ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

НАУЧНЫЙ ЖУРНАЛ №2(24) 2020

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ ВЕСТНИК

Подписано в печать 17.06.2020
Формат В5
Печать офсетная. Усл.печ.л. 11,6
Тираж 500 экз.
Заказ № 82-11
Отпечатано в типографии
ООО «Научный консультант»
г. Москва
Хорошевское шоссе, 35, корп.2

УДК 621.31

Совершенствование управления территориально-распределенной системой ИБ с использованием технологии промышленного интернета-вещей

А.И. Сухотерин, кандидат военных наук, доцент, доцент кафедры «Информационной безопасность»,
Государственное бюджетное образовательное учреждение высшего образования Московской области
«Технологический университет», г. Королев, Московская область

В статье рассматривается проблемы управления ИБ на территориально-распределённых объектах защиты. Во избежание простоев и для сохранения безопасности на предприятии необходимо внедрение технологий, позволяющих обнаруживать и прогнозировать риски. Предлагается с помощью промышленного интернета-вещей обеспечить непрерывный интеллектуальный мониторинг ключевых показателей, что дает возможность определить проблему и принять необходимые меры для ее решения. Оперативный в режиме реального времени анализ поможет специалисту ИБ быстрее находить уязвимые места и предотвратить несанкционированные действия на предприятии.

Информационная безопасность, промышленный интернет-вещей, территориально-распределенная система.

Improving the management of geographically distributed IB system using industrial technology Internet of things

A.I. Sukhoterin, Candidate of Military Sciences, associate professor of Information security Department,
State Educational Institution of Higher Education
Moscow Region «University of technology», Korolev, Moscow region

This article discusses the problems of is management on geographically distributed security objects. In order to avoid downtime and to maintain security at the enterprise, it is necessary to introduce technologies that allow detecting and predicting risks. It is proposed to use the industrial Internet of things to provide continuous intellectual monitoring of key indicators, which makes it possible to identify the problem and take the necessary measures to solve it. Real-time real-time analysis will help the IB specialist find vulnerabilities faster and prevent unauthorized actions in the enterprise.

Information security, industrial Internet of things, geographically distributed system.

Традиционное управление большим предприятием, как правило, крайне пассивно. Тем не менее, цифровая эпоха сделала более гибкими даже самые консервативные рынки – теперь операционные менеджеры получают данные прак-

тически в реальном времени.

Постоянная отчётность и помощь в принятии решений становятся особенно важными в чрезвычайных ситуациях, когда каждая секунда на счету, а системе требуется выполнить множество корректирующих действий.

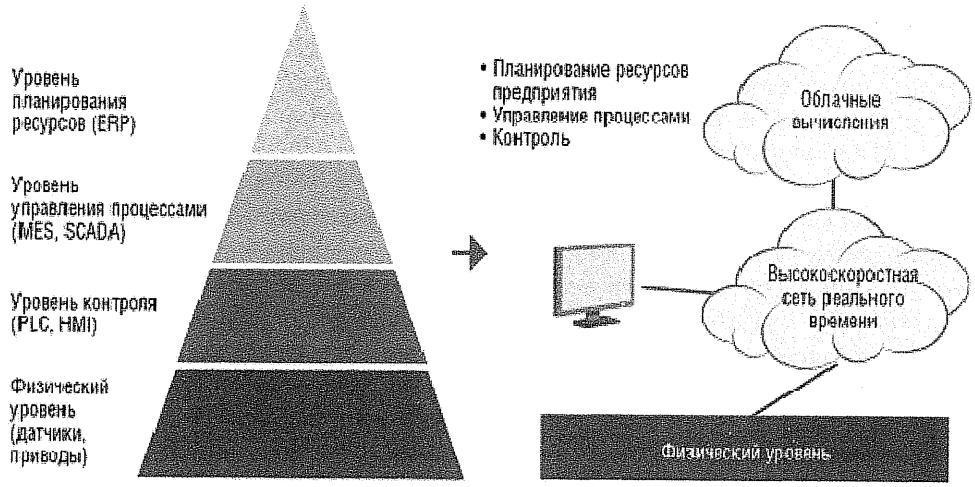

Рисунок 1 – Переход от обычных АСУ ТП к промышленному интернет-вещей

Как правило, аудит носит рекомендации проводить не реже чем раз в полгода. В результате мы получаем перечень инцидентов информационной безопасности и шаблон действий сотрудников, направленных на защиту обрабатываемого информационного ресурса в заданных параметрах.

