Научная статья
УДК 004.056:519.876.5; DOI: 10.61260/2307-7476-2026-1-80-93

ПРОГРАММНЫЙ МОДУЛЬ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ В СЕТИ ОПОВЕЩЕНИЯ МЧС РОССИИ НА ОСНОВЕ ЭПИДЕМИОЛОГИЧЕСКОЙ PSIDR-МОДЕЛИ

✉**Бархатов Константин Сергеевич;**
Гергов Идар Хабасович;
Курданов Халид Солтанович;
Арванова Саният Мухамедовна.
Кабардино-Балкарский государственный университет, Нальчик, Россия
✉***barhatov364@gmail.com***

Аннотация. Разработан программный модуль имитационного моделирования распространения вредоносного программного обеспечения в комплексной системе экстренного оповещения населения МЧС России на основе адаптированной эпидемиологической модели PSIDR. Модель учитывает иерархическую четырехуровневую топологию сети и позволяет оценивать динамику распространения заражения, выявлять критические узлы инфраструктуры и моделировать различные сценарии кибератак. Для реализации используется язык Python с применением численных методов решения систем обыкновенных дифференциальных уравнений и теории графов. Программный комплекс включает графический интерфейс для интерактивного моделирования с возможностью визуализации результатов в режиме реального времени. Проведенный анализ чувствительности показал, что инвестиции в системы обнаружения угроз обеспечивают значительно больший эффект по сравнению с ускорением процессов восстановления узлов, снижая охват эпидемии.

Ключевые слова: комплексная система экстренного оповещения населения, PSIDR-модель, имитационное моделирование, информационная безопасность, критическая инфраструктура, распространение компьютерных вирусов, теория графов

Для цитирования: Бархатов К.С., Гергов И.Х., Курданов Х.С., Арванова С.М. Программный модуль имитационного моделирования распространения компьютерных вирусов в сети оповещения МЧС России на основе эпидемиологической PSIDR-модели // Природные и техногенные риски (физико-математические и прикладные аспекты). 2026. №1 (57). С. 80–93. DOI: 10.61260/2307-7476-2026-1-80-93

Scientific article

SOFTWARE MODULE FOR SIMULATION MODELING OF COMPUTER VIRUS PROPAGATION IN THE EMERCOM OF RUSSIA ALERT NETWORK BASED ON THE EPIDEMIOLOGICAL PSIDR MODEL

✉**Barkhatov Konstantin S.,**
Gergov Idar K.,
Kurdanov Khalid S,
Arvanova Saniyat M.
Kabardino-Balkarian State University, Nalchik, Russia
✉***barhatov364@gmail.com***

Abstract. A software module for simulation modeling of malware propagation in the Integrated Emergency Alert System (KSEON) of the Russian EMERCOM has been developed based on an adapted epidemiological PSIDR model. The model accounts for the hierarchical four-level network topology and enables assessment of infection propagation dynamics, identification of critical infrastructure nodes, and simulation of various cyberattack scenarios. The implementation utilizes Python programming language employing numerical methods for solving systems of ordinary differential equations and graph theory. The software package includes a graphical user interface for interactive modeling with real-time visualization capabilities. Sensitivity analysis demonstrated that investments in threat detection systems (SIEM, SOC) provide significantly greater effectiveness compared to accelerating node recovery processes, reducing the epidemic coverage.

Keywords: KSEON, PSIDR model, simulation modeling, information security, critical infrastructure, computer virus spread, graph theory

For citation: Barkhatov K.S., Gergov I.K., Kurdanov K.S, Arvanova S.M. Software module for simulation modeling of computer virus propagation in the EMERCOM alert network based on the epidemiological PSIDR model // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty) = Natural and man-made risks (physico-mathematical and applied aspects). 2026. № 1 (57). P. 80–93. DOI: 10.61260/2307-7476-2026-1-80-93

Введение

Современная Россия сталкивается с беспрецедентным ростом прицельных кибератак на критически важную инфраструктуру. Комплексная система экстренного оповещения населения (КСЭОН) МЧС России занимает уникальное место в этом пространстве: это не просто транспортный канал информации, а система, от которой может зависеть жизнь тысяч людей при возникновении чрезвычайных ситуаций (ЧС). Нарушение функционирования КСЭОН в период ЧС может привести к критическим последствиям для безопасности населения.

Киберугрозы эволюционируют стремительно. От случайных и демонстрационных атак произошёл переход к систематическим и целевым кампаниям. Государственные и криминальные группировки сосредотачивают свои усилия именно на критической инфраструктуре. Исследования показывают, что процесс распространения вредоносного программного обеспечения (ПО) в компьютерных сетях демонстрирует поразительное сходство с биологическими эпидемиями: каждый инфицированный узел может передать вирус нескольким соседним машинам, создавая цепную реакцию заражения [1].

Традиционные средства защиты информации работают преимущественно в профилактическом режиме: блокируют известные угрозы, обновляют сигнатуры, усиливают аутентификацию. Однако они оставляют без ответа критически важный вопрос: что произойдет, если атакующему все же удастся проникнуть внутрь периметра защиты? С какой скоростью распространится компрометация? Какие узлы инфраструктуры окажутся

наиболее уязвимы к каскадному отказу? На каких критических точках следует сосредоточить внимание при внедрении систем мониторинга и реагирования?

Целью настоящей работы является разработка программного модуля имитационного моделирования распространения вредоносного ПО в сети КСЭОН МЧС России на основе адаптированной эпидемиологической модели PSIDR для оценки динамики киберугроз, выявления критических узлов инфраструктуры и формирования рекомендаций по приоритизации защитных мер.

Ответить на эти вопросы можно только путем применения методов математического моделирования. Эпидемиологические модели, изначально разработанные для изучения распространения инфекционных заболеваний в популяциях, проявляют удивительную универсальность. Феноменологически, биологический вирус, размножаясь в инфицированном организме и передаваясь другим особям, функционально эквивалентен компьютерному вредоносному ПО, распространяющемуся через сетевые соединения. Однако реальные сети критической инфраструктуры имеют сложную иерархическую топологию, где узлы обладают различной степенью важности, а каналы связи – ограниченной пропускной способностью. Это требует адаптации классических моделей.

