

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В УМНЫХ ФЕРМАХ: ЗАЩИТА ИНФРАСТРУКТУРЫ IOT

Г.В. Гвасалия, П.И. Карасев, Г.Ш. Утешева, Алмали Ахмед Аднан Латиф

Кафедра «Информационная безопасность»,
МИРЭА - Российский технологический университет, г. Москва
gvasaliagv@bk.ru, karasev@mirea.ru

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности Интернет вещей агропромышленного комплекса и отдельных ферм. Приведены основные угрозы, уязвимости, которые могут возникнуть на устройствах, в сети и внутренней инфраструктуре комплекса. Также обсуждаются рекомендации по повышению уровня информационной безопасности в условиях цифровизации агропромышленного комплекса. В качестве дополнительных мер защиты рассматриваются многофакторная аутентификация (MFA) и политика создания надежных паролей.

Ключевые слова: Интернет вещей, политика паролей, агропромышленный комплекс, информационная безопасность, защита информации.

ENSURING DATA SECURITY IN SMART FARMS: PROTECTING IOT INFRASTRUCTURE

G.V. Gvasalya, P.I. Karasev, G.Sh. Utesheva, Almali Ahmed Adnan Lateef

Department of Information systems and information protection,
MIREA - Russian Technological University, Moscow
gvasaliagv@bk.ru, karasev@mirea.ru

Abstract. The article discusses the issues of ensuring the information security of the Internet of Things of the agro-industrial complex and individual farms. The main threats and vulnerabilities that can occur on devices, in the network and in the internal infrastructure of the complex are presented. Recommendations on improving the level of information security in the context of digitalization of the agro-industrial complex are also discussed. Multi-factor authentication (MFA) and a strong password creation policy are considered as additional security measures..

Keywords: Internet of Things, password policy, agro-industrial complex, information security, information protection.

Информационные технологии активно, но поспешно внедряются в аграрную промышленность, чтобы оптимизировать ее и сделать фермерское хозяйство более умным. Эти хозяйства используют различные устройства Интернет вещей (IoT) и внутреннюю сеть, которая обеспечивает сбор, обработку и передачу данных, автоматизируя и упрощая процесс. Однако с

ростом таких устройств и внутренней сети в различных фермах и в агропромышленном комплексе возникает проблема их безопасности и безопасности данных.

Угрозы и уязвимости интеллектуальных систем

Интеллектуальные системы, используемые в агропромышленном комплексе, как и любые системы, основанные на технологиях Интернета вещей (IoT), подвержены множеству угроз и уязвимостей. Угрозы, возникающие в агропромышленном комплексе, повреждают, ограничивают или изменяют информацию, которая хранится на устройствах и во внутренней сети. Атаки на устройства происходят с помощью незащищённых соединений, из-за устаревшего программного обеспечения, низкого уровня политики создания паролей и отсутствия дополнительной аутентификации. Недостаточная защищённость данных, может быть использована как внутренним, так и внешним нарушителем, который может повредить автоматизированный процесс в агропромышленном комплексе.

Методы защиты интеллектуальных систем

Для эффективной защиты интеллектуальных систем, используемых в агропромышленном комплексе, необходимо внедрение комплексного подхода, который включает технические и организационные меры связанные с политикой создания паролей и дополнительной аутентификации. На данный момент пароль, состоящий из восьми символов с цифрами и буквами в разных регистрах можно забрутфорсить за 60 часов, но если добавить знаки препинания и различные символы, которые есть на клавиатуре, то время подбора пароля увеличиться до 70 дней, что составляет 2700%.

Вторым вариантом для защиты информации в сети и на устройствах может послужить многофакторная аутентификация, которая может состоять из пароля с рисунком, отпечатком пальцев или любой модальностью, которая зарегистрирована для идентификации человека в Российской Федерации и в Единой биометрической системе. Эти методы повысят эффективность защиты и снизят риски утечек информации.

Примеры успешной защиты интеллектуальных систем в агропромышленной

Одним из примеров является проект "Умные теплицы" в Китае: В Китае реализован проект умных теплиц, где системы управления климатом и поливом интегрированы с IoT-устройствами. В качестве защиты активно используются политика создания паролей и дополнительная аутентификация, которые позволяют выявлять аномалии в работе оборудования и предотвращать потенциальные кибератаки.

Выводы

Информационная безопасность в агропромышленном комплексе становится все более важным аспектом при цифровизации и внедрении технологий Интернета вещей. В условиях растущего количества угроз и уязвимостей необходимо внедрять комплексные меры защиты, которые включают создания политики паролей и внедрение дополнительной

аутентификации. Примеры успешной защиты интеллектуальных систем показывают, что применение современных решений и подходов позволяет снизить риски и повысить надежность работы фермерских хозяйств.

Список литературы

1. IOT Internet of Things /Jade Carter.
2. Аутентификация Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие / А. А. Афанасьев, Л. Т. Веньев, А. А. Воронов, Е. Р. Газизова, А. Л. Доохов, А. В. Кряшков, О. Ю. Поянская, А. Г. Сабанов, М. А. Скиäа, С. Н. Хайяпин, А. А. Шеупанов. – URL: <https://znanium.ru/catalog/document?id=140493> (дата обращения: 05.09.2024).

References

1. IOT Internet of Things, Jade Carter.
2. Authentication Theory and practice of ensuring secure access to information resources : textbook / A. A. Afanasyev, L. T. Veenyev, A. A. Voronov, E. R. Gazizova, A. L. Dookhov, A.V. Kryashkov, O. Y. Poyanskaya, A. G. Sabanov, M. A. Skiäa, S. N. Khayyapin, A. A. Sheupanov. – URL: <https://znanium.ru/catalog/document?id=140493> (accessed 05.09.2024).