиологии за счет сравнительно продвинутого математического обеспечения, а наличие аналитического блока позволяет применять модуль в контексте прогнозирования и исследования сетевых эпидемий. Визуализация результатов работы аналитического блока программного модуля «Epidemics on Networks» представлена на рис. 1 и 2 [7].

Однако реализация лишь SIS и SIR моделей значительно ограничивает возможности применения программного модуля с учётом всех особенностей современных компьютерных сетей и вирусов [2, 4]. Другим значимым недостатком является отсутствие готовых реализаций алгоритмов оценки суммарных ущерба и риска возникновения эпидемического процесса, несмотря на наличие широкого функционала для оценки и ретроспективного анализа отдельных показателей сетевой эпидемии в требуемом масштабе. Также стоит отметить недостаточные возможности учитывать гетерогенную инфраструктуру сети, что в значительной мере ограничивает точность оценки ущерба.

Указанные недостатки модуля на практике создают необходимость его доработки или ручной интерпретации данных аналитического блока с целью оценки и последующего регулирования рисков исследуемой эпидемии.

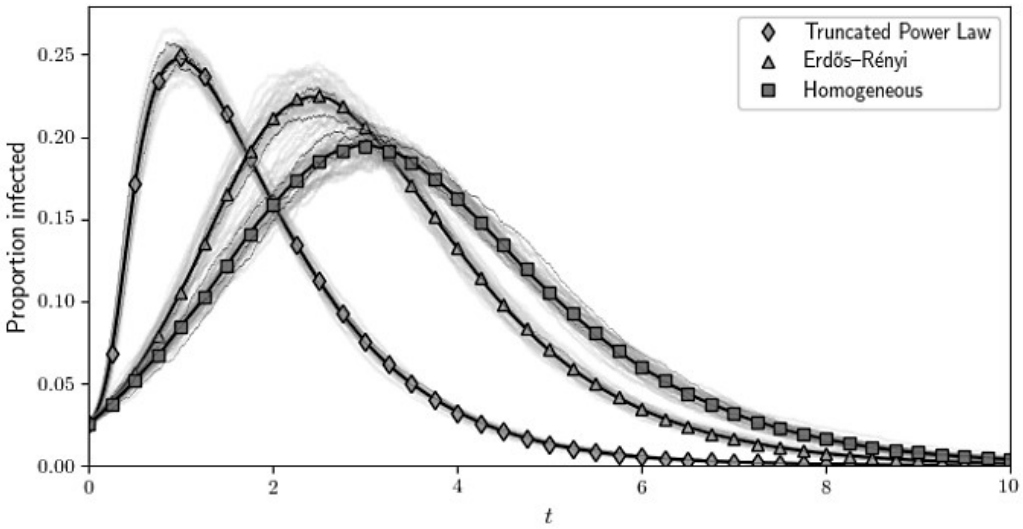

Рис. 1. График статистики эпидемического процесса на основе расчёта доли заражённых узлов в ходе эпидемии, сгенерированный аналитическим блоком «Epidemics on Networks» (для ряда сценариев с различной генерацией сети)

