**DOI 10.36622/VSTU.2022.25.3.008**
**УДК 004.942:519.876.5**

# АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ДИСКРЕТНОГО МОДЕЛИРОВАНИЯ СЕТЕВЫХ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ. ЧАСТЬ 2

**Д.Н. Савищенко, Е.А. Шварцкопф, В.Г. Юрасов**

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 представленном исследовании описан процесс проведения специализированной алгоритмизации моделирования сетевых эпидемических процессов. Разработанные алгоритмы описывают основные функции, выполняемые при моделировании эпидемий, ключевыми особенностями которых стали: возможность загрузки топологии пользователем; поддержка нескольких моделей моделирования эпидемических процессов, в том числе многоэтапных.

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

## Введение

Корпоративные сети стали основой, обеспечивающей работу множества государственных и коммерческих организаций [1], особенно в условиях масштабной информатизации государственного управления и экономической деятельности, в последние годы более ускоренной в условиях всемирной пандемии COVID-19. При этом они применяются для автоматизации различных процессов, нарушение работы которых способно привести к значительному ущербу как для организаций, так и их пользователей, клиентов [1-3]. Нарушение работы внутренних процессов представляет наибольшую угрозу для организаций, основная деятельность которых связана с медицинской, банковской, производственной сферами, сферой телекоммуникаций, а также различными сферами государственного управления и безопасности. Помимо этого, автоматизируемые процессы зачастую связаны с хранением, обработкой и передачей данных, среди которых, в зависимости от конкретной сферы деятельности организации, могут быть персональные данные отдельных пользователей и клиентов, а также данные, представляющие собой коммерческую, служебную или государственную тайну, а также другие виды информации ограниченного доступа.

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.

**Основные задачи и результаты**

Актуальность данной работы видится в успешном решении следующих противоречий между:

– потребностью в алгоритмическом обеспечении, специализированном на прогнозировании и анализе эпидемий в автоматизированных сетях, и отсутствием соответствующих алгоритмов;

– необходимостью обеспечивать адекватное и эффективное моделирование сетевых эпидемических процессов в условиях многообразия сетевых топологий и видов ВПО и отсутствием на рынке программных решений, специализированных под эти нужды проектов.

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 создания специализированного алгоритмического и программного обеспечения.

Для достижения поставленной цели решены следующие задачи:

– осуществить алгоритмизацию автоматизации, специализированную на прогнозирование и анализ эпидемий в автоматизированных сетях и ориентированную выработку мер по регулированию эпистойкости, включая обоснование выбора лингвистического и технологического обеспечения для построения программно-технического комплекса (ПТК);

– создать ПТК и провести его отладку по многовариантным тестовым примерам, включая подготовку необходимой документации, а также внедрение в учебный процесс кафедры.

В связи с этим были получены следующие результаты:

– алгоритм автоматизации прогнозирования и анализа эпидемий в автоматизированных сетях, специализированный под нужды исследователей данных проектов, с описанием структуры и используемых технологий;

– специализированный ПТК, реализованный в виде веб-приложения, готовый к внедрению в учебный процесс кафедры, а также сопроводительная к нему документация.

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

– разработанный алгоритм автоматизации прогнозирования эпидемий автоматизированных сетей, в отличие от аналогов, ориентирован на многоэтапное моделирование эпидемического процесса;

– созданный ПТК, в отличие от аналогов, позволяет работать с несколькими моделями распространения ВПО, а также имеет модульную структуру, упрощающую модификацию и разработку новых моделей.

**Алгоритмизация процессов**

Поскольку разрабатываемый ПТК будет иметь архитектуру веб-приложения с разделенными клиентской и серверной частями имеет смысл разделить алгоритмы на выполняемые пользователем и сервером.

Общий алгоритм действий пользователя будет состоять из следующих этапов:

– загрузка топологии исследуемой сети из файла либо, в случае его отсутствия, генерация случайной сети по одному из поддерживаемых алгоритмов с необходимыми пользователю свойствами;

– выбор модели и ввод начальных параметров эпидемического процесса;

– определение начальных узлов распространений эпидемии (установка одного или нескольких узлов в зараженное состояние) и узлов, помещенных на карантин (такие узлы не могут совершить контактные переходы и не участвуют при их расчете);

– возможна корректировка параметров эпидемического процесса в любой момент до его окончания;

– получение результатов эпидемии на текущий шаг;

– получение итогов эпидемического процесса в виде графиков и сводных таблиц.

