DOI 10.36622/VSTU.2022.25.3.004
УДК 004.49

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА МОДЕЛИРОВАНИЯ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ, ПОРОЖДЕННЫХ САМОРАЗМНОЖАЮЩИМИСЯ И МУТИРУЮЩИМИ ВРЕДОНОСАМИ

К.В. Архипова, А.А. Остапенко, В.В. Сафронова, В.Ю. Остапенко, Ю.Г. Пастернак

В статье представлено исследование многообразия вредоносного программного обеспечения для разработки модулей автоматизированной информационной системы моделирования эпидемических процессов, порожденных саморазмножающимися и мутирующими вредоносами. Приведена классификация саморазмножающихся и мутирующих вредоносов, приводится информационное обеспечение, определяющее параметры саморазмножения и мутации вредоносов, а также антивирусных средств защиты информации. Предложено методическое и алгоритмическое обеспечения, на базе которых были разработаны модули автоматизированной информационной системы моделирования эпидемического процесса в сети с произвольной топологией, порожденного саморазмножающимися и мутирующими вредоносами. В отличие от аналогов разработанные модули автоматизированной информационной системы способствуют моделированию процесса развития эпидемии, а также учитывают снижение способности обнаружения вредоноса в компьютерной сети антивирусным средством защиты информации из-за модификаций, вызванных механизмом мутации вредоноса. Анализируемые методические процедуры и полученные результаты моделирования могут быть востребованы для реализации риск-анализа эпидемических процессов, порожденных мутирующими вредоносами, для последующего обеспечения безопасности компьютерных сетей различного назначения.

Ключевые слова: эпидемический процесс, вредоносное программное обеспечение, вредонос, алгоритмы распространения, механизм мутаций.

Введение

Одним из инструментов для возникновения угроз безопасности информационных систем являются информационные вирусы, так называемые вредоносы[1-3]. Подвергая заражению ресурсы сетевой инфраструктуры, злоумышленник может добиться возникновения эпидемических процессов деструктивного воздействия на информацию, узел и сеть в целом

Вопрос обеспечения информационной безопасности становится более острым не только из-за роста числа пользователей сети Интернет, но и открывающихся возможностей для нарушителей [4]. Существующие модели [1, 5-10] эпидемических процессов, которые описывают распространение вредоносного кода в сети приведены в недостаточном количестве, а также не учитывают всех возможных факторов распространения вредоноса. Вследствие чего защита от вероятность распространения вредоноса в сети, а также адекватно оценить риск вирусных атак не может спрогнозировать возникновения вирусной эпидемии и эпистойкость системы.

Согласно научным исследованиям и отчетам корпораций [11-13] каждый день создается около 1 миллиона вредоносных файлов, при этом киберпреступность наносит ущерб мировой экономике примерно на 6 триллионов долларов ежегодно. Согласно отчету McAfee [14], наблюдается огромный рост бэкдоров, поддельных приложений и банковских троянов для мобильных устройств. Кроме того, растет число вредоносных атак, связанных с социальными сетями, индустрией здравоохранения, облачными вычислениями, интернетом вещей и криптовалютами [15].

Из всего многообразия вредоносного ПО особый интерес представляют саморазмножающиеся и мутирующие вредоносы.

Классификация саморазмножающихся и мутирующих вредоносов

Саморазмножающиеся вредоносы являются одним из самых распространенных

видов вредоносного программного обеспечения. Распространяясь в компьютерных сетях, они попадают на устройство, используя уязвимости операционной системы и, как правило, наносят вред хост-сетям, потребляя наиболее важные ресурсы, например, они могут существенно снизить пропускную способность сети или вызвать перегрузку веб-сервера.

Саморазмножающиеся вредоносы можно разделить на:

—скрытые от пользователя;

—распространяющиеся с участием пользователя.

Скрытые от пользователя в свою очередь подразделяются на:

—слепое (случайное) сканирование;

—пассивное;

—сканирование на основе хит-листов.

Данная классификация представлена по признакам, относящимся к первой фазе заражения вредоносным программным обеспечением, а именно к поиску цели и выбору жертвы.

На следующем этапе процесса заражения вредоносным программными обеспечением восприимчивого узла сети происходит «доставка» вредоносного кода на заражаемую машину [16].

На данном этапе вредоносы делятся по методу заражения, а именно на:

—самонесущие (распространяющие тело внутри вредоноса, как часть процесса заражения);

—двухэтапные (использующие дополнительные поиск связи для передачи тела вредоноса);

—скрытные (добавляющие или заменяющие обычные сообщения).

После попадания вредоноса на узел зачастую требуется действие(активация) вредоносного кода для завершения процесса заражения в данной вершине сети и перехода в активную фазу вредоноса [17-18]: дальнейшее распространение по сети и выполнения кода полезной нагрузки. По способу активации вредоносы можно подразделить на:

—активация человеком;

—активация запланированного процесса;

—активация при использовании сторонних приложений.

Следует отметить, что вредоносное программное обеспечение, распространяющееся скрытно от пользователя и без его вмешательства, несомненно обладают большей скоростью распространения, чем вредоносы, распространяющиеся путем применения методов социальной инженерии. Такой классификационный признак как алгоритм сканирования непосредственно влияет на скорость распространения вредоносного программного обеспечения и представляет интерес для более подробного анализа методов вредоносов, относящихся к данному классу.

Что касается мутирующих вредоносов, то их тоже следует разделить на классы с учетом следующих факторов:

1. Среда обитания:

− файловые – заражают исходные файлы, которые имеют расширение com и exe. Кроме того, могут заражаться неисполняемые файлы Word и Excel.

− сетевые вирусы – передаются компьютерными сетями;

− загрузочные – устанавливаются в Boot-сектор диска или в Master Boot Record сектор диска.

− загрузочно-файловые – инфицируют файлы и загрузочные сектора дисков;

2. Способ заражения:

− резидентный вредонос – подразделяется на две составляющие: инсталятор и резидентный модуль. Инсталятор размещает резидентный модуль вируса в оперативной памяти и выполняет алгоритм, который позволяет резидентному модулю хранится в ней и получать права управления на постоянной основе.

− нерезидентный вирусы не работают постоянно, а срабатывают однократно при запуске инфицированной программы;

3. Деструктивные возможности:

− безобидные – уменьшают свободное место

− не опасные – уменьшают свободное место, провоцируют появление аудио и видео эффектов;

− опасные – нарушают целостность файлов на диске;

− очень опасные – полностью уничтожают данные в системе;

4. Алгоритмы сокрытия от средств защиты информации:

− companion – алгоритм работы заключается в формировании для exe-файлов новых файлов-дубликатов, которые отличаются лишь новым расширением com;

− черви –попадают в память компьютера из компьютерной сети, и благодаря вычислению сетевых адресов других пользователей рассылают по ним копии;

− паразиты – изменяют содержимое дисковых секторов и файлов, но достаточно легко обнаруживаются средствами защиты;

− студенческие – являются одними из самых простых и легко вычисляемых;

− stealth – трудно обнаруживаемые вредоносы, которые используют в качестве маскировки незараженные участки файлов;

− polymorphic – самошифруются различными способами

− макро-вирусы – производят заражение с помощью макро-языков.

Описанная выше классификация не в силах полностью охарактеризовать мутирующие вредоносы, так как не учитывает виды мутации. Следовательно, ее необходимо дополнить.

