DOI 10.36622/VSTU.2022.25.3.007
УДК 004.942:519.876.5

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ДИСКРЕТНОГО МОДЕЛИРОВАНИЯ СЕТЕВЫХ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ. ЧАСТЬ 1

А.И. Шеншин, Е.А. Шварцкопф, И.Л. Батаронов

Стремительное развитие информационных технологий и внедрение их в различные сферы деятельности обуславливает их применение при построении современных корпоративных сетей, что значительно расширяет их функционал и повышает эффективность. Вместе с тем, постоянно возрастает количество атак с применением вредоносного программного обеспечения (ВПО) различного типа, способных наносить значительный ущерб. Особую угрозу для корпоративных сетей представляют вирусы, способные порождать масштабные сетевые эпидемии, деструктивное воздействие которых за последние десятилетия нанесло значительный финансовый ущерб как организациям, так и частным лицам. В рамках представленного исследования было разработано методическое обеспечение автоматизированной информационной системы (АИС) дискретного моделирования сетевых эпидемических процессов на основе глубокой формализации многоэтапного моделирования с учётом таких процессов как: применения карантинных мер, вакцинация элементов сети, а также возможные несинхронные и распределённые по топологии сети вбросы инфекции.

Ключевые слова: автоматизированная информационная система, вредоносное программное обеспечение, корпоративные сети, эпидемический процесс, многоэтапные модели, дискретное моделирование.

Введение

На сегодняшний день, более половины атак на корпоративные сети осуществляются с применением вирусного программного обеспечения (ВПО) различного типа (по итогам 2021 года – доля составила более 63%) [1]. В последние годы в этом отношении имеет место устойчивая тенденция. Так, с конца 2018 года, количество вирусных атак возросло более чем на 137%, а количество связанных с ними инцидентов на промышленных предприятиях возросло более чем на 90% [1, 2]. Основными целями для вирусных атак по всему миру в 2021 году стали государственные и медицинские организации, а также промышленные компании различного масштаба, при этом наибольшая доля атак была направлена на государственные организации (около 16%) [1]. При этом отмечается, что злоумышленники уделяют всё больше внимания совершенствованию методов сокрытия деструктивного воздействия ВПО и эксплуатации сетевых уязвимостей для ускорения его распространения в сетевой среде. Так, в декабре 2021 года появился термин «киберпандемия», связанный с повсеместными вирусными атаками, эксплуатирующими уязвимость популярной библиотеки Log4j [1, 2].

Несмотря на всемирную тенденцию к увеличению количества и качества вирусных атак, на передний план выходят актуальные угрозы, связанные с враждебными и незаконными действиями западных государств в киберпространстве по отношению к РФ на фоне проведения специальной военной операции на территории Украины. В данном контексте происходит создание новых экземпляров ВПО, предназначенных для избирательного поражения сетевой инфраструктуры, расположенной на территории РФ с целью нанесения ущерба отечественным информационным системам, применяемым как в государственной, так и в коммерческой деятельности [1, 3]. Так, в марте 2022 года вредоносный код был обнаружен в популярной библиотеке node-ipc, что нанесло серьёзный ущерб серверам нескольких компаний, вызвало резонанс среди разработчиков открытого программного обеспечения и стало одним из первых случаев распространения вируса, целенаправленно созданного для поражения целей на территории РФ и Республики Беларусь [3].

Стоит отметить опасную тенденцию, связанную с распространением ВПО через цепочку поставок открытого программного обеспечения, используемого по всему миру, что представляет значительную угрозу для информационных систем большого числа организаций и соответствующих корпоративных сетей [1, 3].

В этой связи актуальным остаётся разработка и модернизация инструментария моделирования сетевых эпидемических процессов, предоставляющего функционал по визуализации и риск-моделированию сетевых эпидемий [4, 5]. Для обеспечения конкурентоспособности и эффективности современные программные решения должны обеспечивать высокую точность прогнозирования сетевых эпидемий, а также предоставлять необходимые аналитические данные, на основании которых владельцы сети могут принимать решения по снижению соответствующих рисков [4, 5]. Стоит отметить, что постоянно расширяющиеся экспортные ограничения в области технологий в рамках санкционного давления на РФ со стороны западных государств также в значительной степени повышают актуальность разработки отечественного ПО, включая системы и инструменты моделирования сетевых эпидемических процессов [1, 3].