Применение процессного подхода позволит контролировать качество и результат выполняемых видов работ в режиме реального времени, выявляя при этом недостатки, поэтому для более точного выявления недостатков работы системы аудит не должен быть единственным фактором.

Решением в современном мире будет ситуационный контроль распределенных объектов с помощью IIoT-технологий, безопасность которых обеспечивает технология распределённых реестров.

Сети Промышленного интернета вещей не могут быть ограничены, периметром информационного объекта. Существенное влияние имеет взаимодействие с произведенным изделием («вещью») на всех этапах его существования, кроме того важное значение имеет доступ ко всем сервисам ЦОД (территориально-распределенных центров обработки данных). Ключевой характеристикой IoIoT – технологий.

Обычно, в подобных сценариях играет роль целостный подход к вышестоящим системам мониторинга. Платформа выступает в качестве промежуточного программного обеспечения, агрегируя инциденты со множества разнородных систем мониторинга, управления и контроля нижнего уровня. События, происходящие на физическом уровне, по-прежнему будут связаны, например, пожарная сигнализация или турникет.

Сущность IIoT -технологии заключается в следующем:

- устанавливаются механизмы, выполняющие различные процедуры, контроллеры – датчики и человеко-машинные интерфейсы на самые ответственные компоненты оборудования;
- затем осуществляется сбор, хранение, обработка, выдача информации, которая позволит. осуществить реальную оценку предприятия;
- полученные данные становятся достоянием всех заинтересованных структурных подразделений и помогают формировать предложения руководителю, для принятия решения.

Тревоги уведомляют специалистов в области ИБ о возникновении важного события или превышении каких-либо полномочий сотрудников или злоумышленников, в какой бы части распределённой IIoT-конструкции это не случилось. Без тревог специалист чтобы убедиться в отсутствии проблем должен лично на постоянно основе проводить осмотр помещений, оборудования и других объектов защиты. Тревоги как вспомогательный инструмент заставляют обратить внимание на те или иные моменты работы предприятия.

Система управления инцидентами представляет собой набор «блок-цепочек» – программных модулей, использующихся для сбора, хранения, анализа и визуализации данных из различных источников, а также дальнейшей передачи этих данных в другие элементы корпоративной инфраструктуры.

