**УДК 004.056**

# Проблематика мониторинга информационной безопасности беспроводных сетей Wi-Fi в АСУ ТП промышленного типа

*Д. С. Буренок*

*Национальный исследовательский университет «МИЭТ»*
*г. Москва, г. Зеленоград*
*e-mail: corr.dmitry@yahoo.com*

# Issues of information security monitoring for Wi-Fi wireless network in ICS

*D. S. Burenok*

*National Research University of Electronic Technology*
*Moscow, Zelenograd*
*e-mail: corr.dmitry@yahoo.com*

*Аннотация:* Применение в компонентах АСУ ТП модулей программно-аппаратной поддержки Wi-Fi влечет необходимость осуществлять мониторинг, регистрировать события информационной безопасности и выявлять факты реализации известных киберугроз применительно к данной технологии. В ряде случаев мониторинг может быть обеспечен исключительно внешними средствами. В статье рассматривается ключевая проблематика мониторинга информационной безопасности беспроводных сетей Wi-Fi в АСУ ТП промышленного типа. Для эффективного решения задачи декларируется необходимость применения научного и инженерного подхода.

*Ключевые слова:* информационная безопасность, АСУ ТП, проблематика, Wi-Fi атаки, мониторинг, противодействие киберугрозам

*Abstract:* Information security monitoring, events recording, and detecting known cyber threats are necessary for usage Wi-Fi compatible components in Industrial Control System (ICS). In certain circumstances, monitoring can only be provided by external tools. The article describes the

key issues of Wi-Fi wireless networks security monitoring in ICS. To effectively solve the task, the necessity of applying a scientific and engineering approach is declared.

*Keywords:* information security, ICS, issues, Wi-Fi attacks, monitoring, countering cyber threats

Технология Wi-Fi, наряду с существенными преимуществами ее использования, уязвима к ряду киберугроз. Сведения о соответствующих угрозах известны и включены в Банк данных угроз АСУ ТП ФСТЭК России [1]. Применение технологии Wi-Fi должно учитываться при моделировании угроз безопасности информации для АСУ ТП.

Анализ возможных сценариев применения технологии Wi-Fi операторами АСУ ТП промышленного типа позволил выделить ключевые сценарии применения данной технологии, включая обеспечение сетевой связности компонентов АСУ ТП на всех уровнях, а также применение Wi-Fi для подключения личных устройств работника (в последнем случае Wi-Fi оборудование не входит в состав АСУ ТП).

В связи с широкой доступностью компонентов АСУ ТП, поддерживающих передачу данных по технологии Wi-Fi, наличием технико-эксплуатационных преимуществ применения беспроводного канала связи и подверженностью Wi-Fi ряду угроз практический и научный интерес имеет рассмотрение основных проблем обеспечения информационной безопасности и мониторинга беспроводных сетей Wi-Fi в АСУ ТП.

В качестве наиболее актуальных для АСУ ТП промышленного типа выделены киберугрозы, в случае реализации которых нарушается сетевая связность компонентов АСУ ТП либо блокируется обмен данными по Wi-Fi. Данная группа угроз может быть реализована при некорректном размещении приемо-передающего оборудования Wi-Fi, реализации злоумышленником атаки деаутентификации и диссоциации, поставки помех в радиоэфир посредством отправки множества пакетов.

Соответствующие угрозы могут привести к невозможности осуществления технологических (производственных) процессов, возникновению аварий. Соответственно, ввиду п. 2 ч. 4 ст. 6 Федерального закона от 27.07.2006 № 149-ФЗ [2] и Приказа ФСТЭК России от 14.03.2014 № 31 [3] оператор АСУ ТП обязан внедрить необходимые меры защиты для предотвращения актуальных угроз,

своевременного выявления фактов их реализации и мониторинга событий информационной безопасности.

Отметим, что подключение компонентов промышленной АСУ ТП к Wi-Fi осуществляется единожды техническим персоналом при первичном конфигурировании и далее в рамках модификации АСУ ТП, таким образом угрозы, связанные с реализацией атаки поддельной точки доступа, теряют актуальность ввиду технического характера взаимодействия устройств по Wi-Fi и минимизации антропогенного фактора. Вместе с тем, функционирующие поблизости устройства Wi-Fi могут поставлять помехи в радиоэфир, а также использоваться для проведения иных атак. Их своевременное выявление является одной из задач мониторинга.

В свободной продаже представлены устройства, поддерживающие технологию Wi-Fi и используемые в промышленных АСУ ТП на различных уровнях архитектуры. Был проведен анализ, в область анализа была включена техническая информация [4-11] о следующих компонентах:

– программируемые логические контроллеры RievTech модели EXM-12DC-DA-RT-WIFI, PR-26DC-DAI-RT-WIFI, PR-26DC-DAI-RT-4GWIFI, а также Erqos EQSP32, KinCony KC868-COLB;

– устройство управления с человеко-машинным интерфейсом Coolmay QM3G-70KFH;

– управляемые реле ESP32-S3-Relay-6CH, АГАВА МПР-60;

– датчики Wilow AX-3D, UbiBot WS1, Comet модели W0711, W0741, W3710, W3721, W4710, W5714, W7710;

– преобразователи интерфейсов High-Flying модели HF2211S, HF2211, HF2221, HF9610, HF9610C, W10, W20.

