ТРУДЫ МОЛОДЫХ УЧЕНЫХ

Научная статья
УДК 004.732; DOI: 10.61260/2218-13X-2024-3-175-185

РАЗРАБОТКА МОДЕЛЕЙ И АЛГОРИТМОВ ОЦЕНКИ ФУНКЦИОНИРОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

✉**Потапова Дарья Александровна.**
МИРЭА – Российский технологический университет, Москва, Россия
✉***potapova.daria1998@yandex.ru***

Аннотация. Актуальность статьи обусловлена необходимостью совершенствования существующих систем обнаружения вторжений в условиях постоянно меняющегося арсенала инструментов и техник злоумышленников. Классические алгоритмы работы систем обнаружения вторжений, основанные на сигнатурном и поведенческом анализе, не обеспечивают достаточную степень безопасности сети и не могут предотвратить динамические атаки на системы. Разработка новых алгоритмов и моделей позволит повысить общую безопасность сетевой структуры, сократить количество ложных срабатываний и минимизировать ущерб от компьютерных атак.

Искусственные иммунные системы используют подходы для борьбы с вредоносным влиянием, аналогичные механизмам, наблюдаемым у живых организмов. А именно, обнаружение вирусов и выработка иммунного ответа – антител. Такой подход позволяет компьютерным системам дообучаться в процессе функционирования, самостоятельно выявляя компьютерные вирусы по их активности и самостоятельно вырабатывая средства борьбы с вредоносным кодом.

Ключевые слова: системы обнаружения вторжений, искусственные иммунные системы, критериальная модель, онтологическая модель, когнитивная модель, правила корреляции

Для цитирования: Потапова Д.А. Разработка моделей и алгоритмов оценки функционирования систем обнаружения вторжений // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 175–185. DOI: 10.61260/2218-13X-2024-3-175-185.

Scientific article

DEVELOPMENT OF MODELS AND ALGORITHMS FOR EVALUATING THE FUNCTIONING OF INTRUSION DETECTION SYSTEMS

✉**Potapova Darya A.**
MIREA – Russian technological university, Moscow, Russia
✉***potapova.daria1998@yandex.ru***

Abstract. The relevance of the article is due to the need to improve existing intrusion detection systems in the context of a constantly changing arsenal of tools and techniques of intruders. Classic intrusion detection systems algorithms based on signature and behavioral analysis do not provide a sufficient degree of network security and cannot prevent dynamic attacks on systems. The development of new algorithms and models will improve the overall security of the network structure, reduce the number of false positives and minimize damage from computer attacks.

Artificial immune systems use approaches to combat malicious influence similar to the mechanisms observed in living organisms. Namely, the detection of viruses and the development of an immune response – antibodies. This approach allows computer systems to further learn during operation, independently identifying computer viruses by their activity and independently developing means of combating malicious code.

Keywords: intrusion detection systems, artificial immune systems, criteria model, ontological model, cognitive model, correlation rules.

For citation: Potapova D.A. Development of models and algorithms for evaluating the functioning of intrusion detection systems // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 3. P. 175–185. DOI: 10.61260/2218-13X-2024-3-175-185.

Введение

Алгоритмы оценки функционирования систем обнаружения вторжений и проблематика достаточности таких оценок были рассмотрены в ряде работ Буйневича М.В., Саламатовой Т.А., Максимовой Е.А., Жукова В.Г., Соколовой Л.А., Частиковой В.А., Карпенко А.П., Емельянова В.В, Сиамак Пархизкари и др.

Научные работы, посвященные разработке моделей и алгоритмов оценки функционирования систем обнаружения вторжений (СОВ), представляют собой значимый вклад в область информационной безопасности и обладают высокой научной ценностью. Тем не менее, несмотря на их полноту и детальность, данные исследования сталкиваются с рядом недостатков, которые следует учитывать при их практическом применении и дальнейшем развитии [1].

Во-первых, многие работы страдают от ограниченной репрезентативности экспериментальных данных. Используемые в исследованиях датасеты часто не охватывают полный спектр возможных сетевых атак и нормального трафика, что может снижать обобщающую способность разработанных моделей. Это приводит к необходимости валидации и тестирования моделей на более широком и разнообразном наборе данных, чтобы подтвердить их эффективность в реальных условиях.

Во-вторых, методология оценки часто не учитывает динамическую природу сетевых угроз [2]. Большинство текущих моделей и алгоритмов основываются на статическом анализе, что не позволяет адекватно реагировать на быстро меняющиеся и адаптирующиеся атаки. Это указывает на необходимость разработки более гибких и адаптивных подходов, способных быстро обучаться на новых данных и изменениях в сетевом поведении.

