ТРЕНАЖЁРЫ ОПЕРАТОРОВ АСУ ТП КАК ИНСТРУМЕНТ ОБНАРУЖЕНИЯ И МОДЕЛИРОВАНИЯ КИБЕРУГРОЗ В СИСТЕМАХ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

Г.Г. Доминяк[1], *начальник отдела информационных технологий*
А.В. Борзов[2], *заместитель генерального директора по информационной безопасности*
[1]**АО «Сибгазполимер» – управляющая организация ООО «Полиом» (Омский завод полипропилена)**
[2]**АО «ТГК-11»**
[1,2]**(Россия, г. Омск)**

DOI:10.24412/2500-1000-2026-5-1-306-312

Аннотация. *Рассмотрены тренажеры операторов АСУ ТП как безопасная среда для моделирования киберугроз, проверки средств обнаружения и оценки действий персонала. Показано, что тренажер, включающий динамическую модель процесса, эмуляцию PLC/DCS/SIS, HMI, станцию инструктора и систему регистрации событий, может быть расширен до киберфизического стенда без воздействия на действующее производство. Приведены численные параметры такого стенда, примеры промышленных платформ и сценарии атак, сопоставленные с MITRE ATT&CK for ICS. Выделены метрики: время обнаружения, доля ложных срабатываний, полнота восстановления цепочки событий и качество действий оператора.*

Ключевые слова: *АСУ ТП; тренажер оператора; киберугрозы; промышленная автоматизация; цифровой двойник; MITRE ATT&CK for ICS; обнаружение аномалий.*

Промышленная автоматизация развивается в условиях конвергенции операционных технологий и ИТ-инфраструктуры. Контроллеры, инженерные станции, HMI, архиваторы и сервисные каналы становятся частью связанной цифровой среды, поэтому нарушение целостности команды или доступности канала может повлиять не только на данные, но и на физическое состояние оборудования. NIST SP 800-82 Rev. 3 определяет OT как программируемые системы и устройства, которые взаимодействуют с физической средой через мониторинг и управление процессами [1].

Серия ISA/IEC 62443 рассматривает безопасность промышленных систем как задачу жизненного цикла и распределенной ответственности между владельцем объекта, интегратором и поставщиком компонентов [2]. Однако проверка киберсценариев на действующем объекте ограничена требованиями непрерывности производства и промышленной безопасности. По этой причине требуется среда, где можно воспроизвести технологические последствия атаки, не подключаясь к исполнительным механизмам реального объекта.

Тренажер оператора АСУ ТП подходит для этой цели, так как содержит замкнутую причинно-следственную модель: команда меняет состояние виртуального процесса, а процесс возвращает измерения, тревоги и тренды. Если добавить мониторинг трафика, журналы контроллеров и сценарный инжектор воздействий, тренажер становится киберфизическим стендом. Матрица MITRE ATT&CK for ICS включает 12 тактик и 79 техник, что позволяет формализовать сценарии не как абстрактные «атаки», а как проверяемые действия и наблюдаемые признаки [3].

Актуальность подтверждается статистикой угроз. ENISA Threat Landscape 2024 относит угрозы доступности к ведущим угрозам года, за которыми следуют вымогательское ПО и угрозы данным [4]. Dragos сообщает об отслеживании 23 групп угроз, ориентированных на промышленные организации, из которых 9 были активны в 2024 г. [5]. Claroty по итогам опроса 1100 специалистов указывает, что 45% респондентов столкнулись с финансовым ущербом не менее 500 тыс. долл. США за 12 месяцев, а 27% – не менее 1 млн долл. США [6]. Следовательно, тренажер должен рассматриваться не только как учебное средство, но и как инструмент инженерии киберустойчивости.

Результаты исследования

Тренажер оператора как киберфизический стенд

Классический OTS воспроизводит технологический процесс, рабочие экраны и реакцию контроллеров. Для кибербезопасности этого недостаточно: требуется фиксировать, какие

сетевые события, системные журналы и технологические переменные изменились в момент сценария. Поэтому в состав стенда включаются динамическая модель, эмуляция PLC/DCS/SIS, HMI, станция инструктора, historian, сетевой сенсор, SIEM/IDS и модуль сценариев.

На практике сценарий должен иметь исходное состояние, метку старта, затронутые теги, допустимые границы, ожидаемые признаки и критерии завершения. Например, при подмене уставки важно видеть не только изменение SP, но и динамику PV, действие регулятора, квитирование тревог и время реакции оператора. Такой подход позволяет отличить обычное технологическое возмущение от киберфизической аномалии.

Архитектура стенда приведена на рисунке 1. В ней инжектор сценариев не заменяет средства защиты, а создает контролируемые условия для их проверки. Все активные воздействия выполняются в изолированной среде, на виртуальных контроллерах либо учебных ПЛК, не связанных с исполнительными механизмами.

Рис. 1. Архитектура тренажера АСУ ТП как киберфизического стенда

Для проектирования стенда важны измеримые параметры: шаг модели, число тегов, задержки, частота записи, число рабочих мест и окно анализа. Таблица 1 содержит типовые проектные диапазоны. Они не являются нормативом, но задают проверяемую основу для сопоставления разных OTS и выбора достаточной детализации.