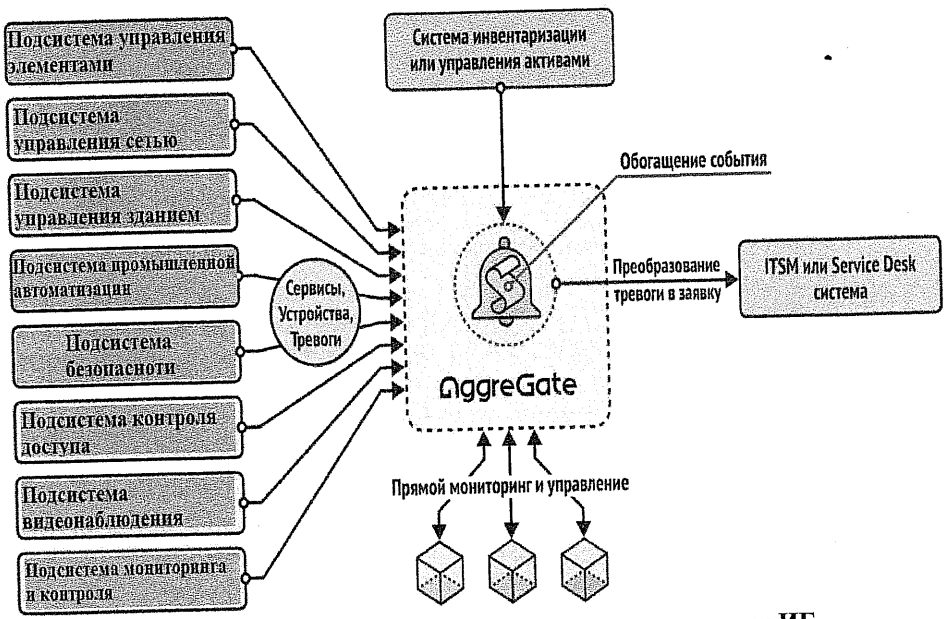

Рисунок 2 – Взаимодействие подсистем управления ИБ

Крупные корпоративные системы, как правило, используются большим количеством сотрудников, включая системных администраторов, инженеров и операторов, бизнес-аналитиков, занимающихся анализом данных, руководителей, просматривающих сводные отчёты, и многих других.

Для таких сложных многопользовательских сред предлагается гибкая архитектура безопасности, которая включает в себя:

1. журналирование событий;
2. безопасность баз данных;
3. ролевой способ управления доступом;
4. состояние защищенности коммуникаций.

Поддержка распределенной архитектуры (распределённого реестра) является одной из немногих в мире платформ промышленного интернета-вещей, которые действительно поддерживают распределенную архитектуру. Такая архитектура может обеспечить весь комплекс задач, которые возлагаются на систему управления информационной безопасностью в ближайшей перспективе.

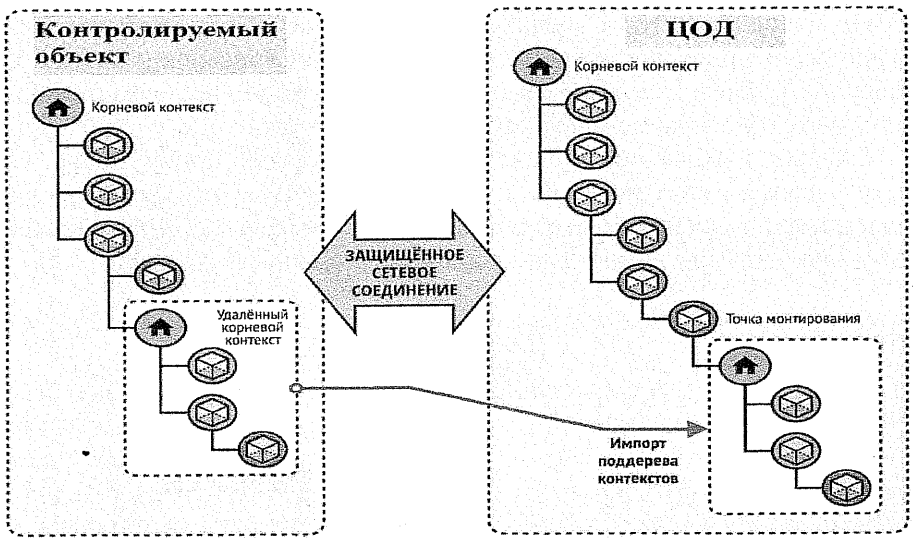

Рисунок 3 – Защищенное сетевое соединение между ТРС

Распределенная архитектура полностью независима от третьих лиц, благодаря этому обеспечивается надежность системы. Причем в таких серверах, сформирован собственный массив данных операторов с соответствующей матрицей доступа и допуска к информационному ресурсу.

Основными целями распределенной архитектуры являются:

1. Адаптация к предъявленным требованиям, подразумевает под собой, что серверы нижнего уровня могут быть сильно нагружены, собирая данные и управляя большим количеством устройств в режиме, близком к реальному времени. Как показывает практика количество устройств, которые могут обслуживаться с помощью одного сервера, ограничено. При адаптации системы для управления разумно установить несколько серверов и объединить их в рамках распределенной установки большим числом устройств.
2. Равномерность нагрузки – сервер обеспечивает управления распределенной сетью (доступ, производительность, обработка различного рода запросов от датчиков, формирование различного рода отчетов и доставка их адресату).