Отдельной проблемой прогнозирования эпидемических процессов в распределённых системах и сетях является многообразие сетевых топологий и видов ВПО, что усложняет подбор оптимальной математической модели распространения вируса и его поведения [4-6].

Многообразие сетевых топологий и связанная с ней проблематика были детально исследованы в отечественных и зарубежных работах, что послужило основой для создания целого ряда математических моделей, позволяющих моделировать распространения вируса в сети с учётом её индивидуальной топологии [4-6]. Наиболее эффективными моделями в таком случае являются дискретные модели, способные учитывать распространение вируса в масштабе отдельного узла [4, 5].

Решение проблемы моделирования в условиях многообразия ВПО и его поведения может быть сведено к разработке тестовых примеров для различных видов вирусов. Данные тестовые примеры способны учитывать статистические особенности конкретного вида вирусов и позволяют повысить точность прогнозирования сетевой эпидемии в случае распространения соответствующих экземпляров. Основная сложность заключается в разработке самих тестовых примеров, так как более сложные по структуре математические модели требуют большей детализации исходных данных для различных параметров по каждому рассматриваемому виду ВПО [4, 5].

Перспективной моделью эпидемического процесса, призванной разрешить противоречия, возникающие при использовании существующего математического аппарата, является модель PSEIDMR, разработанная в рамках исследования двухэтапного моделирования эпидемических процессов сетевых структур [6]. Данная модель является дискретной и позволяет проводить моделирование в масштабе отдельного узла, что позволяет эффективно учитывать индивидуальную топологию сети, а многоэтапное моделирование эпидемического процесса позволяет учитывать особенности обнаружения ВПО и последующую реакцию систем защиты [6]. Алгоритмизация, адаптация к практическому применению модели PSEIDMR и последующая программная реализация являются актуальными задачами в рамках качественного пополнения существующего инструментария дискретного моделирования сетевых эпидемических процессов.

Основные задачи и результаты

В этой связи актуальным представляется исследование корпоративных сетей и протекающих в них сетевых эпидемических процессов. В соответствии с проведенным анализом актуальность данной работы видится в успешном решении следующих противоречий между:

– необходимостью детально учитывать параметры эпидемического процесса и отсутствием программно-реализованных многоэтапных моделей эпидемических процессов;

– потребностью учитывать многообразие ВПО при моделировании сетевых эпидемий и отсутствием необходимого информационного обеспечения.

В данном случае объектом исследования являются корпоративные сети, имеющие внешние сетевые подключения и, следовательно, подверженные риску возникновения сетевых эпидемий.

Предметом исследования являются эпидемические процессы, протекающие в корпоративных сетях.

Целью исследования является повышение защищённости корпоративных сетей от вирусных атак, порождающих сетевые эпидемии, на основе разработки и внедрения автоматизированной информационной системы дискретного моделирования сетевых эпидемических процессов в части методического обеспечения.

Для достижения поставленной цели решены следующие задачи:

– создано и внедрено методическое обеспечение моделирования эпидемических процессов на основе глубокой формализации многоэтапного моделирования, включая учёт карантинных мер, вакцинацию элементов сети и мутацию ВПО в ходе эпидемического процесса в автоматизированных сетях, а также возможность множественного и распределенного по топологии сети вброса инфекции;

– создано информационное обеспечение для вероятностного моделирования сетевых эпидемий в автоматизированных сетях с учётом многообразия ВПО на основе формализации пространства вирусных конструкций и создания базы данных, включающей вероятностные параметры вирусов для различных видов ВПО согласно известной классификации.

В связи с этим были получены следующие результаты:

– результат внедрения методического обеспечения многоэтапного моделирования эпидемических процессов в автоматизированных сетях, учитывающее применение карантинных мер, вакцинацию узлов и мутацию ВПО в ходе эпидемического процесса;

– информационное обеспечение для вероятностного моделирования сетевых эпидемий в автоматизированных сетях с учётом многообразия ВПО, включающее в себя формализацию пространства вирусных конструкций и БД вероятностных параметров вирусов по видам ВПО.