В-третьих, существует проблема высокой вычислительной сложности предложенных алгоритмов. Множество предложенных методов, особенно те, которые основаны на машинном обучении и глубоком обучении, требуют значительных вычислительных ресурсов для их реализации. Это может ограничивать их применение в условиях ограниченных ресурсов, таких как устройства Интернета вещей (IoT) или мобильные системы. Таким образом, важным направлением будущих исследований является оптимизация существующих алгоритмов для повышения их эффективности и снижения потребления ресурсов.

Таким образом, несмотря на значительный прогресс в области разработки СОВ, существующие научные работы имеют ряд недостатков, которые необходимо учитывать и преодолевать для повышения их практической ценности и эффективности.

Методы исследования

Обоснованность и достоверность полученных результатов обеспечена использованием анализа уровня проработки темы на сегодняшний день, а также грамотным использованием апробированного алгоритма [1]. Также они подтверждаются

использованием современных подходов к тестированию, результатами вычислительных экспериментов и соотношением результатов с эталонными значениями. Модели обеспечивают адаптацию к конкретной системе обнаружения вторжений, позволяют одновременно учитывать значимые факторы (инфраструктуру системы комплексной безопасности) и эффективность СОВ. Скомплексированы алгоритмы, реализующие содержание механизма системы обнаружения вторжений [4].

Анализ текущего состояния и постановка проблемы позволили сделать вывод о том, что современные СОВ сталкиваются с ограничениями в точности и производительности, особенно при обработке больших объемов данных и обнаружении новых типов атак. Выбранные методы исследования явились основой для разработки новых критериев и метрик для оценки эффективности СОВ, учитывающие специфические требования современных сетей и угроз. Предложены новые модели для обнаружения вторжений, которые включают гибридные подходы, объединяющие сигнатурный и поведенческий анализ [2]. Модели демонстрируют улучшенную способность к обнаружению неизвестных атак и уменьшение количества ложных срабатываний.

Результаты исследования и их обсуждение

Проведен анализ СОВ. Это включает в себя: анализ видов решения задач в СОВ, а также анализ типовой архитектуры СОВ.

Подсистема сбора информации аккумулирует данные о работе защищаемой автоматизированной системы. Для сбора информации используются автономные модули – датчики. По характеру собираемой информации выделяют следующие типы датчиков: датчики приложений, датчики хоста, датчики сети, межсетевые датчики. СОВ может содержать любую комбинацию из приведенных типов датчиков.

Подсистема анализа обрабатывает данные, выявляет угрозы и передает результаты в подсистему представления данных.

Подсистема представления данных информирует администраторов и обеспечивает их инструментами для реагирования на выявленные угрозы.

Все три подсистемы тесно взаимосвязаны и работают совместно для обеспечения комплексной защиты системы [3–5].

Таким образом, архитектура СОВ обеспечивает полный цикл обнаружения и реагирования на вторжения, начиная от сбора данных и заканчивая представлением результатов анализа для принятия мер по защите системы.

Выявлены следующие основные недостатки структур современных СОВ:

1. Отсутствие общей методологии построения.
2. Высокое потребление аппаратных ресурсов.
3. Недостаточная универсальность, жесткая зависимость от аппаратно-программных платформ.
4. Низкие возможности к обновлению.
5. Отсутствие методик оценивания эффективности применения СОВ в конкретных условиях.

Для выявления обнаружения аномальных запросов в СОВ определен эвристический механизм. В отличие от сигнатурного, ограниченного в обнаружении модифицированных вариантов известной атаки, эвристический механизм позволяет выявлять скрытые закономерности в анализируемых сетевых политиках, благодаря его способности к адаптации к изменениям в системе [6]. При обновлении или изменении системы детектор аномалий может самостоятельно обновлять свою модель, адаптируясь к новым условиям. Кроме того, данный подход позволяет обнаруживать новые виды атак или аномальных ситуаций, которые не были заранее определены в правилах или спецификациях.

Модули на базе эвристического механизма обеспечивают адаптацию к конкретной СОВ, позволяют одновременно учитывать значимые факторы (инфраструктуру системы комплексной безопасности) и эффективность СОВ.

Для обнаружения сетевых атак используются механизмы искусственного интеллекта, в данной работе были выбраны искусственные иммунные системы.

Для реализации в СОВ определены три класса алгоритмов ИИС: алгоритмы негативного отбора, иммунные сети и алгоритмы колонального отбора. Для решения задачи обнаружения аномалий в поступающей на сервер из компьютерной сети информации используется несколько методов искусственных иммунных систем – правило частичного совпадения и отрицательный отбор.

Для реализации нового подхода к работе систем обнаружения вторжений был разработан комплекс моделей аномальных запросов в СОВ, включающий в себя критериальную, онтологическую и когнитивную модели.

