

УДК 004.056

О ПОДХОДАХ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВЫХ ДВОЙНИКОВ

Лазорин Д.С. (РГУ нефти и газа (НИУ) имени И.М. Губкина)

Научный руководитель – к.т.н., заведующий кафедрой комплексной безопасности критически важных объектов **Правиков Д.И.**
(РГУ нефти и газа (НИУ) имени И.М. Губкина)

Введение. Процессы цифровизации всё больше оказывают влияние на развитие современных технологий. Происходит автоматизация: старое оборудование заменяется на более усовершенствованное. Это благотворно сказывается на экономической составляющей компаниях. Цифровой двойник является неотъемлемой частью каждого будущего производства. Его ключевая особенность заключается в непрерывном получении, обновлении и обработке данных, получаемых с реального объекта. Такой подход позволяет вносить различные корректировки, тем самым обеспечивая бесперебойную и безопасную работу целого технологического процесса. Получение информации происходит благодаря датчикам и сенсорам, которые устанавливаются на реальный объект. Передача информации выполняется по защищённому от взлома каналу связи в систему цифрового двойника, который в дальнейшем использует полученные данные в работе. Для обеспечения информационной безопасности требуются новые подходы и методы, которые необходимо совершенствовать не только с технологической стороны, но и с нормативной. Сегодня на производстве интегрированы автоматизированные системы управления технологическим процессом (АСУ ТП) [1]. Это комплексные системы, которые осуществляют автоматический сбор и обработку данных, тем самым оптимизируя управление технологическим объектом. Цифровой двойник является частью автоматизированной системы управления. Заводя разговор про нефтегазовую отрасль, большинство месторождений, действующих или находящихся на завершающем этапе эксплуатации, не оснащены даже АСУ ТП. Это тем или иным образом замедляет процессы добычи. Однако всё меняется: подход к добыче на новых месторождениях. Происходит внедрение не только АСУ ТП, но и цифровых двойников. Происходит обмен данными, следовательно, чрезвычайно важно обеспечить информационную безопасность технологической системы на производстве. Нельзя отрицать, что цифровые двойники становятся всё более популярной технологией нового поколения на пути к информационной трансформации. Это происходит в результате сочетания физического оборудования и цифровой платформы, которая обеспечивает сбор данных датчиков и обработку в режиме реального времени, тем самым повышая эффективность и стратегическую важность компаний. Рассматривая топливно-энергетический комплекс России, цифровой двойник помогает выбирать наиболее продуктивные сценарии работы и проводить эксперименты в цифровой (виртуальной) среде, которые в реальной жизни могут быть связаны с тем или иным риском, например, повреждение оборудования, угроза жизни сотрудникам. Своевременное развитие данных технологий сможет привести к оптимизации процессов в существующих промышленных системах и инфраструктуре. Подобная тенденция приобретает интерес и спрос у существующих компаний. Привлечение новых инвестиций в технологию цифровых двойников поможет корпорациям быть более конкурентоспособными и завершить комплексным образом процессы цифровизации [2].

Основная часть. В ранее проведённой научной работе нами были рассмотрены и проанализированы существующие подходы к обеспечению информационной безопасности цифровых двойников [3]. Выяснено, что использование современных технологий защиты информации в рамках актуальных для цифровых двойников моделей угроз и нарушителя нацелено на решение частных задач. Были проанализированы отечественные решения. Компания Infotecs — лидирующая Российская компания, реализующая решения в сфере информационной безопасности. Она предлагает решения VipNet Industrial Security: линейка

продуктов, которая конструирует систему защиты АСУ ТП и систем межмашинного взаимодействия [4]. Особенность заключается в том, что существуют решения как для промышленных протоколов, которые обеспечивают защиту каналов связи и сетевое экранирование, так и для Windows и Linux с специализированным программным обеспечением.

Выводы. Таким образом, цифровые двойники — это новое решение для технологических систем. Необходимо обеспечить комплексный подход к обеспечению информационной безопасности цифровых двойников. Стоит обратить особое внимание на концепцию многоуровневой платформы, так как она включает в себя реализацию комплексного подхода, состоящего из низкоуровневых способов защиты канала связи при помощи криптографических алгоритмов до высокоуровневых задач.

Был реализован веб-сайт (<https://securedt.ru>) с полноценной и актуализирующийся информацией о научной работе, а также контактами для дальнейшего взаимодействия.

Список использованных источников:

1. Линьков В. А. Централизованные АСУ ТП. Состав и структура АСУ ТП / В. А. Линьков // Международный студенческий научный вестник. – 2019. – № 6. – С. 12. – EDN ВНQBVO.
2. Levaniuk D. Application of digital twins for maintenance in the gas and oil sector. Lappeenranta–Lahti University of Technology LUT, 2022, pp. 7-37.
3. Лазорин Д.С., Правиков Д.И., Щербаков А.Ю. О подходах к обеспечению информационной безопасности цифровых двойников // Вестник современных цифровых технологий. 2022. № 11. С. 48-55.
4. Продуктовые линейки ViPNet [Электронный ресурс] // Infotecs. URL: <https://infotecs.ru/product/> (дата обращения: 01.03.2023)