2020. - Т. 17, № 1. - С. 109–118 // https://doi.org/10.37661/1816-0301-2020-17-1-109-118.

2 G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, The Keccak reference, Version 3.0. - 2011 // http://keccak.noekeon.org/, Keccak-reference-3.0.pdf: 11.10.2021.

3 Мулярчик К. С. // Лавинный эффект в алгоритмах шифрования на основе дискретных хаотических отображений // Доклады БГУИР. - 2013. - № 6 (76). - С. 86-91.

4 Vergili I., Yücel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Cho-sen× S-Boxes // Turk J Elec Engin. - 2001. - Т. 9, №. 2. - С. 137-145.

УДК 004.056.53

Ю.Д. Сандихаев, Д.Е. Сидорчик
Белорусский государственный технологический университет,
Минск, Беларусь

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В АСУТП

Аннотация. *В работе рассматриваются проблемы широкого внедрения автоматизированных систем во все сферы жизни общества, что требует повышенного внимания к защите применяемых для автоматизации управления информационных технологий и непосредственно информации.*

Yu.D. Sandihaev, D.E. Sidorchyk
Belarusian State Technological University,
Minsk, Belarus

INFORMATION SECURITY IN THE AUTOMATED CONTROL SYSTEM OF TECHNOLOGICAL PROCESSES

Abstract. *The paper deals with the problems of widespread introduction of automated systems in all spheres of society, which requires increased attention to the protection of information technologies and information directly used for automation of management.*

Широкое внедрение автоматизированных систем во все сферы жизни общества требует повышенного внимания к защите применяемых для автоматизации управления информационных технологий и непосредственно информации. Любые нарушения и неполадки в работе

автоматизированных/информационных систем (ИС), систем обработки и передачи информации приводят к снижению качества или полной потере управления критичными процессами и, соответственно, к убыткам. Следует отметить, что любая информационная система всегда является частью соответствующей системы управления, а любая автоматизированная информационная система (АИС) - частью автоматизированной системы управления (АСУ). [1]

Основным отличием АСУ от информационных систем является: Работа АСУ осуществляется только в реальном времени, АСУ нельзя перезагрузить для решения проблемы, труднодоступность некоторых систем управления, малое количество свободной памяти, что приводит к невозможности реализации функции безопасности.[2]

Информационная безопасность для АСУ всегда должна опираться на государственные протоколы безопасности. Одним из самых востребованных протоколов является российский ГОСТ Р ИСО/МЭК 27000; или же ISO/IEC 27000 Information Technology, так же применяется стандарт международной энергетической комиссии ISA/IEC 62443 Security for Industrial Automation and Control Systems. Политика информационной безопасности оформляется в виде документированных требований на АСУ. Документы обычно разделяют по уровням детализации процесса защиты. Такие документы обычно выпускаются в двух редакциях – для внешнего и внутреннего рассмотрения. Согласно ГОСТ Р ИСО/МЭК 17799--2005, на верхнем уровне политики информационной безопасности должны быть оформлены следующие документы: «Концепция обеспечения ИБ», «Правила допустимого использования ресурсов информационной системы» [3]

Одним из самых уязвляемых мест в АСУ на данный момент является внедрение в системы MASH сетей для снятия показания с датчиков, на производствах, не имеющих противоаварийной (ПАЗ или ESD) блокировочной системы.

Для создания глушителя WI-FI сигнала потенциальному злоумышленнику необязательно необходимо высококвалифицированное оборудование. Для глушения сигнала роутера с низким RSSI (англ. received signal strength indicator — полная мощность принимаемого приёмником сигнала) может подойти даже самые дешёвые платы. использование глушителя может привести к отключению датчиков, работающих с использованием MASH сетей или беспроводных камер, подключенных к одной беспроводной сети. Так же, глушители сигнала

можно использовать для предотвращения несанкционированного наблюдения.

Ещё одним значимым аспектом в информационной безопасности АСУ ТП является безопасность программируемых логических контроллеров. Программируемый логический контроллер (ПЛК) (или PLC – Programmable Logic Controller) – устройство, используемое для автоматизации технологических процессов. В отличии от встраиваемых систем и микроконтроллеров, ПЛК изготавливается как самостоятельное изделие, отдельно от управляемого при его помощи оборудования.[4]

Рассмотрим самые популярные угрозы:

1. Исполнительные устройства и подсистема телеметрирования

Например, современные промышленные контроллеры могут быть соединены напрямую или через модем. При подключении через модем их часто объединяют с GPRS/GSM-модемами, что по умолчанию наделяет устройство IP-адресом мобильного оператора. При такой конфигурации они очень уязвимы для атак извне. Специализированными утилитами и методами злоумышленник может выявить подобные устройства. Сами исполнительные устройства, как правило, подключаются по последовательному интерфейсу (RS-232 / RS-485) к MODBUS-серверу, а непосредственно MODBUS-сервер имеет управление по TCP/IP через канал Ethernet / Industrial Ethernet с операторами.

2. Парк операторов. Операторы имеют возможность подключаться к системе SCADA, как правило, с разным уровнем привилегий, планировать и внедрять новые проекты, изменять существующие. Несмотря на множество уязвимостей в ПО систем диспетчеризации, основной угрозой по-прежнему остается инсайд.

3. Корпоративная зона

Отдельной угрозой, частично использующей штатные методы для исполнения, является распространение злонамеренного кода для кражи критически важных данных о проектах технологических процессов и нарушения их корректной работы, подтверждение чему является факт распространения вредоносного кода «Rootkit.TmpHider» и «Scope.Rookit.TmpHider.2». Многие популярные системы диспетчеризации (SCADA) базируются на платформе ОС Microsoft Windows, поэтому данный факт указывает на необходимость обеспечения информационной безопасности операционной системы, на которую устанавливается прикладное программное обеспечение.[5]

Исходя из вышеизложенного представляется сделать следующие вывод: Безопасность АСУТП является одной из самых существенных задач нынешней сферы информационной безопасности для предотвращения катастрофических последствий различных кибератак.

Список использованных источников

1. Бондарев, В. В. Б81 Введение в информационную безопасность автоматизированных систем: учебное пособие / В. В. Бондарев. - Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. - 250, [2] с.: ил.
2. Владимир Скляр: Обеспечение безопасности АСУТП в соответствии с современными стандартами. Методическое пособие
3. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Информационная технология. Методы и средства обеспечения безопасности СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Общий обзор и терминология
4. Статья «Система ПАЗ от риска к безопасности» П. Н. КИРЮШИН – эксперт по системам противоаварийной автоматической защиты (ПАЗ)
5. https://www.securitylab.ru/analytics/425304.php

УДК 334.75

Н.А. Сергеев
Казанский национальный исследовательский технический университет
им. А.Н. Туполева – КАИ
Казань, Российская Федерация

ВЛИЯНИЕ ПАНДЕМИИ НА МИРОВУЮ ЭКОНОМИКУ

Аннотация. *Рассмотрена необходимость анализа проблем, связанных с достижением непрерывного и устойчивого экономического роста или экономического развития общества современной России. В настоящее время проблемы экономического роста занимают главное место в экономических дискуссиях и обсуждениях, ведущихся между представителями разных наций, народов и их правительств. Повышающийся объём производства позволяет в какой-то степени решить проблему, с которой сталкивается любая хозяйственная система, а именно.*

N.A. Sergeev
Kazan National Research Technical University