Можно выделить два типа мутации вредоносного кода: постоянные и индуцированные. К постоянным можно отнести мутации, вызванные применением полиморфизма при разработке программного обеспечения, такие мутации происходят каждый раз при репликации вредоноса. Индуцированные мутации в свою очередь вызваны обновлением вредоносного кода по команде злоумышленника или с течением определенного промежутка времени. Отличительной особенностью постоянных мутаций можно считать тот факт, что функционально вредонос не изменяется, новая версия имеет те же параметры, влияющие на ход эпидемии, что и предыдущая, этот тип мутаций применяется для усложнения обнаружения вирусного программного обеспечения антивирусным программным средством. Постоянные мутации помогают обойти сигнатурный анализ, который является наиболее популярным методом, применяемым антивирусными средствами. В свою очередь индуцированная мутация способна изменить такие параметры как:

− скорость заражения вредоносом узлов сети;

− контагиозность;

− показатель смертности узла сети.

Вредоносы по виду мутации подразделяются на:

—полиморфные;

—индуцированные.

Полиморфная мутация не зависит от внешних факторов. Механизмы мутации заложены в самом коде вредоноса и срабатывают каждый раз при контакте с контентом узла сети. При этом его характеристики не меняются.

В случае индуцированной мутации большую роль играет внешняя среда, которая может оказывать воздействие. При этом изменяются его характеристики, которые влияют на распространение вредоноса в сети.

В свою очередь полиморфные вирусы подразделяют на несколько уровней в зависимости от сложности применяемого алгоритма мутации.

Приведенная выше классификация саморазмножающихся и мутирующих вредоносов позволяет рассматривать их более детально и способствует формированию информационного обеспечения автоматизированной информационной системы моделирования эпидемического процесса, порожденного этими вредоносами.

Антивирусное программное обеспечение и его параметры

Проанализировав исследования компании Anti-malware [18], направленные на тестирование обнаружения различных полиморфных вирусов наиболее распространенными антивирусными средствами, можно разделить антивирусное ПО на три типа: высокоэффективное, эффективное и неэффективное.

Исходя из исследования, можно считать, что коэффициент эффективности методов динамического анализа α, принимает значения, приведенные в табл. 1.

Таблица 1

Значение коэффициента эффективности методов динамического анализа

Тип антивирусного программного обеспечения	Коэффициент эффективности методов динамического анализа, α
высокоэффективное	0,9
эффективное	0,75
неэффективное	0,4

Математическая модель эпидемического процесса, порожденного саморазмножающимися и мутирующими вредоносами

Рассмотрим математическую модель, которая описывает влияние эволюционных адаптаций на процессы распространения в информационных системах, а также указывает на недостатки классических моделей эпидемий, которые не учитывают такие возможности вредоносов, как саморазмножение и мутацию, а также наличие защитных мер в сети и вредоносной составляющей ресурса узла.

Предлагаем модель SIMQVR построенная на основе SIR модели. На рис. 1 приведена схема состояний и переходов данной модели.

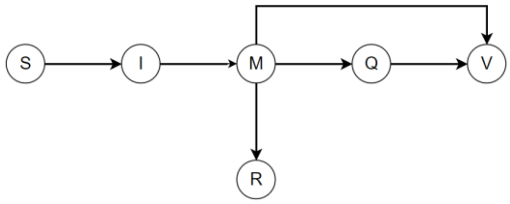

Рис. 1. Граф модели SIMQVR

Описание состояний модели SIMQVR приведено в табл. 2.

Таблица 2

Состояния модели SIMQVR

Обозначение состояния	Описание состояния
S(t)	количество узлов сети, восприимчивых к воздействию мутирующего вредоноса в момент времени t
I(t)	количество узлов сети, инфицированных вредоносным программным обеспечением в момент времени t
M(t)	количество узлов сети, зараженных модифицированных вредоносным программным обеспечением в момент времени t
Q(t)	количество узлов сети, помещенных в карантин в момент времени t
V(t)	количество узлов сети, вакцинированных в момент времени t
R(t)	количество узлов сети, удаленных (выведенных из строя вредоносом) в момент времени t

Следует отметить, что большинство современных саморазмножающихся вредоносов способны мутировать. Применение алгоритмов мутации позволяет злоумышленнику достигнуть следующих целей: уменьшение вероятности обнаружения полезной нагрузки вредоноса и изменение основных характеристик вредоноса в ходе эпидемии.

Необходимо ввести параметры, которые необходимы для характеристики переходов состояний узла в процессе эпидемии, порожденной мутирующими вредоносами. Данные параметры приведены в табл. 3.

Для дальнейшего описания процесса эпидемии воспользуемся терминологией теории взвешенных сетей [10-15]. Исследуемую сеть Net однозначно следует описывать через множества вершин X и дуг A, соединенных между собой инцидентором Г. При этом рассматривается взвешенная сеть со статическим $Res(x_i)$ и динамическим $Res(a_{ij})$ ресурсами.

Предполагается, что в сеть осуществлен вброс вирусного деструктива с дозировкой $\overline{Res}(x_i)$ и задача состоит в том, чтобы осуществить моделирование процесса диффузии вредоноса по сети, начиная с вершины его вброса x_i, которую будем считать ее «нулевым пациентом», т.е. $x_i = x_0$

Все необходимые обозначения сведены в табл. 4.

Таблица 3

Описание параметров эпидпроцесса

Обозначение параметра	Сущность параметра
K_R	базовая скорость репродукции
K_α	индекс контагиозности
K'_R	эффективное репродуктивное число
ν	частота мутации вредоноса
ϑ'	скорость обработки информации антивирусным средством
t	Время
β_i	коэффициент инфицирования узла
Γ	коэффициент восстановления узла
θ	уровень иммунизации помещенного в карантин узла
D_V	доля вакцинированных узлов сети
μ	скорость мутации вредоноса
H	коэффициент обнаружения и реагирования на появление мутирующего вредоноса в узле
Λ	коэффициент поражения вредоносным мутирующим ПО ресурсов узла
Σ	показатель смертности узла сети
A	коэффициент эффективности методов динамического анализа

Таблица 4

Описание параметров используемой модели с точки зрения теории взвешенных сетей

Обозначение параметра	Сущность параметра
$Net(X, A, \Gamma)$	сеть (граф сети) с множеством вершин (узлов) X, пары которых соединены элементами множества A согласно предикату инциденции Γ
$x_i \in X$	элемент (вершина сети) множества X с номером i
$a_{ij} \in A$	элемент (дуга сети) множества A, соединяющий вершины x_i и x_j согласно трехместного предиката инциденции $\Gamma(x_i, a_i, x_j)$
k_i	степень вершины x_i, т.е. количество инцидентных ей вершин сети
$Res(x_i)$	статический ресурс вершины сети x_i, характеризующий объем накопленной в ней информации
$Res(a_{ij})$	динамический ресурс дуги сети a_{ij}, характеризующий объем передаваемой (в единицу времени) информации (трафик)
$\overline{Res}(x_i)$	деструктивный ресурс вершины сети x_i, характеризующий объем накопленной в ней вирусной информации
$Res'(x_i)$	статический ресурс вершины сети x_i, характеризующий объем «вылеченной» информации зараженного узла
z_i	порог вирусной заболеваемости вершины с выраженными симптомами и распространением вредоноса
d_i	порог утраты работоспособности (адекватности) вершины
h_i	порог выздоравления
ω_{ij}	доля распространяемого вершиной x_i вредоноса, передаваемого (диффундирующего) в вершину x_j по трафику a_{ij}
$\langle\cdot\rangle$	Операция вычисления среднего значения

Рассмотрим подробнее вычисляемые показателей применяемых антивирусных параметры, которые зависят от исходных средств.
данных сети, характеристик вредоноса и

Коэффициент инфицирования узла β_i выражается формулой:

$$\beta_i = \frac{K_R}{Res(a_{ij})} \times n,$$

где n – количество сканирований вредоносом доступных узлов в единицу времени.