3. Средства противодействия атакам. Эти серверы могут находиться на значительном удалении и обязательно должны иметь связь с центральным сервером. Что позволяет не подключать VPN, так как все заинтересованные потребители подключены к центральному серверу

4. Централизация, то есть основной сервер, установлен в центральной диспетчерской. Вторичные серверы могут работать в полностью автоматическом режиме, в то время как их настройка и мониторинг осуществляется через основной сервер.

Благодаря распределённой инфраструктуре множество серверов выполняют различные функции независимо от их уровня. Часть из них может работать на IIoT-шлюзах, собирая данные, другие – хранить и обрабатывать информацию, а оставшаяся часть – осуществляет высокоуровневое объединение и распределённые вычисления.

Устройства, которые непосредственно связаны с объектом управления, такое как сенсоры и исполнительное устройство, может быть подключено к серверам напрямую, через агентов, через шлюзы или с помощью их комбинации.

Характерная для крупных компаний многопользовательская среда позволяет создавать огромное количество учётных записей пользователей, объединяя их в блок-цепочку, где каждый блок в прямой зависимости от предыдущего. Каждая попытка доступа к единой модели данных сервером обрабатывается под своим уникальным хэшем согласно правам доступа авторизованного пользователя в определённой цепочке. Активные системные объекты (например, тревоги, сигнатурная подсветка, модели и др.) наследуют права доступа их владельцев, как только обращаются к единой модели данных.

Права доступа пользователей настраиваются с помощью соответствующей таблицы прав, регулирующих уровень доступа пользователя до любого системного ресурса. Это позволяет администратору безопасности реализовывать комплексный подход при формировании доступа должностных лиц организации к обрабатываемому информационному ресурсу (это важно с точки зрения подготовки одновременно документа большим количеством исполнителей, в рамках предложений руководству для принятия решения).

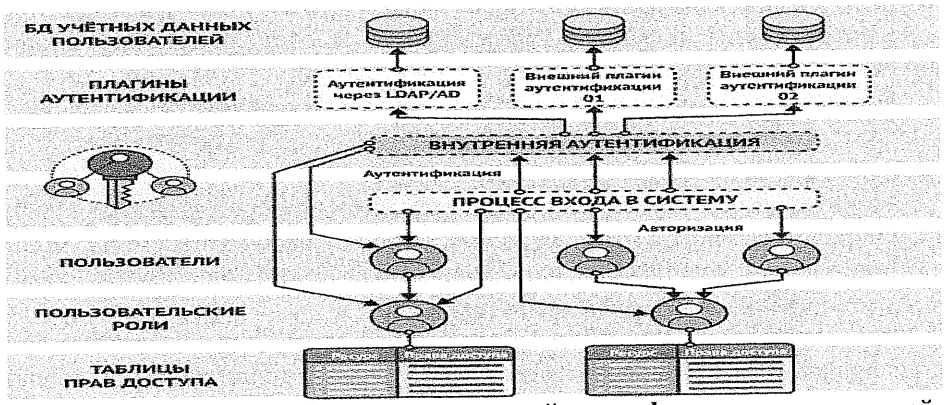

Рисунок 5 – Схема прохождения внутренней аутетификации пользователей

В таблице прав пользователя может задавать уровень доступа каждая запись к одному или нескольким ресурсам, а также к целым поддеревьям, включающим в себя все дочерние ресурсы. Все элементы могут быть объединены и настроены в визуальном виде специальными редакторами, при этом не требуя опыта специалиста IT [15].

Комбинируя распределенный реестр с промышленным интернетом вещей, проще реализовать конфиденциальность и целостность, является важным фактором для обеспечения:

- надежных соединений;
- безопасной обработки между устройствами [15].