Блок-схема данного алгоритма изображена на рис. 1.

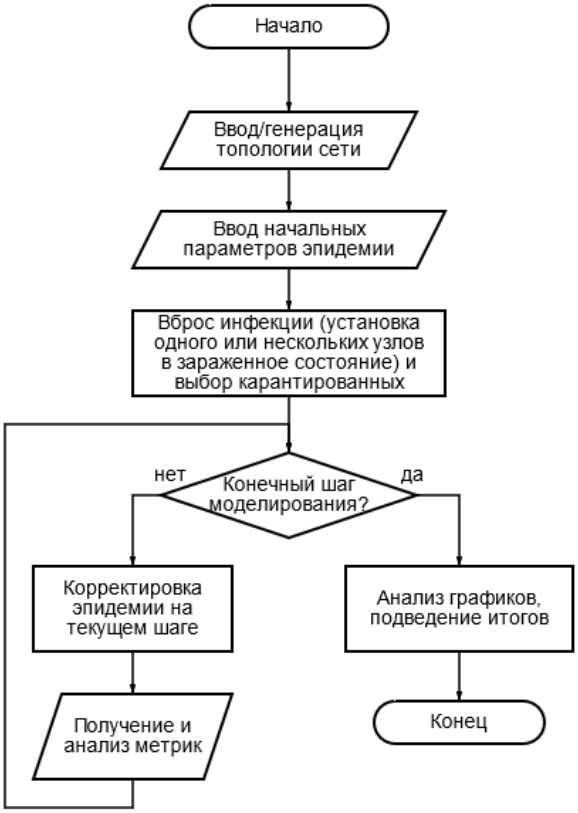


Рис. 1. Блок-схема общего алгоритма

Поскольку любые действия сервера являются ответом на запросы клиентской части ПТК для каждого отдельного действия пользователя сервер должен иметь свой алгоритм.

Алгоритм действий сервера при определении топологии сети:

– получение данных от клиента;

– если пользователем был загружен файл с топологией сети:

а) производится чтение данных из файла;

б) согласно полученным из файла данным, выполняется создание узлов сети и установка связей между ними;

– если файл не был загружен:

а) производится считывание параметров для генерации сети;

б) выполняется генерация графа сети согласно полученным параметрам с применением одного из алгоритмов;

– создание и заполнение матрицы смежности;

– укладка графа с использованием одного из поддерживаемых алгоритмов;

– сохранение полученной сети в сессии.

Блок-схема данного алгоритма изображена на рис. 2.

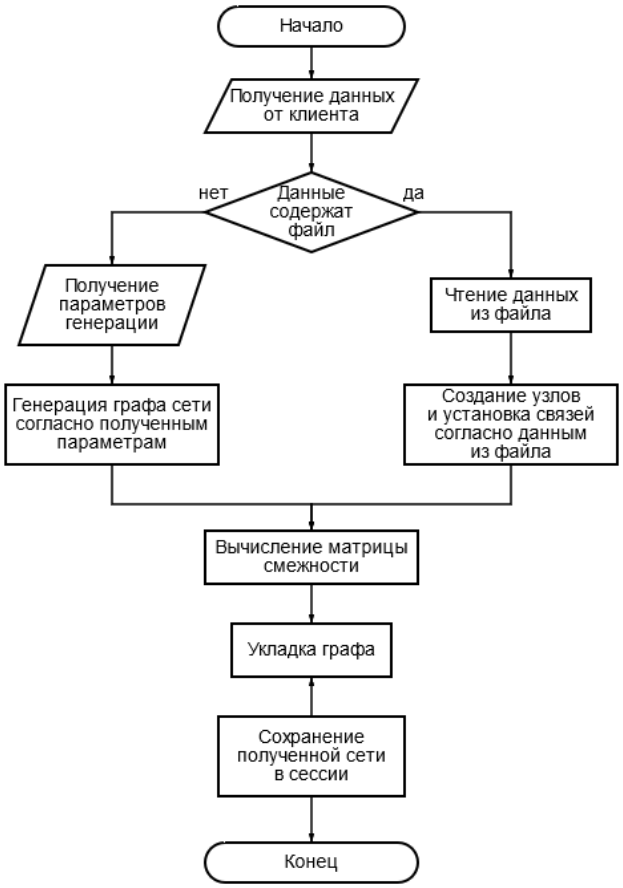


Рис. 2. Алгоритм определения топологии сети сервером

Алгоритм действий сервера при задании начальных параметров эпидемии:

– определение выбранной пользователем модели эпидемического процесса;

– в зависимости от выбранной модели отображаются необходимые для заполнения данных поля;

– сохранение введенных данных.