Коэффициент восстановления узла γ описывается с помощью формулы:

$$\gamma = \frac{\vartheta' \times \left(\frac{m}{T}\right) \times \alpha}{K_R},$$

где $\frac{m}{T}$ – частота обновления сигнатурных баз антивирусных средств, α – коэффициент эффективности методов динамического анализа, применяемого антивирусным средством.

Уровень иммунитета помещенного в карантин узла θ можно рассчитать по формуле:

$$\theta = \frac{\vartheta' \times \left(\frac{m}{T}\right) \times \alpha}{K_R \times t_i},$$

Коэффициент обнаружения и реагирования на появление мутирующего вредоноса в узле вычисляется по следующей формуле:

$$\eta = \frac{\alpha}{\mu}.$$

Коэффициент поражения вредоносным мутирующим ПО ресурсов узла можно найти с помощью формулы:

$$\lambda = \frac{\alpha \quad \times \vartheta' \times t}{\mu \times Res(x_i)}.$$

Доля вакцинированных узлов сети D_V вычисляется по формуле:

$$D_V = \frac{V(t)}{N}.$$

Имеет смысл обратить внимание на параметры, характеризующие прекращение эпидемии в сети, такие параметры описывают переходы в состояние R – узел, выведенный из строя вредоносом, и V – «привитый» антивирусным программным средством узел. Таковыми являются:

—Порог вирусной заболеваемости z_i;

—Порог утраты работоспособности d_i;

—Порог выздоровления h_i.

Порог вирусной заболеваемости z_i вершины x_i, с выраженными симптомами и распространением вредоноса описывается неравенством:

$$0 < \frac{\overline{Res}(x_i, n)}{\langle Res(x_i) \rangle} < z_i.$$

Превышение данного порогового значения означает, что для узла x_i произошел переход $I \to M$, т. е. вредонос перешел в активную фазу размножения и мутации

Порог утраты работоспособности d_i вершины x_i. Неравенство, представленное ниже характеризует ситуацию, когда вредонос выполнил свое предназначение, т. е. заразил необходимое количество ресурса для вывода узла из строя:

$$z_i < \frac{\overline{Res}(x_i, n)}{\langle Res(x_i) \rangle} < d_i.$$

Таким образом, при превышении значения d_i – узел можно считать «мертвым», удаленным из сети.

Порог выздоровления h_i вершины x_i. Для выздоровления необходимо полное удаление вируса из зараженных файлов. Неравенство, представленное ниже описывает случай, при котором информация, обработанная антивирусом и очищенная от вредоноса будет стремиться к объему информации зараженных файлов.

$$\frac{Res'(x_i, n)}{\overline{Res}(x_i, n)} \geq h_i.$$

Среди них важнейшую роль играет также параметр ω_{ij}, который определяет пропорцию распределения вредоноса по дугам (трафикам) сети. Ниже приведена формула расчета данного параметра:

$$\omega_{ij} = \frac{\langle Res(a_{ij})\rangle}{\sum_{j=1}^{k_0}\langle Res(a_{ij})\rangle}.$$

На основе полученных данных можно подготовить тестовые примеры для программного эпидемического моделирования, которые будет учитывать основные состояния узла и характеристики вредоноса.

Входные параметры компьютерной сети для всех случаев одинаковые.

Используя данные обозначения и информацию, полученную при анализе конкретных эпидемий, вызванных диффузией вирусного деструктива, можно составить таблицу численных значений параметров протекания эпидемического процесса. Данные представлены в табл. 5-7.

Таблица 5

Значения основных параметров эпидпроцесса, порожденного саморазмножающимся вредоносом

Наименование	K_R	β_0	Γ	z	d	h
Code Red I	1500	0,00182	0,267	0,00178	0,210	0,89
WannaCry	6000	0,00194	0,326	0,00276	1	-
Code Red II	3000	0,00069	0,441	0.001	-	0,9
Blaster	2500	0,00023	0,508	0,00058	0,443	1
MyDoom.c	5000	0,00168	0,153	0,00117	0,345	0,993
Conficker.A	4500	0,00132	0,225	0,00234	0,599	0,892

Таблица 6

Расчет показателей мутирующих вредоносов

Наименование	K_R	β_0	γ	θ	μ	η	λ
Zeus	11297,6	0,172	0,526	0,175	0,25	3	0,0000531
Citadel	13482,2	0,206	0,441	0,147	0,9	0,83	0,0000147
Poweliks	14587,4	0,223	0,408	0,136	0,437	1,71	0,0000304

Таблица 7

Значения основных параметров эпидпроцесса, порожденного мутирующим вредоносом

Наименование	z	d	h
Zeus	0,00373	0,599	0,997
Citadel	0,00441	0,198	0,9
Poweliks	0,00458	0,443	1

На основе проведенного исследования известных эпидемий, вызванных саморазмножающимися и мутирующими вредоносами, были выделены параметры вредоноса, оказывающие влияние на развитие эпидемического процесса. Было выявлено, что на скорость распространения оказывает непосредственное влияние, применяемый алгоритм сканирования цели, а также динамические ресурсы дуг сети. Следует отметить, что замедление распространения вредосного программного обеспечения происходит также за счет этих двух факторов: поиск новых жертв замедляется из-за попадания в диапазон сканирования большого количества уже зараженных хостов, а также из-за ограничения пропускной способности канала связи.

Рассмотренные параметры и полученные результаты могут послужить основой для разработки методического обеспечения моделирования эпидемических процессов, порожденных саморазмножающимися и мутирующими вредоносами, которое в свою очередь необходимо для разработки алгоритмического обеспечения и модуля автоматизированной информационной системы в целом.

Алгоритмизация распространения вредоноса по сети

В сети существует два основных типа широко используемых моделей моделирования процессов. Это модели с дискретным временем и модели с непрерывным временем; среди них более распространены модели с дискретным временем. В случае моделирования с дискретным временем на каждом временном шаге вирус может передаваться от зараженного узла к чувствительному узлу вдоль каждого ребра с некоторой определенной вероятностью [17]. Кроме того, узел может восстанавливаться (становиться нечувствительным или возвращаться к приемлемости) в течение каждого временного шага. Предположим, что каждое событие заражения и восстановления происходит одновременно в течение определенного интервала времени. При динамическом моделировании сети сеть обычно обновляется на каждом шаге.

Несмотря на то, что способы моделирования с дискретным временем не являются сложными, все же некоторые простые методы реализации могут значительно повысить производительность программного обеспечения.

Другим способом моделирования процесса эволюции в сети является метод непрерывного времени. По сути, принимая во внимание состояние системы, мы можем рассчитать распределение вероятностей момента, когда могут произойти последующие события (т.е. восстановление зараженных узлов или заражение чувствительных узлов). Затем необходимо произвести случайную выборку из этих распределений, определить следующее событие, которое должно произойти, обновить состояние системы и повторить процесс. Однако этот метод требует больших вычислительных затрат, поэтому были разработаны аппроксимации.

