ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДАННЫХ В ЦИФРОВЫХ ПЛАТФОРМАХ ПРОМЫШЛЕННОГО IoT

Сафиуллин Ильдар Рустамович [1]
Российская Федерация, г. Казань, Казанский государственный энергетический университет.

Аннотация: Статья посвящена исследованию вопросов обеспечения информационной безопасности данных в цифровых платформах промышленного интернета вещей. Рассмотрены особенности функционирования систем промышленного IoT и роль цифровых платформ в сборе, обработке и хранении данных, поступающих от промышленного оборудования и датчиков. Предложены основные методы защиты информации, включая применение криптографических механизмов, систем аутентификации устройств и защищённых протоколов передачи данных. Определены направления повышения безопасности цифровых платформ промышленного IoT в условиях развития цифровизации промышленности.

Ключевые слова: промышленный интернет вещей, информационная безопасность, цифровые платформы, защита данных, кибербезопасность, промышленная автоматизация, цифровизация промышленности.

INFORMATION SECURITY OF DATA IN DIGITAL PLATFORMS OF INDUSTRIAL IoT

Safiyllin I.R.
Russian Federation, Kazan, Kazan State Power Engineering University.

Abstract: The article is devoted to the study of information security issues in digital platforms of the Industrial Internet of Things. The features of industrial IoT systems and the role of digital platforms in collecting, processing and storing data obtained from industrial equipment and sensors are considered. The paper proposes key approaches to data protection,

[1]Студент 3 курса бакалавриата Института цифровых технологий и экономики Казанского государственного энергетического университета. Научный руководитель: Сандаков В.Д., кандидат технических наук, доцент кафедры ИТИС Казанского государственного энергетического университета (Sandakov V.D., Candidate of Technical Sciences, Associate Professor of the Department of Information Systems at Kazan State Power Engineering University).

including the use of cryptographic mechanisms, device authentication systems and secure data transmission protocols. The directions for improving the security of industrial IoT digital platforms in the context of industrial digitalization are identified.

Keywords: industrial Internet of Things, information security, digital platforms, data protection, cybersecurity, industrial automation.

Введение

Сейчас уже никого не удивишь тем, что промышленный интернет вещей — это основа управления производством. Цифровые платформы собирают телеметрию, на её основании что-то включается, выключается, регулируется. И если данные утекут или, хуже того, их подменят, последствия могут быть совсем не теоретическими. В литературе пишут, что архитектура таких платформ сложная, многослойная, и это действительно так [1]. Но проблема даже не в сложности, а в разнородности: с одной стороны, старое оборудование с Modbus, который проектировался вообще без мысли о безопасности, с другой — современные облака. Всё это пытается работать вместе. И если для офисных сетей уже придуманы стандартные защиты — поставил антивирус, файрвол, и вроде спишь спокойно, — то для IIoT эти штуки часто не подходят. Там задержки критичны, а устройства маломощные. Получается разрыв: требования по безопасности есть, а инструменты под них приходится изобретать на ходу. Тут, кстати, важно понимать, что комплексный подход, о котором много говорят [3], в промышленности упирается не только в софт, но и в физику процесса.

Ход исследования

Если начать разбираться, где именно в IIoT-платформах самые большие дыры, быстро выясняется: дело не столько в каналах передачи, сколько в точках стыка. Шлюзы, всякие пограничные контроллеры, которые данные собирают и передают дальше. Мы посмотрели три типа архитектуры — чисто облачную, туманные вычисления и гибридную. И везде картина похожая: попытались промоделировать атаки, как внешние, так и инсайдерские. Самое смешное, что шифрование по TLS вроде как помогает, но только если его включить. А на старых контроллерах его просто не вытянуть. Там процессоры слабые, для них сертификаты тяжёлые. Тут недавно попалась работа про анонимизацию и сокрытие каналов [4] — казалось бы, тема из другой оперы, а в наших условиях, если замаскировать трафик, чтобы злоумышленник вообще не понял, где тут критический узел, это может сработать не хуже шифрования. Метод странный, но рабочий.

