УДК 004.056.5

ИССЛЕДОВАНИЕ ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА АВТОМАТИЗАЦИИ БЫТОВОГО ОКРУЖЕНИЯ

Веретельников А. С.

магистрант,

Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,

Шахты, Россия

Клейменкин Д. В.

Ассистент,

Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,

Шахты, Россия

Аннотация

Данная статья посвящена вопросам обеспечения информационной безопасности в программно-аппаратных комплексах (ПАК) автоматизации бытового окружения. Её научная новизна состоит в представлении интегрируемых и применимых к реальным системам автоматизации методов укрепления безопасности ПАК. В ходе исследования проводится анализ угроз и уязвимостей, связанных с этой областью, а также оценивается эффективность существующих методов и средств безопасности. В рамках исследования предложены новые подходы и решения для укрепления безопасности ПАК, включая интеграцию блокчейна, многоуровневую защиту, автоматизированное обнаружение аномалий и другие. Результаты исследования подчеркивают важность обеспечения безопасности в условиях растущей сложности и взаимосвязанности современных систем автоматизации бытового окружения.

Ключевые слова: Безопасность, автоматизация, окружение, угрозы, уязвимости, защита, данные.

RESEARCH OF THE PROBLEM OF ENSURING INFORMATION SECURITY OF THE SOFTWARE AND HARDWARE COMPLEX OF AUTOMATION OF THE HOUSEHOLD ENVIRONMENT

Veretelnikov A. S.
Master's student,
Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,
Shakhty, Russia
Kleimenkin D. V.
Assistant lecturer,
Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,
Shakhty, Russia

Abstract

This article is devoted to the issues of information security in software and hardware complexes (SHC) automation of the household environment. Its scientific novelty consists in the presentation of integrated and applicable to real automation systems methods to strengthen the security of the SHC. The study analyzes the threats and vulnerabilities associated with this area, as well as assesses the effectiveness of existing methods and security tools. The research suggests new approaches and solutions to strengthen the security of the SHC, including blockchain integration, multi-level protection, automated anomaly detection and others. The results of the study emphasize the importance of ensuring safety in the context of the growing complexity and interconnectedness of modern automation systems of the household environment.

Keywords: Security, automation, environment, threats, vulnerabilities, protection, data.

В современном мире, на фоне стремительного развития информационных технологий и автоматизации бытовых процессов, информационная безопасность стала одним из наиболее важных и актуальных аспектов, как в сфере бизнеса и промышленности, так и в повседневной жизни. Особое внимание уделяется обеспечению безопасности программно-аппаратных комплексов (ПАК), применяемых для автоматизации бытового окружения [1].

Сегодняшние бытовые среды все больше зависят от технологических решений, включая умные дома, системы управления энергопотреблением, системы безопасности, и многие другие. Однако, с ростом функциональности и связанной с этим сложности ПАК, также растет и потенциальная уязвимость перед информационными атаками, что может привести к серьезным последствиям для конфиденциальности, целостности и доступности данных, а также для безопасности пользователей [2].

Именно в этом контексте становится необходимым исследование задачи обеспечения информационной безопасности программно-аппаратного комплекса автоматизации бытового окружения. Это исследование направлено на выявление уязвимостей, анализ существующих методов обеспечения безопасности, а также разработку новых подходов и решений, способствующих повышению уровня защиты таких систем.

Для проведения исследования обеспечения информационной безопасности ПАК автоматизации бытового окружения был применён комплексный подход. В рамках методологии выполнены следующие шаги:

- Анализ угроз и уязвимостей;
- Оценка существующих решений;
- Разработка новых подходов;

– Подведение результатов исследования.

Анализ угроз и уязвимостей является критически важным этапом обеспечения информационной безопасности [3]. В данном разделе представлен обобщенный анализ типичных угроз и уязвимостей, с которыми ПАК этого типа могут столкнуться:

Угрозы:

– Неавторизованный доступ: Злоумышленники могут попытаться проникнуть в ПАК, используя слабые пароли или недостаточную аутентификацию, чтобы получить контроль над системой [4].

– Межсетевые атаки: ПАК, как правило, подключены к интернету, что делает их уязвимыми для атак извне. Атаки могут включать в себя сканирование портов, атаки отказа в обслуживании (DoS), атаки на переполнение буфера и другие.