Метод непрерывного времени, очевидно, ближе к идеалу стандартной модели заболевания; однако использование этого метода может быть дорогостоящим с точки зрения вычислений, особенно когда задействованы большие сети. Модели с дискретным временем могут быть приемлемой альтернативой по трем основным причинам. Во-первых, временные шаги, задействованные в модели с дискретным временем, становятся очень малыми, поэтому ожидается, что две модели будут сходиться. Во-вторых, по сравнению со случайными гибридными моделями, неточности, вызванные формулами дискретного времени, могут быть менее важными в сетевых моделях, если только два события не происходят в одной и той же области в течение одного и того же временного шага [17].

Шаги алгоритмизации распространения саморазмножающихся и мутирующих вредоносов для первичной звезды эпидемического процесса с центром в вершине x_0 представлены в табл. 8-9 соответственно.

Таблица 8

Алгоритмизация процесса заражения саморазмножающимся вредоносом в сети

Номер шага	Выполненные на шаге вычисления	Комментарии
Шаг 0 – s_0	$\beta_0(x_0, s_0)$	Вершина x_0 стала зараженной
Шаг 1	$\overline{Res}(x_0, 1) = K_R * \Delta t$	В вершине x_0 произошло дальнейшее размножение вредоноса
Шаг 2	$\overline{Res}(x_j, 2) = \omega_{0j}\overline{Res}(x_0, 1),$ $j = 1(1)k_0$	Вредонос поступил в смежные с x_0 вершины
Шаг 3	$\overline{Res}(x_j, 3) = \overline{Res}(x_j, 2) + \lambda_i \Delta t,$ $j = 1(1)k_0$	Началось размножение вредоноса в смежных с x_0 вершинах
Шаг 4 – s	$\beta_1(x_1, s_1)$	Образовалась эпидемическая звезда с центром в x_1
⋮	⋮	⋮

Продолжение табл. 8

Номер шага	Выполненные на шаге вычисления	Комментарии
Шаг 4 – s_j	$\beta_j(x_j, s_j)$	Образовалась эпидемическая звезда с центром в x_j
⋮	⋮	⋮

Таблица 9

Алгоритмизация процесса заражения мутирующим вредоносом в сети

Номер шага	Выполненные на шаге вычисления	Комментарии
Шаг 0 – s_0	$\beta_0(x_0, s_0)$	Вершина x_0 стала зараженной
Шаг 1	$\overline{Res}(x_0, 1) = K_R * \Delta t$	В вершине x_0 произошло дальнейшее размножение вредоноса
Шаг 2	$\overline{Res}(x_j, 2) = \omega_{0j}\overline{Res}(x_0, 1),$ $j = 1(1)k_0$	Вредонос поступил в смежные с x_0 вершины
Шаг 3	$\overline{Res}(x_j, 3) = \overline{Res}(x_j, 2) + (\lambda_i - \eta_i)\Delta t,$ $j = 1(1)k_0$	Началось размножение вредоноса в смежных с x_0 вершинах
Шаг 4 – s	$\beta_1(x_1, s_1)$	Образовалась эпидемическая звезда с центром в x_1
⋮	⋮	⋮
Шаг 4 – s_j	$\beta_j(x_j, s_j)$	Образовалась эпидемическая звезда с центром в x_j
⋮	⋮	⋮

Стоит отметить, что предлагаемая модель учитывает противоборство средств антивирусной защиты и вредоносного программного обеспечения. В связи с этим необходимо рассматривать шаги алгоритмизации выздоровления узла, посредством применения программного антивирусного средства. Алгоритмизация данного процесса представлена в табл. 10.

Таблица 10

Алгоритмизация процесса выздоровления узла сети, зараженного саморазмножающимся вредоносом

Номер шага	Выполненные на шаге вычисления	Комментарии
Шаг 0 – s_0	$\beta_0(x_0, s_0)$	Вершина x_0 стала зараженной
Шаг 1	$\overline{Res}(x_0, 1) = \beta_0 * K_R * \Delta t$	В вершине x_0 произошла активация вредоноса и дальнейшее размножение
Шаг 2	$\overline{Res}(x_j, 2) = \overline{Res}(x_j, 1) - \alpha\overline{Res}(x_j, 1),$ $j = 1(1)k_0$	Вирус обнаружен, введение карантинных мер
Шаг 3 – s	$Res'(x_j, 3) = \theta\eta_j\overline{Res}(x_j, 1),,$ $j = 1(1)k_0$ $\overline{Res}(x_j, 3) = \overline{Res}(x_j, 2) - \alpha\overline{Res}(x_j, 2)$	Лечение зараженного узла антивирусным средством, повторное сканирование на наличие вируса в узле

Продолжение табл. 10

Номер шага	Выполненные на шаге вычисления	Комментарии
Шаг 3 – s_j	$\frac{Res'(x_0, s_j)}{\overline{Res}(x_0, s_j)} = 1$ $Res'(x_j, s_j) = \theta\alpha\overline{Res}(x_j, s_{j-2}),,$ $j = 1(1)k_0$ $\overline{Res}(x_j, s_j) = \overline{Res}(x_j, s_{j-1}) -$ $\alpha\overline{Res}(x_j, s_{j-1}),$	Выздоровление начального узла, лечение смежного зараженного узла
⋮	⋮	⋮

Индекс контагиозности K_α, который зависит от вирулентности вредоноса и степени восприимчивости узлов сети, обусловленной уровнем иммунитета, а также от наличия условий для реализации механизма передачи вредоноса, и определяется как доля инфицированных узлов от всех восприимчивых узлов, вычисляется по формуле:

$$K_\alpha = \frac{\sum_{j=0}^{t} i_j}{\sum_{j=0}^{t} s_j}.$$

Показатель смертности узла сети ς рассчитывается как доля узлов вышедших из строя в сети от общего числа заразившихся узлов, что отражает формула:

$$\varsigma = \frac{\sum_{j=0}^{t} r_j}{\sum_{j=0}^{t} i_j}.$$

Использование иммунизации понижает заразность заболевания, этот факт отражается так называемым эффективным репродуктивным числом

$$K'_R = K_R - K_R * D_V.$$

В простой модели доля вакцинированных узлов, которая останавливает экспоненциальный рост числа заражённых, равна

$$1 - {}^{1}/_{K_R}.$$

Как уже говорилось ранее, предложенная нами модель SIMQVR отличается от других моделей наличием возможной мутации в сети, а также применением антивирусного средства, которое позволяет защитить узел от вредоноса. В связи с этим необходимо рассматривать шаги алгоритмизации мутации вредоноса и выздоровления узла, посредством применения программного антивирусного средства. Такие алгоритмы приведены в табл. 11 и 12 соответственно.