В классических моделях администратор информационной безопасности занимается не только первоначальной настройкой СОВ, но и участвует в проверке угроз, поступающих по результатам анализа трафика [7]. На основании полученной информации администратор формирует новые правила и политику, которые загружает в СОВ для автоматизации реагирования на подобные инциденты в дальнейшем. Однако число событий и атак может исчисляться десятками в минуту, и в таком случае организации придётся увеличивать нагрузку на администратора информационной безопасности, вплоть до расширения штата, что влечёт за собой дополнительные расходы. В предлагаемой модели взаимодействия процесс добавления политик автоматизируется за счёт самообучения системы на базе алгоритмов интеллектуального анализа пакетов. На рис. 1 представлена критериальная модель уязвимостей в СОВ.

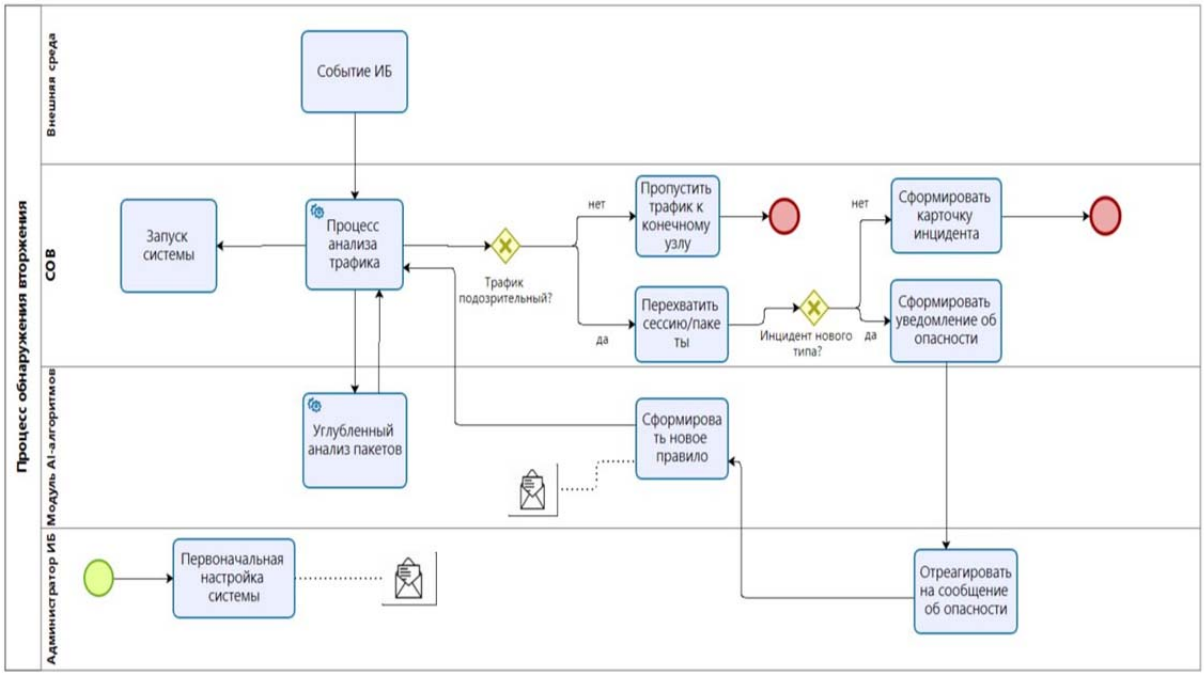

Рис. 1. **Критериальная модель СОВ в нотации BPMN (ИБ – информационная безопасность)**

На рис. 2 представлена блок-схема предлагаемой онтологической модели уязвимостей в СОВ.