Технически поддержка стандарта Wi-Fi компонентом АСУ ТП может быть реализована двумя укрупненными способами:

– посредством применения модулей программно-аппаратной поддержки Wi-Fi, которые интегрированы в датчики, программируемые логические контроллеры либо иные компоненты АСУ ТП;

– посредством применения специального промежуточного устройства, которое принимает данные от компонента АСУ ТП по иному каналу, формирует пакеты и передает их по Wi-Fi.

В представленных сценариях компонент АСУ ТП может выступать не только абонентом Wi-Fi сети, но и работать в режиме точки доступа Wi-Fi. Производителями устройств, включенных в область анализа, не декларирован функционал по обнаружению и предотвращению

вторжений, мониторингу безопасности при работе в режиме точки доступа Wi-Fi. Исходя из сложившейся практики, соответствующие опции доступы только в специализированных точках доступа Wi-Fi с лицензиями на соответствующие программные модули WIPS/WIDS.

В рассмотренном сценарии мониторинг безопасности беспроводных сетей Wi-Fi в АСУ ТП промышленного типа может быть организован внешними средствами. Пример технического решения, на основе которого возможно осуществлять мониторинг безопасности Wi-Fi сети пространственно распределенными внешними датчиками, представлен в [12]. Отметим, что такой подход имеет ряд преимуществ, обусловленных отсутствием необходимости внесения изменений в состав и архитектуру АСУ ТП.

Таким образом, АСУ ТП промышленного типа обладают рядом особенностей, основные среди которых:

– критичность последствий в случае инцидента информационной безопасности, влияющего на технологические (производственные) процессы;

– большая площадь промышленного объекта, многокомпонентность и многоуровневость архитектуры;

– модель нарушителя может включать широкий перечень лиц, включая диверсантов, иностранные спецслужбы, криминальные структуры.

Выделены следующие аспекты, которые должны быть учтены при мониторинге:

– расширение радиочастотного диапазона в последнем поколении стандартов IEEE 802.11 требует осуществления мониторинга в широком диапазоне радиочастот;

– средства мониторинга должны быть сконфигурированы и размещены таким образом, чтобы обеспечить прием пакетов с заданным значением доли пропуска;

– средства мониторинга должны иметь возможность оперативно раскрывать присутствующие в радиоэфире приемо-передающие устройства, включая точки доступа Wi-Fi и их абонентов;

– средства мониторинга должны обеспечивать возможность определения местоположения устройства, с использованием которого осуществляется атака на Wi-Fi сеть.

Для эффективного решения задачи мониторинга необходимо применение научного и инженерного подхода.

**Библиографический список**


1. Банк данных угроз безопасности информации в автоматизированных системах управления технологическими процессами // ФСТЭК России. – URL: https://bduasutp.fstec.ru/
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
4. Wireless IOT Vibration Sensor WiLow AX-3D // BeanAir. – URL: https://www.wireless-iot-sensors.beanair.com/files/Datasheet-wifi-accelerometer-beandevice-Wilow-AX-3D.pdf
5. Wi-Fi Serial Server // High-Flying. – URL: http://www.hi-flying.com/wi-fi-iot/wi-fi-serial-server
6. Remote PLC // RievTech. – URL: https://www.sensinext.com/wp-content/uploads/2020/01/NextControl-wireless-new.pdf
7. Wireless Industrial IoT (IIoT) ESP32 PLC Controller // Erqos Technologies. – URL: https://erqos.com/wp-content/uploads/resources/eqsp32/EQSP32-Datasheet-v0.2.pdf
8. Programmable Logic Controller(Ethernet+WiFi) – KC868-COLB // KinCony. – URL: https://www.kincony.com/programmable-logic-controller-colb.html
9. Coolmay QM3G-70KFH // Промышленные технологии. – URL: http://www.coolmay.com.ru/products/panelnye-kontrollery/7-dyuymov/qm3g-70kfh
10. All-in-one IoT sensor for Environmental Data. UbiBot. – URL: https://www.ubibot.com/ubibot-ws1/
11. User’s Guide. Sensor with WiFi communication // Comet – URL: https://www.cometsystem.com/userfiles/dokumenty_menu/87/ie-wfs-wx7xx-11.pdf
12. Буренок Д. С. Способ обнаружения несанкционированных и поддельных точек доступа Wi-Fi // Роспатент. Патент на изобретение № 2810111 от 21.12.2023.