Классическая эпидемиологическая модель SIR (Susceptible-Infected-Recovered), предложенная Кермаком и Макендриком в 1927 г., описывает три состояния: восприимчивые особи (S), инфицированные (I) и выздоровевшие с иммунитетом (R). Эта модель продемонстрировала эффективность для описания многих биологических эпидемий. Однако для защищенных корпоративных сетей она оказывается неполной. В реальной системе КСЭОН действуют системы детектирования вторжений (IDS/IPS), мониторинга и автоматического реагирования, которые обнаруживают аномалии на различных этапах развития атаки. Это создает промежуточное состояние, которое классическая SIR не учитывает: узел скомпрометирован, атака обнаружена системой защиты, но процесс полной изоляции и восстановления еще не завершен.

Математическая модель эпидемиологической динамики киберугроз

Именно эта недостаточность привела к разработке модели PSIDR (Progressive Susceptible-Infected-Detected-Removed), которая вводит четвертое состояние. Четыре состояния узла сети в PSIDR модели:

– S (Susceptible, восприимчивый): узел функционирует нормально, но уязвим для заражения, все системы защиты еще не активированы против конкретной угрозы.

– I (Infected, инфицированный): вредоносное ПО активно, узел полностью скомпрометирован и служит источником распространения заражения на соседние машины через сетевые каналы.

– D (Detected, обнаруженный): система безопасности зафиксировала аномальное поведение (повышенная активность сети, необычные процессы, сигнатуры в логах), узел изолирован или помещен под усиленный мониторинг, запущен процесс диагностики.

– R (Recovered, восстановленный): узел полностью пролечен (переустановлен, обновлено программное обеспечение, закрыта уязвимость), введены меры, гарантирующие иммунитет к данной угрозе.

Динамика переходов между состояниями описывается системой обыкновенных дифференциальных уравнений [2]:

$$\begin{cases} \frac{dS}{dt} = -\beta \frac{S \cdot I}{N} - \mu S \\ \frac{dI}{dt} = \beta \frac{S \cdot I}{N} - \mu I \\ \frac{dD}{dt} = \mu I - \sigma D \\ \frac{dR}{dt} = \sigma D + \mu S \end{cases}$$

где N = S + I + D + R – общее количество узлов в анализируемом сегменте сети.

Параметры модели имеют четкий физический и практический смысл:

β (коэффициент заражения, диапазон 0...1): вероятность передачи вредоносного ПО при условии контакта восприимчивого узла с инфицированным в течение единицы времени. На практике зависит от агрессивности вируса (скорость распространения), эффективности защиты на хостах (наличие firewall, EDR), пропускной способности и архитектуры сетевых каналов [3].

μ (коэффициент обнаружения, диапазон 0...1): интенсивность, с которой система безопасности обнаруживает инфицированные узлы и переводит их в состояние D. На практике зависит от развертывания систем мониторинга (SIEM, SOC), качества определения сигнатур и поведенческих аномалий, компетентности аналитиков SOC.

σ (коэффициент восстановления, диапазон 0...1): скорость, с которой обнаруженные и изолированные узлы восстанавливаются и возвращаются в строй. На практике определяется наличием автоматизации процессов восстановления, актуальностью резервных копий, скоростью работы команды инцидент-менеджмента, наличием заготовленных стандартных образов систем.

Ключевой показатель, определяющий характер развития эпидемии, базовое репродуктивное число R_0:

$$R_0 = \frac{\beta}{\mu}$$

В условиях, когда практически все узлы восприимчивы (начальная фаза эпидемии), каждый зараженный узел в среднем успевает инфицировать R_0 новых восприимчивых узлов до момента его обнаружения [4]. Если $R_0 > 1$, эпидемия развивается экспоненциально – число инфицированных растет. Если $R_0 < 1$, эпидемия затухает самостоятельно – каждое поколение инфекции меньше предыдущего. Граница $R_0 = 1$ является критическим порогом, разделяющим два режима. Например, если $\beta = 0.30$ и $\mu = 0.15$, то $R_0 = 2.0$, означая, что при отсутствии других мер каждый вирус успевает заразить в среднем двух новых узлов.

Топологическая модель иерархической сетевой инфраструктуры КСЭОН

Реальная КСЭОН имеет четко выраженную иерархическую структуру управления: стратегические решения принимаются на федеральном уровне, передаются в субъекты, затем в муниципалитеты и, в конечном счете, на объектовые терминалы оповещения. При разработке математической модели было принято решение явно отразить эту иерархию через представление сети в виде взвешенного неориентированного графа G = (V, E), где V – множество узлов (компьютеры, серверы, контроллеры), E – множество каналов связи между ними [5]. Граф содержит четыре слоя:

– Уровень 1 (Федеральный): центральный диспетчерский центр МЧС России, ~ 1 узел;

– Уровень 2 (Региональный): серверы управления в субъектах России, ~10 узлов;

– Уровень 3 (Муниципальный): единые диспетчерские центры в районах, ~30 узлов;

– Уровень 4 (Объектовый): терминалы оповещения на опасных объектах, ~59 узлов.

Иерархичность топологии критична для анализа устойчивости: компрометация узла федерального уровня влияет на всю систему оповещения, тогда как вывод из строя одного объектового терминала представляет локальную проблему.

Программная реализация и архитектура вычислительного комплекса

Для реализации разработанного математического аппарата выбран язык программирования Python, обладающий мощной экосистемой научных библиотек. Архитектура приложения построена по принципу разделения ответственности, что обеспечивает модульность, тестируемость и простоту расширения функциональности (рис. 1).

