ЦИФРОВОЙ ДВОЙНИК СЕТИ SCADA-СИСТЕМЫ: МОДЕЛЬ УГРОЗ И РИСК-ОРИЕНТИРОВАННАЯ КИБЕРЗАЩИТА НА ОБЪЕКТАХ НЕФТЕГАЗОВОЙ ОТРАСЛИ

С.А. Глобенко, *магистрант*
В.В. Кириллин, *магистрант*
Научный руководитель: *Р.Ф. Добрянский, старший преподаватель*
Дальневосточный федеральный университет
(Россия, г. Владивосток)

DOI:10.24412/2500-1000-2026-2-1-210-217

Аннотация. *В статье рассматривается применение цифрового двойника сети SCADA-системы на объектах нефтегазовой отрасли для построения модели угроз и выбора риск-ориентированных мер киберзащиты. Цифровой двойник понимается как виртуальное представление топологии промышленной сети, активов (серверов, контроллеров, рабочих станций), технологических связей и потоков данных, обновляемое на основе конфигураций, журналов и телеметрии. Предлагается методика, включающая инвентаризацию активов, выделение зон и каналов, описание угроз и уязвимостей, дается оценка риска по вероятности и последствиям для производства, экологии и безопасности. В среде двойника выполняется безопасная имитация нарушений связи, подмены данных и несанкционированных действий оператора для проверки устойчивости и обнаруживаемости. На основе результатов обосновывается приоритизация контрмер: сегментация, контроль удалённого доступа, принцип наименьших привилегий, мониторинг аномалий и управление обновлениями. Показано, что подход сокращает неопределённость оценки рисков и повышает готовность к реагированию.*

Ключевые слова: *цифровой двойник; SCADA; промышленная сеть; модель угроз; киберриски; риск-ориентированная киберзащита; ISA/IEC 62443; мониторинг аномалий; нефтегазовая отрасль.*

На объектах нефтегазовой отрасли сети SCADA-систем (в составе АСУ ТП/OT-контуров) выполняют роль критической инфраструктуры: через них обеспечиваются сбор телеметрии, диспетчеризация, управление технологическими параметрами и поддержание непрерывности процессов. В отличие от классических IT-систем, OT-среда предъявляет повышенные требования к доступности, предсказуемости и безопасности управления физическим процессом, а последствия инцидентов могут выражаться не только в простоях, но и в рисках для промышленной и экологической безопасности. Эти особенности прямо отражены в подходах к защите OT, где подчеркивается необходимость учитывать технологическую специфику, ограничения по времени реакции и жизненный цикл оборудования [1].

В последние годы рост цифровизации и интеграции производственных контуров (удалённый мониторинг, централизованная аналитика, обмен данными между площадками) усиливает взаимозависимость IT и OT и, как следствие, расширяет поверхность атаки. В подобных условиях управление киберрисками для SCADA-сетей становится задачей не «точечной настройки средств защиты», а системной инженерной работы: нужно понимать, какие активы наиболее критичны, какие сценарии киберинцидентов наиболее вероятны, как они могут повлиять на технологию, и какие меры дадут наибольший эффект при ограниченных ресурсах.

Формирование такой логики опирается на риск-ориентированные отраслевые практики и стандарты. Серия ISA/IEC 62443 задаёт целостный подход к кибербезопасности промышленных систем управления: распределение ответственности по ролям, требования к компонентам и, что особенно важно для проектирования защитных архитектур, концепции сегментации «зоны и каналы (zones & conduits)». Это позволяет описывать промышленную сеть как совокупность доверенных областей и контролируемых связей между

ними, что является фундаментом для обоснования мер защиты и контроля доступа [2].

Вместе с тем на практике организациям часто не хватает «прикладного» инструмента, который соединял бы модель угроз с проверяемыми решениями: описать угрозы и меры недостаточно – важно оценить, как конкретные сценарии скажутся на технологическом процессе и насколько выбранные контрмеры действительно снижают риск. В качестве основы для типизации действий злоумышленников и сопоставления их с защитными контролями может использоваться база MITRE ATT&CK for ICS, содержащая тактики и техники, наблюдаемые в реальных атаках на промышленные системы.

