Беляев Сергей Николаевич, курсант
КВВУ им. С.М. Штеменко
Belyaev Sergey Nikolaevich
KVVU named after S.M. Shtemenko

Гизатуллин Александр Маратович, курсант
КВВУ им. С.М. Штеменко
Gizatullin Alexander Maratovich
KVVU named after S.M. Shtemenko

Новиков Назар Алексеевич, курсант
КВВУ им. С.М. Штеменко
Novikov Nazar Alekseevich
KVVU named after S.M. Shtemenko

Ворончихин Сергей Сергеевич, преподаватель
КВВУ им. С.М. Штеменко
Voronchikhin Sergey Sergeevich
KVVU named after S.M. Shtemenko

Синицын Юрий Юрьевич, преподаватель
КВВУ им. С.М. Штеменко
Sinitsyn Yuri Yurievich
KVVU named after S.M. Shtemenko

АНАЛИЗ УЯЗВИМОСТЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
VULNERABILITY ANALYSIS OF AUTOMATED SYSTEMS OF CRITICAL INFORMATION INFRASTRUCTURE

Аннотация. Статья посвящена актуальной проблеме анализа уязвимостей автоматизированных систем, входящих в состав критической информационной инфраструктуры (КИИ). На основе анализа современных научных публикаций рассматриваются ключевые типы уязвимостей, особенности их эксплуатации в контексте КИИ, а также перспективные подходы к их обнаружению и нейтрализации, с особым акцентом на методы искусственного интеллекта, в частности, нейронные сети. Подчеркивается необходимость комплексного подхода к обеспечению безопасности АС КИИ, учитывающего как технические аспекты, так и стратегические доктрины киберпространства.

Abstract. The article is devoted to the urgent problem of vulnerability analysis of automated systems that are part of the critical information infrastructure (CII). Based on the analysis of modern scientific publications, key types of vulnerabilities, features of their exploitation in the context of CII, as well as promising approaches to their detection and neutralization are considered, with a special focus on artificial intelligence methods, in particular, neural networks. The need for an integrated approach to ensuring the security of Asia is emphasized, taking into account both technical aspects and strategic doctrines of cyberspace.

Ключевые слова: Критическая информационная инфраструктура (КИИ), автоматизированные системы (АС), уязвимости, кибербезопасность, нейронные сети, искусственный интеллект (ИИ), обнаружение атак, сетевая безопасность, веб-приложения.

Keywords: Critical information infrastructure (CII), automated systems (AS), vulnerabilities, cybersecurity, neural networks, artificial intelligence (AI), attack detection, network security, web applications.

Введение

Критическая информационная инфраструктура (КИИ) является основой функционирования современного общества и государства, обеспечивая работу ключевых отраслей: энергетики, транспорта, здравоохранения, финансов, связи. Автоматизированные системы (АС), составляющие техническую основу КИИ, в силу своей сложности, распределенности и интеграции в глобальные сети, обладают множеством уязвимостей. Эксплуатация этих уязвимостей злоумышленниками может привести к катастрофическим последствиям – масштабным авариям, дестабилизации общества, угрозе национальной безопасности. Поэтому анализ уязвимостей АС КИИ, разработка эффективных методов их выявления и устранения представляют собой стратегически важную научно-практическую задачу. Целью данной статьи является анализ современных представлений о природе уязвимостей АС КИИ и оценка перспективности применения передовых технологий, таких как искусственный интеллект (ИИ) и нейронные сети (НС), для их обнаружения и противодействия угрозам.

1. Особенности уязвимостей АС КИИ и современные угрозы

1.1. АС КИИ характеризуются рядом особенностей, повышающих их уязвимость:

1. **Высокая критичность:** Последствия успешной атаки могут быть фатальны, что делает их привлекательной целью для злоумышленников (включая государственно спонсируемые группы).
2. **Длительный жизненный цикл:** Использование устаревших (legacy) систем и ПО с известными, но не устраненными уязвимостями.
3. **Сложность и гетерогенность:** Интеграция разнородных компонентов и технологий создает сложные конфигурации, где уязвимости могут возникать на стыке систем.
4. **Операционная технология (ОТ):** Наличие компонентов ОТ (SCADA, ICS), изначально не предназначенных для работы в открытых сетях и имеющих специфические уязвимости.
5. **Удаленный доступ:** Необходимость дистанционного управления и мониторинга расширяет поверхность атаки.