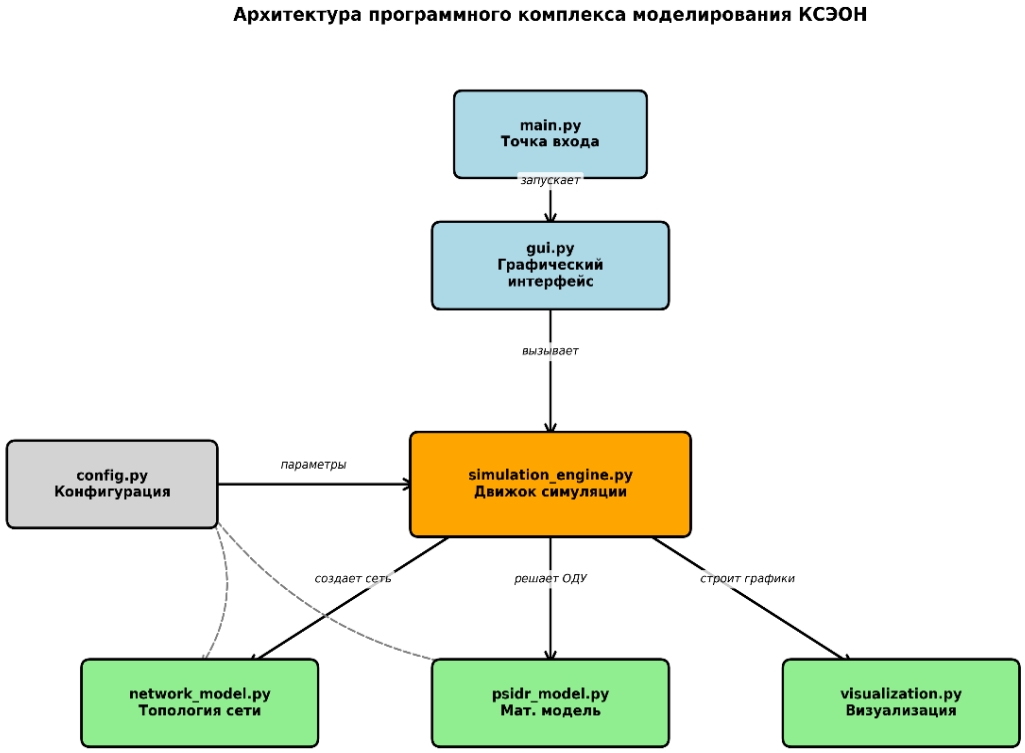

Рис. 1. **Архитектура программного комплекса: модули, функции и их взаимосвязь**

Центральный модуль simulation_engine координирует работу network_model (топология), psidr_model (математика) и visualization (отображение результатов). GUI служит интерфейсом для пользователя.

Ключевые модули системы:

1. – config.py – конфигурационный модуль, где централизованно заданы все начальные значения параметров модели (β, μ, σ), размеры сети на каждом уровне иерархии, параметры численного интегрирования (шаг времени delta_t, количество временных шагов). Это «точка входа» для адаптации модели под конкретные условия и сценарии. Изменение параметров не требует редактирования основного кода.

2. – network_model.py – модуль создания и анализа топологии сети. Реализует класс KSEONNetwork, который генерирует граф сети с учетом иерархии: создает узлы четырех уровней в соответствии с конфигурацией, соединяет их по правилам иерархии, добавляет резервные каналы для повышения отказоустойчивости. Также вычисляет три типа метрик центральности каждого узла: степень (Degree Centrality), близость (Closeness Centrality), посредничество (Betweenness Centrality). Эти метрики необходимы для выявления критически важных узлов.

3. – psidr_model.py – основной математический модуль. Содержит два класса, первый – PSIDRModel, реализует детерминированное моделирование путем численного решения системы ОДУ (используется scipy.integrate.odeint). Второй класс – NetworkPSIDRModel, реализует стохастическое моделирование, где процесс заражения моделируется как случайная ходьба по графу; каждый зараженный узел имеет вероятность β*delta_t передать вирус каждому соседнему узлу в текущем временном шаге.

4. simulation_engine.py – «оркестр» системы. Управляет взаимодействием всех компонентов:

– инициализирует граф сети через network_model;

– задает начальное состояние (выбирает стартовые инфицированные узлы);

– запускает процесс моделирования (детерминированное или стохастическое);

– собирает статистику (пик инфекции, время достижения пика, финальный охват, время затухания активной фазы);

– передает результаты в visualization для отображения.

5. visualization.py – модуль визуализации. Создает набор графиков:

– линейный график динамики S(t), I(t), D(t), R(t);

– диаграмма stacked area для распределения состояний – визуализация топологии сети с цветовой раскраской узлов по состоянию;

– графики метрик центральности (Degree, Closeness, Betweenness);

– сводная статистика в формате комбинированного графика.

6. gui.py – графический интерфейс, который позволяет пользователю без знания Python интерактивно менять параметры симуляции, видеть результаты в режиме реального времени в виде пяти вкладок визуализации, сохранять графики в PNG.

7. main.py – точка входа приложения, обеспечивает запуск либо GUI в интерактивном режиме, либо консольной версии для пакетной обработки.

Результаты численного моделирования динамики заражения сетевой инфраструктуры

Тестовый сценарий выбран как репрезентативный для «среднестатистического» вирусного воздействия с параметрами: $\beta = 0.30$ (достаточно агрессивный вирус), $\mu = 0.15$ (низкая скорость обнаружения), $\sigma = 0.25$ (средняя скорость восстановления). Сеть содержит 100 узлов (распределены иерархически: 1 федеральный, 10 региональных, 30 муниципальных, 59 объектовых), начальное количество инфицированных – 5 узлов, выбранных случайно. На рис. 2 показан главный экран приложения с параметрами слева и основным графиком справа.

