УДК 004.056.53

Качанов Аркадий Дмитриевич, Слушатель
Военная академия защиты информации
имени генерала армии С.М. Штеменко

Афанасьев Максим Николаевич, Слушатель
Военная академия защиты информации
имени генерала армии С.М. Штеменко

Акишин Андрей Владимирович, Доцент
Военная академия защиты информации
имени генерала армии С.М. Штеменко

ПРИМЕНЕНИЕ РОЕВОГО АЛГОРИТМА ДЛЯ ОПТИМИЗАЦИИ ВЫБОРА И РАЗМЕЩЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МЕТОДОВ МНОГОАЛЬТЕРНАТИВНОЙ ОПТИМИЗАЦИИ

Аннотация. В статье рассматривается проблема автоматизации проектирования систем защиты информации (СЗИ) в сложных корпоративных вычислительных сетях в условиях непрерывного роста киберугроз. Опираясь на концепции выполненных работ, разработан модифицированный дискретный роевой алгоритм (на базе метода роя частиц – PSO) для решения NP-трудной задачи выбора и оптимального размещения СЗИ на узлах ИТ-инфраструктуры. Предложенный подход позволяет минимизировать финансовые затраты на внедрение и эксплуатацию подсистемы безопасности при максимизации интегрального показателя защищенности и строгом соблюдении требований программно-аппаратной совместимости.

Ключевые слова: Средства защиты информации, многоальтернативная оптимизация, роевой алгоритм, автоматизация проектирования, информационная безопасность, алгоритм роя частиц, оценка рисков, NP-трудная задача.

1. Введение

На современном этапе развития информационных технологий усложнение архитектуры корпоративных информационных систем (внедрение облачных вычислений, концепции BYOD, технологий Интернета вещей) сопровождается пропорциональным ростом количества и изощренности кибернетических угроз. Традиционный, «ручной» или экспертный подход к выбору и размещению средств защиты информации (СЗИ) становится неэффективным. Ошибки на этапе проектирования приводят либо к возникновению критических уязвимостей (из-за несовместимости средств или неполного перекрытия векторов атак), либо к необоснованному перерасходу ИТ-бюджета организации.

В связи с этим процесс проектирования СЗИ требует строгого математического обоснования и автоматизации. Фундаментальные основы для решения данной проблемы заложены в ряде научных трудов, среди которых особо выделяется математическая модель многоальтернативной оптимизации, глубоко исследованная в работе «Автоматизация проектирования систем защиты информации с использованием методов многоальтернативной оптимизации». В рамках данного подхода синтез системы безопасности рассматривается как задача выбора наилучшего набора решений из множества доступных рыночных альтернатив для каждого структурного элемента сети.

Однако с ростом масштабов вычислительной сети пространство поиска оптимального решения возрастает экспоненциально, превращая задачу в класс NP-трудных. Классические методы точного поиска (например, метод ветвей и границ или полное дерево перебора) становятся вычислительно неприменимыми (проблема комбинаторного взрыва). Для

преодоления этого ограничения в настоящей статье предлагается использовать метаэвристические методы роевого интеллекта, в частности, адаптированный дискретный алгоритм роя частиц (Particle Swarm Optimization, PSO).

2. Постановка задачи многоальтернативной оптимизации СЗИ

В соответствии с методологией многоальтернативной оптимизации, защищаемая ИТ-инфраструктура представляется в виде ориентированного или неориентированного графа, где узлами выступают сегменты сети, серверы, рабочие станции или каналы связи, требующие оснащения механизмами безопасности.

Пусть N – общее количество подсистем или узлов сети. Для каждого i-го узла (i = 1, 2,..., N) существует множество альтернативных вариантов СЗИ (различные вендоры, версии, конфигурации): Ai = {ai1, ai2,..., aiK}, где K – количество доступных на рынке решений данного класса (например, межсетевые экраны, IDS/IPS, антивирусы, DLP-системы).

Каждая альтернатива aij характеризуется набором технико-экономических параметров:

- C (aij) – совокупная стоимость владения СЗИ (TCO), включающая затраты на закупку, лицензирование и внедрение;
- E (aij) – показатель эффективности (вероятность успешного блокирования профильных угроз, рассчитываемая на основе баз уязвимостей, например CVE/CVSS);
- R (aij) – ресурсоемкость (требования к вычислительным мощностям, пропускной способности, оперативной памяти узла).

Кроме того, вводится матрица совместимости Comp, определяющая возможность совместного функционирования выбранных СЗИ без программно-аппаратных конфликтов.

Математическая постановка задачи заключается в формировании вектора решений X = (x1, x2,..., xN), где xi ∈ Ai, максимизирующего общую защищенность системы E_total (X) при соблюдении следующих жестких ограничений:

1. Финансовое ограничение: суммарные затраты не должны превышать выделенный бюджет B_max.
2. Ресурсное ограничение: потребление ресурсов на каждом узле не должно превышать доступную мощность.
3. Ограничение совместимости: все выбранные элементы должны быть попарно совместимы.

3. Разработка модифицированного дискретного роевого алгоритма

Классический алгоритм роя частиц оперирует в непрерывном математическом пространстве. Поскольку выбор конкретного СЗИ из каталога является задачей целочисленной (дискретной) оптимизации, в рамках исследования был разработан модифицированный бинарно-дискретный роевой алгоритм.