В отличии от рассмотренных аналогов имеет место быть следующая новизна результатов:

– впервые осуществлена глубокая формализация многоэтапного моделирования с учётом применения карантинных мер, а также процессов вакцинации узлов и мутации ВПО в ходе эпидемического процесса;

– в результате информационно-параметрической и структурно-функциональной адаптации вероятностных моделей заражения элементов автоматизированных сетей к многообразию ВПО, впервые осуществлена формализация пространства вирусных конструкций и создана БД вероятностных параметров вирусов по видам ВПО.

Формализация процесса мутации ВПО по ходу эпидемического процесса

Потребность учитывать процессы мутации ВПО напрямую связана с необходимостью детально учитывать при моделировании особенности распространения различных видов вирусов. Проблематика, связанная с наличием явления мутации ВПО, является особенно актуальной в контексте обнаружения и противодействия соответствующих угрозам, что, в первую очередь, связано с спецификой сигнатурного метода обнаружения вирусов в устройствах-узлах сети [7].

Существуют два независимых механизма мутации, имеющие место в ходе эпидемического процесса [7]:

– индивидуальная мутация ВПО, является основным методом маскировки полиморфных и метаморфных видов ВПО, использующих, так называемый, «мутационный двигатель» реализующий функционал криптографических преобразований;

– последовательная мутация всех активных экземпляров конкретного ВПО вследствие получения обновления от центра управления C2 (Command and Control).

Таким образом, формализация процесса мутации ВПО по ходу эпидемического процесса сводится к отдельному рассмотрению соответствующего вопроса для вышеупомянутых механизмов мутации [6].

Доработка модели PSEIDMR

В результате доработки модели PSEIDMR [6], получена модель, эффективно учитывающая мутацию ВПО, применение карантинных мер и множественный распределённый вброс вируса в сети по ходу эпидемии. Доработанный вариант модели является основой для методического обеспечения разрабатываемой АИС.

В соответствии с добавленным переходом из иммунизированного состояния M в состояние латентно заражённого узла E, была составлена обновленная схема состояний модели второго этапа эпидемического процесса, показанная на рис. 1. Схема состояний для первого этапа осталась без изменений.

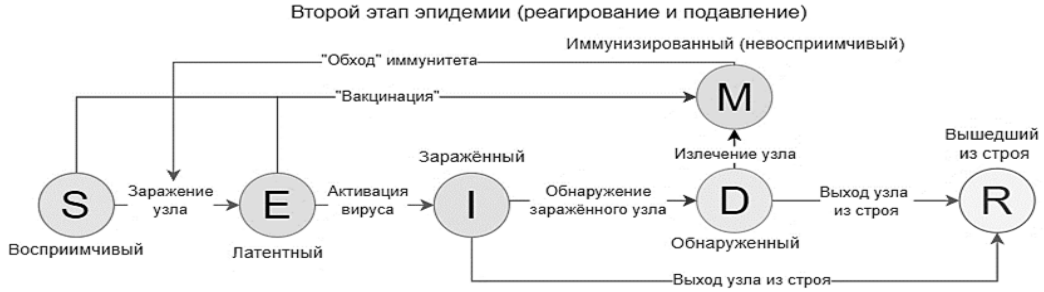

Рис. 1. Поэтапная схема состояний доработанной модели PSEIDMR (второй этап)

Дополненный набор параметров модели имеет следующий вид:

– *N*– общее число узлов в сети;

– m– общее число состояний эпидемического процесса;

– $A = \left[a_{ij}\right]_{N\text{x}N}$ – матрица смежности сети;

– $S_i(n) = \left[S_{i,1}(n), S_{i,2}(n), \dots, S_{i,m}(n)\right]$ – вектор состояний узла сети, где i – номер узла, k – состояние i-го узла, n – шаг процесса;

– $p_i(n) = \left[p_{i,1}(n), p_{i,2}(n), \dots, p_{i,m}(n)\right]$ – вектор функций вероятностей состояний узла сети, где $p_{i,j}(n)$ – вероятности нахождения i-го узла в k-м состоянии на n-м шаге процесса;