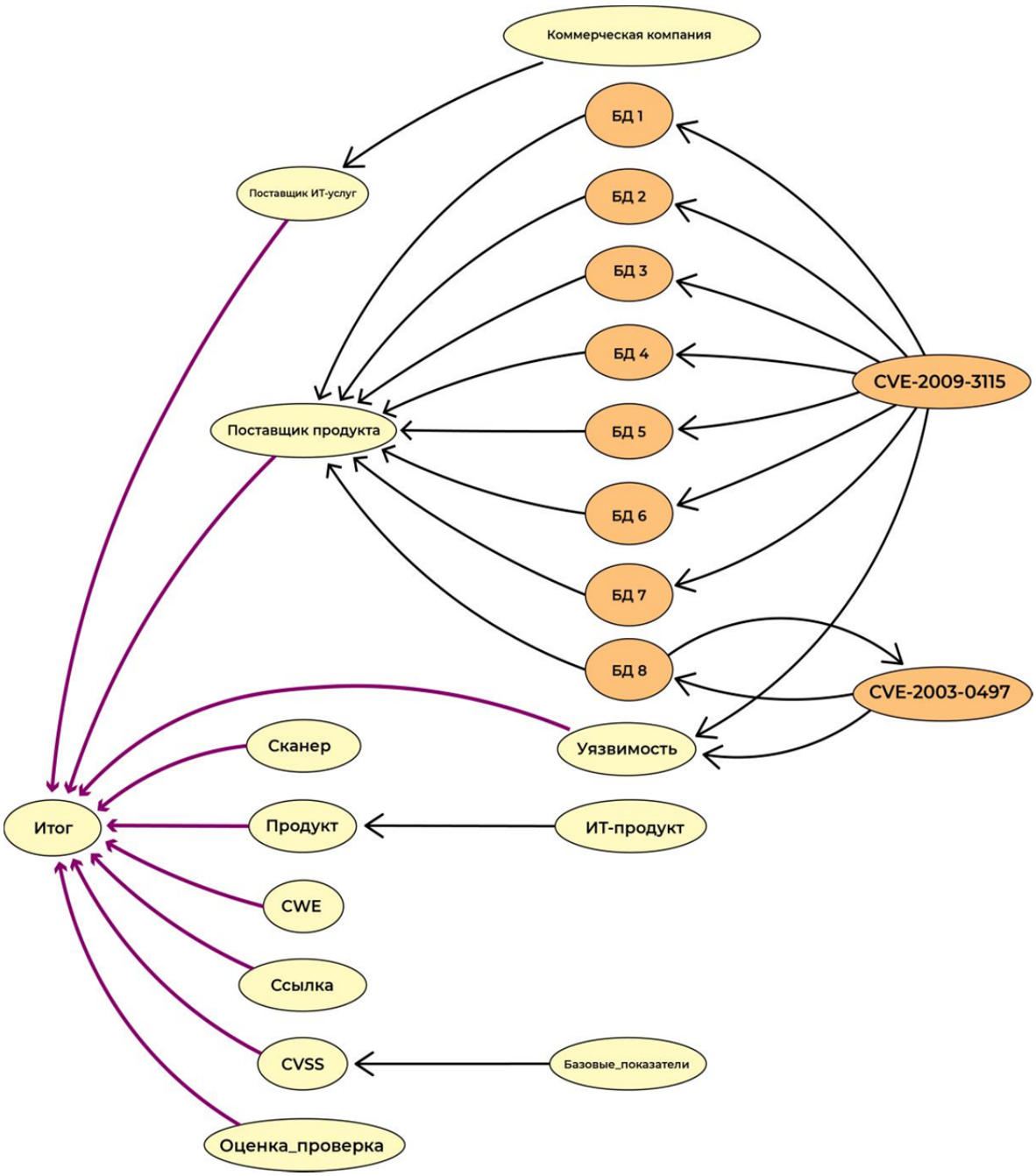

Рис. 2. **Онтологическая модель СОВ**
(БД – база данных)

В представленной модели отношения между программными продуктами (CVE) и аппаратными компонентами (сканер, продукт), совокупность которых приводит к возникновению уязвимости, задаются с помощью дескрипционной логики [8]. Связи между концептами представлены в основном через подклассы, а не через свойства объектов. Таким образом, логический вывод здесь сводится к задаче классификации, что повышает скорость обработки событий информационной безопасности.

На рис. 3 представлена когнитивная модель СОВ, основанная на принципе кластеризации.