Блок-схема данного алгоритма изображена на рис. 3.

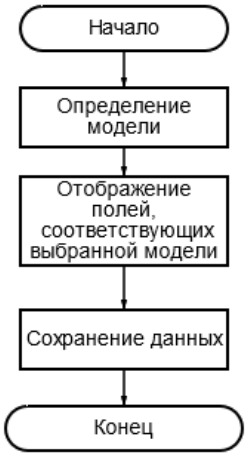


Рис. 3. Алгоритм задания начальных параметров эпидемии

Алгоритм моделирования эпидемического процесса:

– загрузка данных сети и параметров эпидемии;

– определение текущих состояний узлов (все узлы, кроме выбранных пользователем как узлы начала эпидемии, устанавливаются в начальное состояние);

– получение от клиента данных о длительности эпидемии (количество шагов);

– каждый шаг эпидемии выполняется:

а) определение текущего состояния узлов сети, согласно выбранной модели;

б) вычисление текущих метрик;

– после завершения эпидемии подводятся итоги и производится визуализация результатов в виде таблиц и графиков.

Блок-схема данного алгоритма изображена на рис. 4.

Поскольку каждая из имеющихся моделей имеет собственные особенности работы, проведем алгоритмизацию каждой из них.

Алгоритм действий для модели SEMARD:

– определяются состояния узлов на текущий шаг;

– для каждой изначально инфицированной на данном шаге вершины определяются соседние и составляется их список;

– по заданным значениям вероятности производится выбор новых состояний узлов;

– переход на следующий шаг эпидемии.

Блок схема данного алгоритма представлена на рис. 5.


Рис. 4. Алгоритм моделирования эпидемии

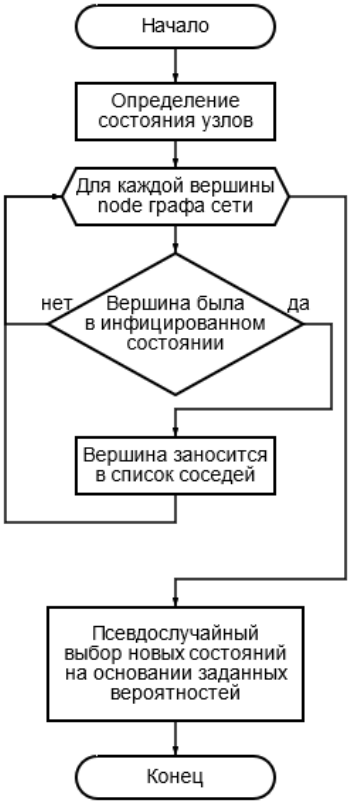


Рис. 5. Блок схема расчета состояний узлов модели SEMARD

Алгоритм действий для модели PSEIDMR будет выглядеть следующим образом:

– определяются состояния узлов на текущий шаг;

– производится расчет вероятностей переходов узлов на следующий шаг;

– на основании рассчитанных вероятностей и этапа эпидемии производится выбор новых состояний узлов;

– переход на следующий шаг эпидемии.

Блок схема данного алгоритма изображена на рис. 6.

