ОБЗОР СОВРЕМЕННЫХ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ СОЗДАНИИ ИНФРАСТРУКТУРЫ ИНТЕРНЕТА ВЕЩЕЙ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Абалуев Р. Н.,
доцент кафедры математики, физики
и информационных технологий
ФГБОУ ВО Мичуринский ГАУ,
г. Мичуринск, РФ
abaluevrn@mgau.ru
Крумкаченко А. А.,
студент 3 курса Инженерного института
ФГБОУ ВО Мичуринский ГАУ,
г. Мичуринск, РФ.
krumkachenko@mail.ru

Аннотация. В статье проводится обзор современных подходов к обеспечению информационной безопасности при создании инфраструктуры интернета вещей в агропромышленном комплексе. Выполнен анализ лучших практик, изложенных в документе Европейского агентства по сетевой и информационной безопасности.

Ключевые слова: цифровизация, промышленный интернет вещей, информационная безопасность.

Развитие агропромышленного комплекса невозможно без поиска оптимальных путей инновационного развития аграрных предприятий посредством цифровизации данной отрасли. На сегодняшний день в нашей стране реализуется программа «Цифровая экономика Российской Федерации», которая была утверждена распоряжением Правительства РФ от

28 июля 2017 года № 1632-р [1]. В данном документе приводится перечень основополагающих для развития экономики России цифровых технологий, в частности технологии промышленного «интернета вещей».

Сегодня под промышленным «интернетом вещей» (Industrial Internet of things. IIoT) подразумевают концепцию построения промышленных вычислительных сетей из физических объектов (иначе – «вещей»), обладающих возможностями взаимодействия с окружающей средой или друг с другом. Отличием этих технологий от используемых в бытовом «интернете вещей» является более высокие требования к обеспечению безопасности информации и отказоустойчивости оборудования.

Европейское агентство по сетевой и информационной безопасности (ENISA) выпустила документ, содержащий информацию о лучших практиках по обеспечению информационной безопасности «интернета вещей» в контексте их промышленного использования [2]. Рассмотрим основные подходы к обеспечению информационной безопасности изложенные в данном документе, применительно к промышленному «интернету вещей» аграрной индустрии.

Первоначально приводятся результаты экспертной оценки критичности активов с точки зрения их влияния на информационную безопасность. К минимальному риску отнесены следующие компоненты инфраструктуры: серверы приложений, серверы баз данных, системы ERP и CRM, программное обеспечение (операционные системы, антивирусное программное обеспечение). Это объясняется, на наш взгляд тем, что данные активы традиционно используются в инфокоммуникационных системах и имеется достаточно большой опыт обеспечения их информационной безопасности.

Следует обратить внимание на группу, отнесенную к максимальному риску – промышленные контроллеры, АСУТП, промышленные компьютеры, устройства связи с объектами, шлюзы IIoT и датчики. То есть, те объекты

автоматизации, которые традиционно эксплуатируются в защищённой сети промышленного предприятия.

Приведена подробная классификация с описанием возможных угроз, применительно к области промышленного «интернета вещей». Выделены основные классы угроз:

Недобросовестная деятельность и злоупотребления – противозаконные манипуляции с данными и устройствами;

Прослушивание / перехват / хакинг – сбор информации и взлом системы;

Непреднамеренные (случайные) повреждения – ошибки в конфигурировании, администрировании и применении;

Отключения – перебои в работе, связанные с потерей электропитания, коммуникаций или сервисов;

Катастрофы – разрушительные внешние воздействия природного и техногенного характера;

Физические атаки – воровство, вандализм и саботаж, производимый непосредственно на оборудовании;

Отказы и нарушения в работе – отказы аппаратного обеспечения, сервисов доступа в интернет, уязвимости программного обеспечения;

Правовые вопросы – несоответствие законодательству.

В разделе 4 данного документа рассматриваются лучшие практики, направленные на защиту компонентов IIoT. В практики включены три категории: политики, организационные практики и технические практики. Полный перечень практик изложен в виде таблицы в Приложении В документа.

В заключении можно сделать вывод, что на сегодняшний день достаточно мало исследований посвящено информационной безопасности промышленного «интернета вещей». Документ ENISA разработанный в ноябре 2018, является на сегодняшний момент одним из самых подробных руководств в области информационной безопасности «интернета вещей»,

содержащий свод накопленных знаний, полученный на основе анализа сотни документов от ведущих экспертных организаций в области IIoT, которые необходимо использовать при разработке инфраструктуры «интернета вещей» в агропромышленном комплексе.

Список использованных источников

1. Программа «Цифровая экономика Российской Федерации»: утверждена распоряжением Правительства РФ от 28 июля 2017 года № 1632-р [Электронный ресурс]. – URL: http://government.ru/docs / 28653 (дата обращения 1.03.2019).

2. Good Practices for Security of Internet of Things in the context of Smart Manufacturing [Электронный ресурс]. – URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot? fbclid = IwAR1q-chv88kZRsIESHtGTEwbA0Mbx8mb9hV1Euqy-Y–IHVYvLuFhGuvi6o (дата обращения 1.03.2019).

REVIEW OF MODERN APPROACHES TO ENSURING INFORMATION SECURITY IN CREATING THE INFRASTRUCTURE OF THE INTERNET THROUGH AGRO INDUSTRIAL COMPLEX

Abaluev R. N.,
Associate Professor of the
Department mathematics, physics and information technology,
Michurinsk State Agrarian University,
Michurinsk, Russia.
abaluevrn@mgau.ru
Krumkachenko A. A.,
3rd year student
Engineering Institute
Michurinsk State Agrarian University,
Michurinsk, Russia.
krumkachenko@mail.ru

Annotation. The article reviews modern approaches to ensuring information security while building the infrastructure of the Internet of things in the agro-industrial complex based on the analysis of best practices outlined in the document of the European Network and Information Security Agency.

Keywords: Digitalization, Industrial Internet of Things, Information Security.