– $q_i(n) = [q_1(n), q_2(n), \dots, q_N(n)]$ – вектор индикаторов карантинных мер, компоненты которого указывают на то, применены ли карантинные меры к узлу i на шаге процесса n;

– $v_i(n) = [v_1(n), v_2(n), \dots, v_N(n)]$ – вектор индикаторов вброса вируса, компоненты которого указывают на то, имел ли место вброс вируса в узлел i на шаге процесса n;

– $B = \left[\beta_{lk}\right]_{\text{mxm}}$ – матрица вероятностей контактных переходов состояний узлов;

– $\Delta = \left[\delta_{lk}\right]_{\text{mxm}}$ – матрица вероятностей спонтанных (неконтактных) переходов состояний узлов;

– $C_{i,k}(n)$ – количество узлов, соседних с узлом i, которые находятся в k-м состоянии на n-м шаге процесса;

– $N_k(n)$ – количество узлов сети, находящихся в k-м состоянии, на n-м шаге процесса;

– T – число шагов до обнаружения распространения ВПО в сети.

В контексте доработки модели была проведена формализация применения карантинных мер, что повлекло усложнение соответствующих аналитических выражений. В данном случае целесообразным решением является добавление вспомогательного аналитического выражения для связи между узлами, которое будет являться индикатором того, заблокирована ли соответствующая связь в результате применения карантинных мер. Таким образом получим следующее выражение для индикации того, что связь между узлами i и j не заблокирована на шаге n (узлы i и j не находится в карантине):

$$A_{i,j}(n) = 1 - \min\left(q_i(n), q_j(n)\right), \text{где } \min(x,y) = \begin{cases} x, x < y \\ y, y < x \\ x, x = y \end{cases}.$$

Основным результатом доработки модели в математической части является обновлённая методика построения модели, содержащая аналитические выражения для расчёта вероятностей переходов между состояниями узлов сети.

Покажем этапы предлагаемой методики.

Первый этап эпидемии (n ≤ T). Считаем, что распространение вируса в сети происходит согласно модели SEIR. Набор параметров следующий:

$$S_i(n) = \left[S_{i,S}(n), S_{i,E}(n), S_{i,I}(n), S_{i,R}(n)\right],$$

$$p_i(n) = \left[p_{i,S}(n), p_{i,E}(n), p_{i,I}(n), p_{i,R}(n)\right],$$

$$B = \begin{bmatrix} \beta_{SS} & \beta_{SE} & \beta_{SI} & \beta_{SR} \\ \beta_{ES} & \beta_{EE} & \beta_{EI} & \beta_{ER} \\ \beta_{IS} & \beta_{IE} & \beta_{II} & \beta_{IR} \\ \beta_{RS} & \beta_{RE} & \beta_{RI} & \beta_{RR} \end{bmatrix} = \begin{bmatrix} 0 & \beta & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

где β_{XY} – вероятности перехода узла из состояния X в состояние Y, например, β_{SE} – вероятности перехода узла из восприимчивого состояния S в латентно зараженное E,

$$\Delta = \begin{bmatrix} \delta_{SS} & \delta_{SE} & \delta_{SI} & \delta_{SR} \\ \delta_{ES} & \delta_{EE} & \delta_{EI} & \delta_{ER} \\ \delta_{IS} & \delta_{IE} & \delta_{II} & \delta_{IR} \\ \delta_{RS} & \delta_{RE} & \delta_{RI} & \delta_{RR} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \gamma \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

где δ_{XY} – вероятности перехода узла из состояния X в состояние Y, например, δ_{EI} – из латентного состояния E в зараженное I, δ_{IR} – из состояния заражения E в состояние выхода из строя I.

Векторы состояний узла содержат компоненты S, E, I и R. Матрицы вероятностей контактных и неконтактных переходов состояний узла содержат вероятности $\beta_{SE} = \beta$, $\delta_{EI} = \lambda$ и $\delta_{IR} = \gamma$, соответствующие переходам состояний узлов [6], происходящим на рассматриваемом этапе эпидемического процесса. Соответствующий граф переходов состояний узла представлен на рис. 2, где прямыми линиями показаны неконтактные переходы, изогнутыми - контактные.

