DOI: 10.58168/MoInSyTe2024_81-88
УДК 004.9

РАЗВИТИЕ СИСТЕМ АВТОМАТИЗАЦИИ КОНТРОЛЯ И ОБНАРУЖЕНИЯ УГРОЗ В ИНФОРМАЦИОННЫХ СРЕДАХ

М.М. Качан[1], В.И. Анциферова[1], Р.Г. Дмитриев[1]

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. Изучение развития систем Автоматизации Обнаружения и Контроля угроз (АОК) в информационных средах - это одна из важнейших задач современной кибербезопасности. Анализ актуального положения выявил необходимость в реализации непрерывного отслеживания и адаптации к новым угрозам. Принципы работы автоматизированных систем включают использование передовых технологий и соблюдение основных правил безопасности. Результаты исследования выявили необходимость развития средств АОК для обеспечения безопасности в цифровой среде. Также немаловажно уделить особое внимание повышению уровня защиты информации путём использования самообучающихся алгоритмов в целях прогнозирования и предотвращения кибератак. Активное развитие систем АОК открывает новые горизонты возможностей в сфере эффективной защиты информационных ресурсов.

Ключевые слова: обнаружение угроз, автоматизированные системы контроля, АОК, технологическое развитие, информационная безопасность, искусственный интеллект, сотрудничество.

DEVELOPMENT OF AUTOMATED THREAT DETECTION AND CONTROL SYSTEMS IN INFORMATION ENVIRONMENTS

M.M. Kachan[1], V.I. Antsiferova[1], R.G. Dmitriev[1]

[1]Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. Studying the development of Automated threat Detection and Control (ADC) systems in information environments is one of the most important tasks of modern cybersecurity. Analysis of the current situation revealed the need to implement continuous monitoring and adaptation to new threats. The operating principles of automated systems include the use of advanced technologies and compliance with basic safety rules. The results of the study revealed the need to develop ADCtools to ensure security in the digital environment. It is also important to pay special attention

to increasing the level of information security through the use of self-learning algorithms to predict and prevent cyber attacks. The active development of AOK systems opens up new horizons of possibilities in the field of effective protection of information resources.

Key words: threat detection, automated control systems, ADC, technological development, information security, artificial intelligence, cooperation.

Введение

Мир сегодня тесно переплетен с цифровыми технологиями, которые играют важную роль в развитии бизнеса и организации общественной жизни. Однако с распространением цифровых технологий, возросла и угроза информационной безопасности. Кибератаки становятся всё более изощренными и широкомасштабными, что соответственно требует улучшения эффективности в сфере контроля и обнаружения угроз в информационных средах. Поэтому вопрос обеспечения безопасности данных является одним из ключевых в современном обществе.

Цель данного исследования заключается в изучении актуальных тенденций и подходов в развитии систем АОК. Работа направлена на определение главенствующих принципов функционирования подобных систем, а также выявление вызовов и обозначение перспектив развития в данной области. Посредством изучения указанных аспектов будут выведены технологические и методологические рекомендации по обеспечению максимального уровня безопасности информационных сред.

Обзор подходов и недостатков существующих систем

Современные системы контроля и обнаружения угроз являются ключевым элементом обеспечения безопасности данных в информационных средах. Рассмотрим основные подходы и недостатки таких систем:

Один из наиболее широко используемых методов обнаружения угроз – это сигнатурный анализ. Метод базируется на поиске известных сигнатур угроз в сетевых пакетах или файлах. Главным недостатком данного подхода является его ограниченность в обнаружении новых - ранее неизвестных угроз. Указанная проблема обычно решается путём постоянного обновление баз сигнатур.

Второй по счёту, но не по значению подход - это анализ аномалий. Он базируется на выявлении нестандартного (аномального) поведения компонентов информационной среды. Такой метод помогает выявлять новые угрозы, но и приводит к большему числу ложных срабатываний.