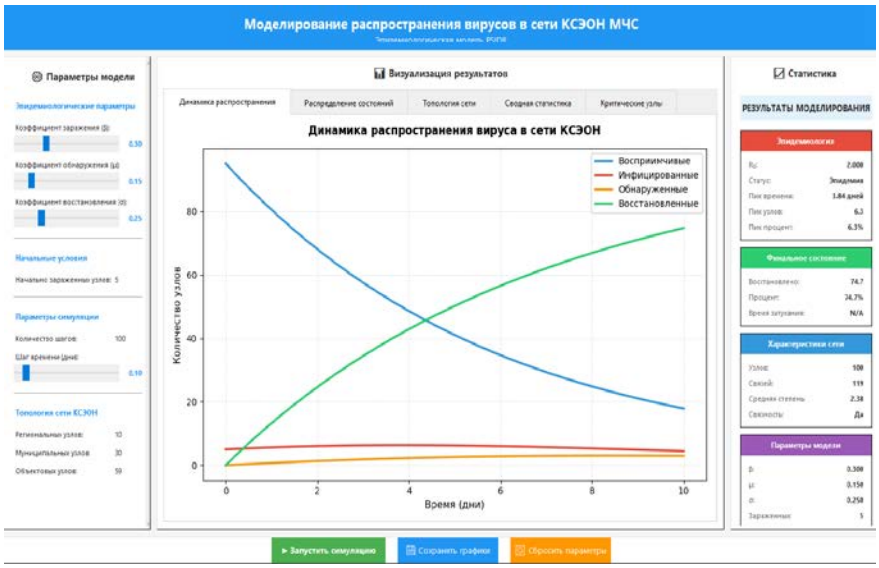

Рис. 2. **Интерфейс программного комплекса**

Тестовый сценарий демонстрирует развитие эпидемии. Базовое репродуктивное число:

$$R_0 = \frac{\beta}{\mu} = \frac{0.30}{0.15} = 2.0$$

Значение $R_0 = 2.0 > 1$ указывает на развитие эпидемии. На рис. 3 представлена динамика состояний узлов.

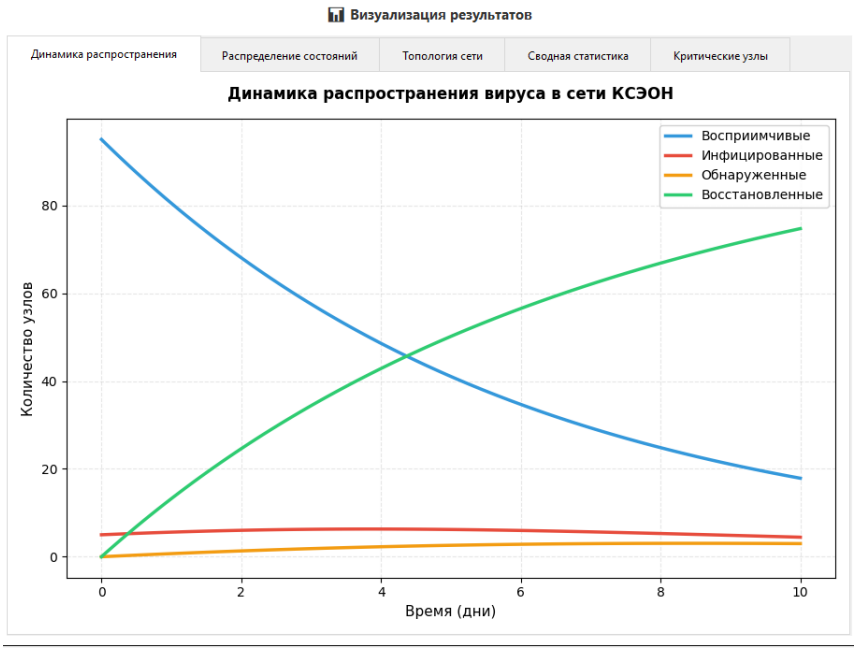

Рис. 3. **Динамика распространения вредоносного ПО во времени при базовых параметрах**

По оси X – время в днях (0...10), по оси Y – количество узлов (0...100). Синяя линия S(t) (восприимчивые): резко убывает с 95 до ~0 за 2 дня, так как узлы либо заражаются, либо срабатывает система обнаружения. Красная линия I(t) (инфицированные): экспоненциально растет в начале, достигает пика ~6.3 узлов в момент t ≈ 3.84 дня, затем спадает к нулю. Оранжевая линия D(t) (обнаруженные): растет с задержкой после пика I, достигает максимума ~6 узлов, затем спадает. Зеленая линия R(t) (восстановленные): логистически растет, асимптотически приближаясь к 74.7 узлам к концу периода.

Анализ графика рис. 3 показывает:

1. На начальном этапе (t = 0...2 дня): экспоненциальный рост числа инфицированных узлов. Вирус имеет временное преимущество – множество восприимчивых узлов, система безопасности еще полностью не мобилизована. За 2 дня 95 % узлов либо заражены, либо включены в процесс обнаружения.

2. На пике эпидемии (t ≈ 3.84 дня): максимальное число одновременно инфицированных узлов. На этот момент активно инфицировано ~6.3 узлов (6.3 % от сети), однако число обнаруженных уже превышает число активно инфицированных. Система защиты зафиксировала пик эпидемии в точке максимума, но процесс восстановления еще не завершен.

3. На завершающем этапе (t = 4...10 дней): затухание активной фазы эпидемии. Число активно инфицированных узлов падает экспоненциально, доля восстановленных растет. К концу периода наблюдения (t = 10 дней) 74.7 % сети получили иммунитет.

Распределение состояний можно наглядно видеть на рис. 4 в формате диаграммы. Данная форма визуализации позволяет проследить эволюцию системы как непрерывный процесс перераспределения узлов между состояниями. Характерной особенностью графика является отчетливо выраженная фаза активного противоборства между инфицированными и обнаруженными узлами в интервале 2–6 дней, когда площади соответствующих областей сопоставимы по величине. Это свидетельствует о том, что система безопасности работает с задержкой, но достаточно эффективно. Итоговое распределение указывает на то, что атака была частично успешной – значительная доля сети подверглась компрометации, хотя полного каскадного отказа удалось избежать благодаря системам обнаружения и восстановления.