– Фишинг и социальная инженерия: Злоумышленники могут использовать манипуляции или маскировку, чтобы убедить пользователей предоставить конфиденциальные данные, такие как пароли или персональная информация.

– Вредоносные программы: Установка вредоносных программ, таких как вирусы, трояны или шпионские программы, может привести к компрометации ПАК и утечке данных.

– Физические угрозы: Угрозы могут не ограничиваться только цифровыми атаками. Физический доступ к оборудованию ПАК может привести к несанкционированным манипуляциям или кражам.

Уязвимости:

– Недостаточная аутентификация и авторизация: Слабые механизмы аутентификации могут позволить злоумышленникам получить доступ к системе.

– Необновленное программное обеспечение: Отсутствие регулярных обновлений и патчей может оставить уязвимости открытыми для эксплуатации.

– Сложность управления правами доступа: Неправильно настроенные права доступа могут привести к разглашению конфиденциальных данных.

– Недостаточная шифрование данных: Недостаточное или отсутствие шифрования данных может привести к утечкам информации.

– Отсутствие многоуровневой защиты: Недостаточная сегментация сети и многоуровневая защита могут сделать ПАК уязвимым для атак с разных точек.

– Неудовлетворительное обучение и осведомленность пользователей: Пользователи могут стать слабым звеном в защите, если не осведомлены о методах атак и безопасности.

Анализ этих угроз и уязвимостей позволяет разработать более эффективные меры безопасности и стратегии обеспечения информационной безопасности для ПАК автоматизации бытового окружения.

Существует ряд методов и средств обеспечения информационной безопасности, которые могут быть применены в контексте ПАК умных домов. Однако их эффективность может сильно варьироваться в зависимости от конкретных потребностей и особенностей системы [5]. Ниже приведен обзор некоторых из них и их оценка:

– Аутентификация и авторизация: Методы аутентификации, такие как двухфакторная аутентификация (2FA) или биометрическая аутентификация, могут обеспечить высокий уровень безопасности, если правильно реализованы. Однако использование слабых паролей или недостаточная аутентификация может оставить систему уязвимой. Эффективность высокая.

– Шифрование данных: Применение сильных алгоритмов шифрования для защиты данных в покое и в движении является важным

элементом безопасности. Однако ключевым фактором является правильная установка и управление ключами. Эффективность высокая.

– Многоуровневая защита: Многоуровневая защита, включая брандмауэры, обнаружение вторжений (IDS) и системы предупреждения о вторжениях (IPS), может эффективно обнаруживать и блокировать несанкционированные активности. Однако требуется правильная настройка и обновление для поддержания высокой эффективности. Эффективность высокая.

– Обновления и патчи: Регулярное обновление операционных систем и приложений является неотъемлемой частью обеспечения безопасности. Несвоевременные обновления могут оставить уязвимости открытыми. Эффективность высокая.

– Сегментация сети: Разделение сети на сегменты с ограниченным доступом может существенно снизить риск распространения атак и облегчить мониторинг сетевой активности. Эффективность высокая.

– Обучение и осведомленность пользователей: Обучение пользователей основам информационной безопасности и сознательное использование системы могут снизить вероятность успешных атак, но не исключают риска человеческой ошибки. Эффективность средняя.

– Мониторинг и анализ журналов: Постоянный мониторинг событий и анализ журналов могут помочь выявлять аномалии и несанкционированные действия в реальном времени. Эффективность высокая.

– Физическая безопасность: Физический доступ к оборудованию должен быть ограничен и контролируем. Эффективность высокая.

Эффективность методов и средств обеспечения информационной безопасности в контексте ПАК автоматизации бытового окружения зависит от их правильной реализации, настройки и управления. Комплексный подход, включающий в себя несколько уровней защиты, является наиболее надежным способом обеспечения безопасности в этой области.

На основе анализа угроз и уязвимостей, а также с учетом эффективности существующих методов и средств безопасности, предлагаются следующие подходы и решения для укрепления безопасности:

– Интеграция блокчейн-технологии: Использование технологии блокчейн для регистрации и подтверждения транзакций и событий в ПАК может обеспечить надежную и неизменяемую запись операций. Это снижает риск манипуляции данными и обеспечивает прозрачность.