Таблица 11

Алгоритмизация процесса индуцированной мутации вредоноса в узле сети

Номер шага	Выполненные на шаге вычисления	Комментарии
Шаг 0 – s_0	$\beta_0(x_0, s_0)$	Вершина x_0 стала зараженной
Шаг 1	$\overline{Res}(x_0, 1) = K_R * \Delta t$	В вершине x_0 произошло дальнейшее размножение вредоноса
Шаг 2	$\overline{Res}(x_j, 2) = \omega_{0j}\overline{Res}(x_0, 1),$ $j = 1(1)k_0$	Вредонос поступил в смежные с x_0 вершины
Шаг 3	$\overline{Res}(x_j, 3) = \overline{Res}(x_j, 2) + (\lambda_i -$ $\eta_i)\Delta t,$ $j = 1(1)k_0$	Началось размножение вредоноса в смежных с x_0 вершинах

Продолжение табл. 11

Номер шага	Выполненные на шаге вычисления	Комментарии
Шаг s	$\beta_1(x_1, s_1)$	Образовалась эпидемическая звезда с центром в x_1
⋮	⋮	⋮
Шаг s_{j-1}	$\beta_j(x_j, s_j)$ $\overline{Res}(x_j, s_{j-1}) = \overline{Res}(x_j, s_{j-2}) + \mu\Delta t$	В вершине x_j под действием внешних факторов произошла мутация вредоноса. Вершина стала зараженной новой модификацией вредоноса.
Шаг s_j	$\overline{Res}(x_j, s_j) = \omega_{0j}\overline{Res}(x_j, s_{j-1})$, $j = 1(1)k_0$	Вершина x_j начала распространение мутирующего вредоноса. Вредонос поступил в смежные с x_j вершины
Шаг s_{j+1}	$\overline{Res}(x_j, s_{j+1}) = \overline{Res}(x_j,\ s_j) + (\lambda_i - \eta_i)\Delta t$	Началось размножение вредоноса в смежных с x_j вершинах

Таблица 12

Алгоритмизация процесса выздоровления узла сети, зараженного мутирующим вредоносом

Номер шага	Выполненные на шаге вычисления	Комментарии
Шаг 0 – s_0	$\beta_0(x_0, s_0)$	Вершина x_0 стала зараженной
Шаг 1	$\overline{Res}(x_0, 1) = \mu * K_R * \Delta t$	В вершине x_0 произошла мутация и дальнейшее размножение вредоноса
Шаг 2	$\overline{Res}(x_j, 2) = \overline{Res}(x_j, 1) - \eta_j\overline{Res}(x_j, 1)$, $j = 1(1)k_0$	Вирус обнаружен, введение карантинных мер
Шаг 3 – s	$Res'(x_j, 3) = \theta\eta_j\overline{Res}(x_j, 1)$,, $j = 1(1)k_0$ $\overline{Res}(x_j, 3) = \overline{Res}(x_j, 2) - \eta_j\overline{Res}(x_j, 2)$,	Лечение зараженного узла антивирусным средством, повторное сканирование на наличие вируса в узле
⋮	⋮	⋮
Шаг 3 – s_j	$\frac{Res'(x_0, s_j)}{\overline{Res}(x_0, s_j)} = 1$ $Res'(x_j, s_j) = \theta\eta_j\overline{Res}(x_j, s_{j-2})$,, $j = 1(1)k_0$ $\overline{Res}(x_j, s_j) = \overline{Res}(x_j, s_{j-1}) - \eta_j\overline{Res}(x_j, s_{j-1})$,	Выздоровление начального узла, лечение смежного зараженного узла
⋮	⋮	⋮

Мутация вредоноса происходит внутри зараженного узла. Следовательно, вирус мутирует каждый раз при заражении исполняемого файла. Стоит отметить, что при полиморфной мутации не изменяются такие характеристики как базовая скорость репродукции, индекс контагиозности, показатель смертности узла.

В свою очередь при индуцированной мутации вредоноса под внешним воздействием изменяются характеристики вредоноса, влияющие на размножение.

Обратим внимание, процесс мутации вредоноса стоит рассматривать совместно с алгоритмизацией процесса заражения в сети. Так как при попадании в сеть вредонос начинает распространяться и мутировать неограниченное количество раз.

Управление эпистойкостью сети

Управление рисками, как правило, сводится к снижению ключевых показателей эффективности злоумышленников и ограничению избыточной толерантности сети при исследовании за счет повышения общего уровня сетевой безопасности. В этом случае критерием будет уравнение:

$$J = min\{\overline{Res}(x_i, n)(\beta_i - \varphi_i)T\},$$

где за величину первого члена произведения ответственны собственные фильтры узла x_i, а следующий член определяется количеством зараженных и извлеченных файлов (в единицу времени). Таким образом можно выделить несколько направлений для регулирования.

1. Минимизация дозы вредоноса, который поступает в узел сети

Данная политика нацелена на выполнение условия:

$$min[\overline{Res}(x_i, n)].$$

Целью этой политики является предотвращение эпидемического процесса, который можно охарактеризовать как меру профилактики эпидемии. Можно повысить эффективность, фильтруя трафик в сети и обновляя антивирусные фильтры, чтобы уменьшить количество входящего вредоноса. Если узел все-таки подвергся заражению (начался эпидпроцесс), то следует перейти к следующему этапу.

2. Минимизация вирусной нагрузки в узле сети

В этом направлении реализуется функционал:

$$max[z_i].$$

Это делается непосредственно во время распространения паразитов по сетевым компонентам. Заключается в ведении противоборства, а именно в реальном масштабе времени оперативно восстанавливать пораженный объем информации за счет автоматизированных антивирусных средств защиты информации. Кроме того, чтобы снизить скорость самостоятельной передачи вируса, необходимо установить антивирусную систему для вновь выявленных деструктивных узлов.

3. Минимизация объема вредоноса в трафике сети

Здесь на уровне отдельно взятого узла обеспечивается:

$$min[(\beta_i - \varphi_i)].$$

Когда порог вирусной нагрузки узла превышен, в сеть начинают выбрасываться деструктивные материалы. Способ избежать этого - быстро обнаружить зараженные сетевые узлы и ввести для них меры изоляции, чтобы уменьшить распространение вируса.

Указанные методы информационной устойчивости дают общее представление о развитии конфликта злоумышленника, вбрасывающего вирус в сеть, и администратора сети, стремящегося защитить ее от эпидемического процесса, реализовав управление эпистойкойстью сети:

$$E = \frac{|X|}{|X_z| + |X_d| + |X_h|} - 1.$$

Стратегия подразумевает использование вышеописанных выражений (23)-(26) с целью минимизации мощности множества инфицированных вершин $|X_z|$, а также утративших работоспособность $|X_d|$ и выздоровившихся вершин атакуемой сети.

Программная реализация модуля АИС

Реализуемый модуль АИС для моделирования процесса саморазмножающихся и мутирующих вредоносов необходимо разделить на следующие составляющие: ввод характеристик вершин и узлов сети, визуализация полученного графа и непосредственно моделирование процесса заражения.

Для начала моделирования необходимо задать характеристики узлов и дуг сети. Для достижения этой цели был реализован модуль настроек графа загрузка информации из файла. Пользователь должен внести необходимые сведения об узле, к таковым относятся количество ресурса и потенциала, скорость репродукции и пороговые значения, а также отметить, используется ли антивирус и каковы его параметры.

Так как ручная настройка не всегда удобна и может занимать довольно много времени, то был реализован способ импорта и экспорта данных из файлов формата JSON и XML. Интерфейс загрузки и выгрузки файлов с параметрами сети представлен на рис. 2.