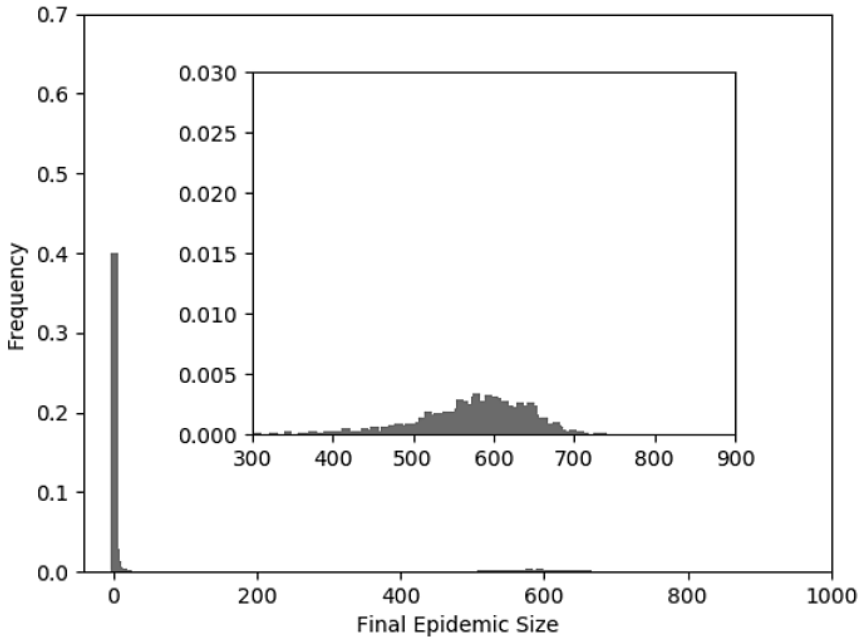

Рис. 2. График зависимости частоты возникновения эпидемии от предполагаемого количества заражённых узлов, сгенерированный аналитическим блоком «Epidemics on Networks»

Автоматизированная информационная система дискретного моделирования сетевых эпидемий на основе программно-технического комплекса «NetEpidemic»

Программно-технический комплекс (ПТК) «NetEpidemic» представляет собой программный продукт, ориентированный на моделирование сетевых эпидемических процессов, включая функционал визуализации эпидемий и риск-мониторинга. Данное решение было разработано аспирантско-студенческим объединением кафедры СИБ.

В ходе научно-исследовательской работы в области сетевой эпидемиологии на основе данного комплекса была разработана автоматизированная информационная система (АИС) дискретного моделирования сетевых эпидемий, обладающая расширенным набором моделей эпидемических процессов (одновременная поддержка моделей SEMARD и PSEIDMR) и доработанным аналитическим блоком [5]. В отличие от программного модуля «Epidemics on Networks», данная система предоставляет возможности по расчету суммарного риска по

ходу эпидемического процесса, что облегчает последующую интерпретацию результатов. Помимо этого, данная система учитывает возможность несинхронного вброса вируса в сеть, что повышает точность моделирования с учетом распространённости подобного явления во время вирусных атак в реальных сценариях. Также стоит отметить реализацию механизмов, позволяющих учитывать применение карантинных мер к отдельным узлам сети, что повышает точность в сценариях с активным противодействием эпидемии. Визуализация результатов работы соответствующего аналитического блока представлена на рис. 3 и 4 [5].