Современные системы АОК всё чаще применяют методы машинного обучения и искусственного интеллекта. Такой подход позволяет создавать более точные модели обнаружения и легко приспосабливается к новым сценариям атак. Однако для успешной его реализации необходимо иметь большой массив данных для обучения модели.

Для повышения общей эффективности выявления угроз может производиться объединение разных подходов (гибридизация). Гибридные системы сочетают в себе анализ сигнатур и анализ аномалий или машинного обучения, что способствует уменьшению количества ложных срабатываний.

Несмотря на значительные достижения в сфере обнаружения, существующие системы имеют свои ограничения и нуждаются в постоянном усовершенствовании и приспособлении к новым угрозам.

Принципы функционирования автоматизированных систем контроля

Один из ключевых принципов функционирования АОК – реализация многоуровневой защиты, подразумевающая под собой использование нескольких методов обнаружения угроз на разных уровнях.

Современные системы контроля всё чаще используют методы автоматизации и анализ данных для наиболее эффективного выявления возможных угроз. Эти методы включают как обработку больших объемов информации и поиск аномалий, так и принятие решений на основе алгоритмов машинного обучения.

Важным аспектом работы систем контроля является способность правильно реагировать на обнаруженные угрозы, что включает автоматическую изоляцию инфицированных узлов, блокирование подозрительного трафика, запуск систем оповещения и процедур восстановления.

Примеромявляется SIEM (Security Information and Event Management). Это интегрированная система, объединяющая в себе сбор, анализ и реакцию на событиядо наступления существенного ущерба. Многие компании уже успешно используют указанную систему для наиболее точного выявления угроз и адаптации к новым видам атак.

Технологические аспекты развития систем автоматизации контроля

Существенную роль в развитии систем автоматизации контроля и обнаружения угроз в информационных средах играет искусственный интеллект (ИИ) и аналитика данных. Использование ИИ дает возможность создавать алгоритмы,

способные адаптироваться к постоянно модифицирующимся угрозам и принимать решения в реальном времени, а анализ данных помогает в обнаружении аномалий, паттернов и связей между событиями, что способствует эффективному реагированию на инциденты и, как следствие, их предотвращению.

ИИ можно применять для создания моделей, которые способны предугадывать угрозы, обнаруживать масштабные атаки и идентифицировать новые виды рисков. Например, системы могу подготавливаться на больших объемах данных, используя машинное обучение, что предполагает выявление нестандартных ситуаций и оперативное реагирование на потенциальные угрозы.

Большие данные (BigData) и облачные технологии значительно расширяют возможности систем контроля и обнаружения угроз. Обработка и анализ обширных объемов данных позволяют быстро обнаружить скрытые угрозы и аномалии, которые могут быть незамеченными при традиционных методах мониторинга. Системы контроля, основанные на биг-дата, способны обрабатывать информацию о поведении пользователей, трафике и событиях в реальном времени, обеспечивая тем самым более глубокий анализ и поддержку в принятии решений.

Облачные технологии также играют немаловажную роль в современных системах контроля, так как они позволяют масштабировать системы в зависимости от потребностей, обеспечивая высокую доступность и гибкость, помогают быстро внедрять обновления, улучшать защиту данных и управлять централизованной системой контроля на распределенной инфраструктуре.

Вызовы и перспективы развития систем контроля и обнаружения

Поскольку современные технологии не стоят на месте, можно ожидать, что вскоре произойдут значительные изменения в области безопасности информационных систем. Одна из основных тенденций – это углубленное использование искусственного интеллекта в системах контроля и обнаружения угроз. Можно спрогнозировать, что ИИ будет активно применяться для предотвращения кибератак, выявления вредоносного поведения и анализа потенциальных угроз. Развитие новых методов машинного обучения и нейронных сетей позволит улучшить реакцию на угрозы и повысит эффективность защиты информационных ресурсов.