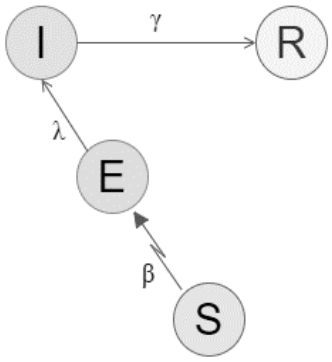

Рис. 2. Граф переходов состояний узла доработанной модели PSEIDMR на первом этапе эпидемии

Для состояний i-го узла функции вероятностей следующие:

$$p_{i,s}(n+1) = S_{i,s}(n)\prod_{j=1}^{N}\left(1 - A_{i,j}(n)\beta a_{ij}S_{j,I}(n)\right),$$

$$p_{i,E}(n+1) = S_{i,S}(n)\left[1 - \prod_{j=1}^{N}\left(1 - A_{i,j}(n)\beta a_{ij}S_{j,I}(n)\right)\right] + S_{i,E}(n)(1-\lambda),$$

$$p_{i,I}(n+1) = S_{i,E}(n)\lambda + S_{i,I}(n)(1-\gamma),$$

$$p_{i,R}(n+1) = S_{i,I}(n)\gamma + S_{i,R}(n).$$

Второй этап эпидемии (n > T). На втором этапе развитие эпидемического процесса происходит по модели SEIDMR. Набор параметров следующий:

$$S_i(n) = \left[S_{i,S}(n), S_{i,E}(n), S_{i,I}(n), S_{i,D}(n), S_{i,M}(n), S_{i,R}(n)\right],$$

$$p_i(n) = \left[p_{i,S}(n), p_{i,E}(n), p_{i,I}(n), p_{i,D}(n), p_{i,M}(n), p_{i,R}(n)\right],$$

$$B = \begin{bmatrix} \beta_{SS} & \beta_{SE} & \beta_{SI} & \beta_{SD} & \beta_{SM} & \beta_{SR} \\ \beta_{ES} & \beta_{EE} & \beta_{EI} & \beta_{ED} & \beta_{EM} & \beta_{ER} \\ \beta_{IS} & \beta_{IE} & \beta_{II} & \beta_{ID} & \beta_{IM} & \beta_{IR} \\ \beta_{DS} & \beta_{DE} & \beta_{DI} & \beta_{DD} & \beta_{DM} & \beta_{DR} \\ \beta_{MS} & \beta_{ME} & \beta_{MI} & \beta_{MD} & \beta_{MM} & \beta_{MR} \\ \beta_{RS} & \beta_{RE} & \beta_{RI} & \beta_{RD} & \beta_{RM} & \beta_{RR} \end{bmatrix} = \begin{bmatrix} 0 & \beta & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \chi & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\Delta = \begin{bmatrix} \delta_{SS} & \delta_{SE} & \delta_{SI} & \delta_{SD} & \delta_{SM} & \delta_{SR} \\ \delta_{ES} & \delta_{EE} & \delta_{EI} & \delta_{ED} & \delta_{EM} & \delta_{ER} \\ \delta_{IS} & \delta_{IE} & \delta_{II} & \delta_{ID} & \delta_{IM} & \delta_{IR} \\ \delta_{DS} & \delta_{DE} & \delta_{DI} & \delta_{DD} & \delta_{DM} & \delta_{DR} \\ \delta_{MS} & \delta_{ME} & \delta_{MI} & \delta_{MD} & \delta_{MM} & \delta_{MR} \\ \delta_{RS} & \delta_{RE} & \delta_{RI} & \delta_{RD} & \delta_{RM} & \delta_{RR} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & \theta & 0 \\ 0 & 0 & \lambda & 0 & \tau & 0 \\ 0 & 0 & 0 & \varepsilon & 0 & \gamma \\ 0 & 0 & 0 & 0 & \varphi & \psi \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