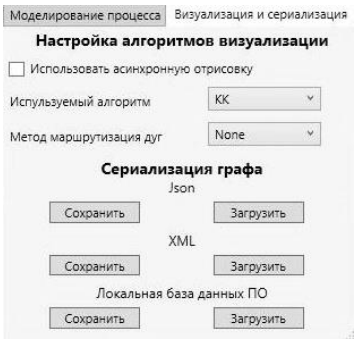

Рис. 2. Импорт из файла параметров графа

Визуализация симуляции, а также ее результатов может проводиться в различных форматах, однако учитывая специфику входных и выходных данных, наиболее наглядным и дающим полную информационную карту диффузии вредоноса в сетевых звездах дает визуализация, с использованием картографической системы. Полный список реализованных алгоритмов визуализации графа и способов маршрутизации представлен на рис. 3 и рис. 4 соответственно.

Рис. 3. Выбор используемого алгоритма укладки графа

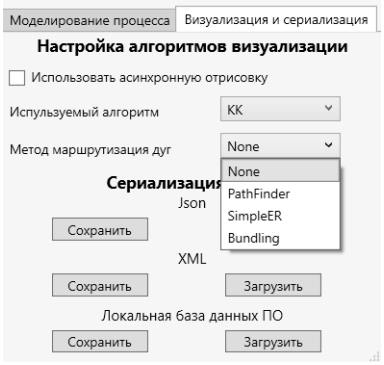

Рис. 4. Выбор метода маршрутизации дуг

Заключительным этапом подготовки к моделированию является настройка параметров моделирования процесса, данная функция позволяет пользователю задать шаг дискретизации и выбрать способ моделирования. Если выбрана функция «Рассчитать по шагам», то система позволит рассмотреть процесс моделирования на каждом шаге, опция «Рассчитать мгновенно» позволяет сразу попасть на заключительный шаг эпидемии. Интерфейс для этого блока настроек представлен на рис. 5.

Рис. 5. Настройка параметров моделирования

При клике на кнопку «Начать» происходит отображение графа, на данном этапе пользователь может задать количество зараженных хостов на первом шаге эпидемии. Стоит отметить, что как динамическая, так и статическая информация о вершине представлена в правом верхнем углу, и появляется по клику на определенную вершину.

Стоит отметить, что для того, чтобы запустился процесс мутации вредноса, необходимо выбрать эту функцию в левом углу окна работы программы.

Визуализация симуляции, а также ее результатов может проводиться в различных форматах, однако учитывая специфику входных и выходных данных, наиболее наглядным и дающим полную информационную карту диффузии вредоноса в сетевых звездах дает визуализация, с использованием картографической системы.

После запуска процесса симуляции программа демонстрирует распространение вредоноса по компьютерной сети. Пример работы программы в режиме симуляции приведен на рис. 6.

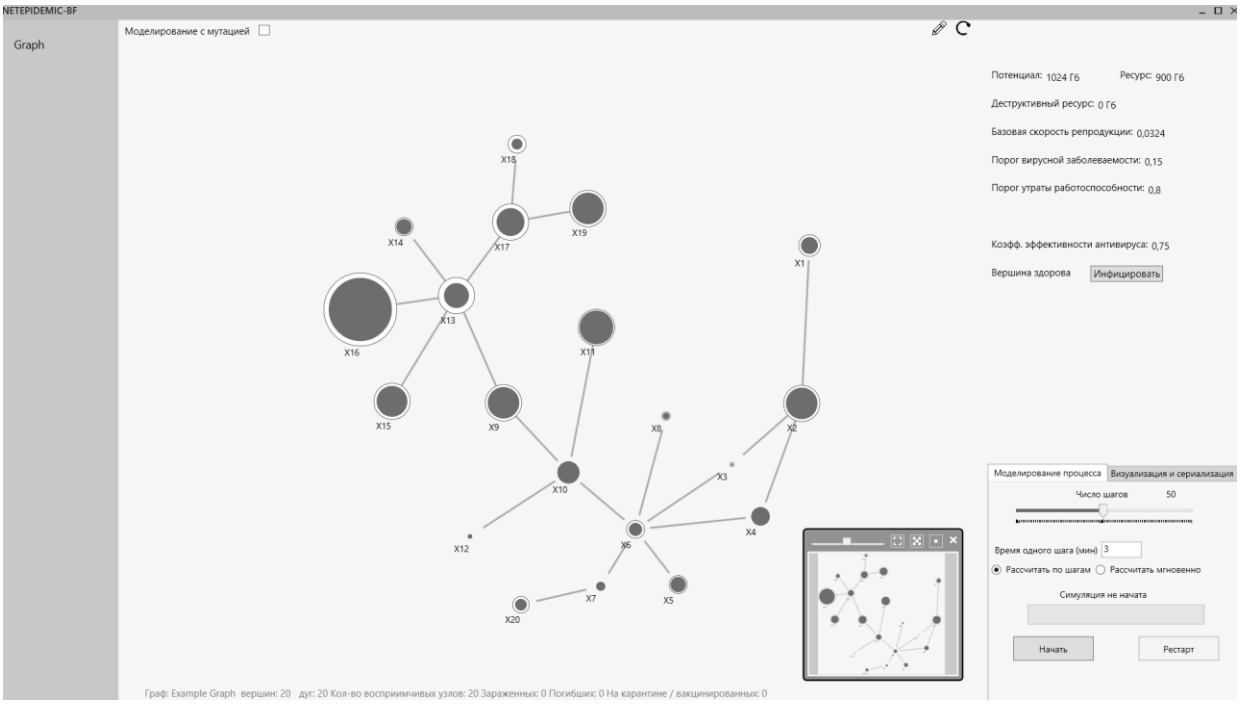

Рис. 6. Моделирование эпидемического процесса

Помимо статистики по ресурсам внутри узла система выводит информацию о сети в целом на каждом шаге эпидемии. Данная информация представлена в левом нижнем углу интерфейса.

В программном модуле используются обозначения состояний, описанных ранее. Для полноты визуализации у каждого состояния также присвоен свой цвет. Символ «+» обозначает, что вершина перешла в состояния R, то есть была выведена из строя. На рис. 7 представлена активная фаза заражения.