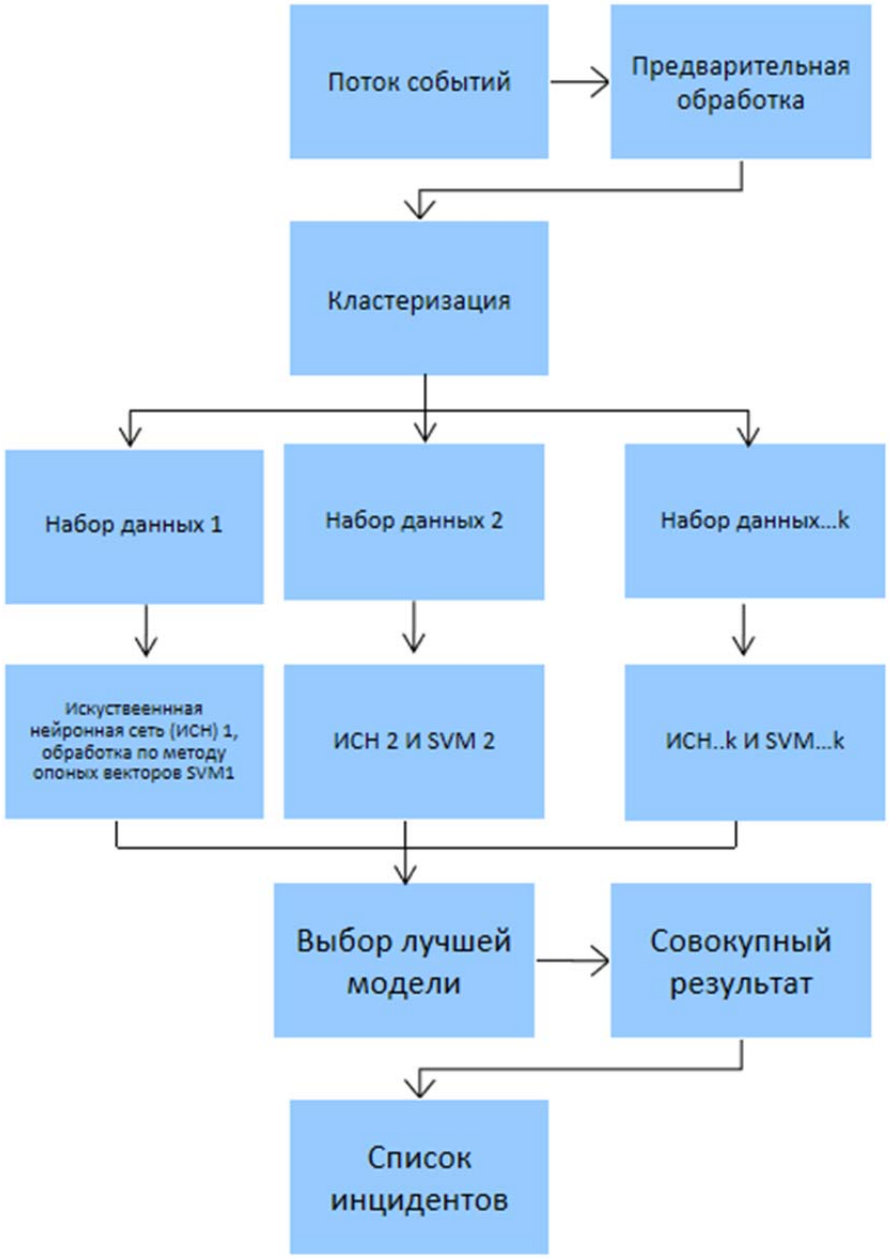

Рис. 3. **Когнитивная модель СОВ**

После предварительной обработки набор данных с помощью алгоритма среднего сдвига может быть разделен на K-кластер (от DS1 до ДСк) [9]. Это усложнение уменьшения набора данных приводит к достижению более высокой точности модели за счет использования глубоких нейронных сетей (DNNk). Примечательно, что K не является постоянной величиной и зависит от реализации среднего сдвига.

На основе комплекса моделей были созданы алгоритмы функциональности СОВ, основанные на правилах корреляции и на внедрении модуля искусственной иммунной системы. Основные компоненты алгоритма корреляции представлены на рис. 4.