Как отмечают Алашеев В. В., Акишин А. В., Чеснаков М. Н [2], взгляды ведущих государств (в частности, США) на ведение действий в киберпространстве эволюционируют в сторону разработки комплексных доктрин, включающих в себя выявление и эксплуатацию уязвимостей инфраструктур противника. Это подчеркивает стратегический характер угроз для КИИ и необходимость опережающего анализа и защиты.

2. Перспективы применения искусственного интеллекта и нейронных сетей для анализа и защиты от уязвимостей

Традиционные методы обнаружения уязвимостей и атак (сигнатурные системы, статический анализ) зачастую неэффективны против современных сложных и целевых атак (APT), а также новых, неизвестных (zero-day) уязвимостей. В этой связи активно развиваются подходы на основе искусственного интеллекта:

2.1. Обнаружение сетевых атак:

Исследования, представленные Гладковым В. В., Тараскиной А. Г., Кузнецовым С. И. и др [1], демонстрируют эффективность применения нейронных сетей для анализа сетевого трафика. НС способны выявлять сложные, слабо выраженные аномалии и паттерны, характерные для атак, которые не детектируются правилами сигнатурных систем. Это особенно актуально для защиты периметра и внутренних сегментов сетей КИИ.

2.2. Построение средств защиты информации (СЗИ):

Ушаков С. П., Акишин А. В., Енин Н. Н. и др [3] рассматривают применение нейронных сетей как ключевого компонента при создании современных СЗИ. НС могут использоваться для:

- Анализа поведения пользователей и систем (UEBA, SIEM) на предмет аномалий.
- Классификации угроз и инцидентов безопасности.
- Предсказания потенциальных векторов атак на основе анализа конфигураций и данных об уязвимостях.
- Оптимизации работы других компонентов СЗИ.

2.3. Обнаружение атак на веб-приложения:

Веб-интерфейсы являются частым вектором атаки на АС КИИ. Акишин А. В., Енин Н. Н., Сопин К. Ю. и др [4] показывают, что методы ИИ, в частности, глубокое обучение, позволяют эффективно обнаруживать сложные атаки на веб-приложения (такие как SQLi, XSS, Path Traversal, brute-force, логические уязвимости), анализируя HTTP-запросы и ответы, выявляя отклонения от нормального поведения приложения. Это критически важно, так как веб-приложения часто служат точкой входа в инфраструктуру КИИ.

Преимущества подхода на основе ИИ/НС:

- **Обнаружение неизвестных угроз:** Способность выявлять аномалии и новые типы атак без предварительных сигнатур.
- **Обработка больших объемов данных:** Эффективный анализ сетевого трафика, журналов событий, пользовательских действий в реальном времени.
- **Адаптивность:** Возможность обучения на новых данных и адаптации к изменяющимся условиям и тактикам злоумышленников.
- **Автоматизация:** Снижение нагрузки на аналитиков SOC за счет автоматического выявления и приоритизации инцидентов.

Вызовы и ограничения:

- **Требовательность к данным:** Необходимость больших объемов качественных размеченных данных для обучения.
- **"Черный ящик":** Сложность интерпретации решений, принимаемых сложными НС, что затрудняет анализ причин срабатывания и доверие к системе.
- **Ресурсоемкость:** Вычислительная сложность обучения и работы современных моделей ИИ.
- **Возможность Adversarial Attacks:** Целенаправленные манипуляции с входными данными для обмана ИИ-моделей.
- **Интеграция:** Сложность интеграции ИИ-решений в существующие сложные и унаследованные АС КИИ без нарушения их функционирования.

3. Комплексный подход к защите АС КИИ

Анализ литературы [1, 3, 4] подтверждает, что применение ИИ, и в частности НС, является крайне перспективным направлением для усиления защиты АС КИИ. Однако, как подчеркивается в работе [2], безопасность КИИ не может быть обеспечена исключительно техническими средствами. Требуется комплексный подход, включающий:

Регулярную оценку уязвимостей и пентестинг: Систематическое выявление слабых мест в АС КИИ.