Перспективным способом «сшить» угрозы, риск-оценку и проверку мер киберзащиты является применение цифрового двойника. В общем виде цифровой двойник определяется как динамическая виртуальная репрезентация реального объекта/процесса/системы, которая поддерживает обмен данными с физическим прототипом и позволяет проводить мониторинг, анализ и прогнозирование поведения. При переносе этой идеи в контекст кибербезопасности ключевой ценностью становится возможность безопасного моделирования: в виртуальной среде можно воспроизводить сетевую топологию SCADA, логику взаимодействия сегментов, критические сервисы и «нормальное» поведение потоков данных, а затем проверять, как меняются параметры и наблюдаемость системы при различных отклонениях и инцидентах.

Дополнительный аргумент в пользу такого подхода связан с тем, что сами цифровые двойники рассматриваются как значимая технология, требующая внимания к вопросам доверия и безопасности. В NIST IR 8356 отдельно обсуждаются аспекты «безопасность и доверие для цифрового двойника» и приводятся примеры применимости цифровых двойников к промышленным процессам и производственным системам, что делает релевантной постановку задачи «цифровой двойник + безопасность» именно для индустриальных сред [3].

Таким образом, цифровой двойник может выступать не только «моделью для оптимизации», но и инструментом для управляемого анализа киберустойчивости.

В отечественной научной повестке цифровые двойники также рассматриваются в привязке к системам управления и критическим информационным инфраструктурам: анализируются области применения, подходы к классификации и предлагаются концептуальные модели взаимодействия цифрового двойника с физической сущностью [4]. Это создает основу для дальнейшего прикладного шага – построения цифрового двойника именно сети SCADA как объекта защиты, где «физическая сущность» описывается не только технологическим оборудованием, но и сетевыми сегментами, узлами, каналами связи, сервисами и регламентами управления доступом.

Исходя из изложенного, актуальной задачей является разработка подхода к формированию модели угроз и выбору риск-ориентированных мер киберзащиты, в котором цифровой двойник сети SCADA используется как средство:

- структурирования активов и связей;
- описания и ранжирования сценариев киберинцидентов по вероятности и последствиям;
- безопасной проверки эффективности выбранных контрмер до внедрения в активном контуре.

При этом риск-ориентированность трактуется как приоритезация защитных мер на основе критичности технологических функций и ожидаемого снижения риска, а не на основе формального «максимума контроля» для всех компонентов сразу.

Сеть SCADA-системы на нефтегазовом объекте – это не просто «передача телеметрии», а инфраструктура, через которую реализуются диспетчеризация, выдача управляющих воздействий и контроль технологических ограничений. В OT-контуре приоритеты безопасности отличаются от классического IT: критичны доступность, предсказуемость и безопасность процесса, а киберинцидент может привести к простоям, отказам оборудования и вторичным последствиям (в т.ч. промышленным и экологическим). В руководстве NIST по безопасности OT прямо подчеркивается необходимость учитывать эти уникальные требования и особенности угроз/уязвимостей именно для OT-среды.

На практике защита SCADA-сетей часто строится как набор разрозненных мер: сег-

ментация неопределенности, периметровые правила, контроль удалённого доступа, сигнатурный мониторинг и регламенты администрирования.

Проблема в том, что такой подход плохо отвечает на два ключевых вопроса:

а) какие сценарии атак и нарушений действительно наиболее рискованные именно для данного объекта;

б) как доказательно проверить, что выбранные меры реально снижают риск, не нарушая технологию.

Для ОТ характерна ограниченная «экспериментальность»: тестировать агрессивные сценарии, изменения политик доступа или новые механизмы мониторинга на живом контуре опасно и организационно сложно.

Здесь появляется идея цифрового двойника сети SCADA: виртуальная модель топологии, активов, каналов связи и технологических потоков данных, которая позволяет безопасно проигрывать сценарии киберинцидентов, наблюдать эффекты и обосновывать контрмеры. При этом сам цифровой двойник и каналы его синхронизации – тоже объект доверия и защиты: NIST отдельно рассматривает параметр «защита и доверие» для цифровых двойников и отмечает, что вся система цифрового двойника (инструментация, каналы управления/данных, вычислительная часть) должна проектироваться с учетом киберрисков.