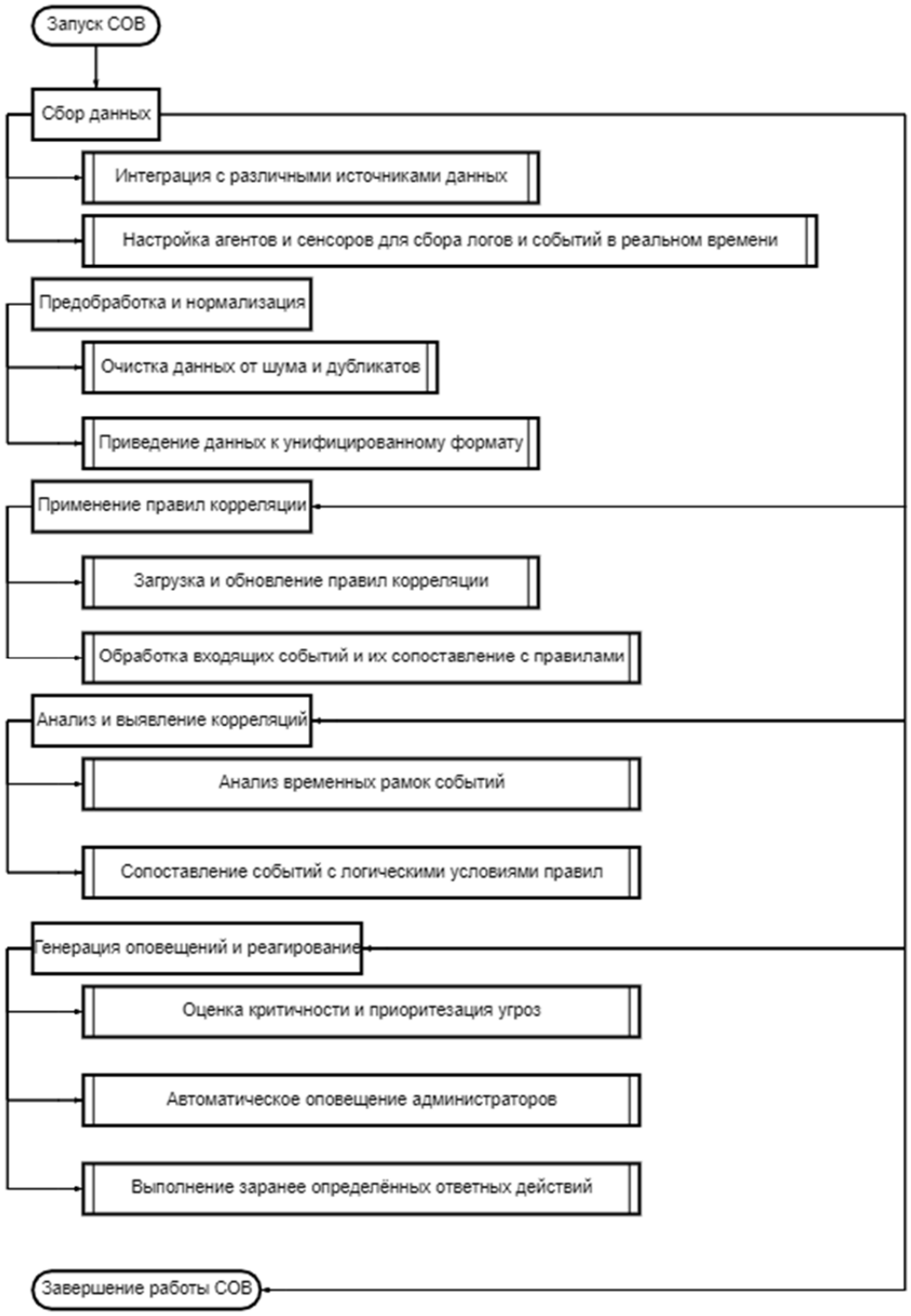

Рис. 4. **Алгоритм работы СОВ на правилах корреляции**

Основными этапам алгоритмов корреляции являются:
1. Сбор данных.
1.1. Интеграция с различными источниками данных.
1.2. Настройка агентов и сенсоров для сбора логов и событий в реальном времени.
2. Предобработка и нормализация.
2.1. Очистка данных от шума и дубликатов.

2.2. Приведение данных к унифицированному формату.

3. Применение правил корреляции.

3.1. Загрузка и обновление правил корреляции.

3.2. Обработка входящих событий и их сопоставление с правилами.

4. Анализ и выявление корреляций.

4.1. Анализ временных рамок событий.

4.2. Сопоставление событий с логическими условиями правил.

5. Генерация оповещений и реагирование.

5.1. Оценка критичности и приоритезация угроз.

5.2. Автоматическое оповещение администраторов.

5.3. Выполнение заранее определённых ответных действий.

На основании алгоритма выделены преимущества правил корреляции:

1. Повышенная точность – корреляция событий позволяет уменьшить количество ложных срабатываний за счёт более комплексного анализа.

2. Раннее обнаружение атак – выявление многоэтапных атак на ранних стадиях позволяет быстрее реагировать и минимизировать ущерб.

3. Автоматизация – правила корреляции автоматизируют процесс анализа событий, что снижает нагрузку на аналитиков безопасности.

Алгоритмы функциональности СОВ, основанные на правилах корреляции, являются мощным инструментом для выявления сложных и многоэтапных атак, что делает их неотъемлемой частью современной системы безопасности.

Алгоритмы функциональности СОВ, основанные на искусственных иммунных системах, используют принципы и механизмы биологических иммунных систем для защиты компьютерных сетей [10]. Эти алгоритмы имитируют процессы распознавания и реагирования на вторжения, подобно тому, как иммунная система организма выявляет и уничтожает патогены. Ниже представлены основные компоненты и этапы алгоритмов искусственных иммунных систем (ИИС) для СОВ. К основным компонентам ИИС для СОВ относятся [11, 12]:

1. Антиген. Представляет собой потенциальные угрозы или аномалии, которые система должна выявлять и нейтрализовать. В контексте СОВ антигены могут быть аномальными сетевыми пакетами, несанкционированными попытками доступа или другими подозрительными действиями.

2. Антитело. Модель, представляющая нормальное состояние системы или сеть известных угроз. Антитела используются для выявления антигенов путём их сопоставления.

3. Клональная селекция. Механизм адаптации и обучения, при котором наиболее эффективные антитела (те, которые лучше всего распознают антигены) клонируются и модифицируются (мутация) для улучшения распознавания угроз.

4. Генерация и регенерация антител. Процесс создания новых антител и обновления существующих на основе анализа текущих угроз и их характеристик.

5. Память иммунной системы. Система хранения информации о ранее обнаруженных угрозах и соответствующих антителах, что позволяет быстрее реагировать на повторные атаки.

В качестве этапов алгоритмов ИИС для СОВ рассматриваются следующие:

1. Сбор и предобработка данных. Сбор сетевых данных и логов с различных устройств и систем, их предобработка и нормализация для дальнейшего анализа.

2. Инициализация системы. Создание начального пула антител на основе нормальных данных сети и известных угроз. Этот этап включает инициализацию памяти иммунной системы.

3. Распознавание угроз. Сравнение входящих данных (антигенов) с существующими антителами для выявления аномалий или подозрительных действий. При совпадении антигена с антителом система инициирует соответствующие действия.