Еще одна важная тенденция – это усиленное внимания к защите персональных данных и конфиденциальной информации. Расширение цифровизации общества и бизнеса ведет к возрастанию потребности в повышенной безопасности,

создавая новые вызовы для систем контроля и обнаружения. Необходимо усиление требований к защите данных, включая соблюдение законодательства о конфиденциальности и обеспечение приватности пользователей.

Киберпреступность создает новые виды угроз, к которым системы контроля должны быстро адаптироваться, а также незамедлительно реагировать на них. В последнее время наблюдается увеличение числа целевых атак, направленных на конкретные компании, государственные учреждения или критическую инфраструктуру. Чтобы успешно бороться с этими угрозами необходимо развивать системы контроля, способные реагировать на индивидуальные сценарии атак и адаптировать свои методы обнаружения.

Также следует обратить внимание на угрозы, связанные с распространением и использованием новых технологий: интернет вещей (IoT) и искусственного интеллекта. В таких системах существуют потенциально уязвимые места, что активизирует разработку специализированных методов АОК.

Среди основных проблем для системы контроля и обнаружения угроз можно выделить следующие:

-неоднородность данных

-недостаток обученного персонала

-сложность интеграции различных систем безопасности.

Для решения этих проблем необходимо стремиться к созданию универсальных стандартов обработки данных, расширению образовательных программ по кибербезопасности и разработке совместимых технологий, способных выявлять угрозы на всех уровнях сетевой инфраструктуры.

В перспективе развития систем контроля и обнаружения угроз важно уделять внимание не только техническим аспектам, но и обучению персонала, соблюдению правовых норм и этических принципов информационной безопасности. Только комплексный подход во всех этих направлениях позволит создать действенные системы, способные эффективно защищать информационные ресурсы и минимизировать риски.

Заключение

Можно сделать вывод, что необходимо постоянное изучение и совершенствование систем контроля и обнаружения угроз в информационных средах, так как с развитием технологий и киберугроз сложность в обеспечении информационной безопасности возрастает. Эффективность автоматизированных систем

контроля напрямую зависит от использования передовых технологий и соблюдения основополагающих принципов безопасности.

Чтобы улучшить работу систем автоматизации контроля необходимо активно внедрять искусственный интеллект, обучаемые модели и другие инновационные технологии, уделяя внимание обновлению и мониторингу защитных механизмов, а также повышая осведомленность пользователей о методах защиты информации.

В будущем можно предположить несколько направлений развития систем АОК в информационных средах:

1. Системы автоматизации контроля и обнаружения угроз будут быстрее интегрироваться с широким спектром устройств и приложений, обеспечивая комплексную защиту информационных сред.

2. Увеличится использование интеллектуальных алгоритмов для прогнозирования новых видов угроз и адаптации систем к ним.

3. Появятся прогрессивные методы, помогающие в создании самообучающихся систем безопасности.

Таким образом, уделяя большее внимание взаимодействию и сотрудничеству между различными организациями в сфере безопасности, обмену информацией об угрозах и совместным мерам по противодействию кибератакам, можно обеспечить надежную защиту информационных сред и минимизировать риски для организаций и пользователей.

Список литературы

1. Сазонова С.А. Разработка программных продуктов с использованием символьных и строковых переменных в объектно-ориентированной среде // Моделирование систем и процессов. – 2022. – Т. 15, № 3. – С. 44-54.

2. Полуэктов А.В., Макаренко Ф.В., Ягодкин А.С. Использование сторонних библиотек при написании программ для обработки статистических данных // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 33-41.

3. Тихомиров П.В., Скрыпников А.А., Володина Ю.Ю., Бондарев А.Б., Боровлев Ю.А., Викулин И.А. Информационно-интеллектуальные системы определения геометрических элементов лесовозных автомобильных дорог // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 83-93.

4. Тун Юйлинь, Новикова Т.П., Евдокимова С.А. Разработка алгоритма повышения эффективности протокола маршрутизации C-LEACH // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 93-99.