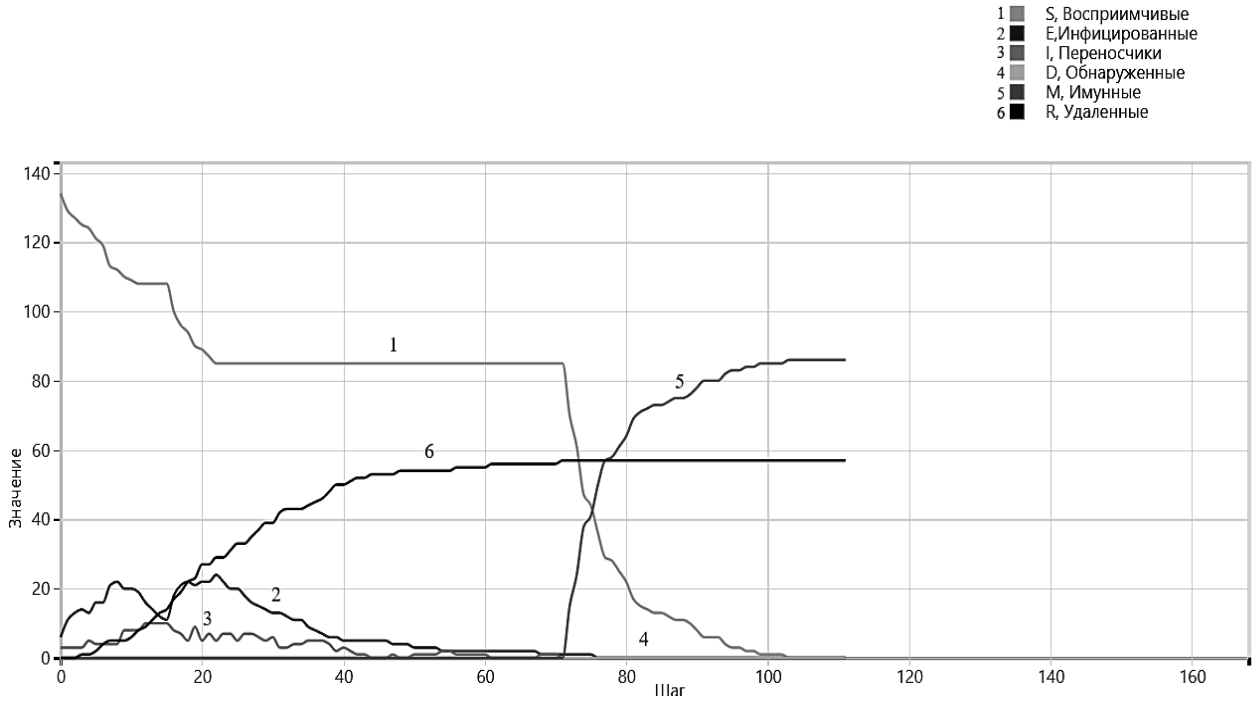

Рис. 3. График статистики эпидемического процесса, сгенерированный аналитическим блоком АИС дискретного моделирования сетевых эпидемий (сценарий моделирования с использованием дискретной двухэтапной модели PSEIDMR)

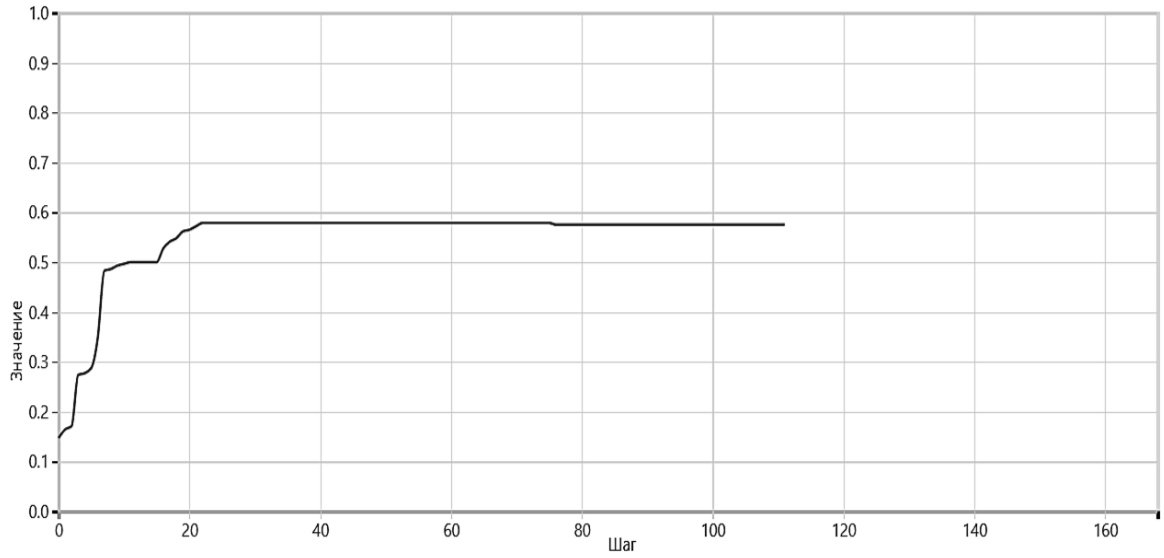

Рис. 4. График суммарного риска эпидемического процесса, сгенерированный аналитическим блоком АИС дискретного моделирования сетевых эпидемий (сценарий моделирования с использованием дискретной двухэтапной модели PSEIDMR)

Несмотря на достигнутые результаты в контексте расширения возможностей моделирования сетевых эпидемий, существует ряд проблем, требующих дальнейшей доработки математического аппарата аналитического блока. Так, текущая реализация обладает недостаточной точностью расчета риска с учетом различной ценности узлов сети, а также различного характера ущерба, наносимого отдельными видами ВПО (например, шпионскими вирусами) [5].