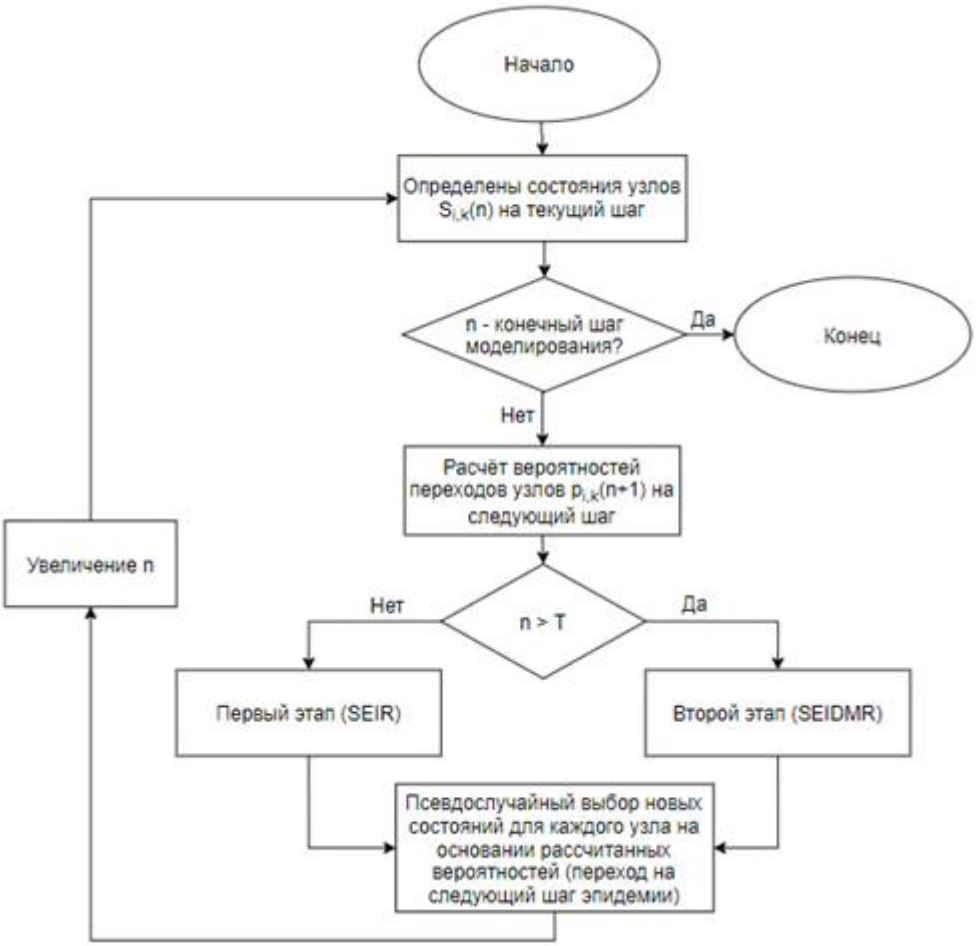


Рис. 6. Блок-схема расчета состояний узлов модели PSEIDMR

**Заключение**

Практическая перспектива результатов работы такова:

– разработанный алгоритм позволяет любым владельцам корпоративных сетей эффективно моделировать эпидемические процессы различных ВПО и способствовать регулированию эпистойкости и уменьшению рисков на основании полученных результатов;

– разработанный ПТК позволяет автоматизировать прогнозирование и анализ эпидемий в автоматизированных корпоративных сетях, а наличие подробно описанной документации позволяет легко внедрить ПТК в соответствующие процессы любой организации.

При этом теоретическая значимость результатов состоит в следующем:

– разработанный алгоритм может быть теоретически развит в рамках внедрения многоэтапного моделирования в области сетевой эпидемиологии на социо-информационные системы и сети;

– использование модульной архитектуры по образу и подобию разработанного ПТК позволит, в долгосрочной перспективе, более эффективно адаптировать методическое обеспечение моделирования эпидемических процессов для различных сетевых структур и 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: 20.05.2022 г.).

2. Эпидемии в телекоммуникационных сетях : монография / А.Г. Остапенко [и др.] ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 1. М. : Горячая линия-Телеком, 2017. 282 с.

3. Сетео-информационная эпидемиология : учеб. пособие для вузов / А.Г. Остапенко [и др.] ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 6. М. : Горячая линия-Телеком, 2021. 216 с.

Воронежский государственный технический университет
Voronesh State Technical University

Поступила в редакцию 15.06.2022

**Информация об авторах**

**Савищенко Дмитрий Николаевич** – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

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

**Юрасов Владислав Георгиевич** – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

## AUTOMATED INFORMATION SYSTEM FOR DISCRETE MODELING OF NETWORK EPIDEMIC PROCESSES. PART 2

**D.N. Savishchenko, E.A. Shvartskopf, V.G. Yurasov**

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. The present study describes the process of conducting a specialized algorithmization of modeling network epidemic processes. The developed algorithms describe the main functions performed in modeling epidemics, the key features of which are: the ability to load the topology by the user; support for several models of modeling epidemic processes, including multi-stage ones.

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

Submitted 15.06.2022

**Information about authors**

**Dmitry N. Savishchenko** – Student, Voronezh State Technical University, e-mail: mnac@comch.ru

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

**Vladislav G. Yurasov** – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru