УДК 004.415.24

ПРИМЕНЕНИЕ УСТРОЙСТВ ОДНОНАПРАВЛННОЙ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ЗАЩИТЫ УЗЛОВ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Поликарпов А.А.

ООО «Специальный Технологический Центр», 195220, Россия, г. Санкт-Петербург, Гжатская ул., дом 21, лит. Б, офис 53, e-mail: office@stc-spb.ru

В статье рассматривается построение архитектуры автоматизированной системы управления с применением устройства однонаправленной передачи данных в свете требований приказов ФСТЭК России

Ключевые слова: устройство однонаправленной передачи данных, кибер-атака, IP-шлюз, информационная безопасность.

APPLICATION OF UNIDIRECTIONAL DATA TRANSFER DEVICES FOR THE PROTECTION OF AUTOMATED SYSTEM NODES IN ACCORDANCE WITH THE REQUIREMENTS FOR ENSURING THE SAFETY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES.

Polikarpov A.A.

LLC Special Technological Center, 195220, Russia, St. Petersburg, Gzhatskaya St., 21, Lit. B, office 53, e-mail: office@stc-spb.ru

The article deals with the construction of an automated control system architecture using a unidirectional data transfer device in light of the requirements of the orders of the FSTEC of Russia.

Keywords: unidirectional data transmission device, cyber-attack, IP-gateway, information security.

Индустрия 4.0, часто называемая «Четвертая промышленная революция», охватывает обширную группу технологий, связанных автоматизацией обмена данных и производственных процессов. На сегодняшний день это собирательное понятие определяет принципы функционирования так называемого «Умного предприятия», основанного на взаимодействии различных устройств, машин, датчиков, обмениваться информацией посредством интернета вещей (IoT) и межмашинного взаимодействия (M2M).

Группы подобных устройств способны автономно обеспечивать производственные процессы при минимальном вмешательстве арбитров высокого уровня. Наиболее распространенными протоколами взаимодействия таких устройств на сегодняшний день являются Fieldbus (до 66%) и Industrial Ethernet (до 59%). Для данных протоколов характерны следующие модели взаимодействия: точка-точка; широковещательная рассылка (broadcast); подписочная модель (multicast); запросная модель (Request/response).

Стек протоколов, реализуемых в данных моделях на транспортном уровне, как правило основан на стеке протоколов TCP/IP, что предопределяет возможности организации различных кибер-атак, особенно чувствительных для критической информационной инфраструктуры. Наиболее известный пример кибер-атаки на автоматизированную систему управления – вирус Stuxnet физически разрушающий инфраструктуру, использованный против иранской ядерной программы. Для противостояния угрозам кибер-атак на критически важные информационные инфраструктуры в Российской Федерации были приняты следующие нормативные акты:

– Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ;

– Приказ ФСТЭК N 235 (Требования к созданию систем безопасности значимых объектов КИИ РФ и

обеспечению их функционирования);

– Приказ ФСТЭК N 239 (Требования по обеспечению безопасности значимых объектов КИИ РФ).

На сегодняшний день для решения задач обеспечения безопасности КИИ предлагается несколько проектов национальных стандартов:

– ПНС «Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi);

– Проект ПНС «Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением».

Разработанные ТК194 в 2019 году и методические рекомендации ТК26:

– МР 26.4.003-2018 «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств»;

– МР 26.4.001-2019 «Протокол защищенного обмена для индустриальных систем (CRISP 1.0)» (CRISP - Cryptographic Industrial Security Protocol).

На базе указанных документов уже разработаны комплексные решения для защиты информации в АСУ.

Однако, данные решения не охватывают ряд мер обеспечения безопасности, определенных в Приказе ФСТЭК №239 «Требования по обеспечению безопасности значимых объектов КИИ РФ». В частности, в составе мер обеспечения безопасности значимого объекта требуется:

в части защиты ИС/АСУ и ее компонентов:

– ЗИС.3 Эшелонированная защита информационной (автоматизированной) системы;

– ЗИС.4 Сегментирование информационной (автоматизированной) системы;

– ЗИС.17 Защита информации от утечек;

– ЗИС.20 Обеспечение доверенных канала, маршрута;

– ЗИС.34 Защита от угроз отказа в обслуживании (DOS, DDOS-атак);

в части управления доступом:

– УПД.14 Контроль доступа из внешних информационных систем.

Отметим также, что во многих системах наиболее приоритетной задачей защиты информации является защита от утечек и непрерывность функционирования, а не конфиденциальность циркулирующей информации.

Для обеспечения комплексной защиты АИС и ее компонентов предлагается гибридное решение с применением устройства однонаправленной передачи данных. Однонаправленный шлюз – сетевое устройство, обеспечивающее потоковую передачу информации в одном направлении и не позволяющее передачу в обратном. Такое устройство обеспечивает невозможность неправомерного доступа к информации, обрабатываемой значимыми объектами критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования и изменения функционирования информационной системы, а также гарантированную защиту от утечек информации.

