• *Развитие новых продуктов и услуг*: ИИ анализирует данные и выявляет новые возможности для развития бизнеса. Это помогает компаниям предлагать инновационные продукты и услуги, которые привлекут новых клиентов и увеличат прибыль.

Вызовы внедрения искусственного интеллекта в цифровизацию бизнес-операций представляют собой:

1. Технические сложности: внедрение ИИ требует значительных инвестиций в инфраструктуру, включая мощные вычислительные ресурсы и специализированное программное обеспечение. Кроме того, необходимо обучать персонал для работы с новыми технологиями, что также требует времени и ресурсов.

2. Этические вопросы: использование ИИ поднимает множество этических вопросов, таких как конфиденциальность данных, прозрачность алгоритмов и потенциальная дискриминация. Компании должны разрабатывать и внедрять этические нормы и стандарты для использования ИИ, чтобы избежать негативных последствий.

3. Сопротивление изменениям: сотрудники могут сопротивляться внедрению новых технологий из-за страха потери работы или изменения привычных рабочих процессов. Важно проводить обучение и разъяснительную работу, чтобы помочь сотрудникам адаптироваться к изменениям.

4. Качество данных: для эффективного функционирования ИИ необходимы большие объемы качественных данных. Недостаток или низкое качество данных может привести к ошибкам в работе ИИ-систем и снижению их эффективности.

5. Безопасность: ИИ-системы могут быть уязвимы для кибератак и других угроз безопасности. Компании должны обеспечивать надежную защиту своих ИИ-инфраструктур и данных, чтобы предотвратить возможные инциденты.

6. Регуляторные ограничения: в разных странах существуют различные регуляторные требования и ограничения, касающиеся использования ИИ. Компании должны учитывать эти требования при внедрении ИИ, чтобы избежать юридических проблем.

Будущие тенденции предполагают:

1. Развитие автономных систем: будущее ИИ связано с развитием автономных систем, способных принимать решения без вмешательства человека.

2. Интеграцию ИИ с другими технологиями: сочетание ИИ с технологиями Интернета вещей (IoT) и блокчейна откроет новые возможности для бизнеса.

3. Этичное использование ИИ: важным аспектом станет разработка этических норм и стандартов для использования ИИ.

Таким образом, использование искусственного интеллекта в цифровизации бизнес-операций открывает широкие возможности для повышения эффективности и конкурентоспособности компаний. Однако для успешного внедрения ИИ необходимо учитывать технические, этические и организационные аспекты.

УДК 620

ПРОМЫШЛЕННЫЕ СЕТИ В УСЛОВИЯХ КИБЕРУГРОЗ

Т. К. Эбердиева, Дж. Г. Агамырадова, А. Г. Реджебова

Государственный энергетический институт Туркменистана, г. Мары

Рассмотрены методы повышения безопасности промышленных сетей и систем управления. Отмечено, что один из основных шагов на пути к безопасной промышленной сети – ее сегментация, создание безопасных зон и определение защищенных путей передачи данных между ними. Показано, что при этом необходимо строго регламентировать, какие

данные должны передаваться, и кто имеет к ним доступ. Также выделен тот факт, что для обеспечения защиты промышленного сектора следует применять технологии и решения, специально разработанные именно для него.

Ключевые слова: кибербезопасность, Интернет, промышленные сети, *Ethernet*, АСУ ТП.

INDUSTRIAL NETWORKS IN THE CONTEXT OF CYBER THREATS

T. K. Eyeberdieva, J. G. Agamyradova, A. G. Redzhebova

State Energy Institute of Turkmenistan, Mary

This article discusses methods for improving the security of industrial networks and control systems. One of the main steps towards a secure industrial network is its segmentation, creation of secure zones and definition of protected data transmission paths between them. At the same time, it is necessary to strictly regulate what data should be transmitted and who has access to it. It is also necessary to highlight the fact that in order to ensure the protection of the industrial sector, it is necessary to use technologies and solutions specially developed for it.

Keywords: cybersecurity, Internet, industrial networks, *Ethernet*, APCS.