4. Клональная селекция и мутация. Если антитело успешно распознаёт антиген, оно клонируется и модифицируется. Мутация позволяет улучшить способность антител распознавать новые или изменённые угрозы.

5. Обновление памяти иммунной системы. Сохранение информации о новых угрозах и соответствующих антителах в память системы для ускорения реакции на повторные атаки.

6. Реагирование на угрозы. При обнаружении угроз система инициирует действия по нейтрализации угрозы, такие как блокировка сетевого трафика, уведомление администратора или изоляция скомпрометированных узлов.

Алгоритм иммунной сети моделирует взаимодействие антител для создания сети, способной выявлять сложные паттерны и взаимосвязи между угрозами.

Алгоритмы функциональности СОВ, основанные на искусственных иммунных системах, используют адаптивные и обучаемые методы для эффективного распознавания и нейтрализации как известных, так и новых угроз [13].

По результатам исследования определены следующие критерии, позволяющие оценить эффективность СОВ:

1. Количество аномалий взаимодействия контролируемых объектов.
2. Количество сигнатур всех узнаваемых атак.
3. Степень искажения эталонной профильной информации.

Заключение

В ходе работы изложено новое научно-обоснованное решение и разработка, а именно модель и алгоритм модуля СОВ, основанные на механизмах ИИС, имеющий существенное значение для развития сферы информационной безопасности, следовательно, безопасного развития Российской Федерации.

В ходе разработки предлагаемого решения смоделирован процесс выборки критериев выявления аномальных запросов; проанализированы виды и методы построения сложных систем, функциональность СОВ; определена проблема обнаружения аномальных запросов; определены основные этапы алгоритмизации искусственной иммунной системы; даны определения элементов искусственной иммунной системы и их метрики, разработана онтологическая модель системы управления информационной безопасностью.

Разработанные модели и алгоритмы могут быть использованы для повышения эффективности и точности работы СОВ в реальных условиях эксплуатации.

Полученные результаты могут быть применены в различных сферах, включая информационную безопасность, киберзащиту организаций и государственных структур.

Дальнейшие исследования в данной области могут быть направлены на углубление анализа специфических аспектов функционирования СОВ, таких как анализ новых видов киберугроз и улучшение методов оценки их эффективности. Важным направлением является также интеграция разработанных моделей и алгоритмов с существующими системами обеспечения информационной безопасности с целью создания комплексных решений.

Список источников

1. Ван К., Столфо С.Дж. Аномальная полезная нагрузка на основе обнаружения сетевых вторжений // Последние достижения в сфере обнаружения вторжений. 2004. С. 203–222.

2. Лаборатория Линкольна Массачусетского технологического института: информационные системы Технологии. URL: http://www.ll.mit.edu/mission/коммуникации/ist/corpora/ideval/данные/index.html (дата обращения: 20.04.2004).

3. Паршенкова Ю.А., Максимова Е.А. Угроза безопасности субъектов критической информационной инфраструктуры Российской Федерации // Кибербезопасность: технические и правовые аспекты защиты информации: сб. науч. трудов I Нац. науч.-практ.

конф. М.: МИРЭА – Российский технологический университет, 2023. С. 71–74. EDN JQDLQV.

4. Максимова Е.А. Анализ жизненного цикла субъекта критической информационной инфраструктуры в контексте инфраструктурного деструктивизма // Защита информации. Инсайд. 2021. № 5 (101). С. 4–10. EDN RYYOSO.

5. Максимова Е.А. Модели и методы оценки информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза: дис. … д-ра техн. наук СПб., 2022. 448 с. EDN OHDNPO.

6. Jamal Al-Enezi. Artificial immune systems based committee machine for classification application. URL: https://bura.brunel.ac.uk/bitstream/2438/6826/1/FulltextThesis.pdf (дата обращения: 23.05.2024).

7. Zhou Ji and Dasgupta D. Real-valued negative selection algorithm with variable-sized detectors. In LNCS 3102, Proceedings of GECCO 2004, Seattle, Washington, June 2004.

8. Zhengbing H., Ji Z., Ping M. A Novel Anomaly Detection Algorithm Based on RealValued Negative Selection System. 2008 Workshop on Knowledge Discovery and Data Mining, 23–24 January, Adelaide, SA. 2008. С. 499–502.

9. Буланова Н.С. Исследование эффективности применения вспомогательных оптимизируемых величин при использовании методов оптимизации на основе искусственных иммунных систем. URL: http://is.ifmo.ru/diploma-theses/2015/master/bulanova/bulanova.pdf (дата обращения: 23.05.2024).

10. Николенко С.И., Тулупьев А.Л. Самообучающиеся системы. М., 2009.