Таким образом, для устранения вышеуказанных недостатков аналитического блока АИС требуется доработка методического обеспечения в аспектах оценки ущерба сетевых эпидемий с учетом всех особенностей гетерогенной инфраструктуры сетей.

Программа моделирования эпидемических процессов «Бахчисарайский фонтан»

В [4] предложена модель «Бахчисарайский фонтан», представляющая собой дискретную модель процесса диффузии вредоноса. Модель учитывает «дозировку» вируса в элементах сети. Для моделирования задаются топология и параметры сети в виде матрицы ресурсов (рис. 5), где обозначено: $\langle Res(x_i, n)\rangle$ – усредненное значение ресурса *i*-той вершины сети x_i, $\langle Res(a_{ij}, n)\rangle$ – усредненное значение динамического ресурса дуги сети a_{ij},, n – номер дискрета моделирования.

	x_1	⋯	x_i	⋯	x_m
x_1	$\langle Res(x_1)\rangle$	⋯	$\langle Res(a_{i1})\rangle$	⋯	$\langle Res(a_{m1})\rangle$
⋮	⋮	⋱	⋮	⋰	⋮
x_i	$\langle Res(a_{1i})\rangle$	⋯	$\langle Res(x_i)\rangle$	⋯	$\langle Res(a_{mi})\rangle$
⋮	⋮	⋰	⋮	⋱	⋮
x_m	$\langle Res(a_{1m})\rangle$	⋯	$\langle Res(a_{im})\rangle$	⋯	$\langle Res(x_m)\rangle$

Рис. 5. Матрица усредненных значений ресурсов элементов сети [4]

Аналогичная матрица строится для потенциалов сети $\langle Pot\rangle$. В результате моделируется процесс диффузии вирусного контента в сети, показанный на рис. 6. Соответствующий алгоритм приведен в [4]. На рис. 6 вершины изображены кругами разного диаметра, соответствующего их потенциалу, в которых серое заполнение соответствует ресурсу, а черное заполнение – поражению вредоносом (z_i – уровни заболеваемости узлов). Постоянное размножение вируса приводит к переполнению уровней заражения и тем самым обеспечивает его постоянное пребывание в сети.

Модель «бахчисарайский фонтан» учитывает дозировку, размножение и диффузию вирусов.

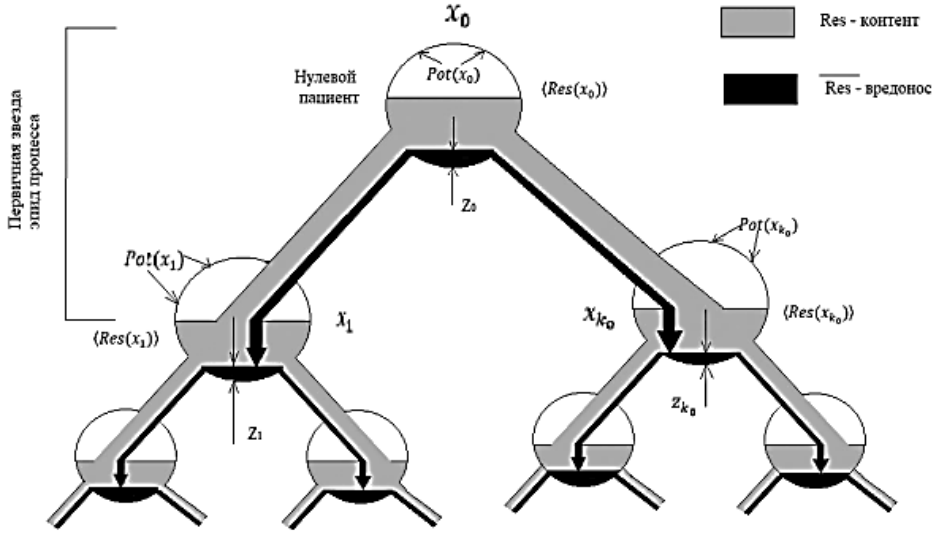

Рис. 6. Диффузии вредоноса в модели «бахчисарайского фонтана» [4]

С помощью этой модели изучается противоборство стратегий злоумышленника и специалиста по информационной безопасности.