На втором этапе выражения, характеризующие состояния S, E, I, R и переходы между ними аналогичны выражениям для первого этапа. Добавляются состояния D – обнаруженный зараженный узел и M – иммунизированный узел. Соответственно добавляются вероятность перехода узла из иммунизированного состояния M в латентно зараженное E, а матрица вероятностей неконтактных переходов содержит вероятности перехода из восприимчивого состояния в иммунизированное $\delta_{SM} = \theta$, из латентно зараженного в иммунизированное $\delta_{EM} = \tau$, перехода из зараженного в состояние обнаружения заражения $\delta_{ID} = \varepsilon$, из обнаруженного заражения в состояние иммунизации $\delta_{DM} = \varphi$, из обнаруженного зараженного состояния в состояние выхода из строя $\delta_{DR} = \psi$.

Граф переходов представлен на рис. 3, где прямыми линиями показаны неконтактные переходы, ломаными линиями – контактные.

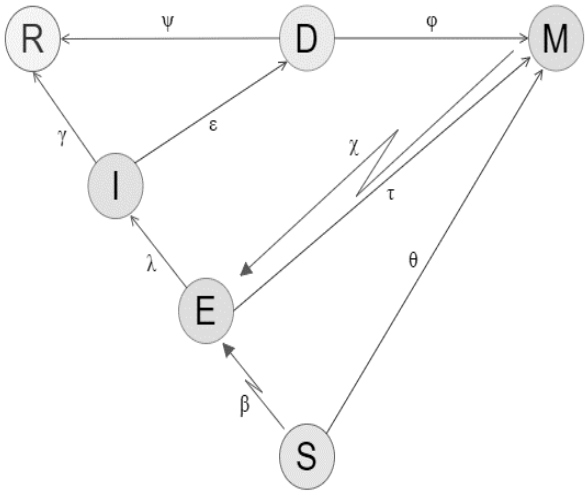

Рис. 3. Граф переходов состояний узла доработанной модели PSEIDMR на втором этапе эпидемии

Таким образом, для описания состояний i-го узла получаем следующие выражения:

$$p_{i,S}(n+1) = S_{i,S}(n)(1-\theta)\prod_{j=1}^{N}\left(1 - A_{i,j}(n)\beta a_{ij}S_{j.I}(n)\right),$$

$$p_{i,E}(n+1) = \left(S_{i,S}(n) + S_{i,M}(n)\right)\left[1 - \prod_{j=1}^{N}\left(1 - A_{i.j}(n)\left(\beta S_{i,S}(n) + \chi S_{i,M}(n)\right)a_{ij}S_{j,I}(n)\right)\right] +$$

$$+S_{i,E}(n)(1-\lambda-\tau),$$

$$p_{i,I}(n+1) = S_{i,E}(n)\lambda + S_{i,I}(n)(1-\varepsilon-\gamma),$$

$$p_{i,D}(n+1) = S_{i,I}(n)\varepsilon + S_{i,D}(n)(1-\varphi-\psi),$$

$$p_{i,M}(n+1) = S_{i,S}(n)\theta + S_{i,E}(n)\tau + S_{i.D}(n)\varphi + +S_{i,M}(n)\left[\prod_{j=1}^{N}\left(1 - A_{i,j}(n)\chi a_{ij}S_{j,I}(n)\right)\right],$$

$$p_{i,R}(n+1) = S_{i,I}(n)\gamma + S_{i,D}(n)\psi + S_{i,R}(n).$$

Заключение

В результате доработки модели PSEIDMR было получено методическое обеспечение в виде методики построения модели, соответствующее требованиям, сформулированным в первой задаче исследования, и подходящее для использования в разрабатываемой АИС дискретного моделирования эпидемических процессов.

В рамках разработки методического обеспечения АИС дискретного моделирования сетевых эпидемических процессов, на основе глубокой формализации многоэтапного моделирования создано методическое обеспечение в виде доработанной модели PSEIDMR, учитывающее применение карантинных мер, вакцинацию элементов сети и мутацию ВПО в ходе эпидемического процесса, а также возможность множественного и распределенного по топологии сети вброса инфекции. В контексте доработки модели PSEIDMR были формализованы процессы мутации ВПО для различных механизмов данного явления.