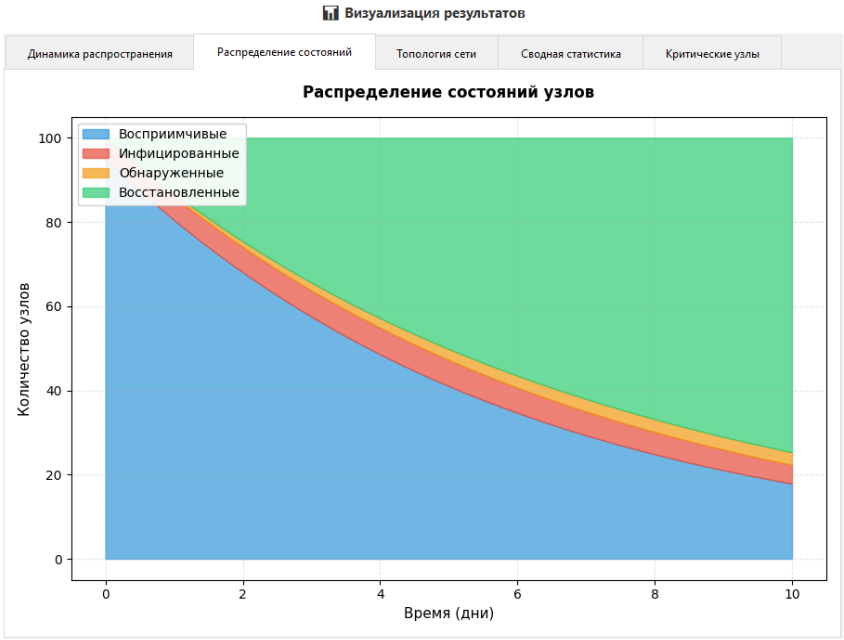

Рис. 4. **Распределение состояний узлов во времени**

Четыре цветные полосы, наложенные друг на друга, показывают, как меняется абсолютное и относительное число узлов в каждом состоянии. Визуально видно, как система переходит от состояния «почти все восприимчивы» к «почти все восстановлены», проходя через фазы активного заражения.

На рис. 5 представлена топология сети с цветовой индикацией статусов узлов.

Иерархическая структура: федеральный узел (красный, большой, вверху), региональные узлы (средние, большинство красные), муниципальные (маленькие, смешанные цвета), объектовые (маленькие, в основном синие). Размер узла пропорционален его степени центральности. Хорошо видно, что вирус в первую очередь поражает узлы верхних уровней иерархии – федеральные и региональные.

Анализ графика показывает критическую уязвимость централизованных архитектур: компрометация федерального узла приводит к каскадному отказу всей системы оповещения. Это подчеркивает необходимость эшелонированной защиты центральных узлов и физической изоляции от публичных сетей [6].

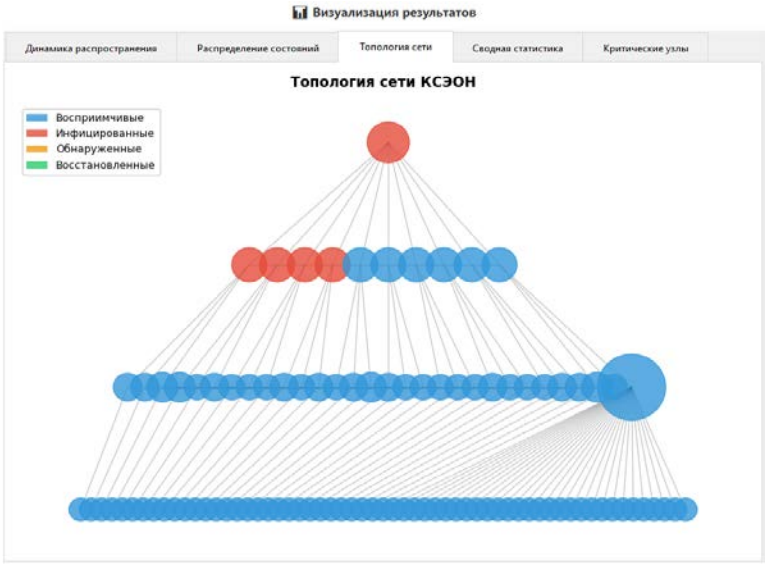

Рис. 5. **Топология сети КСЭОН при t ≈ 3 дня (пик эпидемии)**

Параметрический анализ чувствительности модели к изменению характеристик защиты

Для оценки влияния различных мер защиты и характеристик потенциальных угроз проведен анализ чувствительности модели. В таблице представлены результаты моделирования для пяти различных сценариев, показывающих, как изменение параметров модели влияет на динамику эпидемии.

Таблица

Анализ чувствительности: влияние параметров на динамику эпидемии в сети из 100 узлов

Сценарий	β	μ	σ	R_0	Время пика (дни)	Макс инфиц. узлов	Охват сети (%)
1. Базовый	0.30	0.15	0.25	2.00	3.84	6.3	74.7
2. Слабый вирус	0.10	0.15	0.25	0.67	–	2.1	18.5
3. Быстрое обнаружение	0.30	0.50	0.25	0.60	–	1.8	12.3
4. Медленное восстановление	0.30	0.15	0.05	2.00	3.92	6.8	76.1
5. Агрессивный вирус	0.70	0.05	0.10	14.0	1.21	18.5	95.2

Можно сделать следующие выводы, что сценарий 2 (слабый вирус, $\beta = 0.10$) несмотря на низкий уровень обнаружения, слабость вируса гарантирует, что эпидемия не разовьется. $R_0 = 0.67 < 1$. Охват – лишь 18.5 %.

Сценарий 3 (быстрое обнаружение, $\mu = 0.50$) – даже при агрессивном вирусе, если система обнаружения работает эффективно, эпидемия не развивается. $R_0 = 0.60 < 1$. Охват сокращается до 12.3 %. Это убедительно показывает, что инвестиции в SIEM-системы дают наибольший эффект.

Сценарий 4 (медленное восстановление, $\sigma = 0.05$) – медленное восстановление незначительно влияет на R_0 (он остается 2.0), так как параметр σ не входит в формулу R_0. Охват возрастает незначительно (76.1 % vs 74.7% в базовом).

Сценарий 5 (агрессивный вирус, $\beta = 0.70$, $\mu = 0.05$) – катастрофический сценарий, моделирующий распространение zero-day эксплойта. $R_0 = 14.0$. Вирус распространяется взрывоопасно, охватывает 95.2 % сети.

На основании тестовых значений можно сделать стратегические выводы:

1. Критическим параметром является коэффициент обнаружения (μ), а не скорость восстановления (σ). Переход μ с 0.15 на 0.50 снижает охват с 74.7 % на 12.3 %, тогда как изменение σ с 0.25 на 0.05 дает меньший эффект.

2. Для предотвращения эпидемии необходимо, чтобы $R_0 < 1$, то есть $\beta < \mu$. При текущих параметрах это требует либо снижения β (что сложно, зависит от вируса), либо увеличения μ (вполне достижимо через внедрение средств защиты).

3. Инвестиции в системы обнаружения и мониторинга дают лучший ROI, чем инвестиции в автоматизацию восстановления.

Идентификация критических узлов на основе метрик сетевой центральности

На рис. 6 показаны метрики центральности для выявления критически важных узлов. Слева показана степень узлов, посередине отображается близость узлов, а справа посредничество узлов. Горизонтальные столбчатые диаграммы показывают топ узлов по каждой метрике.

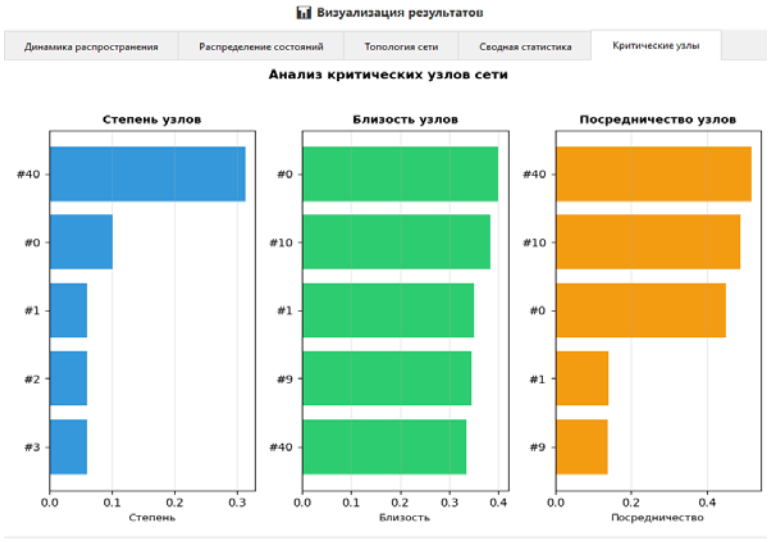

Рис. 6. **Анализ критических узлов сети по трем метрикам центральности**

Три типа центральности имеют разный практический смысл. Левый график показывает узлы с максимальным числом прямых соединений. Узел #40 имеет максимум (~0.35), что означает, что он подключен к 35 % всех остальных узлов. Практически, если такой узел скомпрометирован, вирус немедленно получает доступ к большому количеству соседей.

Средний график измеряет, насколько близко узел находится до всех остальных в среднем. Узел #0 (федеральный) имеет максимум (~0.55), что означает, кратчайший путь от него до любого другого узла минимален. Практически это главный «командный центр», от него быстрее всего распространяются команды управления, а значит, и вирус.

Правый график показывает долю кратчайших путей, проходящих через данный узел. Узел #40 имеет максимум (~0.4), означая, что 40 % кратчайших путей в сети проходят через него. Практически это критическая «точка отказа», его компрометация разобщает сеть.

На рис. 7 показана сводная статистика моделирования в формате четырех подграфиков.

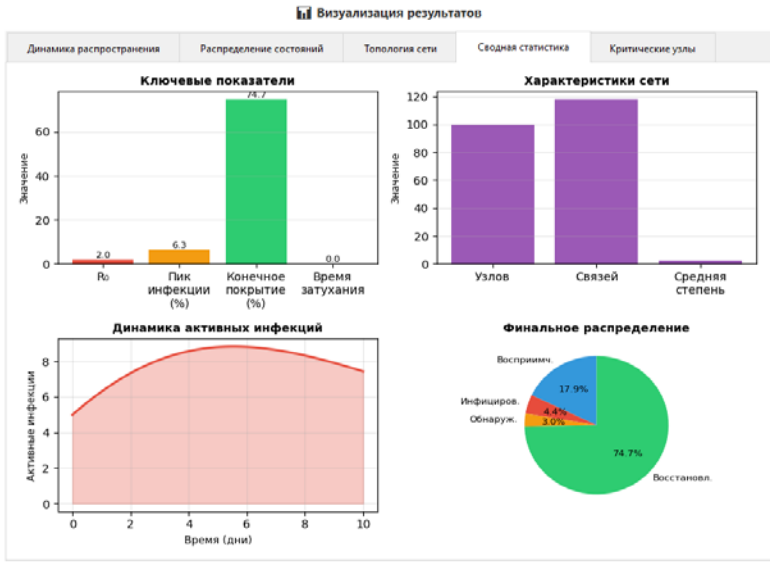

Рис. 7. **Сводная статистика моделирования при базовых параметрах**

Верхний левый – ключевые показатели (R_0, пик инфекции %, конечное покрытие %, время затухания). Верхний правый – характеристики сети (100 узлов, 119 связей, средняя степень 2.38). Нижний левый – динамика активных инфекций (область под кривой I(t)). Нижний правый – финальное распределение состояний (pie chart: 17.9 % восприимчивые, 74.7 % восстановленные).

Практическое применение программного комплекса в системе защиты КСЭОН

Разработанный программный модуль имеет прямое практическое применение:

1. Планирование инвестиций в защиту. На основе анализа чувствительности четко видно, что наиболее эффективно направлять финансирование на развертывание систем обнаружения (SIEM, SOC, EDR). Внедрение быстрого обнаружения ($\mu = 0.50$) снижает охват эпидемии с 74.7 % до 12.3 %.

2. Выявление критических узлов и приоритизация защиты. На основе метрик центральности определяются узлы, требующие особой внимательности: федеральный центр и реги ональные узлы требуют усиленной защиты, физической изоляции от публичных сетей.

3. Сценарное моделирование «что-если». Перед принятием важных решений администраторы могут смоделировать различные сценарии. Например: «Что произойдет, если мы внедрим новую SIEM-систему и поднимем коэффициент обнаружения μ с 0.15 до 0.40?»

4. Обучение и обоснование стратегии для руководства. Наглядные графики позволяют объяснить руководству, почему защита критической инфраструктуры требует постоянного внимания и инвестиций.

5. Подготовка процедур восстановления после инцидента. На основе моделирования можно оценить, за какое время при заданном σ удастся восстановить 50 %, 75 %, 95 % сети.

На текущем этапе реализована основная функциональность. Для реального использования потребуется:

– Калибровка параметров модели (β, μ, σ) на реальных данных инцидентов;

– Интеграция с системами мониторинга КСЭОН для получения актуальных значений параметров в реальном времени;

– Расширение для учета multi-phase атак;

– Добавление стоимостного анализа для оптимизации распределения ресурсов.

Заключение

Разработанный программный комплекс представляет собой практический инструмент для анализа устойчивости сети КСЭОН к киберугрозам. Адаптация эпидемиологической модели PSIDR к специфике иерархической сетевой инфраструктуры позволяет количественно оценивать эффективность различных стратегий защиты и моделировать сценарии «что-если» [7].

Проведенный анализ чувствительности показывает критическую роль систем обнаружения угроз: инвестиции в SIEM дают больший эффект, чем инвестиции в скорость восстановления. Выявление критических узлов сети позволяет приоритизировать защитные меры [8].

Тестовый сценарий ($R_0 = 2.0$) демонстрирует, что при текущих параметрах защиты система подвергается значительному риску, охватывая 74.7 % сети за 10 дней. Однако агрессивное внедрение систем обнаружения может привести систему в режим $R_0 < 1$, при котором эпидемия затухает самостоятельно.

Модульная архитектура программного комплекса позволяет легко расширять функциональность и адаптировать модель под конкретные условия. Дальнейшее развитие предполагает интеграцию с реальными данными КСЭОН, применение методов машинного обучения для автоматической калибровки параметров, и разработку интеграции с SIEM-системами для обновления параметров в реальном времени [9].

Разработанный программный продукт представляет собой практический инструмент для количественной оценки устойчивости сети КСЭОН МЧС России к киберугрозам.

Адаптация эпидемиологической модели PSIDR к специфике иерархической четырехуровневой топологии критической инфраструктуры позволяет моделировать сценарии «что-если» и оценивать эффективность различных стратегий защиты.

Основные результаты исследования:

1. Проведенный анализ чувствительности продемонстрировал критическую роль систем обнаружения угроз: повышение коэффициента обнаружения μ с 0,15 до 0,50 снижает охват эпидемии в 6 раз (с 74,7 % до 12,3 %), что значительно превосходит эффект от ускорения восстановления узлов.

2. Выявлены критические узлы инфраструктуры на основе метрик центральности (степень, близость, посредничество), компрометация которых приводит к каскадному отказу системы оповещения. Федеральный и региональные узлы требуют приоритетной защиты и физической изоляции от публичных сетей.

3. Установлено, что для предотвращения эпидемии необходимо обеспечить условие $R_0 < 1$, что достигается превышением скорости обнаружения над скоростью распространения ($\beta < \mu$).

Дальнейшее развитие инструмента предполагает калибровку параметров модели на реальных данных инцидентов, интеграцию с системами мониторинга КСЭОН для получения актуальных значений в режиме реального времени, расширение для учета многоэтапных атак и добавление стоимостного анализа для оптимизации распределения ресурсов. Модульная архитектура программного комплекса обеспечивает простоту адаптации под специфические условия различных регионов и уровней иерархии системы оповещения МЧС России[10].

Список источников

1. Арванова С.М., Ксенофонтов А.С., Москаленко Л.А. Криптографические механизмы безопасности // Научный альманах. 2015. № 7(9). С. 578–580.

2. Лаврова Д.С. Моделирование сетевой инфраструктуры сложных крупномасштабных объектов, в том числе критического назначения, с использованием теории графов // Проблемы информационной безопасности. Компьютерные системы. 2019. № 1. С. 26–33.

3. Калениченко С.Е., Тарасова Л.Д., Григорян Д.Р. Модель вероятно-клеточного автомата PSIDR // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сб. науч. ст. СПб.: СПбГУТ. 2022. Т. 1. С. 516–520.

4. Рябко А.В., Печкуров А.В. Математическая модель защиты компьютерной сети от вирусов // Программные продукты и системы. 2016. №4. С. 125–128.

5. Гущин Г.В. Системы оповещения населения: назначение, задачи и требования к функционированию // Гражданская оборона и защита от чрезвычайных ситуаций в учреждениях, организациях и на предприятиях. 2024. № 1. С. 25–32.

6. Метельков А.Н. Моделирование сценариев кибератак в киберполигонах // Научно-аналитический журнал «Вестник Санкт-Петербургского университета ГПС МЧС России». 2023. № 2. С. 161–176.