Автоматизированная информационная система моделирования эпидемических процессов, порожденных саморазмножающимися и мутирующими вредоносами

Следующим шагом на пути развития моделей эпидемического заражения сетей в научной работе кафедры было учесть факторы саморазмножения, мутаций и снижения способности обнаружения вирусов. В [3] представлен соответствующий алгоритм моделирования. Предложена модель SIMQVR (S – восприимчивый, I – инфицированный, M – зараженный, Q – в карантине, V – вакцинированный, R – удаленный), учитывающая возможные мутации вируса в сети и ответные реакции антивирусного программного обеспечения.

Реализованный модуль имеет ручную настройку и настройку автоматическую на основе экпорта и импорта файлов форматов JSON и XML. На рис. 7 представлен результат моделирования эпидемического процесса в сети. Кроме этого, рассматриваемый блок симуляции представляет возможность визуализации топологии заражения с использованием блока картографирования.

На сегодняшний день эта модель представляется наиболее продуктивной для решения задач оценки динамики развития, дозировки, диффузии вируса в сети, изучения противоборства вирусного и антивирусного программного обеспечения.

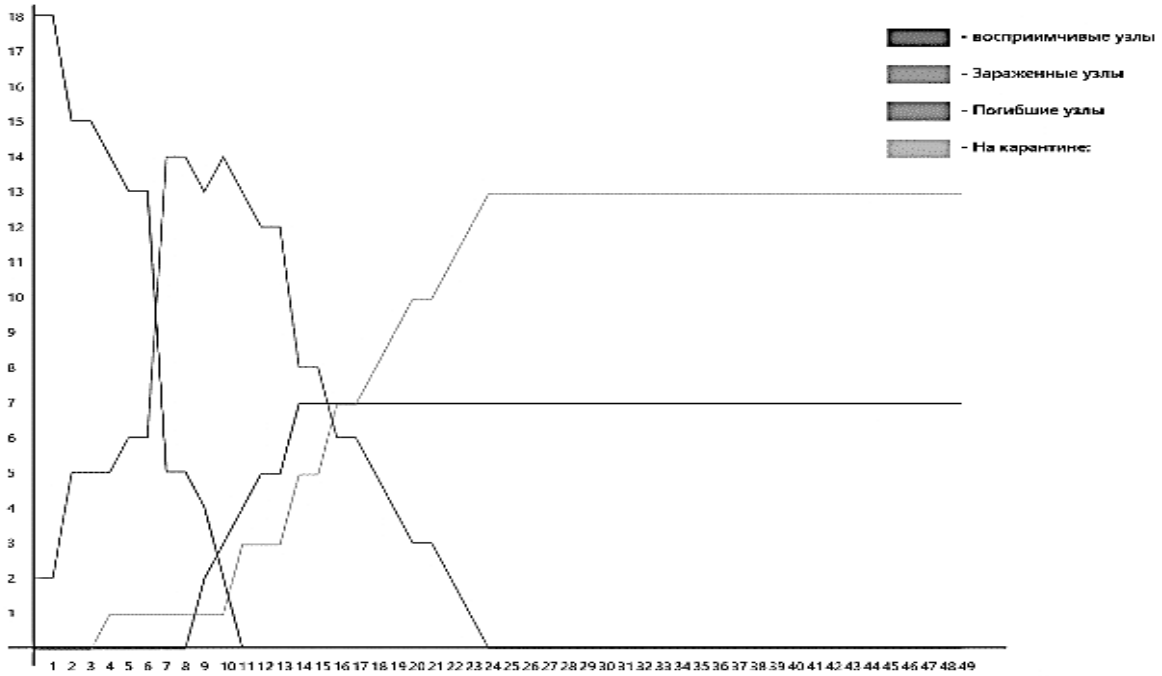

Рис. 7. Результат моделирования эпидемического процесса

Заключение

В статье проведен анализ актуальных разработок и наиболее конкурентоспособных решений для моделирования атак вирусным программным обеспечением телекоммуникационных сетей. Разработанные дискретные модели SEMARD, «Бахчисарайский фонтан», PSEIDMR, SIMQVR предоставляют широкие возможности прогнозирования сетевых эпидемий в различных сценариях, а также учитывают особенности распространения вирусов в условиях их многообразия и реакцию систем защиты.