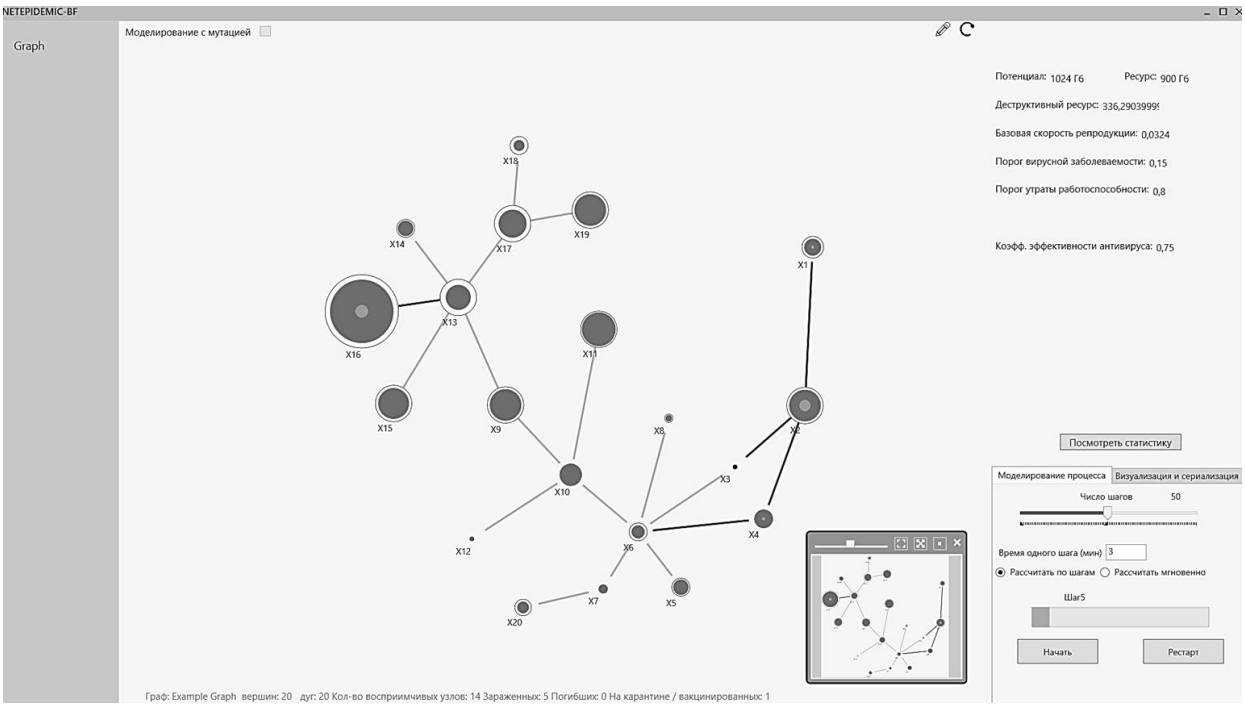

Рис. 7. Моделирование процесса распространение вредоноса в сети

Программа выводит расчетные параметры и значения ресурсов для каждой вершины, на каждом шаге итерации, а также общие данные по сети. Статистика по сети представлена внизу экрана, визуализированное представление отображается по клику на кнопку «Посмотреть статистику».

По окончанию моделирования можно получить сведения о динамике прохождения эпидемии на каждом шаге итерации, проанализировать результат и определить наиболее уязвимые вершны. На рис. 8 и 9 представлен результат эпидемии.

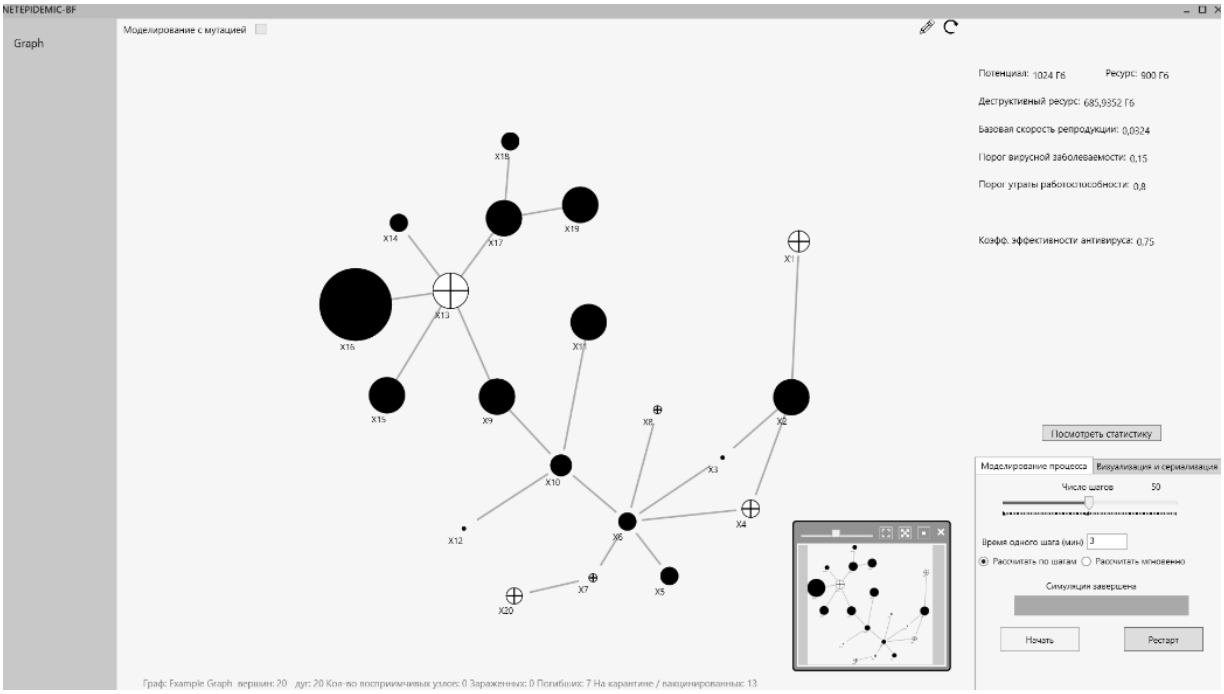

Рис. 8. Завершение эпидемии

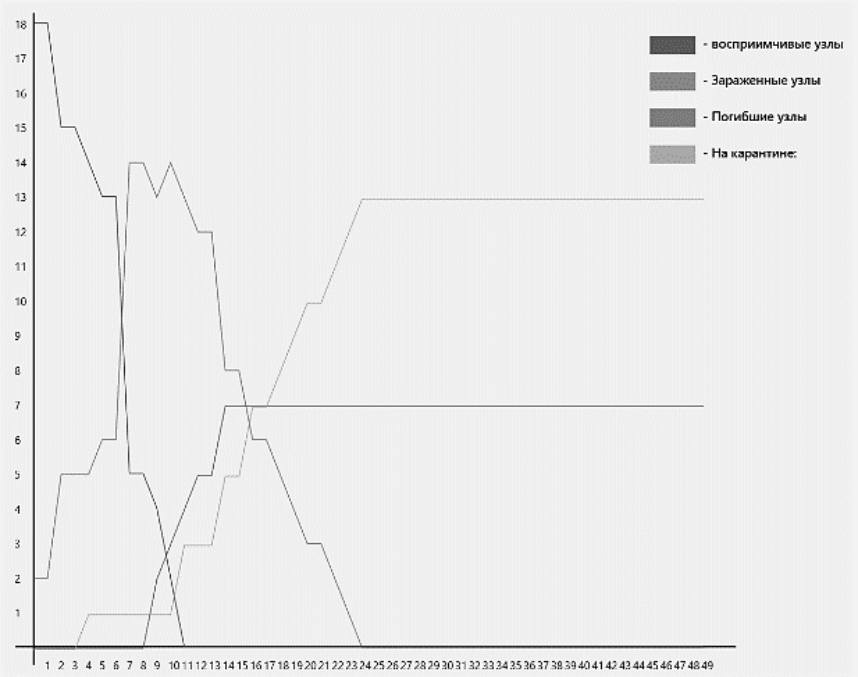

Рис. 9. Результат эпидемического процесса

Заключение

В ходе применения разработанного методического подхода было разработано программное обеспечение, которое позволяет произвести симуляцию эпидемиечского процесса, а также понять процесс моделирования эпидемического процесса, порожденного мутирующим вредоносом, на любом этапе симуляции.

Это позволяет спрогнозировать возможные сценарии распространения вредоноса в компьютерной сети. Эти данные способствуют выявлению рисков возникновения эпидемических процессов заражения компьютерных сетевых структур, а также повышению общего уровня защищенности сети.

Кроме того, реализованное в работе программное обеспечение открывает возможности для дальнейшего изучения сетевого противоборства и рисков, связанных с диффузией деструктива в сети. Полученные аналитические выражения позволяют в ходе проведения симуляции оценивать динамики дозировки вредоноса в процессе его диффузии по атакуемой сетевой структуре.