Ещё пытались прикрутить поведенческую аналитику. То есть машинное обучение смотрит на временные ряды с датчиков и учится

отличать нормальную работу от аномалий. Идея красивая: система видит, что данные вдруг пошли не так, и бьёт тревогу раньше, чем случится авария. На практике всё упёрлось в ложные срабатывания. Если система думает, что это атака, а на самом деле просто датчик сбойнул или регулировка плановая пошла, она может отключить линию. А останавливать производство просто так — себе дороже. Так что настройка таких систем — это искусство, и подходить к ней надо с учётом конкретного производства, а не по общим шаблонам [5].

Отдельная боль — обновление прошивок. Устройств много, они разбросаны по цехам, и обновлять их вручную невозможно. Нужны OTA-обновления (over-the-air). Но тут риск: если прошивка не подписана криптографически, злоумышленник может впендюрить бэкдор прямо по воздуху. И это не теория, были случаи. В учебниках чёрным по белому написано, что сегментация сети обязательна, что IIoT-устройства нельзя держать в одной сети с офисными компами [2]. А на практике заходишь на предприятие — и видишь эту картину своими глазами. Всё в одной куче. Экономия на всём.

На тестовом стенде мы гоняли нагрузку от криптографии. Сравнивали RSA и эллиптические кривые (ECC). Так вот, ECC даёт сопоставимую защиту, но процессор меньше греется и медленнее стареет, если так можно выразиться. Для автономных датчиков это критично. Но стандартов под это до сих пор нет, каждый вендор городит своё, и нормативка за ними не поспевает [1]. И ещё один момент вскрылся неожиданно. Когда мы моделировали атаки на канальном уровне и пытались включить шифрование, чтобы защититься, вдруг поплыли временные метки. Задержка в несколько микросекунд, а для прецизионных приводов это уже рассогласование. То есть мы защитили данные, но сломали синхронизацию. Тут нужны протоколы типа Time-Sensitive Networking, где безопасность вшита в обмен данными изначально. Но в коммерческих платформах это пока экзотика. И получается дурацкий выбор: либо система работает чётко, но уязвима, либо защищена, но тормозит. Для критической инфраструктуры такой выбор неприемлем в принципе. Поэтому простой установкой межсетевых экранов тут не обойтись, нужна глубокая настройка систем обнаружения вторжений прямо под технологический процесс, со всеми его нюансами [5].

Полученные результаты и выводы (Заключение)

Если коротко, то старые методы защиты, когда строили забор вокруг периметра, в IIoT не работают. Там периметра как такового нет. Нужна модель нулевого доверия, когда каждый запрос проверяется, каждое устройство подтверждает свою личность. Исследование показало, что универсальной таблетки не существует. Эффективность

достигается только комплексным подходом, базирующимся на фундаментальных принципах защиты информационных систем [2] и адаптированным к реалиям конкретного производства. Промышленные цифровые платформы будущего должны проектироваться с учетом принципов security-by-design, где безопасность встроена в ядро обработки данных, а не надстраивается над уже работающей системой. Дальнейшие исследования в этой области должны быть направлены на создание унифицированных протоколов обмена для разнородных устройств без потери уровня защищенности, а также на интеграцию передовых методов мониторинга и анонимизации в промышленную практику.

Список использованных источников

1) Баланов, А. Н. Цифровые платформы и системы: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 452 с.

2) Баланов, А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — 3-е изд., стер. — Санкт-Петербург: Лань, 2026. — 280 с.

3) Баланов, А. Н. Комплексная информационная безопасность: учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург: Лань, 2025. — 400 с.

4) Нефедов, В. С. Основы обеспечения анонимности в сети Интернет: учебное пособие / В. С. Нефедов, А. А. Криулин, Г. Ю. Потерпеев. — Москва: РТУ МИРЭА, 2022. — 81 с.

5) Шипулин Г.Ф. Мониторинг инцидентов информационной безопасности. Средства защиты информации: межсетевые экраны, системы обнаружения и предотвращения вторжений: учебное пособие / Г.Ф. Шипулин. — Москва: РТУ МИРЭА, 2025. — 151 с.