Для задач киберзащиты цифровой двойник сети SCADA целесообразно описывать не как «3D-модель объекта», а как киберфизическую модель из нескольких слоев (рис. 1):

- слой активов: SCADA-серверы, HMI/АРМы, инженерные станции, контроллеры (PLC/RTU), сетевое оборудование, средства удалённого доступа, сервисы синхронизации времени, журналы/серверы логирования;
- слой связности: L2/L3-топология, VLAN/VRF, маршрутизация, межсетевые экраны, «узкие места» и критические линковки;
- слой протоколов и потоков: какие направления обмена допустимы, какие типы команд/телеметрии ходят между зонами;
- слой технологических зависимостей: какие узлы критичны для каких функций процесса (например, контур поддержания давления/расхода/уровня, защитные блокировки и т.п.), какие отказоустойчивые режимы предусмотрены.

Именно такая структура позволяет объединить киберсобытия (изменение маршрута, подмена регистрационных данных, потеря связи, ошибочная команда) с технологическими последствиями и перейти к риск-ориентированному выбору защитных мер [5].

Рис. 1. Архитектура цифрового двойника сети SCADA для киберрисков

Чтобы модель угроз была не «перечнем страшилок», а инструментом для проектирования защиты, удобна структуризация через тактики/техники. В промышленном контексте для этого часто используют базу MITRE ATT&CK for ICS, где описаны типовые тактики и техники злоумышленников именно для ICS/SCADA.

Ниже показано, что разные тактики представлены неодинаково – это полезно при формировании «карты угроз» и выделении приоритетов мониторинга и контрмер.

Таблица 1. Тактики MITRE ATT&CK for ICS и число техник (по матрице ICS) [6]

№ п/п	Тактика (ICS)	Число техник
1	Initial Access (первичный доступ)	12
2	Execution (исполнение)	10
3	Persistence (закрепление)	6
4	Privilege Escalation (повышение привилегий	2
5	Evasion (уклонение)	7
6	Discovery (разведка)	5
7	Lateral Movement (латеральное перемещение)	7
8	Collection (сбор)	11
9	Command and Control (управление)	3
10	Inhibit Response Function (подавление функции реагирования)	14
11	Impair Process Control (нарушение управления процессом)	5
12	Impact (воздействие/ущерб)	12

Практический смысл для нефтегаза: даже если «точка входа» лежит в IT-периметре, итоговые цели часто проявляются в OT-тактиках уровня Inhibit Response Function / Impact – например, деградация видимости, подавление сигнализации/реагирования, нарушения в управлении процессом. Поэтому цифровой двойник сети полезен тем, что позволяет моделировать не только «кибершаги», но и системные эффекты: потерю наблюдаемости, задержки/разрывы связи, неверную спектр событий и управленческие решения, принятые на её основе.

Риск-оценка для SCADA-сети должна учитывать не только вероятность реализации угрозы, но и последствия для технологического процесса. В OT-руководствах NIST акцентируется, что для таких систем важно учитывать требования безопасности/надёжности и потенциальные физические последствия инцидентов [7].

На уровне практики удобно разделять последствия на несколько «линеек» (их потом можно свести к единой шкале риска):

- производственные (простои, деградация режима, потери сырья/продукта);
- промышленная безопасность (рост вероятности аварийных режимов, отказ защитных функций);
- экологические и ресурсосберегающие (утечки, выбросы, нарушения режимов утилизации/очистки);
- информационные (компрометация конфигураций, учетных данных, журналов, доверия к данным).

Цифровой двойник позволяет сделать эти последствия «проверяемыми»: сценарий в модели можно связать с тем, что именно изменится в наблюдаемости, как быстро оператор/автоматика это увидит, и какие барьеры/контрмеры реально «сработают».

Фундамент для риск-ориентированной защиты – корректная сегментация промышленной сети на зоны и каналы связи (conduits), чтобы политика доступа и мониторинга строилась не «по устройствам», а по логике доверия и критичности. Подход «зоны покрытия и трубопроводы» является ключевым понятием в практике ISA/IEC 62443 и в прикладных разъяснениях к стандарту: зоны группируют компоненты с общими требованиями безопасности, а каналы описывают контролируемые связи между зонами (рис. 2).