С целью выявления ключевых недостатков и противоречий, которые позволят уточнить наиболее перспективные направления исследования, проведен анализ моделирования вирусных эпидемий на базе киберполигона.

Список литературы

1. Актуальные киберугрозы: итоги 2022 года. URL:

https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2022-rus.pdf (дата обращения: 25.08.2023 г.).

2. Шеншин А.И. Математическое обеспечение двухэтапной модели эпидемических процессов сетевых автоматизированных структур. / А.И. Шеншин, Е.А. Шварцкопф, К.А. Разинкин // Информация и безопасность. 2021. Т. 24. Вып. 3. С. 431-452.

3. Архипова К.В. Автоматизированная информационная система моделирования эпидемических процессов, порождённых саморазмножающимися и мутирующими вредоносами. / К.В. Архипова, А.А. Остапенко, В.В. Сафронова, В.Ю. Остапенко, Ю.Г. Пастернак // Информация и безопасность. 2022. Т. 25. Вып. 3. С. 349-366.

4. Остапенко А.Г. Математическое обеспечение комплекса моделирования эпидемических процессов с учетом дозировки вирусов: модель «бахчисарайский фонтан» / А.Г. Остапенко, Е.А. Шварцкопф, А.А. Остапенко, В.В. Сафронова, К.В. Сибирко, Е.А. Болгова // Информация и безопасность. 2021, Т. 24, Вып. 4. С. 553-560.

5. Шеншин А.И. Автоматизированная информационная система дискретного моделирования сетевых эпидемических процессов. / А.И. Шеншин, Е.А. Шварцкопф, И.Л. Батаронов // Информация и безопасность. 2022. Т. 25. Вып. 3. С. 389-396.

6. Остапенко Г.А. Киберполигон как проект управления информационными рисками / Г.А. Остапенко, В.И. Белоножкин, А.А. Остапенко, М.Е. Волкова // Информация и безопасность. 2023. Т. 26. Вып. 1. С. 9-16.

7. Epidemics on Networks (EoN) // URL: https://github.com/springer-math/Mathematics-of-Epidemics-on-Networks/blob/master/docs/EoN.rst (дата обращения: 25.09.2023 г.)

Воронежский государственный технический университет
Voronezh State Technical University

Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России
State science research experimental institute of technical information protection problem of Federal service of technical an export control

Поступила в редакцию 6.09.2023

Информация об авторах

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, Воронежский государственный технический университет, email: alexanderostapenkoias@gmail.com

Шеншин Александр Игоревич – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Каданцев Игорь Александрович – канд. техн. наук, заместитель начальника управления, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: kadanstevigor@mail.com

POLYGON CYBER EXERCISES ON THE EXAMPLE OF SIMULATION OF COMPUTER EPIDEMICS OF NETWORKS

E.A. Moskaleva, A.I. Shenshin, I.A. Kadantsev

Currently, the widespread use of cyber ranges continues to gain momentum, expanding the capabilities and increasing the efficiency of information protection of systems. The number and quality of deliberate information threats is steadily growing, including attacks using malicious software. Malware that can cause large-scale network epidemics poses a significant threat, since their destructive effects can quickly and effectively cause significant financial and reputational damage to organizations and individuals. Despite significant progress in research in the field of network epidemiology, the issue of effective assessment and regulation of the risks of computer epidemics in networks remains relevant. The article discusses a technique for modeling a network epidemic that takes into account the diffusion of virus software. The technique under consideration involves a software implementation of modeling the processes of reproduction and diffusion of viral software in an attacked telecommunications network. Based on the methodology, cyber exercises were conducted at the cyber training ground of the Department of Information Security Systems of Voronezh State University.

Keywords: cyber training ground, cyber testing ground, epidemic process, computer epidemic, malicious software, discrete modeling, information security.

Submitted 6.09.2023

Information about the authors

Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Alexander I. Shenshin – Graduate Student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Igor A. Kadantsev – Cand. Sc. (Technical), Deputy Head of Department, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: kadanstevigor@mail.com