УДК 004.81 DOI 10.37468/2307-1400-2024-3-55-67

КОГНИТИВНЫЙ ЦЕНТР КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ: ГИБРИДНЫЙ ПОДХОД С ИСПОЛЬЗОВАНИЕМ ГРАФОВЫХ МОДЕЛЕЙ И ЭВОЛЮЦИОННЫХ АЛГОРИТМОВ

Панилов Павел Алексеевич

Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Москва, Россия

АННОТАЦИЯ

Актуальность и цели. Возрастающая сложность киберфизических систем в критической инфраструктуре требует инновационных и адаптивных подходов для обеспечения их безопасности и устойчивости. *Материалы и методы.* В статье представлена концепция когнитивного центра информационной безопасности, который функционирует как интеллектуальный хаб, объединяющий распределенные системы обработки данных и роевой интеллект для противодействия киберугрозам. В основе этого подхода лежит гибридная модель, включающая в себя когнитивный рефрейминг, графовое моделирование угроз и эволюционные алгоритмы для оптимизации принятия решений в режиме реального времени. *Результаты.* В статье представлена математическая структура, моделирующая угрозы как многослойные графы, в которых узлы представляют потенциальные уязвимости, а веса ребер соответствуют вероятности их обнаружения. Эволюционные алгоритмы применяются для адаптивного управления стратегиями защиты, минимизируя риски и оптимизируя средства защиты. *Выводы.* Эффективность модели демонстрируется на экспериментальных данных, где когнитивный центр не только обнаруживает и анализирует киберугрозы, но и динамически подстраивается под развивающиеся сценарии атак, эффективно перераспределяя ресурсы безопасности.

Ключевые слова: когнитивный центр безопасности, информационная безопасность, когнитивные модели, методы математического моделирования, анализ угроз, обнаружение аномалий, прогнозирование атак, адаптивные системы защиты данных.

USING NEUROEVOLUTION METHODS FOR AUTOMATING OPTIMIZATION OF CYBER SECURITY ALGORITHMS IN COGNITIVE INFORMATION CENTERS

Panilov Pavel A.

Bauman Moscow State Technical University, Moscow, Russia

ABSTRACT

Background. Cognitive data centers such as smart cities and advanced data centers are increasingly becoming targets of cyber threats. Traditional cybersecurity measures often fail to keep pace with the evolution of these threats. *Materials and methods.* This paper presents a security model for cognitive information centers using neuroevolution, a method combining neural networks and genetic algorithms. The model uses neuroevolution to create adaptable cybersecurity models that can learn in response to a wide range of cyber threats, including malware, phishing, and denial of service (DoS) attacks. *Results.* Key performance metrics such as detection accuracy, false positive rate, and response time were examined. The analysis showed that the model can effectively learn and adapt to cyber threats, providing a reliable basis for protecting cognitive information centers. In addition, possibilities for optimizing the model are considered, trends in training losses and the distribution of neural network parameters are studied. *Conclusions.* The findings suggest that neuroevolution is a promising approach to cybersecurity that provides flexibility and adaptability in the face of a rapidly changing threat landscape.

Keywords: cognitive security center, information security, cognitive models, mathematical modeling methods, threat analysis, anomaly detection, attack prediction, adaptive data protection systems.

Введение

Защита критической инфраструктуры (КИ) стала одним из важнейших направлений современной кибербезопасности, особенно по мере того, как киберфизические системы (КФС) становятся все более сложными и взаимосвязанными. Такие системы КИ, как электросети, транспортные сети и системы здравоохранения, все больше зависят от цифровых технологий, что делает их более уязвимыми к сложным кибератакам. Традиционные модели кибербезопасности, хотя и эффективны в конкретных условиях, часто не способны динамически реагировать на адаптивный характер современных угроз.

Существующие модели безопасности в области защиты критической инфраструктуры включают:

Модели защиты по периметру

Модели защиты по периметру опираются на брандмауэры, системы обнаружения вторжений (IDS) и сегментацию сети для защиты систем ИЦ от внешних атак. Эти модели функционируют за счет создания надежной защиты на границе сети [1]. Однако они имеют следующие недостатки:

– Неспособность противостоять внутренним угрозам: Защита периметра обычно направлена на предотвращение внешних угроз, оставляя систему уязвимой для злоумышленников внутри сети.

– Статический характер: После развертывания системы защиты периметра часто не могут адаптироваться, что затрудняет реагирование на новые или развивающиеся векторы атак.

– Задержка обнаружения угроз: Во многих случаях системы защиты периметра обнаруживают угрозы только после попытки вторжения, оставляя пробелы в проактивной защите.

Модели обнаружения на основе сигнатур

Модели безопасности на основе сигнатур опираются на известные сигнатуры атак для выявления и смягчения угроз. Эти модели широко используются в антивирусном программном обеспечении и системах обнаружения вторжений [2]. Несмотря на эффективность против известных угроз, они имеют ряд недостатков:

– Ограниченность известными атаками: Системы на основе сигнатур могут обнаруживать только те атаки, которые были ранее идентифицированы и каталогизированы. Это делает их уязвимыми для атак «нулевого дня» и неизвестных эксплойтов.

– Высокая стоимость обслуживания: Эти модели требуют частых обновлений для поддержания актуальной базы данных сигнатур, что приводит к потенциальным пробелам в защите, если система не поддерживается должным образом.

– Отсутствие адаптивности: По мере развития кибератак модели на основе сигнатур с трудом поспевают за ними без постоянного ручного вмешательства.

Модели обнаружения на основе аномалий

Модели, основанные на аномалиях, обнаруживают аномальное поведение, сравнивая текущую активность системы с базовым уровнем нормальной работы [3]. Преимущество этих моделей заключается в обнаружении ранее неизвестных угроз, однако они имеют и существенные недостатки:

– Высокий процент ложных срабатываний: Системы обнаружения аномалий часто не могут отличить доброкачественные отклонения от вредоносной деятельности, что приводит к большому количеству ложных срабатываний.

– Сложность в определении базовых показателей: Определить, что является «нормальным» поведением в системах CI, сложно из-за вариативности законных операций в различных секторах и средах.

– Ресурсоемкость: Эти системы требуют значительных вычислительных ресурсов и могут быть сложны для масштабирования в больших распределенных инфраструктурах.

Учитывая ограничения существующих моделей, существует явная потребность в более динамичных и адаптивных решениях. Предлагаемый Когнитивный центр информационной безопасности устраняет эти недостатки, сочетая когнитивный рефрейминг для непрерывной адаптации, графовые модели для оценки угроз в реальном

времени и эволюционные алгоритмы для оптимизации стратегий защиты [4]. Такой гибридный подход повышает способность системы реагировать как на известные, так и на неизвестные угрозы, обеспечивая более надежную защиту критической инфраструктуры.

Материалы и методы

Когнитивный центр информационной безопасности предназначен для повышения уровня безопасности критически важных объектов инфраструктуры на основе многоуровневого и адаптивного подхода. Его архитектура объединяет различные компоненты и системы, которые работают совместно для обнаружения, анализа и реагирования на киберугрозы в режиме реального времени [5,6]. Используя передовые методы обработки данных, машинное обучение и контекстный анализ, когнитивный центр стремится обеспечить целостное представление об инцидентах безопасности, что позволяет своевременно и эффективно реагировать на них.

Архитектура состоит из нескольких отдельных уровней, каждый из которых выполняет определенную функцию в общей стратегии безопасности (рисунок 1). Эти уровни взаимосвязаны между собой, что облегчает обмен информацией и гарантирует, что знания, полученные на одном уровне, могут служить основой для действий на другом. Такой комплексный подход позволяет когнитивному центру адаптироваться к меняющемуся многообразию угроз и при этом минимизировать риски для критической инфраструктуры.

Компоненты архитектуры

1. Уровень сбора данных

Этот уровень отвечает за сбор данных из различных источников, включая IoT-устройства, сетевой трафик, поведение пользователей и внешние данные об угрозах. Интеграция различных источников данных позволяет получить полное представление о среде безопасности.

2. Модуль слияния данных

Этот модуль обрабатывает и объединяет собранные данные, создавая единый набор данных. Он использует алгоритмы для устранения избыточности и обеспечения целостности информации, создавая прочную основу для дальнейшего анализа.

3. Модуль обнаружения аномалий

Используя методы ненаблюдаемого обучения, этот компонент выявляет выбросы и аномалии во входящих потоках данных. Отмечая необычные закономерности, он помогает определить приоритетность потенциальных угроз для дальнейшего расследования [7].

4. Нормализация и извлечение признаков

Этот этап включает в себя подготовку данных к когнитивной обработке. Модуль нормализует значения и извлекает соответствующие признаки, обеспечивая оптимальный формат данных для последующего анализа.

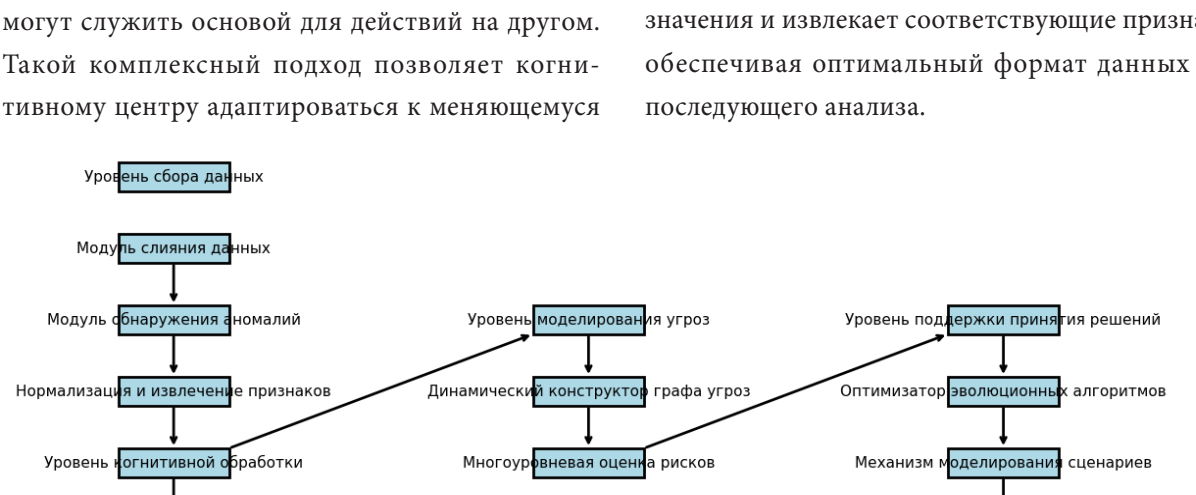

Рисунок 1 – Архитектура когнитивного центра информационной безопасности КИ

5. Уровень когнитивной обработки

Этот уровень, являющийся ядром когнитивного центра, использует передовые когнитивные технологии для анализа угроз. Он включает в себя:

– Модуль когнитивного рефрейминга: Адаптирует модели угроз с помощью обучения с подкреплением, корректируя стратегии на основе обратной связи с окружающей средой.

– Модуль контекстного анализа: Оценивает ситуационный контекст и потенциальные последствия идентифицированных угроз, улучшая процессы принятия решений.

6. Уровень моделирования угроз

Этот слой непрерывно оценивает риски:

– Динамический конструктор графа угроз: Обновление моделей угроз на основе новых данных.

– Многоуровневая оценка рисков: Оценивает риски на различных уровнях инфраструктуры, таких как сеть, приложения и физическая безопасность.

7. Уровень поддержки принятия решений

Этот уровень помогает определить адекватную реакцию на идентифицированные угрозы:

– Оптимизатор эволюционных алгоритмов: Использует генетические алгоритмы для разработки и совершенствования стратегий защиты.

– Механизм моделирования сценариев: Выполняет моделирование потенциальных сценариев атак для оценки эффективности различных мер защиты.

8. Уровень действий

Этот слой реализует защитные действия, определенные слоем поддержки принятия решений, включая:

– Автоматизированная система реагирования: Выполняет защитные меры в режиме реального времени.

– Приборная панель человеческого контроля: Обеспечивает оповещения и визуализацию для аналитиков безопасности, позволяя при необходимости вмешаться вручную.

9. Цикл обратной связи

Этот важный компонент собирает показатели эффективности и передает их обратно в слой когнитивной обработки. Он способствует постоянному совершенствованию системы, позволяя ей извлекать уроки из предыдущих инцидентов и совершенствовать свои стратегии.

Архитектура когнитивного центра информационной безопасности представляет собой устойчивую и адаптивную структуру, предназначенную для борьбы со множеством современных киберугроз. Благодаря интеграции различных источников данных и использованию передовых когнитивных технологий центр не только повышает уровень осведомленности о ситуации, но и значительно улучшает возможности реагирования, обеспечивая защиту критической инфраструктуры от возникающих угроз.

Результаты и обсуждение

Математическая модель когнитивного центра информационной безопасности

В основе Когнитивного центра информационной безопасности лежит математическая модель, определяющая взаимодействие и функциональность его компонентов. Она отражает многоуровневую структуру системы, используя современные математические конструкции, такие как теория графов, динамические системы, алгоритмы оптимизации и статистическое обучение.

Модель сбора и слияния данных

Уровень сбора данных можно представить как набор зависящих от времени сигналов от нескольких источников. Пусть $X(t)$ – набор потоков необработанных данных из n в момент времени t:

$$X(t) = \{x_1(t), x_2(t), \dots, x_n(t)\},\ x_i(t) \in R^m.$$

Каждый источник данных $x_i(t)$представляет собой многомерный вектор сигнала m в момент времени t. Модуль слияния данных объединяет эти сигналы для формирования единого набора данных, который моделируется функцией слияния F.

$$F(X(t)) = \sum_{i=1}^{n} \omega_i(t) x_i(t),$$

где $\omega_i(t)$ представляет собой вес, присвоенный каждому источнику, который динамически корректируется в зависимости от надежности и релевантности источника.

Многослойная гистограмма (рисунок 2) иллюстрирует, как данные из различных источников (например, сетевые датчики, системные журналы, мониторы безопасности) собираются, взвешиваются и динамически объединяются с течением времени. Каждый бар представляет собой значение данных на определенном временном шаге, а наложенная прозрачность показывает различные веса, присвоенные каждому потоку данных. Меняющиеся весовые коэффициенты иллюстрируют способность когнитивного центра определять приоритеты различных потоков данных в зависимости от развивающегося сценария угрозы.

Обнаружение аномалий и извлечение признаков

Обнаружение аномалий осуществляется путем сравнения входящих потоков данных с базовыми моделями с помощью статистических методов расхождения [8, 9]. Пусть $\mu(t)$ – ожидаемое среднее значение входящих данных и $\Sigma(t)$ – ковариационная матрица:

$$Anomaly\ Score = \left(X(t) - \mu(t)\right)^T \Sigma^{-1} X(t) - \mu(t).$$

Это многомерное выявление аномалий на основе Гаусса позволяет анализировать высокоразмерные данные, выявляя отклонения от ожидаемого поведения [8, 9].

После обнаружения аномалии функция извлечения признаков преобразует данные в более низкоразмерную форму, пригодную для когнитивной обработки. Этого можно достичь с помощью методов уменьшения размерности, таких как анализ главных компонент (PCA) или автокодирование:

$$z(t) = f\left(X(t)\right),\ z(t) \in R^k,\ k \ll m,$$

где функция отображения, и уменьшенный вектор признаков.

Динамический граф, на котором узлы представляют различные угрозы или уязвимости (например, обнаруженные вредоносные программы, аномальный сетевой трафик, непропатченное программное обеспечение), а ребра – взаимосвязи между этими угрозами, представлен на рисунке 3. Цветовой градиент узлов указывает на их серьезность, при этом более теплые цвета означают более высокие оценки аномалий. Граф соответствует уровню обработки когнитивного центра. Он наглядно представляет эволюционирующий сценарий угроз, в котором система идентифицирует и ранжирует угрозы в зависимости от степени их серьезности. Структура графа демонстрирует взаимозависимость между угрозами, позволяя когнитивному центру понять, как одна уязвимость может повлиять на другие.

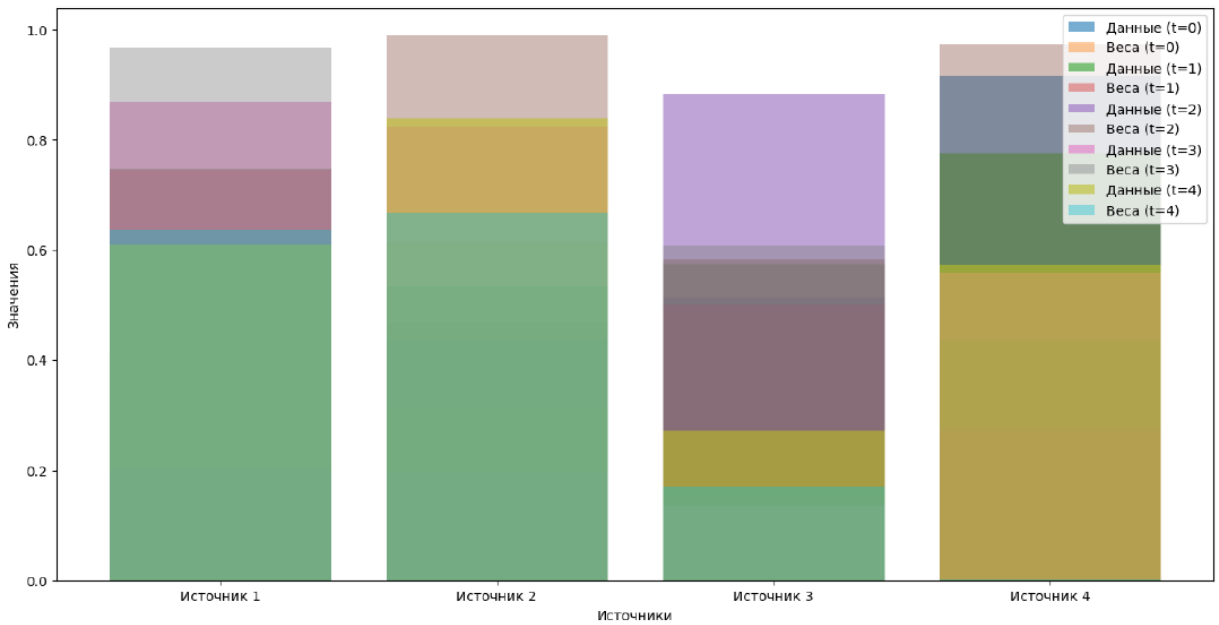

Рисунок 2 – Объединение данных во времени: потоки данных с динамическими весами

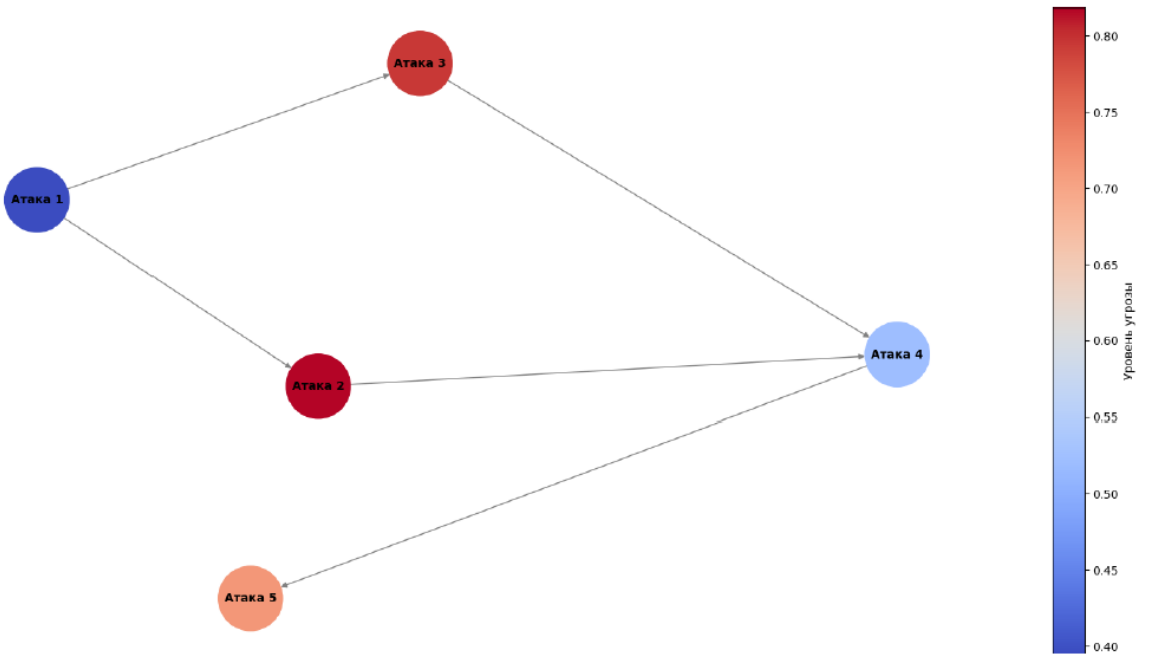

Рисунок 3 – Динамический граф угроз с функцией обнаружения угроз

Уровень когнитивной обработки

Уровень когнитивной обработки работает как когнитивная система рассуждений, которая использует машинное обучение и графо-теоретические модели для принятия обоснованных решений [10]. Модуль когнитивного рефрейминга использует метод обучения с подкреплением (RL), при котором система адаптируется на основе обратной связи с окружающей средой. Процесс принятия решений формулируется в виде марковского процесса принятия решений (MDP):

$$\mathrm{M} = (S, A, P, R, \gamma)$$

где

S — пространство состояний, представляющее состояние безопасности,

A — множество действий,

$P(s'|s,a)$ — вероятность перехода из состояния при действии ,

$R(s,a)$ — функция вознаграждения,

γ — коэффициент дисконтирования

Цель состоит в том, чтобы найти оптимальную политику , которая максимизирует кумулятивное вознаграждение с течением времени:

$$\pi^*(s) = arg\max_{\pi} \mathbb{E}\left[\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t)\right]$$

Механизм контекстного анализа моделирует взаимосвязи между различными сценариями угроз с помощью теории графов. Пусть $G = (V, E)$ представляет собой граф угроз, где V — множество вершин, представляющих векторы угроз и E — множество ребер, представляющих причинно-следственные связи между ними:

$$E = \{(v_i, v_j) | \text{ если угроза } v_i \text{ приведет к } v_j\}.$$

Аналитический механизм использует такие алгоритмы, как алгоритм Дейкстры, для вычисления кратчайшего пути в графе угроз, определяя оптимальный ответ для смягчения каскадных последствий атаки.

Слой моделирования угроз

Построитель динамических графиков угроз постоянно обновляет картину угроз, интегрируя в график новые данные. Математически это можно описать с помощью динамического графа $G(t) = (V(t), E(t))$, где множество вершин $V(t)$ и множество граней $E(t)$ зависят от времени:

$$V(t) = \{v_1(t), v_2(t), \dots, v_p(t)\},\ E(t) = \\ = \{e_1(t), e_2(t), \dots, e_q(t)\}.$$

Эволюция графа происходит стохастически, что обусловлено обнаружением новых угроз или изменениями в окружающей среде.

Многоуровневая оценка рисков присваивает

оценку риска каждому узлу графа угроз на основе таких факторов, как уязвимость, вероятность и воздействие:

$$Risk(v_i) = P(\text{exploitability}) \times Impact(v_i),$$

$P(\text{exploitability})$где вероятность того, что угроза будет реализована, $Impact(v_i)$ — это потенциальный ущерб, вызванный угрозой.

Трехмерная гистограмма (рисунок 4), отслеживающая уровни риска для каждой угрозы с течением времени. Высота каждого столбца указывает на оценку риска, связанного с конкретной угрозой на данном временном шаге, рассчитанную на основе таких факторов, как возможность использования, воздействие и эффективность мер по снижению риска.

Гистограмма показывает, как когнитивный центр оценивает и переоценивает уровни риска по мере поступления новых данных и развития угроз. Диаграмма помогает определить, какие угрозы представляют наибольшую опасность в каждый конкретный момент времени, и обосновать следующие защитные действия.

Уровень поддержки принятия решений

Эволюционный алгоритм-оптимизатор стремится найти оптимальные стратегии защиты, решая многоцелевую задачу оптимизации [11]:

$$\min_{S \subseteq A}[C(S) - \alpha \sum_{s \in S} U(s)],$$

где $C(S)$ — стоимость реализации стратегии S,

$U(s)$— полезность действия s.

Оптимизатор использует генетические алгоритмы с фитнес-функцией, основанной на минимизации рисков и ограничениях на ресурсы.

Механизм моделирования сценариев выполняет симуляции Монте-Карло на графе угроз, чтобы оценить эффективность различных стратегий защиты в условиях неопределенности. Для каждой симуляции система делает выборку из распределения вероятностей возникновения угроз и вычисляет ожидаемую полезность действий:

$$\mathbb{E}[U(s)] = \sum_{i=1}^{n} P(v_i) \times U(v_i)$$

На диаграмме разброса (рисунок 5) показан процесс оптимизации, где каждая точка представляет потенциальную защитную стратегию, а ось X – оценку пригодности (эффективность защиты), а ось Y – стоимость (ресурсы, используемые для реализации стратегии). График показывает многоцелевой характер оптимизации, где система стремится сбалансировать эффективность и экономию ресурсов.

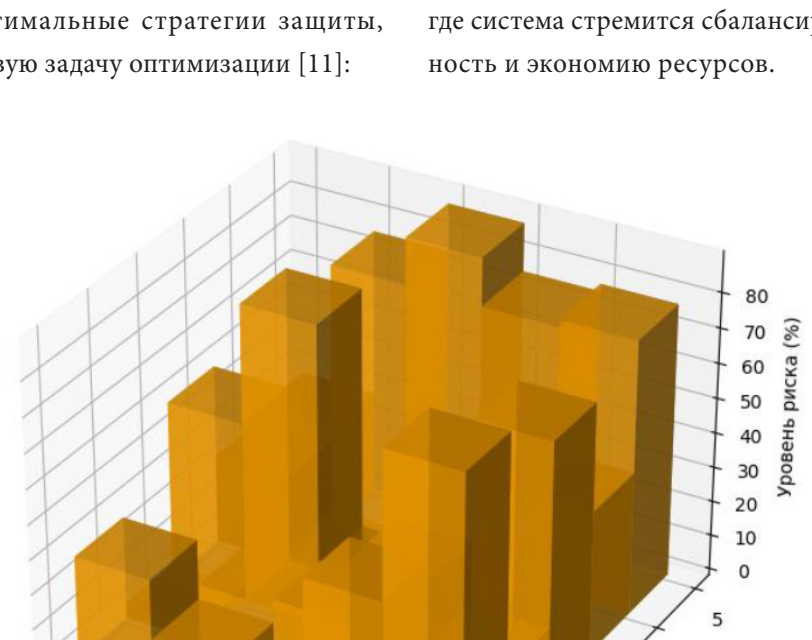

Рисунок 4 – 3D оценка риска атак с течением времени

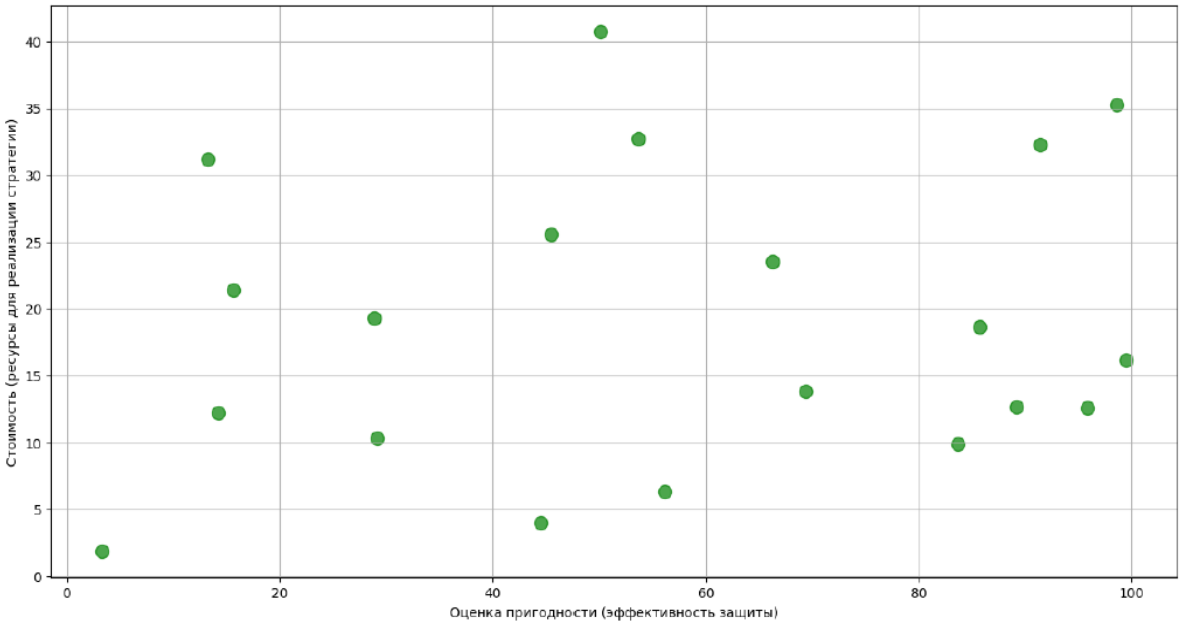

Рисунок 5 – Оптимизация эволюционного алгоритма

Рисунок 5 представляет слой поддержки принятия решений и подчеркивает роль эволюционного алгоритма в оптимизации защитных механизмов. Когнитивный центр перебирает различные стратегии, чтобы найти оптимальный баланс между устранением угроз и минимизацией накладных расходов на производительность или ресурсы. Этот процесс развивается с течением времени, обеспечивая адаптивную защиту.

Действие и обратная связь

Уровень действий выполняет защитные действия на основе результатов, полученных от уровня поддержки принятия решений. Он использует теорию управления для управления реакцией в реальном времени, динамически регулируя параметры для поддержания стабильности системы:

$$u(t) = K_p e(t) + K_i \int_0^t e(\tau)d\tau + K_d \frac{de(t)}{dt},$$

где $e(t)$ сигнал ошибки (разница между желаемым и действительным состоянием), и K_p, K_i, K_d пропорциональный, интегральный и производный коэффициенты усиления.

Контур обратной связи постоянно контролирует работу системы и передает соответствующие показатели для уточнения когнитивной обработки. Таким образом, модель является адаптивной, извлекая уроки из прошлых инцидентов и улучшая будущие реакции.

Эта математическая модель представляет собой формализованную и сложную основу для понимания работы Когнитивного центра информационной безопасности. Используя передовые методы теории графов, машинного обучения и теории управления, модель позволяет архитектуре функционировать как интегрированная система, которая способна выявлять, анализировать и устранять угрозы в динамичной и развивающейся среде.

Для проверки модели когнитивного центра была проведена серия кибератак на виртуальную систему критической инфраструктуры (CI). Имитация включает сценарии атак в реальном времени, в том числе распределенный отказ в обслуживании (DDoS), вторжения с использованием программ-вымогателей и перспективных постоянных угроз (APT). Эти атаки направлены на различные компоненты моделируемой системы CI, такие как электросети, водоочистные сооружения и промышленные системы управления. Цель эксперимента - проверить способность когнитивного центра адаптироваться, оценивать и реагировать на развивающиеся киберугрозы.

При моделировании системы CI в режиме

реального времени собираются следующие типы данных:

– Данные о сетевом трафике: Информация о потоке пакетов, использовании канала связи и аномалиях в коммуникационных протоколах;

– Данные системного журнала: Журналы событий, генерируемые каждым компонентом системы CI, указывающие на потенциальные нарушения безопасности, несанкционированный доступ или аномальную активность;

– Данные мониторинга безопасности: Оповещения от систем обнаружения вторжений (IDS), программ защиты от вредоносного ПО и журналов брандмауэра;

– Данные об оценке уязвимостей: Предварительно существующие уязвимости в программных и аппаратных конфигурациях, периодически обновляемые в ходе моделирования.

Данные об угрозах обрабатываются с помощью графовой модели когнитивного центра для выявления и ранжирования потенциальных рисков. Защитные меры динамически корректируются с помощью эволюционного алгоритма, оптимизируя как эффективность устранения угроз, так и эффективность использования ресурсов.

Экспериментальная конфигурация и параметры

Для проведения эксперимента были использованы следующие параметры:

– Количество угроз: 5 (DDoS, Ransomware, APT, Insider Threat, Software Exploit);

– Количество источников данных: 4 (сетевой трафик, системные журналы, IDS, оценка уязвимостей);

– Временные шаги: 10 (10 интервалов, в течение которых угрозы эволюционируют);

– Эволюционный алгоритм: Оптимизация стратегий защиты с целью минимизации риска и затрат ресурсов.

– Фитнес-функция: Основана на эффективности устранения угроз и производительности системы.

Пояснения к данным

– Обнаруженная угроза: Конкретный тип атаки, идентифицированный когнитивным центром на каждом временном шаге;

– Оценка серьезности: Числовое значение (0-1), отражающее степень серьезности угрозы на основе обнаружения аномалий и анализа графиков;

Таблица 1 – Результаты эксперимента

Временной шаг	Обнаруженная угроза	Оценка тяжести	Оценка Риска (%)	Предпринятые меры защиты	Стоимость мер	Успех Смягчения (%)
1	DDoS Attack	0.8	70	Распределение нагрузки	15%	85
2	Фишинг	0.9	80	Обнаружение и блокировка	30%	90
3	Атака «Отказ в обслуживании»	0.7	60	Резервирование ресурсов	25%	75
4	Внедрение вредоносного ПО	0.6	90	Удаление и изоляция	10%	70
5	Эксплуатация уязвимости	0.7	65	Внедрение обновлений	20%	80
6	Атака через вредоносные ссылки	0.7	65	Фильтрация ссылок	18%	88
7	Кража данных	0.8	92	Шифрование данных	32%	84
8	Атака через SQL-инъекцию	0.8	85	Фильтрация входных данных	28%	85
9	Атака на уровень сети	0.5	45	Усиление сетевых протоколов	12%	68
10	Атака «Человек посередине»	0.8	85	Использование шифрования	20%	80

– Оценка риска: Процентное значение, отражающее общий риск, связанный с угрозой, с учетом таких факторов, как уязвимость системы, потенциальное воздействие и возможность использования;

– Принятые меры защиты: Действие, предпринятое эволюционным алгоритмом когнитивного центра для устранения угрозы;

– Стоимость действия: Процент системных ресурсов (например, процессор, пропускная способность, трудовые ресурсы), потребляемых защитным действием;

– Успех смягчения: Эффективность защитного действия по нейтрализации или снижению воздействия угрозы;

После обобщения результатов эксперимента, представленных в таблице, следует перейти к визуальному представлению различных этапов эксперимента (рисунок 6). Эти графики позволяют лучше понять, как работают адаптивные механизмы когнитивного центра в условиях моделирования сценариев кибератак. Изображение процесса объединения данных, эволюции взаимосвязей между угрозами, оценки рисков и оптимизации стратегий смягчения последствий позволяет получить полное представление о возможностях динамического реагирования системы.