В условиях поточного производства промышленное оборудование работает в непрерывном режиме с минимальными периодами простоя и временем жизни от 10 до 20 лет. Для повышения уровня кибербезопасности сети технологического оборудования, используемого в поточном производстве, замена оборудования – невыгодный вариант. Важно применять технологии и решения, предназначенные именно для промышленного сектора.

Межсетевые экраны – необходимый элемент для сегментации сети. Для использования на промышленном предприятии устройства должны иметь промышленное исполнение и функции. По своему назначению промышленные межсетевые экраны можно разделить на два вида: устройства, применяемые на границе сети, и устройства для защиты производственных ячеек. Одни предназначены для отделения промышленного сегмента от офисной или корпоративной сети. Вторые позволяют сегментировать промышленную сеть и наделены специальными функциями, призванными обезопасить промышленные протоколы. Применяемая в них технология глубокого анализа пакетов DPI (Deep Packet Inspection) дает возможность обезопасить техпроцессы от вредоносного ПО, передаваемого в пакетах, разрешенных классическим брандмауэром.

В промышленных сетях особо важных объектов, требующих применения технологий резервирования, высокоточной синхронизации времени, контроля полосы пропускания и применения средств сетевой безопасности, должны использоваться управляемые коммутаторы. Однако существует много гораздо менее требовательных задач, решение которых можно возложить на неуправляемые устройства.

Большинство жилых зданий не имеет специально приспособленного помещения для установки коммуникационного оборудования, поэтому его размещение часто носит стихийный характер. Коммутаторы устанавливаются на чердаках, в подвалах, плохо отапливаемых помещениях. Вместе с тем компьютерное и сетевое оборудование для домашнего использования давно оснащается портами Gigabit Ethernet, поэтому вполне логично использовать для предоставления услуг широкополосного доступа к сети Интернет гигабитные каналы передачи данных. В коммутаторе применяется неблокируемая архитектура, что позволяет длительное время эксплуатировать его при полной загрузке каналов (например, если большинство жителей дома вдруг решат посмотреть по выделенному каналу футбольную трансляцию). Расширенный диапазон

рабочих температур дает возможность установить устройство в нежилом помещении. Коммутатор не требует настройки и удаленного администрирования. Выпускается версия с 16 комбинированными портами RJ-45/SFP, поэтому при необходимости сеть легко масштабируется на любые расстояния с применением оптических кабелей и сменных оптических модулей. Преимущество SFP-портов также в том, что они повышают ремонтпригодность и сокращают время простоя сетей: вышедший из строя модуль легко заменить новым.

Также данный коммутатор можно применять при автоматизации технологических процессов, нетребовательных ко времени восстановления сети после сбоя и не предъявляющих требований к безопасности сети и эффективному управлению потоками данных.

Для достижения быстрых результатов с минимальными затратами клиенты могут придерживаться пошагового подхода. Для этого необходимо следующее: идентифицировать пробел в системе обеспечения безопасности, который может привести к наиболее серьезным для предприятия последствиям; выявить конкретные производственные зоны, с которыми эти последствия связаны; описать наиболее серьезные уязвимости в данной области; минимизировать или устранить эти уязвимости.

Обеспечив безопасность наиболее критической зоны, компания сможет перейти к устранению уязвимостей в другой области. Такой сфокусированный пошаговый подход позволит избежать необходимости менять всю систему сразу и избавит от связанного с этой задачей «аналитического ступора». Он не только гарантирует, что немедленно будут устранены проблемы, ведущие к серьезным последствиям для деятельности предприятия, но и не даст «распылять» силы и средства, т. е. добиться максимального результата от инвестиций.

Реализация системы информационной безопасности АСУ ТП представляет собой комплексную задачу. Ее решение зависит от выполнения правил на всех уровнях: административный – формирование руководством программы работ по информационной безопасности; процедурный – определение норм и правил для персонала, обслуживающего сеть; программно-технический – управление доступом; обеспечение целостности; обеспечение безопасного межсетевого взаимодействия; антивирусная защита; анализ защищенности; обнаружение вторжений; непрерывный мониторинг состояния, выявление инцидентов, реагирование.