Управление конфигурациями и обновлениями: Своевременное устранение известных уязвимостей путем установки патчей и корректной настройки систем.

Сегментацию сетей: Ограничение распространения атаки в случае компрометации одного сегмента.

Разработку и соблюдение регламентов безопасности: Четкие политики и процедуры для персонала.

Подготовку и обучение специалистов: Повышение осведомленности и навыков в области кибербезопасности.

Реализацию стратегических доктрин кибербезопасности: Формирование государственной политики и нормативно-правовой базы в области защиты КИИ [2].

Заключение

Автоматизированные системы критической информационной инфраструктуры обладают специфическими уязвимостями, делающими их привлекательной мишенью для злоумышленников, включая группы, действующие в интересах государств. Современные угрозы требуют применения передовых методов защиты. Анализ представленных научных работ [1, 2, 3, 4] убедительно демонстрирует высокую эффективность и перспективность использования технологий искусственного интеллекта, особенно нейронных сетей и глубокого обучения, для обнаружения сетевых атак, анализа поведения, защиты веб-приложений и построения интеллектуальных средств защиты информации в контексте АС КИИ. Эти методы позволяют выявлять сложные и неизвестные угрозы, анализировать большие объемы данных и адаптироваться к изменяющейся тактике противника.

Однако, успешное применение ИИ сопряжено с решением задач по обеспечению качества данных, интерпретируемости решений, ресурсной эффективности и защите от adversarial-атак. Важно понимать, что технологии ИИ – это мощный инструмент, но не панацея. Обеспечение безопасности АС КИИ требует комплексной стратегии, объединяющей передовые технические решения (включая ИИ), строгие организационные меры, постоянное обучение персонала и реализацию продуманных государственных доктрин в области кибербезопасности. Дальнейшие исследования должны быть направлены на повышение устойчивости ИИ-моделей к целенаправленным атакам, разработку методов эффективного обучения на ограниченных или слабо размеченных данных, характерных для специфических систем КИИ, и создание стандартов интеграции ИИ-решений в высококритичные инфраструктуры.

Список литературы:

1. Применение нейронных сетей для обнаружения сетевых атак / В. В. Гладков, А. Г. Тараскина, С. И. Кузнецов [и др.] // Региональная информатика и информационная безопасность, Санкт-Петербург, 01–03 ноября 2017 года. Том Выпуск 4. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. – С. 73-74. – EDN UUJNKC.

2. Алашеев, В. В. Взгляды США на разработку доктрины информационного воздействия в киберпространстве / В. В. Алашеев, А. В. Акишин, М. Н. Чеснаков // Проблемы технического обеспечения войск в современных условиях: Труды III Межвузовской научно-практической конференции, Санкт-Петербург, 16 февраля 2018 года. Том 1. – Санкт-Петербург: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ВОЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЕННАЯ АКАДЕМИЯ СВЯЗИ ИМЕНИ МАРШАЛА СОВЕТСКОГО СОЮЗА С. М. БУДЕННОГО" МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, 2018. – С. 67-71. – EDN XMGZPF.

3. Применение нейронных сетей при постороении средств защиты информации / С. П. Ушаков, А. В. Акишин, Н. Н. Енин [и др.] // Проблемы научно-практической деятельности. Поиск и выбор перспективных решений: сборник статей VI международной научной конференции, Вологда, 25 февраля 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью «Международный институт перспективных исследований имени Ломоносова», 2025. – С. 32-39. – EDN ERREXB.

4. Применение искусственного интеллекта для обнаружения атак на веб-приложения / А. В. Акишин, Н. Н. Енин, К. Ю. Сопин [и др.] // Научные инструменты и механизмы перспективного инновационного развития общества: сборник статей XX международной научной конференции, Санкт-Петербург, 08 февраля 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью «Международный институт перспективных исследований имени Ломоносова», 2025. – С. 17-25. – EDN WMPULQ.