Графики показывают ключевые аспекты экспериментального моделирования за 10 временных шагов:

– Оценка серьезности (красная пунктирная линия): Отражает серьезность угроз, обнаруженных на каждом временном шаге. Показатель колеблется в зависимости от типа и характера кибератак, при этом более высокие значения указывают на более серьезные угрозы;

– Оценка риска (синяя сплошная линия): Представляет собой расчетный риск для каждой угрозы, учитывающий возможность использования, потенциальное воздействие и уязвимость системы. Чем выше балл риска, тем выше угроза для системы;

– Успех смягчения (зеленая сплошная линия): Показывает процент успешного устранения угроз после применения стратегий защиты Когнитивного центра. Линия показывает, насколько эффективно защитные действия нейтрализуют или снижают риск угрозы;

– Стоимость действий (фиолетовая сплошная линия): Указывает на стоимость ресурсов (в терминах производительности системы или использования ресурсов), необходимых для реализации стратегий защиты. Более высокие значения указывают на более ресурсоемкие меры защиты.

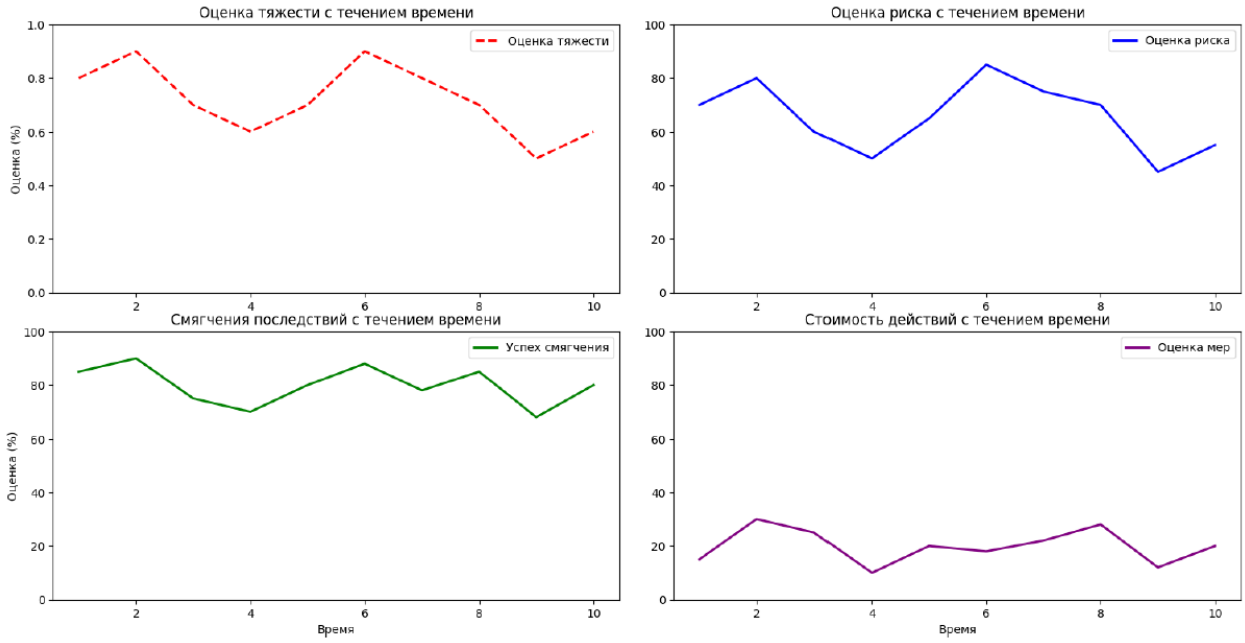

Рисунок 6 – Графики эксперимента

Представленные метрики дают подробную оценку работы когнитивного центра в ответ на сценарии кибератак. Анализируя эффективность объединения данных, динамику графа угроз, колебания оценки риска и оптимизацию стратегий смягчения последствий, мы увидели, как модель эффективно адаптируется к изменяющимся условиям угроз. Динамика рисков и успешность смягчения последствий свидетельствуют о надежном балансе между упреждающей защитой и эффективным распределением ресурсов, что важно для защиты критической инфраструктуры.

Заключение / Выводы

В данном исследовании предложен когнитивный центр информационной безопасности критической инфраструктуры, который включает в себя расширенный синтез данных, графовый подход к моделированию угроз, методы оценки рисков и эволюционный алгоритм для адаптивной оптимизации.

Результаты экспериментов показали, что предложенная архитектура может эффективно обнаруживать и снижать уровень меняющихся угроз, оптимизируя при этом использование ресурсов. Благодаря сочетанию когнитивных моделей, анализа угроз в реальном времени и механизма адаптивного принятия решений когнитивный центр обеспечивает повышенный уровень безопасности, обеспечивая устойчивость и непрерывность функционирования критической инфраструктуры. Дальнейшая работа будет направлена на масштабирование модели для использования более сложных, гетерогенных систем CI и дальнейшее повышение ее эффективности и адаптивности в реальных сценариях.

Список литературы

1. Zhang S., Li S., Chen P., Wang S., Zhao C. Generating network security defense strategy based on cyber threat intelligence knowledge graph // International Conference on Emerging Networking Architecture and Technologies. – Singapore: Springer Nature Singapore, 2022. – P. 507-519. – DOI: https://doi.org/10.1007/978-981-19-9697-9_41

2. Khraisat A., Gondal I., Vamplew P. et al. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. – 2019. – V. 2. – No 1. – P. 1-22. – DOI: https://doi.org/10.1186/s42400-019-0038-7

3. Abbas N.N., Ahmed T., Shah S.H.U. et al. Investigating the applications of artificial intelligence in cyber security // Scientometrics. – 2019. – V. 121. – P. 1189-1211. – DOI: https://doi.org/10.1007/s11192-019-03222-9

4. Цибизова Т.Ю., Панилов П.А., Кочешков М.А. Мониторинг безопасности системы защиты информации критической информационной инфраструктуры на основе когнитивного моделирования // Известия Тульского государственного университета. Технические науки. – 2023. – № 6. – С. 33-41. – DOI 10.24412/2071-6168-2023-6-33-41. – EDN BGUWZW.

5. Панилов П.А., Цибизова Т.Ю., Воскресенский Г.А. Методология экспертно-агентного когнитивного моделирования предупреждения воздействия на критическую информационную инфраструктуру // Ключевые тренды развития искусственного интеллекта: наука и технологии: Международная ИТ-конференция, Москва, 21 апреля 2023 года. – М.: Издательство МГТУ им. Н.Э. Баумана, 2023. – С. 98-104. – EDN FVBYOV.