– Усиление аутентификации и авторизации: Реализация более сильных методов аутентификации, таких как многофакторная аутентификация (MFA) или биометрия, помогает защитить систему от несанкционированного доступа [6].

– Автоматизированное обнаружение аномалий: Внедрение систем машинного обучения и искусственного интеллекта для поиска аномалий в сетевом трафике и поведении устройств может помочь выявлять потенциальные атаки в реальном времени.

– Централизованное управление устройствами: Использование централизованных систем управления, которые могут отслеживать и управлять всеми устройствами в ПАК, обеспечивает более эффективное контролируемость и обнаружение несанкционированных изменений.

– Безопасные разработки и обновления: Инкорпорирование принципов безопасной разработки и регулярное обновление ПАК с установкой последних патчей и обновлений безопасности обеспечивают защиту от известных уязвимостей.

– Физическая безопасность: Установка физических барьеров и систем контроля доступа к оборудованию ПАК ограничивает физический доступ к устройствам.

– Регулярное тестирование на проникновение: Проведение тестирования на проникновение (pentesting) помогает выявить уязвимости в системе до того, как они будут использованы злоумышленниками.

– Резервное копирование и восстановление: Регулярное резервное копирование данных и разработка планов восстановления после инцидентов (Disaster Recovery) снижают последствия атак и сбоев.

– Соблюдение стандартов безопасности: Соблюдение стандартов безопасности, таких как ISO 27001 или NIST, может помочь в установлении строгих политик безопасности и практик [7].

Эти подходы и решения являются компонентами комплексной стратегии обеспечения информационной безопасности. При этом важно настраивать и интегрировать их в контексте конкретной системы, учитывая ее уникальные особенности и потребности.

Подведение результатов исследования об обеспечении информационной безопасности подразумевает суммирование ключевых выводов и подчеркивание их важности. Комплексы автоматизации бытового окружения становятся все более сложными и взаимосвязанными. Это увеличивает вероятность уязвимостей и атак, делая безопасность приоритетом. Анализ угроз выявил потенциальные риски, такие как несанкционированный доступ, вредоносные программы, атаки на переполнение буфера и социальная инженерия. Существующие методы безопасности, такие как аутентификация, шифрование и обнаружение вторжений, могут быть эффективными при правильной реализации, но оставаться недостаточными. На основе анализа были предложены новые подходы и решения для укрепления безопасности ПАК, включая интеграцию блокчейна, многоуровневую защиту, автоматизированное обнаружение аномалий и другие. Исследование подчеркивает, что обеспечение информационной безопасности является неотъемлемой необходимостью, особенно в контексте быстрого развития

технологий и повышения уровня угроз. На практике, реализация рекомендаций и строгое соблюдение стандартов безопасности становятся критически важными шагами для обеспечения защиты пользователей и их данных в этой сфере.

Библиографический список:

1. Стариковский А. В., Жуков И. Ю., Михайлов Д. М., Шептунов А. А., Савчук А. В., Крымов А. С. Повышение защищенности систем автоматизации управления зданиями от компьютерных атак // Спецтехника и связь. 2012. №4. (Дата обращения 17.09.2023).
2. Хромова А.Р., Петросян Л.Э. Анализ уязвимостей в системах безопасности данных // ИВД. 2023. №6 (102). (Дата обращения 21.09.2023).
3. Анищенко В. А. Анализ угроз и уязвимостей информационной безопасности организации // Достижения науки и образования. 2017. №5 (18). (Дата обращения 23.09.2023).
4. Программно-аппаратная защита информации [Электронный ресурс] – Режим доступа – URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/programmno-apparatnaya/ (Дата обращения 10.10.2023)
5. Снегуров А. В., Ткаченко Е. А., Кравченко А. Д. Риски информационной безопасности систем, построенных по технологии «Умный дом» // ВЕЖПТ. 2011. №3 (52). (Дата обращения 15.10.2023).
6. Многофакторная аутентификация [Электронный ресурс] – Режим доступа – URL: https://rt-solar.ru/events/blog/3421/ (Дата обращения 06.11.2023).
7. ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection [Электронный ресурс] – Режим доступа – URL: https://www.iso.org/standard/27001 (Дата обращения 19.11.2022).

Оригинальность 86%