Это позволяет подключенным устройствам реагировать на производственные атаки и модификации, таким образом, повышает доверие между сторонами в общении. В частности, технология распределенного реестра очень хорошо зашифрован с помощью сложного математического шифрования, способного реагировать на атаки извне. Кроме того, вместо централизованного метода распределенного реестра использует децентрализованный метод, который затрудняет хакерам установление целей. Эта функция сводит к минимуму влияние отдельных атак на устройства IIoT, а затем и на все устройство. Основанные на доверии услуги между устройствами IIoT суммированы ниже:

- децентрализованная структура распределяет задачи, затрудняя для злоумышленников установление этих целей. В случае частной цепочки блоков, если развитие вычислений ограничено, проблемы безопасности могут быть решены путем защиты сети с помощью инструмента «Безопасный IP»;
- можно поддерживать прозрачность через доверительные сети, обмениваться данными о транзакциях участников и надежно их хранить.
- это гарантирует целостность деталей транзакции для ответа на фальшивые атаки и подделку – каждый участник подтверждает детали транзакции;
- процедура аутентификации и авторизации основных устройств IIoT обязательна;
- в общедоступной цепочке блоков можно улучшить эффективность строительства и обслуживания в соответствии с ее распределением. Кроме того, децентрализация повышает эффективность за счет сокращения затрат на строительство и эффективного распределения ресурсов.

В результате сети, использующие распределенный реестр, могут обеспечить надежную среду не только для обмена данными, но и для администраторов, управляющих сетью, и для пользователей.

Мониторинг значимых событий в реальном времени является критической функцией для многих отраслей, таких как учет рабочего времени, мониторинг IT-инфраструктуры или контроль доступа. Отслеживание текущих событий является основной из задач операторов таких систем.

Возможности выбираются от простых оповещений о внештатных ситуациях до продвинутой обработки данных модулями интеллектуальной машины, позволяющими находить слабые места и предсказывать события, например, несанкционированные действия на предприятии.

Промышленный Интернет вещей позволяет объединять производствен-

ные, человеческие, транспортные и другие ресурсы предприятия в цифровые сети в целях автоматизации его бизнес-процессов. Основные цели внедрения технологий IIoT – сокращение издержек и повышение произвольности. Кроме того, технологии Интернета вещей позволяют создавать новые кросс-индустриальные решения и услуги для конечных потребителей за счет объединения различных отраслей в единые коммуникационные сети.

Литература

1. Доктрина информационной безопасности Российской Федерации утверждена Указом Президента Российской Федерации от 5 декабря 2016 года N 646.
2. ФЗ № 149 от 27.07.2006 г. (ред. от 18.03.2019г.) «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ.
4. Воронин А. Мошенничество в платежной сфере. Бизнес-энциклопедия // М.: Издательский дом «Альпина Паблишер». 2016. 352 с.
5. Андреев Ю.С., Третьяков С.Д., Промышленный интернет вещей // СПб: Университет ИТМО. 2019. 54 с.
6. Мачей Кранц: Интернет вещей. Новая технологическая революция, Переводчик: Мамедьяров З. // Издательство: Бомбора. 2018 г.
7. Тихвинский В.О., Коваль В.А., Бочечка Г.С. Интернет вещей: международная стандартизация // Электросвязь. 2017. № 2.
8. Пушкарев М.С. Интернет вещей (IoT): понятие и значение для формирования правовой основы цифровой трансформации экономики // Вопросы российского и международного права. 2018. Том 8. № 1А. С. 16-27.
9. Тихвинский В.О., Коваль В.А., Бочечка Г.С., Бабин А.И. Сети IoT/M2M: технологии, архитектура и приложения // М.: Издательский дом «Медиа Паблишер». 2017.
10. [Электронный ресурс]. URL: https://geektimes.ru/company/wirex/blog/277438/ (дата обращения 20.04.2020).
11. [Электронный ресурс]. URL: https://www.pwc.ru/ (дата обращения 20.04.2020).
12. [Электронный ресурс]. URL: https://22century.ru/popular-science-publications/blockchain (дата обращения 20.04.2020).
13. [Электронный ресурс]. URL: https://habrahabr.ru/post/323128/ (дата обращения 20.04.2020).
14. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php (дата обращения 20.04.2020).
15. [Электронный ресурс]. URL: https://aggregate.tibbo.com/ru/technology/architecture/distributed-architecture.html (дата обращения 20.04.2020).