УДК 111.11

Методика защиты функционирования протоколов сетевого взаимодействия автоматизированных систем от кибератак на основе программного комплекса идентификации опасных состояний конфигураций систем безопасности

Руссу В.Ю. (ВКА им. А.Ф.Можайского), **Казьмин Д.Ю.** (ВКА им. А.Ф.Можайского)

Научный руководитель – доктор технический наук, доцент Бирюков Д.Н. (ВКА им. А.Ф.Можайского)
Научный консультант - доктор технический наук, доцент Пилькевич С.В. (ВКА им. А.Ф.Можайского)

Введение. В современном мире сетевые приложения передачи данных в автоматизированных системах стали неотъемлемой частью бизнеса, государственных структур и личной жизни пользователей. Однако с увеличением их значимости растёт и количество кибератак, нацеленных на уязвимости в их защите. В условиях постоянной эволюции методов атак злоумышленников крайне важно не только обеспечивать надёжную защиту сетевых систем, но и своевременно обновлять конфигурации безопасности. Несвоевременное или некорректное реконфигурирование защитных систем может привести к компрометации данных, финансовым потерям и утрате доверия пользователей [1].

Основная часть. Целью проекта является разработка и внедрение методов и инструментов, обеспечивающих оперативное и адаптивное реконфигурирование системы безопасности в условиях кибератак. Это позволит минимизировать время реакции на инциденты, снижать вероятность успешной компрометации системы и повышать уровень её устойчивости к современным угрозам [2].

Для достижения этой цели в рамках проекта были решены следующие задачи:

Автоматизация процесса мониторинга конечных точек и сетевого оборудования АС и оценка работоспособности системы;

Разработка системы динамической адаптации конфигурации безопасности АС на основе Марковского процесса принятия решения (МППР*) (рис.1)* и обучения с подкреплением [3];

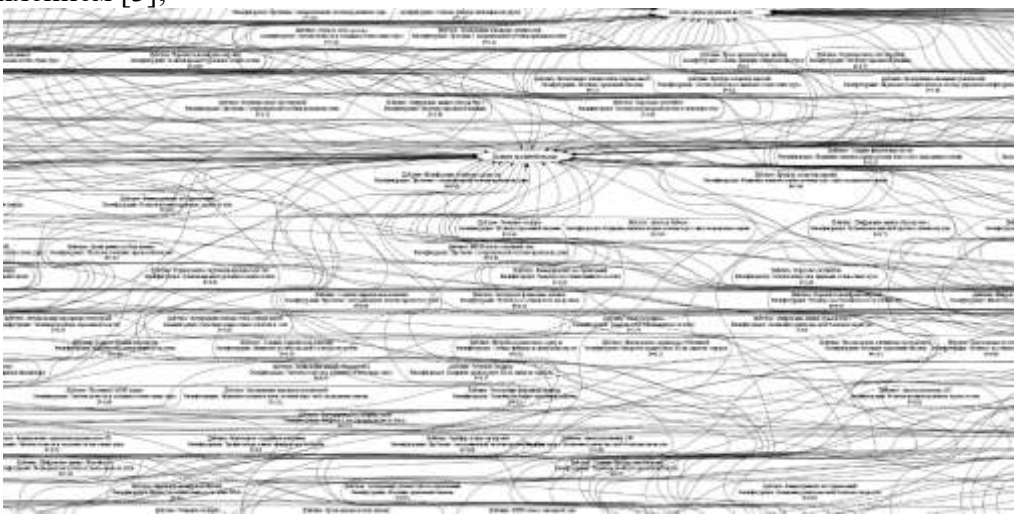

Рисунок 1. Модель МППР

Создание гибкой подсистемы реконфигурирования системы безопасности с помощью инструмента автоматизации реконфигурирования инфраструктуры Ansible.

Для реализации вышеописанной методики целесообразно создать подсистему реконфигурации, которую можно будет представить в виде функции, которой передаются аргументы (параметры системы безопасности), при этом функция будет возвращать новое

состояние системы. Для создания такой подсистемы удобно использовать Ansible Playbook. Ansible — это инструмент автоматизации, который позволяет управлять конфигурацией серверов, обеспечивая их безопасность и адаптацию к изменяющимся условиям. В рамках данной работы мы рассматриваем Ansible Playbook как функцию, зависящую от множества параметров безопасности.

Разрабатываемая система реконфигурирования позволяет динамически изменять конфигурацию безопасности серверов и сетевых приложений на основе входных параметров (текущего состояния системы, сетевой активности, угроз).

В рамках создания среды RL, которая дает вознаграждение за действие агента (специалиста по безопасности), надо генерировать новые угрозы для поддержания обученной модели в актуальном состоянии. Для этого была создана система поиска уязвимостей нулевого дня в сетевом программном обеспечении АС. Для решения этой задачи было решено использовать методы машинного обучения, так как они хорошо себя зарекомендовали в работах [4], [5], [6] при решении задачи поиска идентичных участков дизассемблированного кода.

Для создания методики обнаружения уязвимостей нулевого дня в исполняемых файлах следует решить ряд задач:

- выбрать классификацию уязвимостей, которая будет учитывать наиболее распространённые, а впоследствии и все выявленные ранее ошибки, специфичные для исполняемых файлов;
- собрать тестовые программы с документированными недостатками под каждый класс уязвимостей и стандартизировать их для создания обучающей выборки.

Выводы. В рамках представленной работы обобщен опыт исследований в области повышения защищенности сетевых приложений автоматизированных систем передачи данных путём своевременного реконфигурирования системы безопасности.

Дальнейшая работа будет сосредоточена на обогащении Ansible Playbook новыми модулями конфигураций, начиная с уровня операционной системы серверов, персональных компьютеров, коммутационного оборудования и их сетевых приложений и до настроек облачных серверов, средств контейнеризации и виртуализации. Для этого планируется создание виртуальной среды на основе ESXI и K8S. Так же предполагается создание системы централизованного сбора логов на основе ELK с помощью, которой будет оцениваться состояние функционирования системы в целом.

Список использованных источников:

1. OWASP ТОП-10 рисков безопасности за 2023 год. - [Электронный ресурс]: https:// owasp.org/www-project-top-ten/ (дата обращения: 14.01.2025).
2. Актуальные киберугрозы: II квартал 2024 года. - [Электронный ресурс]: https:// www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-ii-kvartal-2024-goda/ (дата обращения: 14.01.2025).
3. Майн Х., Осаки С. Марковские процессы принятия решений // Главная редакция физико-математической литературы издательства "Наука"– 1977. – С. 16-51.
4. Qian Feng, Rundong Zhou, Chengcheng Xu, Yao Cheng, Brian Testa, and Heng Yin. Scalable graph-based bug search for firmware images. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 480–491. ACM, 2016.
5. Diane Duros Hosfelt. Automated detection and classification of cryptographic algorithms in binary programs through machine learning. arXiv preprint arXiv:1503.01186, 2015.
6. Xiaojun Xu, Chang Liu, Qian Feng, Heng Yin, Le Song, and Dawn Song. Neural network-based graph embedding for cross-platform binary code similarity detection. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pages 363–376. ACM, 2017.