7. Корчагин С.А., Рубцов Д.Ю., Беспалова Н.В., Сердечный Д.В. Разработка интеллектуальных моделей проактивной защиты критической инфраструктуры финансового сектора // Моделирование, оптимизация и информационные технологии. 2024. Т. 12. № 4.

8. Мельников А.В. Модель оценки эффективности организационных мер для обеспечения информационной безопасности автоматизированных систем специального назначения при появлении неизвестной вредоносной программы // Экономика. Информатика. 2023. Т. 50. № 4. С. 873–882.

9. ГОСТ Р 22.7.05-2022. Безопасность в чрезвычайных ситуациях. Локальные системы оповещения. Общие технические требования. М.: Российский институт стандартизации, 2022. 16 с.

10. Методические рекомендации по поддержанию в состоянии постоянной готовности к использованию систем оповещения населения (утв. МЧС России 26.06.2024 № 2). М.: МЧС России, 2024.

References

1. Arvanova S.M., Ksenofontov A.S., Moskalenko L.A. Kriptograficheskie mekhanizmy bezopasnosti // Nauchnyj al'manah. 2015. № 7(9). S. 578–580.

2. Lavrova D.S. Modelirovanie setevoj infrastruktury slozhnyh krupnomasshtabnyh ob''ektov, v tom chisle kriticheskogo naznacheniya, s ispol'zovaniem teorii grafov // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy. 2019. № 1. S. 26–33.

3. Kalenichenko S.E., Tarasova L.D., Grigoryan D.R. Model' veroyatno-kletochnogo avtomata PSIDR // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii: sb. nauch. st. SPb.: SPbGUT. 2022. T. 1. S. 516–520.

4. Ryabko A.V., Pechkurov A.V. Matematicheskaya model' zashchity komp'yuternoj seti ot virusov // Programmnye produkty i sistemy. 2016. №4. S. 125–128.

5. Gushchin G.V. Sistemy opoveshcheniya naseleniya: naznachenie, zadachi i trebovaniya k funkcionirovaniyu // Grazhdanskaya oborona i zashchita ot chrezvychajnyh situacij v uchrezhdeniyah, organizaciyah i na predpriyatiyah. 2024. № 1. S. 25–32.

6. Metel'kov A.N. Modelirovanie scenariev kiberatak v kiberpoligonah // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta GPS MCHS Rossii». 2023. № 2. S. 161–176.

7. Korchagin S.A., Rubcov D.YU., Bespalova N.V., Serdechnyj D.V. Razrabotka intellektual'nyh modelej proaktivnoj zashchity kriticheskoj infrastruktury finansovogo sektora // Modelirovanie, optimizaciya i informacionnye tekhnologii. 2024. T. 12. № 4.

8. Mel'nikov A.V. Model' ocenki effektivnosti organizacionnyh mer dlya obespecheniya informacionnoj bezopasnosti avtomatizirovannyh sistem special'nogo naznacheniya pri poyavlenii neizvestnoj vredonosnoj programmy // Ekonomika. Informatika. 2023. T. 50. № 4. S. 873–882.

9. GOST R 22.7.05-2022. Bezopasnost' v chrezvychajnyh situaciyah. Lokal'nye sistemy opoveshcheniya. Obshchie tekhnicheskie trebovaniya. M.: Rossijskij institut standartizacii, 2022. 16 s.

10. Metodicheskie rekomendacii po podderzhaniyu v sostoyanii postoyannoj gotovnosti k ispol'zovaniyu sistem opoveshcheniya naseleniya (utv. MCHS Rossii 26.06.2024 № 2). M.: MCHS Rossii, 2024.

Информация о статье:
Статья поступила в редакцию: 01.12.2025; одобрена после рецензирования: 15.02.2026;
принята к публикации: 19.02.2026

The information about article:
The article was submitted to the editorial office: 01.12.2025; approved after review: 15.02.2026;
accepted for publication: 19.02.2026

Сведения об авторах:
Арванова Саният Мухамедовна, старший преподаватель кафедры компьютерных технологий и информационной безопасности института электроники, робототехники и искусственного интеллекта Кабардино-Балкарского государственного университета, (360004, г. Нальчик, ул. Чернышевского, д. 175**)**, email: sani_07@mail.ru, SPIN-код: 6933-0937
Бархатов Константин Сергеевич, студент института электроники, робототехники и искусственного интеллекта Кабардино-Балкарского государственного университета, (360004, г. Нальчик, ул. Чернышевского, д. 175**)**, e-mail: barhatov364@gmail.com
Гергов Идар Хабасович, студент института электроники, робототехники и искусственного интеллекта Кабардино-Балкарского государственного университета, (360004, г. Нальчик, ул. Чернышевского, д. 175**)**, e-mail: gergov44559@gmail.com
Курданов Халид Солтанович, студент института электроники, робототехники и искусственного интеллекта Кабардино-Балкарского государственного университета, (360004, г. Нальчик, ул. Чернышевского, д. 175**)**, e-mail: khalidkurdanov@mail.ru
Information about the authors:
Arvanova Saniyat M., senior lecturer at of the department of computer technology and information security of the institute of electronics, robotics and artificial intelligence of Kabardino-Balkarian State university, (360004, Nalchik, Chernyshevsky str., 175), email: sani_07@mail.ru, SPIN: 6933-0937
Barkhatov Konstantin S., student of the institute of electronics, robotics and artificial intelligence of Kabardino-Balkarian State university, (360004, Nalchik, Chernyshevsky str., 175), e-mail: barhatov364@gmail.com
Gergov Idar K., student of the institute of electronics, robotics and artificial intelligence of the Kabardino-Balkarian State university, (360004, Nalchik, Chernyshevskogo str., 175), e-mail: gergov44559@gmail.com
Kurdanov Khalid S., student of the institute of electronics, robotics and artificial intelligence of the Kabardino-Balkarian State university, (360004, Nalchik, Chernyshevskogo str., 175), e-mail: khalidkurdan