Системы контроля уязвимостей – один из эффективных методов противодействия промышленным киберугрозам. Это узкопрофильные программы, разработанные специально для промышленных систем автоматизации. Они позволяют определить целостность внутренней среды устройства, зафиксировать все попытки изменить прикладную программу контроллера, изменения в конфигурации сетевых устройств защиты и управления в энергосетях.

Появление новых стандартов, таких как МЭК 61850 в области энергетики, отражает необходимость приведения нормативной базы в соответствие с новыми реалиями и техническими решениями, а также проникновение технологий Ethernet в эту область. Новые стандарты резервирования (IEC 62439), позволяющие обеспечить нулевое время восстановления после сбоя и гарантированную доставку информации, применяются для построения сетей промышленных предприятий и, в частности, внедряются на объектах энергетики. Появление новых коммутаторов с поддержкой технологии PoE и рост бюджета мощности обеспечивают расширение сфер их применения и функциональности систем управления и безопасности. Увеличение скоростей передачи данных расширяет области применения коммутационной техники, повышает качество обслуживания объектов и пользователей и дает возможность

масштабировать сети без потерь и задержек данных. Также гигабитные сети стали, очевидно, доступнее. Появление новых технических решений и устройств для защиты сетевой инфраструктуры АСУ ТП, улучшение методик и подходов к сетевой безопасности, их стандартизация и сертификация позволяют создать системы, устойчивые к негативным внешним и внутренним воздействиям. Постоянное совершенствование программной и технической составляющей сетевых устройств, выпуск новых версий ПО, его регулярное обновление и установка патчей способствуют повышению безопасности и расширяют функциональные возможности устройств связи.

Успешная кибератака на промышленную систему может повлечь за собой производственные потери, урон системе безопасности и окружающей среде, кражу интеллектуальной собственности, включая информацию из корпоративной сети предприятия. Также взлом промышленного сегмента сети образует «дверь» в общую корпоративную сеть предприятия.

Организациям стоит изучить свои информационные активы, определить слабые места и возможные угрозы. В первую очередь, необходимо установить возможные события, которые недопустимы для функционирования бизнеса, и регулярно проводить верификацию таких событий на практике с помощью тестирования на проникновение или размещения цифровых двойников на киберполигонах. Такой подход поможет выстроить систему комплексной защиты и мониторинга, которые не позволят злоумышленникам нанести ущерб организации и ее клиентам. Из-за тенденции к нарушению основной деятельности промышленных организаций с помощью различного ВПО (шифровальщики, вайперы) решения резервного копирования позволят быстро восстановиться, если атака все-таки достигла своей цели. Важно помнить о влиянии человеческого фактора на успешность кибератак и проводить мероприятия для повышения бдительности и осведомленности в сфере кибербезопасности, а также обучение по противодействию атакам методами социальной инженерии.

Результативная кибербезопасность в электроэнергетике. Системы кибербезопасности следует увязывать с технологическими системами управления и ИТ-системами. На промышленных предприятиях нужно разработать процессную модель и регламенты взаимодействия специалистов по ИБ и оперативно-диспетчерского персонала. Они должны видеть единую картину, в которой коррелируются данные об инцидентах в ИТ-инфраструктуре, поведение основного оборудования и события с систем управления. При таком подходе можно добиться того, что недопустимые для индустриального объекта и энергосистемы события станут действительно неосуществимыми.

Литература

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере / А. Е. Фаронов. – Москва : ИНУИТ, 2016. – 155 с.
2. Добротун, Е. Б. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действия нарушителя / Е. Б. Добротун // Программные продукты и системы. – 2016. – № 3. – С. 42–50.
3. Шишов, О. В. Конфигурирование, программирование и работа в сети базовых компонентов систем промышленной автоматизации / О. В. Шишов. – Саранск : ИП В. С. Афанасьев, 2014. – 160 с.