6. Гаврилов А.Г. Когнитивное моделирование в информационной безопасности. – М.: Издательский дом «Академия», 2018. – 160 с.

7. Губанов В.П., Закиров И.Ф. Методы анализа уязвимостей информационных систем // Информационные технологии и вычислительные системы. – 2015. – №. 2. – С. 31-39.

8. Лавриненко А.А., Гончаренко В.М. Методы анализа графов в задачах информационной безопасности // Информационные технологии и вычислительные системы. – 2016. – №. 3. – С. 63-70.

9. Грибенюкова В.А. Анализ защищенности информационной системы с использованием агентного моделирования // Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки

специалистов в области информационной безопасности. – 2017. – № 1(8). – С. 259-261. – EDN EIQLGI.

10. Панилов П.А., Цибизова Т.Ю., Чернега Е.В. Разработка алгоритма управления когнитивными функциями в интеллектуальных системах безопасности // Известия Тульского государственного университета. Технические науки. – 2023. – № 10. – С. 47-61. – DOI 10.24412/2071-6168-2023-10-47-48. – EDN IGDUCN.

11. Панилов П.А., Кокорев А.В. Эволюционные алгоритмы оптимизации управления безопасностью критической инфраструктуры на основе когнитивных карт // Информатизация и информационная безопасность правоохранительных органов: Сборник трудов Международной научно-практической конференции, Москва, 07 июня 2024 года. – М.: Академия управления Министерства внутренних дел Российской Федерации, 2024. – С. 232-238 . – EDN BPCWNO.

References

1. Zhang S., Li S., Chen P., Wang S., Zhao C. Generating network security defense strategy based on cyber threat intelligence knowledge graph // International Conference on Emerging Networking Architecture and Technologies. – Singapore: Springer Nature Singapore, 2022. – P. 507-519. – DOI: https://doi.org/10.1007/978-981-19-9697-9_41

2. Khraisat A., Gondal I., Vamplew P. et al. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. – 2019. – V. 2. – No 1. – P. 1-22. – DOI: https://doi.org/10.1186/s42400-019-0038-7

3. Abbas N.N., Ahmed T., Shah S.H.U. et al. Investigating the applications of artificial intelligence in cyber security // Scientometrics. – 2019. – V. 121. – P. 1189-1211. – DOI: https://doi.org/10.1007/s11192-019-03222-9

4. Tsibizova T.Y., Panilov P.A., Kocheshkov M.A. Security monitoring of critical information infrastructure information protection system based on cognitive modeling // Izvestiya Tula State University. Technical Sciences. – 2023. – No 6. – P. 33-41. – DOI 10.24412/2071-6168-2023-6-33-41. – EDN BGUWZW.

5. Panilov P.A., Tsibizova T.Y., Voskresensky G.A. Methodology of expert-agent cognitive modeling of preventing the impact on critical information infrastructure // Key trends in the development of artificial intelligence: science and technology: International IT Conference, Moscow, April 21, 2023. – Moscow: Bauman Moscow State Technical University Publishing House, 2023. – P. 98-104. – EDN FVBYOV.

6. Gavrilov A.G. Cognitive modeling in information security. - Moscow: Academia Publishing House, 2018. – 160 c.

7. Gubanov V.P., Zakirov I.F. Methods of analyzing vulnerabilities of information systems // Information technologies and computer systems. – 2015. – No 2. – P. 31-39.

8. Lavrinenko A.A., Goncharenko V.M. Methods of graph analysis in information security tasks // Information technologies and computing systems. – 2016. – No 3. – P. 63-70.

9. Gribenyukova V.A. Analysis of information system security using agent-based modeling // Information security - an urgent problem of our time. Improvement of educational technologies for training specialists in the field of information security. – 2017. – No 1(8). – P. 259-261. – EDN EIQLGI.

10. Panilov P.A., Tsibizova T.Y., Chernega E.V. Development of the algorithm for controlling cognitive functions in intelligent security systems // Izvestia Tula State University. Technical Sciences. – 2023. – No 10. – P. 47-61. – DOI 10.24412/2071-6168-2023-10-47-48. – EDN IGDUCN.

11. Panilov P.A., Kokorev A.V. Evolutionary algorithms for optimization of critical infrastructure security management based on cognitive maps // Informatization and information security of law enforcement agencies: Proceedings of the International Scientific and Practical Conference, Moscow, June 07, 2024. – Moscow: Management Academy of the Ministry of Internal Affairs of the Russian Federation, 2024. – P. 232-238. – EDN BPCWNO.

Статья поступила в редакцию 2 сентября 2024 г.
Принята к публикации 27 сентября 2024 г.

Ссылка для цитирования: Панилов П.А. Когнитивный центр кибербезопасности критической инфраструктуры: гибридный подход с использованием графовых моделей и эволюционных алгоритмов // Национальная безопасность и стратегическое планирование. 2024. № 3(47). С. 55-67. DOI: https://doi.org/10.37468/2307-1400-2024-3-55-67

For citation: Panilov P.A. Using neuroevolution methods for automating optimization of cyber security algorithms in cognitive information centers // National security and strategic planning. 2024. №3(47). pp. 55-67. DOI: https://doi.org/10.37468/2307-1400-2024-3-55-67

Сведения об авторах

ПАНИЛОВ ПАВЕЛ АЛЕКСЕЕВИЧ – *ассистент, аспирант кафедры систем автоматического управления, Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), г. Москва, Россия*
ORCID: https://orcid.org/0009-0005-7663-5576
SPIN-код: 4112-3750
e-mail: panilovp.a@bmstu.ru

Information about authors:

PANILOV PAVEL A. – *Assistant, Postgraduate student of the Department of Automatic Control Systems, Bauman Moscow State Technical University, Moscow, Russia*
ORCID: https://orcid.org/0009-0005-7663-5576
SPIN: 4112-3750
e-mail: panilovp.a@bmstu.ru