Различные сценарии организации передачи данных с помощью таких программно-аппаратных средств позволяют организовать множество сегментов хранения данных и формирование доверенного канала их доставки. Помимо обеспечения гарантированного невыхода информации через однонаправленное устройство передачи данных в обратном направлении, считаем целесообразным реализацию на их базе следующих функций обеспечения безопасности: анализ передаваемого трафика и блокировку определенных типов протоколов (защита от D-DOS); анализ портов отправителя данных и блокировку несанкционированных портов (фильтрация трафика); аппаратный шейпинг канала доставки информации (выравнивание трафика и распределение приоритетов передачи данных). При этом, нет необходимости регулярного аудита настроек сетевого оборудования ввиду невозможности удаленного изменения параметров однонаправленного шлюза. Использование устройства однонаправленной передачи данных в качестве IP-шлюза позволяет сопрягать его с такими сетевыми устройствами, как:

– Шлюз беспроводной сети (Wireless Gateway), обеспечивающий соединение самоорганизующихся сетей и «умных датчиков» с хост-системами и информационными приложениями. Обмен данными шлюза с системой верхнего уровня производится по протоколу Ethernet (протокол TCP/IP). Дополнительные устройства можно добавить в любой момент. При этом нет необходимости настраивать каналы связи, поскольку шлюз управляет сетью в автоматическом режиме.

– Сетевой маршрутизатор (router), обеспечивающий передачу информации между различными сегментами сети. Сопрягаемые сети могут обладать различными скоростями передачи, задержками, процедурами безопасности. Кроме того, могут использоваться различные протоколы (TCP и UDP), технологии и даже среды передачи (оптическое волокно и витая пара).

– Виртуальный маршрутизатор (Edge gateway), соединяющий внешнюю и внутреннюю сеть обеспечивает

такие механизмы, как NAT, брандмауэр, load balancer и VPN. DHCP позволяет автоматически назначать IP-адреса виртуальным серверам из предопределенных диапазонов. Указанные функции позволяют осуществить трансляцию информации в центр управления устройствами для дальнейшей обработки и анализа (IoT Hub).

Для обеспечения доставки информации, загружаемой из сетей общего пользования, в том числе сети Интернет, возможно использование выделенного канала доставки с применением устройства однонаправленной передачи данных, обеспечивающего невозможность утечки информации в общедоступную сеть, с ограничением UDP-портов подключения к внешней сети для фильтрации информационных потоков, а также парольной аутентификацией для повышения достоверности источника передаваемой информации.

Особенно стоит отметить возможность реализации такого устройства, обеспечивающего скорость доставки информации на скоростях до 10 Гбит/с, что критически важно при проектировании ситуационных центров в различных инфраструктурных отраслях, обусловленное тенденцией роста сетевой организации бизнес-процессов. Таким образом, реализация устройства однонаправленной передачи данных с расширенным функционалом позволит решить целый комплекс задач по обеспечению информационной безопасности автоматизированной системы на базе одного устройства с возможностью адаптации в различные архитектуры информационной системы, обеспечивая гарантированную защиту от утечки конфиденциальной информации.

Список литературы

1. КиберЛеника Индустрия 4.0: практические аспекты реализации в российских условиях [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/industriya-4-0-prakticheskie-aspekty-realizatsii-v-rossiyskih-usloviyah (дата обращения 26.02.2020).

2. КиберЛеника Перспективы использования российских средств защиты информации в инфраструктурных отраслях [Электронный ресурс]. https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-rossiy skih-sredstv-zaschity-informatsii-v-infrastrukturnyh-otraslyah (26.02.2020).

3. Компания AS WaveCom [Электронный ресурс]. Режим доступа: https://www.wavecom.ee/ru/edge-gateway (дата обращения 27.02.2020).

4. Федеральная служба по техническому и экспортному контролю [Электронный ресурс].Режим доступа: https://fstec.ru/indextekhn icheskaya- zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1704-prikaz-fstek-rossii-ot-9-avgusta-2018-g-n-138 (дата обращения 26.02.2020).

5. Full Spectrum Systems Что такое Индустрия 4.0? [Электронный ресурс]. Режим доступа: https://fss.by/blog/что-такое-индустрия-4-0 (дата обращения 26.02.2020).

References

1. CyberLenika Industry 4.0: practical aspects of implementation in the Russian environment [Electronic resource]. Access mode: https://cyberleninka.ru/article/n/industriya-4-0-prakticheskie-aspekty-realizatsii-v-rossiyskih-usloviyah (circulation date 26.02.2020).

2. CyberLenika Prospects for the use of Russian information protection means in infrastructure industries [Electronic resource]. https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-rossiy skih-sredstv-zaschity-informatsii-v-infrastrukturnyh-otraslyah (26.02.2020).

3. AS WaveCom [Electronic resource]. Access mode: https://www.wavecom.ee/ru/edge-gateway (circulation date 27.02.2020).

4. Federal Service for Technical and Export Control [Electronic resource]. Access mode: https://fstec.ru/indextekhn icheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1704-prikaz-fstek-rossii-ot-9-avgusta-2018-g-n-138 (circulation date 26.02.2020).

5. Full Spectrum Systems What is Industry 4.0? [Electronic resource]. Access mode: https://fss.by/blog/что-такое-индустрия-4-0 (circulation date 26.02.2020).