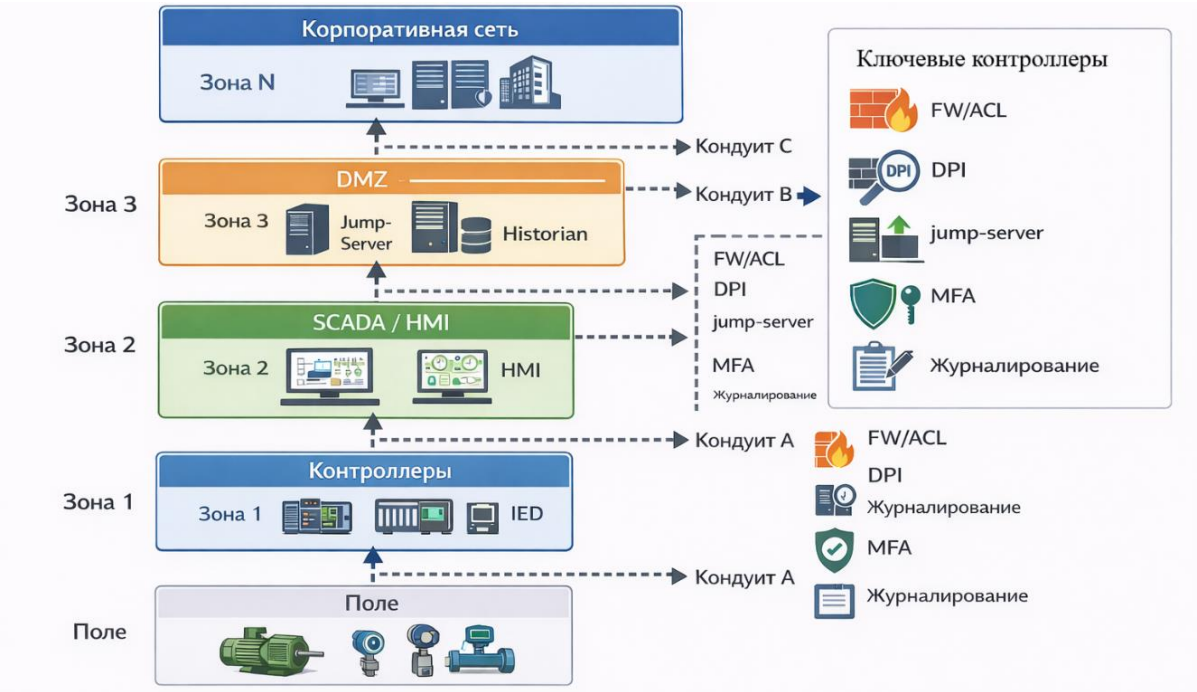

Рис. 2. Пример сегментации SCADA-сети по зонам и каналам

Чтобы риск-ориентированная защита была доказательной, в цифровом двойнике имеет смысл проверять как минимум два класса вещей:

1) устойчивость архитектуры: что происходит при нарушении связи/задержках, деградации сегментов, отказе отдельных сервисов (включая средства защиты);

2) обнаруживаемость и скорость реакции: как быстро и с какой точностью мониторинг выявляет опасные отклонения (аномалии), каков уровень ложных срабатываний, какова задержка детектирования.

Показательно, что в исследованиях по SCADA-безопасности цифровой двойник применяют именно как основу для гибридного обнаружения аномалий и проверки реакций.

К примеру, в работе A. Sayghe (Sensors, 2025) приводятся количественные метрики для цифрового двойника, который синхронизируется в реальном времени и используется для тестирования сценариев нарушений [8].

Таблица 2. Паспорт пилотного цифрового двойника сети SCADA для риск-оценки и верификации киберзащиты (пример для типового нефтегазового объекта)

Показатель (фиксация)	Пример значения для «пилота»	Комментарий
Граница моделирования	OT-контур + OT-DMZ + удаленный доступ (без корпоративной сети)	Риск считается по реально управляемой области, в ином случае размывается ответственность
Кол-во SCADA-серверов	2 (основной/резерв)	Проверка отказоустойчивости и сценариев деградации
Кол-во HMI/АРМ операторов	10-14	Нагрузка на сеть/сервисы, риск компрометации операторских станций
Инженерные станции	2	Критичный актив: изменения конфигураций/логики, управление жизненным циклом
PLC/RTU/контроллеры	60-90	Масштаб поверхности атаки в «полевом» уровне и зависимость функций процесса
Сетевые коммутаторы OT	12-20	Риск отказов/ошибок конфигурации, критичность L2-топологии
Межсетевые экраны/шлюзы	3-5	Ключевые точки контроля каналов, включая проверку правил, отказоустойчивости
Кол-во сетевых зон	6	Основа ISA/IEC 62443-логики «зоны/каналы»: на этом строятся политики доступа
Кол-во каналов	8-12	Места, где реально можно измерить эффект контрмер (ACL, DPI, jump-server, MFA)