Список литературы

1. Остапенко А.Г. Сетевая вирусология: прогнозирование развития двувирусных эпидемических процессов в сетях. / А.Г. Остапенко, Е.В. Зарочинцев, О.А. Остапенко, К.В. Сибирко, В.В. Сафронова, П.Д. Федоров. // Информация и безопасность. 2021. Т. 24. Вып. 2. С. 203-222.

2. Остапенко А.Г. К вопросу о трендах и инструментарии социо-информационного глобального противоборства. / А.Г. Остапенко, А.А. Остапенко, Н.М. Лантюхов, С.Д. Трубицын, И.А. Боков. // Информация и безопасность. 2020. Т. 23. Вып. 4. С. 519-524.

3. Остапенко А.Г. Мультисетевая организация человеческой деятельности и возникающие в этой связи информационные риски / А.Г. Остапенко, А.О. Калашни-ков, Г.А. Остапенко, Е.Ю. Чапурин, Н.Ю. Щербакова // Информация и безопасность. 2017. Т. 20. Вып. 3. С. 306-313.

4. Остапенко А.Г. Тактические приемы сетевого противоборства / А.Г. Остапенко, Д.Г. Плотников, Ю.Н. Гузев // Информация и безопасность. 2016. Т. 19. Вып. 2. С. 204-211.

5. Остапенко А.Г. Эпидемии в телекоммуникационных сетях [текст]/ А. Г. Остапенко, Н.М. Радько, А.О. Калашников и др.; Под редакцией чл.-корр РАН Д.А. Новикова – М.: Горячая линия – Телеком, 2018. – 284с.

6. Остапенко А.Г. Атакуемые взвешенные сети [текст] / А.Г. Остапенко, Д.Г. Плотников, А.О. Калашников и др.; Под

редакцией чл.-корр РАН Д.А. Новикова – М.: Горячая линия – Телеком, 2018. – 248с.

7. Остапенко А.Г. Модели информационного инфицирования онлайн социальных сетей / А.Г. Остапенко, В.В. Исламгулова, Д.О. Карпеев, Д.А. Савинов // Ин-формация и безопасность. 2016. Т. 19. Вып. 2. С. 192-203.

8. Guo, Hong & Cheng, Hsing & Kelley, Ken. (2016). Impact of Network Structure on Malware Propagation: A Growth Curve Perspective. Journal of Management Information Systems. 33. 296-325. – Электрон. Дан. Режим доступа: https://www.researchgate.net/publication/304069396_Impact_of_Network_Structure_on_Malware_Propagation_A_Growth_Curve_Perspective

9. Радько, Н.М. Вирусные эпидемии в информационно-телекоммуникационных сетях: цель и задачи исследования / Радько Н.М., Калашников А.О., Корнеева Н.Н., Пономаренко Е.Н., Шевченко И.В. // Информация и безопасность. 2015. №2, Т. 18. С. 198-217.

10. Mieghem, Piet & Omic, Jasmina & Kooij, Robert. (2009). Virus Spread in Networks. Networking, IEEE/ACM Transactions on. 17. 1 - 14. 10.1109/TNET.2008.925623 – Электрон. Дан. Режим доступа: https://www.nas.ewi.tudelft.nl/people/Piet/papers/IEEEToN_virusspread.pdf

11. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 //Cyberwarfare In The C-Suite. - Sausalito, Calif. – Nov. 13, 2020 – Электрон. Дан. Режим доступа: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

12. The McAfee Consumer Mobile Threat Report 2022 – Электрон. Дан. Режим доступа: https://www.mcafee.com/blogs/mobile-security/mcafee-2022-consumer-mobile-threat-report/

13. Ghosh, D., Santra, P.K., Mahapatra, G.S. et al. A discrete-time epidemic mod-el for the analysis of transmission of COVID19 based upon data of epidemiological pa-rameters. Eur. Phys. J. Spec. Top. (2022). – Электрон. Дан. Режим доступа: https://doi.org/10.1140/epjs/s11734-022-00537-2

14. Skormin, Victor A.. “Emulation of the Active Immune Response in a Computer Network.” – 2009 – Электрон. Дан. Режим доступа: https://archive.org/details/DTIC_ADA574395. –

15. Govindaraju, Aditya, "Exhaustive Statistical Analysis for Detection of Metamorphic Malware" (2010). Master's Projects. – Электрон. Дан. Режим доступа: https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1065&context=etd_projects.

16. Семенов С.Г. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управле-ния технологическим процессом / С.Г. Семенов, В.В. Давыдов // Вестник НТУ «ХПИ». – 2012. № 38. – С. 163-171.

17. Al Daoud, Essam & Jebril, Iqbal & Zaqaibeh, Belal. (2008). Computer virus strategies and detection methods. Int. J. Open Problems Compt. Math. 1. – Электрон. Дан. Режим доступа: https://www.researchgate.net/publication/28937695_Computer_virus_strategies_and_detection_methods

18. C. C. Zou, D. Towsley and Weibo Gong, "Email worm modeling and defense," Proceedings. 13th International Conference on Computer Communications and Networks (IEEE Cat. No.04EX969), 2004, pp. 409-414, doi: 10.1109/ICCCN.2004.1401687. . – Электрон. Дан. Режим доступа: https://ieeexplore.ieee.org/document/1401687 -

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 07.07.2022

Информация об авторах

Архипова Ксения Владимировна– студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

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

Сафронова Виктория Витальевна – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Остапенко Владимир Юрьевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Пастернак Юрий Геннадьевич – д-р техн. наук, заведующий кафедрой, Воронежский государственный технический университет, e-mail: mnac@comch.ru

AUTOMATED INFORMATION SYSTEM FOR MODELING EPIDEMIC PROCESSES GENERATED BY SELF-PROPAGATING AND MUTATING MALWARE

K.V. Arhipova, A.A. Ostapenko, V.V. Safronova, V.Yu. Ostapenko, Yu.G. Pasternak

This article is aimed at investigating the variety of malicious software for the development of modules of an automated information system for modeling epidemic processes generated by self-propagating and mutating malware. The paper describes the classification of self-propagating and mutating malware, provides information support that determines the parameters of self-propagatingand mutation of malware, as well as anti-virus information protection tools. The article proposes methodological and algorithmic support, on the basis of which modules of an automated information system for modeling the epidemic process in a network with an any topology generated by self-propagating and mutating malware were developed. Unlike analogues, the developed modules of the automated information system contribute to modeling the epidemic development process, and also take into account the decrease in the ability to detect a malware in a computer network by an antivirus information protection tool, due to modifications caused by the mutation mechanism of this very malware. The analyzed methodological procedures and the obtained modeling results can be used to implement risk analysis of epidemic processes generated by mutating malware, for subsequent security of computer networks for various purposes.

Keywords: epidemic process, malicious software, propagation algorithms, mutation mechanism.

Submitted 07.07.2022

Information about the authors

Ksenia V. Arhipova – Student, Voronezh State Technical University, e-mail: mnac@comch.ru

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

Victoria V. Safronova– Student, Voronezh State Technical University, e-mail: mnac@comch.ru

Vladimir Yu. Ostapenko – Student, Voronezh State Technical University, e-mail: mnac@comch.ru

Yuriy G. Pastrnak – Dr. Sc. (Technical), Head of Department, Voronezh State Technical University, e-mail: mnac@comch.ru