5. Стариков А.В., Бунаков П.Ю., Старикова А.А., Мешков Д.А. Особенности распределенного проектирования в мультиагентной среде ВКБМ с использованием облачных технологий // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 110-120.

6. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – 2012 – С. 82-83.

7. Сазонова С.А., Николенко С.Д., Осипов А.А. Оценка технического состояния оснований, фундаментов и железобетонных колонн каркасного здания // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 67-83.

8. Хрящев, В.В. Эффективность внедрения одноранговой распределенной системы хранения и обработки защищаемой информации (TheOoLProject) / В.В. Хрящев, А.В. Ненашев // Моделирование систем и процессов. – 2021. – Т. 14, №3. – С. 82-89. – DOI: 10.12737/2219-0767-2021-14-3-82-89.

9. https://geopositive.ru/rabota-siem-sistemy-principy-i-preimushhestva-dlya-obespeceniya-bezopasnosti-informacionnyx-sistem/

10. Информационная безопасность: Защита и нападение / А.А. Бирюков. – 2012 – С. 60-64.

11. https://www.computerra.ru/289698/oblaka-v-promyshlennosti-zachem-predpriyatiya-rabotayut-s-oblachnymi-vychisleniyami/

12. https://it-vacancies.ru/blog/tendencii-razvitiia-iskusstvennogo-intellekta-v-it-sfere/

References

1. Sazonova S.A. Development of software products using character and string variables in an object-oriented environment // Modeling of systems and processes. – 2022. – T. 15, No. 3. – P. 44-54.

2. Poluektov A.V., Makarenko F.V., Yagodkin A.S. Using third-party libraries when writing programs for processing statistical data // Modeling of systems and processes. – 2022. – T. 15, No. 2. – P. 33-41.

3. Tikhomirov P.V., Skrypnikov A.A., VolodinaYu.Yu., Bondarev A.B., Borovlev Yu.A., Vikulin I.A. Information-intelligent systems for determining the geometric elements of logging roads // Modeling of systems and processes. – 2022. – T. 15, No. 2. – P. 83-93.

4. Tong Yulin, Novikova T.P., Evdokimova S.A. Development of an algorithm for increasing the efficiency of the C-LEACH routing protocol // Modeling of systems and processes. – 2022. – T. 15, No. 2. – P. 93-99.

5. Starikov A.V., BunakovP.Yu., Starikova A.A., Meshkov D.A. Features of distributed design in the multi-agent environment of VKBM using cloud technologies // Modeling of systems and processes. – 2022. – T. 15, No. 2. – P. 110-120.

6. Information protection in computer systems and networks / V.F. Shangin. – 2012 – P. 82-83.

7. Sazonova S.A., Nikolenko S.D., Osipov A.A. Assessment of the technical condition of foundations, foundations and reinforced concrete columns of a frame building // Modeling of systems and processes. – 2022. – T. 15, No. 2. – P. 67-83.

8. Khryashchev, V.V. Efficiency of implementing a peer-to-peer distributed system for storing and processing protected information (The OoL Project) / V.V. Khryashchev, A.V. Nenashev // Modeling of systems and processes. – 2021. – T. 14, No. 3. – P. 82-89. – DOI: 10.12737/2219-0767-2021-14-3-82-89.

9. https://geopositive.ru/rabota-siem-sistemy-principy-i-preimushhestva-dlya-obespeceniya-bezopasnosti-informacionnyx-sistem/

10. Information security: Protection and attack / A.A. Biryukov. – 2012 – P. 60-64.

11. https://www.computerra.ru/289698/oblaka-v-promyshlennosti-zachem-predpriyatiya-rabotayut-s-oblachnymi-vychisleniyami/

12. https://it-vacancies.ru/blog/tendencii-razvitiia-iskusstvennogo-intellekta-v-it-sfere/