Показатель (фиксация)	Пример значения для «пилота»	Комментарий
VLAN/сегменты	10-16	Связь сегментации с реальной L2/L3-реализацией, риск «перекинутых мостов»
Основные пром. протоколы	OPC UA, Modbus/TCP	В двойнике можно проверять аномалии по «нормальным» профилям протоколов
Кол-во критичных сервисов	7-10 (SCADA, истории, время снихронизации, авторизации, выход и т.д.)	Определяет сценарии “потеря сервиса - потеря видимости/управления”
Источник валидации по активам	CMDB/инвентаризация	Без точной инвентаризации модель угроз становится декларативной
Кол-во «тегов»	12000	Масштаб данных и нагрузка, в том числе пригодно для расчёта объёмов телеметрии
Средняя частота обновления «тегов»	1 с (критические: 250 мс)	Проверка «подмены/искажения данных» и время обнаружения аномалий
Оценка телеметрии	8-15 ГБ/сутки	Планирование хранения/аналитики
Поток технологических сообщений	300-900 пакетов/с	Проверка влияния контрмер (DPI/логирование) на задержки и доступность
Средняя задержка «обновления двойника»	200-400 мс (отклик)	Чем выше задержка, тем хуже применимость
Джиттер задержки синхронизации	50-120 мс	Важно для устойчивости детекторов аномалий
Объем событий журналирования OT/сутки	120 000-300 000 событий	Достаточность доказательной базы
NetFlow/телеметрия сети	1-3 ГБ/сутки	Для сценариев «латеральное перемещение/аномальный трафик»
Удержание логов	30 суток (горячее), 180 суток (архив)	Практика расследований + сравнение “до/после” по метрикам и инцидентам
Частота резервного копирования	1 раз/сутки + инкремент каждые 4ч	Верификация сценария восстановления после инцидента/саботажа
Целевое RTO ключевых функций	15 мин (видимость), 30 мин (управление)	Конкретизирует «ущерб от недоступности» в риск-модели OT
Доля «удаленных» подключений	5-15% сессий/сутки	Риск-фактор удалённого доступа; проверка MFA, jump-server, журналирования
Вычислительные ресурсы стенда	24 vCPU, 96 ГБ RAM, 2 ТБ SSD	Реалистичность моделирования и нагрузочного теста (без «игрушечной» модели)
Режим тестирования контрмер	3 сценария/сутки, окно 15-30 мин.	Безопасная проверка на повторяемость и сопоставимость количественных данных
Критерий «контрмера» сработала	Задержки < 5%, FPR < 3%, детект < 1 с	Пороговые требования

Эти цифры важны методически: они показывают, что цифровой двойник может быть достаточно «живым», чтобы работать в почти в режим реальном времени и использоваться как полигон для проверки мер мониторинга и реакции, не влезая в реальный технологический контур.

Для SCADA-сетей критичны не только «найти атаку», но и сделать это быстро и с приемлемым числом ложных тревог (иначе оператор перестает доверять сигнализации). В исследовании, использующем цифровой двойник для обнаружения киберфизических аномалий, приведено сравнение гибридного подхода с сигнатурным IDS (Snort) и «physics-only» детектором.

Таблица 3. Пример сравнения методов детектирования в SCADA-контуре (метрики из эксперимента)

№ п/п	F1-score, %	FPR, %	Задержка детектирования, мс
DT-ID (цифровой двойник и гибридная аналитика)	96,3	2,4	480
Сигнатурный IDS (Snort)	80,5	4,7	1650
Только физический детектор	89,2	7,8	510

Для риск-ориентированной киберзащиты это напрямую полезно: метрики позволяют оцифровать вклад мониторинга в снижение риска.

Если собрать описанное в единую процедуру, цифровой двойник сети SCADA становится инструментом, который обеспечивает замкнутый цикл:

- формирование актуальной модели активов/связей;
- построение модели угроз (структурированной по тактикам/техникам);
- оценка рисков с учетом технологических последствий;
- подбор и приоритизация контрмер (архитектура/доступ/мониторинг/процессы);
- верификация в двойнике: «видим ли мы сценарий», «как быстро реагируем», «что ломается/не ломается», «какая цена ложных тревог».