11. Потапова Д.А., Брысин А.Н. Антропоморфизм компьютерных вирусов. ISSN 2223-2966 // Современная наука: актуальные проблемы теории и практики. Естественные и технические науки. 2024. № 3. С. 93–96.

12. Анализ ограничений при симметричном и ассиметричном шифровании данных / Д.А. Потапова [и др.] // Современная наука: актуальные проблемы теории и практики. Естественные и технические науки. 2024. № 3. С. 142–146.

13. John H. Holmes Knowledge Discovery in Biomedical Data: Theory and Methods. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.2a7631fb-61cafbec-883f06a9-74722d776562/https/www.sciencedirect.com/topics/immunology-and-microbiology/artificial-immune-system (дата обращения: 23.05.2024).

References

1. Van K., Stolfo S.Dzh. Anomal'naya poleznaya nagruzka na osnove obnaruzheniya setevyh vtorzhenij // Poslednie dostizheniya v sfere obnaruzheniya vtorzhenij. 2004. S. 203–222.

2. Laboratoriya Linkol'na Massachusetskogo tekhnologicheskogo instituta: informacionnye sistemy Tekhnologii. URL: http://www.ll.mit.edu/mission/kommunikacii/ist/corpora/ideval/dannye/index.html (data obrashcheniya: 20.04.2004).

3. Parshenkova Yu.A., Maksimova E.A. Ugroza bezopasnosti sub"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii // Kiberbezopasnost': tekhnicheskie i pravovye aspekty zashchity informacii: sb. nauch. trudov I Nac. nauch.-prakt. konf. M.: MIREA – Rossijskij tekhnologicheskij universitet, 2023. S. 71–74. EDN JQDLQV.

4. Maksimova E.A. Analiz zhiznennogo cikla sub"ekta kriticheskoj informacionnoj infrastruktury v kontekste infrastrukturnogo destruktivizma // Zashchita informacii. Insajd. 2021. № 5 (101). S. 4–10. EDN RYYOSO.

5. Maksimova E.A. Modeli i metody ocenki informacionnoj bezopasnosti sub"ekta kriticheskoj informacionnoj infrastruktury pri destruktivnyh vozdejstviyah infrastrukturnogo geneza: dis. … d-ra tekhn. nauk SPb., 2022. 448 s. EDN OHDNPO.

6. Jamal Al-Enezi. Artificial immune systems based committee machine for classification application. URL: https://bura.brunel.ac.uk/bitstream/2438/6826/1/FulltextThesis.pdf (data obrashcheniya: 23.05.2024).

7. Zhou Ji and Dasgupta D. Real-valued negative selection algorithm with variable-sized detectors. In LNCS 3102, Proceedings of GECCO 2004, Seattle, Washington, June 2004.

8. Zhengbing H., Ji Z., Ping M. A Novel Anomaly Detection Algorithm Based on RealValued Negative Selection System. 2008 Workshop on Knowledge Discovery and Data Mining, 23–24 January, Adelaide, SA. 2008. S. 499–502.

9. Bulanova N.S. Issledovanie effektivnosti primeneniya vspomogatel'nyh optimiziruemyh velichin pri ispol'zovanii metodov optimizacii na osnove iskusstvennyh immunnyh sistem. URL: http://is.ifmo.ru/diploma-theses/2015/master/bulanova/bulanova.pdf (data obrashcheniya: 23.05.2024).

10. Nikolenko S.I., Tulup'ev A.L. Samoobuchayushchiesya sistemy. M., 2009.

11. Potapova D.A., Brysin A.N. Antropomorfizm komp'yuternyh virusov. ISSN 2223-2966 // Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Estestvennye i tekhnicheskie nauki. 2024. № 3. S. 93–96.

12. Analiz ogranichenij pri simmetrichnom i assimetrichnom shifrovanii dannyh / D.A. Potapova [i dr.] // Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Estestvennye i tekhnicheskie nauki. 2024. № 3. S. 142–146.

13. John H. Holmes Knowledge Discovery in Biomedical Data: Theory and Methods. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.2a7631fb-61cafbec-883f06a9-74722d776562/https/www.sciencedirect.com/topics/immunology-and-microbiology/artificial-immune-system (data obrashcheniya: 23.05.2024).

Информация о статье:
Статья поступила в редакцию: 17.09.2024; одобрена после рецензирования: 27.09.2024; принята к публикации: 30.09.2024
The information about article:
The article was submitted to the editorial office: 17.09.2024; approved after review: 27.09.2024; accepted for publication: 30.09.2024

Информация об авторах:
Потапова Дарья Александровна, преподаватель кафедры КБ-1 «Защита информации» Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, Москва, пр. Вернадского, д. 78), e-mail: potapova.daria1998@yandex.ru

Information about the authors:
Potapova Daria A., lecturer department KB-1 «Information Security» of Institute of cybersecurity and digital technologies of the Russian technological university (119454, Moscow, Vernadsky ave., 78), e-mail: potapova.daria1998@yandex.ru