Практическая перспектива результатов работы такова:

– программная реализация методического обеспечения многоэтапного моделирования эпидемических процессов в автоматизированных сетях позволит проводить моделирование сетевых эпидемий в корпоративных сетях в условиях многообразия сетевых топологий с учётом особенностей обнаружения ВПО и реакции систем защиты;

– информационное обеспечение для вероятностного моделирования сетевых эпидемий в автоматизированных сетях с учётом многообразия ВПО предполагает практическое применение в сфере обеспечения безопасности корпоративных и иных автоматизированных сетей, подверженных угрозам сетевых эпидемий.

При этом теоретическая значимость результатов состоит в следующем:

– предложенное методическое обеспечение может быть адаптировано для многоэтапного моделирования эпидемических процессов в других сетевых структурах, таких как социальные сети и сети АСУ технологических процессов предприятий;

– созданное информационное обеспечение может быть расширено для использования в контекстах исследования новых видов ВПО и модернизации аппарата вероятностного моделирования эпидемических процессов.

Подробнее рассмотреть и оценить результаты исследования возможно, ознакомившись с одноименной выпускной квалификационной работой в РИНЦ.

Список литературы

1. Актуальные киберугрозы: итоги 2021 года. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2021-rus.pdf (дата обращения: 20.06.2022).

2. Актуальные киберугрозы: итоги 2020 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения: 20.06.2022).

3. Protestware - How node-ipc turned into malware, 2022 г. URL: https://www.lunasec.io/docs/blog/node-ipc-protestware/ (дата обращения: 20.06.2022).

4. Эпидемии в телекоммуникационных сетях / Остапенко А.Г., Радько Н.М., Калашников А.О., и др.; [Под ред. гл.–корр. РАН Д.А. Новикова] Сер. Теория сетевых войн. Вып. 1. М.: Горячая линия – Телеком, 2018.

5. Сетео – информационная эпидемиология / Остапенко А.Г., Белов Е.Б., Калашников А.О. и др.; [Под ред. гл.–корр. РАН Д.А. Новикова] Сер. Теория сетевых войн. Вып. 6. М.: Горячая линия – Телеком, 2021. 216 с.

6. 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.

7. Naidu V. Identifying Polymorphic Malware Variants Using Biosequence Analysis Techniques. URL: https://www.researchgate.net/publication/329415014_Identifying_Polymorphic_Malware_Variants_Using_Biosequence_Analysis_Techniques (дата обращения: 25.06.2022).

Воронежский государственный технический университет
Voronesh State Technical University

Поступила в редакцию 04.08.22

Информация об авторах

Шеншин Александр Игоревич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Шварцкопф Евгения Андреевна – ассистент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Батаронов Игорь Леонидович – д-р физ.-мат. наук, заведующий кафедрой, Воронежский государственный технический университет, e-mail: mnac@comch.ru

AUTOMATED INFORMATION SYSTEM FOR DISCRETE MODELING OF NETWORK EPIDEMIC PROCESSES. PART 1

A.I. Shenshin, E.A. Shvartskopf, I.L. Bataronov

The rapid development of information technologies and their introduction into various fields of activity determines their use in the construction of modern corporate networks, which significantly expands their functionality and increases efficiency. At the same time, the number of attacks using various types of malware that can cause significant damage is constantly increasing. A particular threat to corporate networks is viruses that can generate large-scale network epidemics, the destructive impact of which over the past decades has caused significant financial damage to both organizations and individuals. As part of the presented study, methodological support was developed for an automated information system (AIS) for discrete modeling of network epidemic processes based on deep formalization of multi-stage modeling, taking into account such processes as: the application of quarantine measures, vaccination of network elements, as well as possible non-synchronous and distributed over the network topology injection of infection.

Keywords: automated information system, malicious software, corporate networks, epidemic process, multi-stage models, discrete modeling.

Submitted 04.08.22

Information about authors

Alexander I. Shenshin – Student, Voronezh State Technical University, e-mail: mnac@comch.ru

Evgeniya A. Shvartskopf – Assistant, Voronezh State Technical University, e-mail: mnac@comch.ru

Igor L. Bataronov – Dr. Sc. (Physical and mathematical), Voronezh State Technical University, e-mail: mnac@comch.ru