Применение цифрового двойника сети SCADA-системы позволяет перевести киберзащиту объектов нефтегазовой отрасли из «наборов разрозненных мер» в управляемый риск-ориентированный процесс. В отличие от традиционного подхода, где упор делается на периметр и формальные проверки, цифровой двойник дает единое представление об активах, топологии, зонах и каналах связи, а также о технологических зависимостях, что делает модель угроз прикладной – привязанной к реальным маршрутам данных, точкам администрирования и критичным функциям управления.

Ключевая ценность подхода состоит в возможности безопасной верификации: в виртуальной среде можно воспроизводить типовые киберинциденты и измерять не только факт DDoS-атаки, но и её последствия для наблюдаемости, устойчивости и времени реагирования, не подвергая риску производственную площадь риска. Это создает основу для обоснованной приоритизации контрмер, а также процедур восстановления и управления изменениями.

Библиографический список

1. Кузнецова Н.М. Построение цифрового двойника основных автоматизированных систем промышленного предприятия с целью определения уровня информационной безопасности / Т.В. Карлова, А.Ю. Бекмешов // Эргодизайн. – 2021. – № 2(12). – С. 97-102. – DOI: 10.30987/2658-4026-2021-2-97-102.

2. Understanding ISA/IEC 62443: A Guide for OT Security Teams // Dragos. – [Электронный ресурс]. – Режим доступа: https://www.dragos.com/blog/isa-iec-62443-concepts.

3. Voas J. Security and Trust Considerations for Digital Twin Technology / P. Mell, P. Laplante, V. Piroumian // National Institute of Standards and Technology. – 2025. – P. 25. – DOI: 10.6028/NIST.IR.8356.

4. Минзов А.С. Цифровые двойники в системах управления / А.Ю. Невский, О.Р. Баронов, С.В. Немчанинова // Вопросы кибербезопасности. – 2024. – № 2(60). – С. 29-35. – DOI: 10.21681/2311-3456-2024-2-29-35.

5. Водопьянов А.С. Использование цифровых двойников с целью обеспечения информационной безопасности киберфизических систем // Вопросы кибербезопасности. – 2024. – № 4(62). – С. 140-144. – DOI: 10.21681/2311-3456-2024-4-140-144.

6. ICS Matrix // MITRE ATT&CK. – [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/matrices/ics/.

7. Stouffer K. Guide to Operational Technology (OT) Security / M. Pease, C.-Y. Tang, T. Zimmerman et al. // National Institute of Standards and Technology. - 2023. – P. 299 – DOI: 10.6028/NIST.SP.800-82r3

8. Sayghe A. Digital Twin-Driven Intrusion Detection for Industrial SCADA: A Cyber-Physical Case Study // Sensors. – 2025. – Vol. 25. – № 16. – DOI: 10.3390/s25164963. – [Электронный ресурс]. – Режим доступа: https://www.mdpi.com/1424-8220/25/16/4963.

THE DIGITAL TWIN OF THE SCADA SYSTEM NETWORK: A THREAT MODEL AND RISK-ORIENTED CYBER DEFENSE AT OIL AND GAS FACILITIES

S.A. Globenko, *Graduate Student*
V.V. Kirillin, *Graduate Student*
Supervisor: *R.F. Dobryansky, Senior Lecturer*
Far Eastern Federal University
(Russia, Vladivostok)

Abstract. *The article discusses the application of a digital twin of a SCADA system network at facilities of the oil and gas industry for building a threat model and selecting risk-oriented cyber protection measures. A digital twin is understood as a virtual representation of the topology of an industrial network, assets (servers, controllers, workstations), technological links and data flows, updated based on configurations, logs and telemetry. A methodology is proposed that includes asset inventory, allocation of zones and channels, description of threats and vulnerabilities, creation of cyber incident scenarios, and assessment of risk based on probability and consequences for production, ecology, and security. In the twin environment, secure simulation of communication failures, data substitution, and unauthorized operator actions is performed to test resilience and detectability. Based on the results, the prioritization of countermeasures is justified: segmentation, remote access control, least privilege principle, anomaly monitoring, and management of updated.*

Keywords: *digital twin; SCADA; industrial network; threat model; cyber risks; risk-based cyber protection; ISA/IEC 62443; anomaly monitoring; oil and gas industry.*