Кодирование решения: Каждая частица роя представляет собой потенциальный проект комплексной системы безопасности. Положение частицы задается вектором X = (x1,..., xN), где координата xi – целочисленный индекс выбранного СЗИ.

Целевая функция (Fitness Function): Для оценки качества «положения» частицы используется аддитивно-мультипликативная функция, учитывающая как эффективность защиты, так и динамические штрафы за нарушение ограничений:

$$F(X) = E_{total}(X) - \lambda 1 * \max(0, \Sigma C - B_{max}) - \lambda 2 * \Phi(Comp)$$

где λ1 и λ2 – адаптивные коэффициенты штрафа, а Φ (Comp) – функция, подсчитывающая количество конфликтующих пар СЗИ в решении.

Движение частиц: Ввиду дискретности пространства, скорость частицы V интерпретируется как вероятность изменения текущей альтернативы. Обновление положения частицы на итерации t+1 происходит по следующим правилам:

1. Вычисляется вероятность замены компонента на основе дистанции между текущим вектором X, лучшим персональным вектором частицы P_best и лучшим глобальным вектором всего роя G_best.

2. Для предотвращения преждевременной сходимости (застревания в локальных оптимумах) внедрен оператор направленной мутации: с вероятностью γ координата xi случайным образом заменяется на другую альтернативу из множества Ai, что обеспечивает достаточный уровень исследования пространства поиска (exploration).

4. Архитектура системы автоматизированного проектирования

Для практического применения предложенного математического аппарата разработана концептуальная архитектура программного комплекса автоматизированного проектирования СЗИ. Система включает следующие модули:

- Модуль инвентаризации и сканирования инфраструктуры – собирает топологию сети и определяет узлы защиты;
- Модуль моделирования угроз – формализует актуальные векторы атак;
- База знаний СЗИ – регулярно обновляемый справочник доступных на рынке решений с их характеристиками (стоимость, эффективность, совместимость);
- Оптимизационное ядро – программная реализация предложенного роевого алгоритма, выполняющая поиск конфигурации;
- Модуль генерации проектной документации – выводит итоговую спецификацию оборудования и ПО.

5. Экспериментальные исследования и моделирование

Для верификации предложенного алгоритма было проведено имитационное моделирование в программной среде Python. Тестовая инфраструктура представляла собой модель корпоративной сети из 150 защищаемых узлов. Для каждого узла база знаний предлагала от 10 до 30 альтернатив СЗИ. Общая размерность пространства поиска составила свыше 10^150 вариантов.

Разработанный дискретный роевой алгоритм (DPSO) сравнивался с точным методом (метод ветвей и границ), стандартным генетическим алгоритмом (GA) и «жадным» эвристическим алгоритмом. Размер популяции (роя) был задан равным 200 частицам, критерий останова – 1000 итераций или отсутствие улучшений на протяжении 100 итераций.

Результаты моделирования продемонстрировали следующие показатели:

1. Вычислительная сложность: Точный метод не смог найти решение за приемлемое время (таймаут составил 24 часа), что подтверждает NP-трудность задачи. Алгоритм DPSO достигал стабильного субоптимального решения в среднем за 2,5 минуты (210-250 итераций), что на 40% быстрее скорости сходимости генетического алгоритма.
2. Качество решения (Fitness): Проекты СЗИ, синтезированные роевым алгоритмом, оказались на 4.5% эффективнее решений GA и на 21% превосходили результаты «жадного» алгоритма по уровню итоговой защищенности.
3. Экономическая выгода: Применение DPSO позволило сформировать конфигурации СЗИ, обеспечивающие требуемый (нормативный) уровень безопасности при снижении совокупных капитальных затрат на 16-18% по сравнению с экспертными спецификациями, составленными ИБ-аналитиками вручную.

6. Заключение

Интеграция метаэвристических методов, в частности алгоритмов роевого интеллекта, в процесс автоматизации проектирования систем защиты информации показала высокую научно-практическую значимость. Использование концептуальной модели многоальтернативной оптимизации в связке с предложенным дискретным роевым алгоритмом позволяет эффективно преодолевать проблему комбинаторного взрыва.

Разработанный метод обеспечивает нахождение оптимальных или близких к ним конфигураций СЗИ в условиях жестких ресурсных, финансовых ограничений и требований программно-аппаратной совместимости. Дальнейшие векторы исследований предполагают переход к многокритериальной оптимизации (построение фронта Парето для баланса «стоимость-безопасность») и внедрение алгоритма в системы класса SOAR для динамической реконфигурации средств защиты в момент развития кибератаки.

Список литературы:

1. Гаецький, Б. Б. Адаптивный вариант алгоритма роя частиц для оптимизации задач с множественными ограничениями / Б. Б. Гаецький, Д. Ю. Скворцов, А. В. Акишин // Вектор научной мысли. – 2026. – № 4 (33). – С. 203-205. – EDN QUQGYC

2. Карпенко А.П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2014. – 446 с.

3. Котенко И.В., Саенко И.Б. Автоматизация управления политиками безопасности в современных корпоративных сетях // Информационные технологии и вычислительные системы. 2018. № 2. С. 67-78.

4. Kennedy J., Eberhart R. Particle swarm optimization // Proceedings of ICNN'95 – International Conference on Neural Networks. – IEEE, 1995. – Vol. 4. – P. 1942-1948