Таблица 1. Состав и параметры тренажера АСУ ТП для задач кибербезопасности

Элемент	Назначение	Численные параметры стенда	Данные для обнаружения
Динамическая модель	Расчет давлений, расходов, уровней, температур, состояний агрегатов	Шаг 0,05-1 с; 500-50000 тегов; скорость 0,5-10x; целевой RMSE по PV 1-5%	Эталонные траектории PV/SP/MV, скорость отклонения, физическая согласованность
PLC/DCS/SIS	Эмуляция логики, PID, блокировок, последовательностей	Цикл 10-500 мс; 10-1000 контуров; режимы SIL/HIL	Изменение логики, уставок, контрольных сумм, статусов защит
HMI/SCADA	Рабочая среда оператора, тревоги, тренды, команды	Обновление 0,5-2 с; 2-6 рабочих мест; 3-5 классов тревог	Журнал команд, квитирование, переходы между экранами
Станция инструктора	Запуск отказов, атак, снимков состояния и оценок	20-100 снимков; 4-50 сценариев; отметки времени до 1 с	Метка сценария, момент воздействия, критерии восстановления
Historian и журналы	Хранение технологических и системных событий	0,1-1 с для критичных тегов; 1-10 с для фоновых; 30-180 суток	Корреляция сетевых событий с PV/SP/MV и командами
Сетевой эмулятор	Задержки, потери, сегментация, протокольные условия	10-250 мс; 0-5% потерь; OPC UA/DA, Modbus TCP, PROFINET, EtherNet/IP	Необычные сессии, частота команд, повторы, аномалии протокола

Синхронизация времени является отдельным требованием. В АСУ ТП команда и технологическое следствие часто разделены секундами или минутами: команда клапану отражается в журнале сразу, давление меняется позже, а тревога появляется после достижения порога. Для учебных сценариев достаточно точности порядка 1 с, для проверки детекторов аномалий желательно фиксировать события с точностью не хуже 100 мс.

Промышленные платформы и примеры тренажеров

Siemens SIMIT применяется для виртуального пуска и операторского обучения, поддерживает тестирование автоматизированных проектов до ввода в эксплуатацию и создание реалистичной обучающей среды [7]. В материалах Siemens дополнительно указаны hardware-in-the-loop и software-in-the-loop, сценарии возмущений и оценивание обучения; также приведена оценка, что около 80% аварий и до 6% потерь производительности связаны с человеческим фактором [8].

Yokogawa описывает OTS как виртуальную установку, позволяющую обучать персонал до пуска и в течение жизненного цикла объекта без воздействия на реальную установку [9]. OmegaLand Trainer использует Visual Modeler, основанный на балансах массы и энергии; указывается возможность расчетов быстрее реального времени даже для крупной установки [10]. Honeywell UniSim Design Suite поддерживает динамические модели, сценарный анализ и применение модели как цифрового двойника [11], а UniSim Tutor включает режимы What-If, Hypothesis и Diagnose для анализа причинно-следственных связей [12].

Emerson DeltaV Mimic позиционируется как динамическая симуляция и цифровой двойник для обучения, тестирования управления и снижения риска пусконаладки [13]. DeltaV Mimic Field 3D использует CAD-модели, лазерное сканирование или фотосъемку объекта и может применяться на гарнитуре, экране или купольном дисплее [14]. AVEVA Dynamic Simulation/DYNSIM предназначена для динамического моделирования, пусконаладки и OTS, включая локальный и облачный доступ [15]. ABB 800xA Simulator поддерживает обучение, проверку логики и работу внешней модели через OPC Data Access [16]. CORYS указывает более 35 лет опыта поставки учебных и инженерных симуляторов [17].

Таблица 2. Примеры промышленных тренажеров операторов АСУ ТП

Платформа	Заявленная основа	Данные и параметры	Применимость к моделированию киберугроз
Siemens SIMIT	Виртуальный пуск, OTS, цифровой двойник, HIL/SIL	Сценарии пуска/останова, возмущений, отказов; оценка 80% аварий и до 6% потерь от человеческого фактора [8]	Проверка логики, задержек, команд оператора и реакции на ложные/искаженные состояния
Yokogawa OmegaLand	Виртуальная установка с DCS/SIS-средой [9]	Visual Modeler: балансы массы/энергии, расчеты быстрее реального времени [10]	Повторные ускоренные прогоны атак на уставки, регуляторы и тревоги
Honeywell UniSim	Динамическое моделирование и цифровой двойник [11]	API Python/.NET; режимы What-If, Hypothesis, Diagnose [12]	Диагностика причин отклонения, проверка гипотез о подмене данных
Emerson DeltaV Mimic / Field 3D	Динамическая модель, HMI, 3D/VR для полевых операторов [13; 14]	CAD, лазерные сканы, фотосъемка; устройства: гарнитура, экран, купол [14]	Совместные сценарии диспетчерской и полевого обхода при кибераномалиях
AVEVA Dynamic Simulation	Высокоточная динамическая симуляция для OTS [15]	Локальный и облачный доступ, runtime-лицензии для тренажеров [15]	Проверка регламентов пуска, отклонений качества, энергопотребления
ABB 800xA Simulator	Тестирование логики, обучение, оптимизация [16]	Внешняя модель стимулирует I/O через OPC Data Access [16]	Безопасная проверка изменений логики и библиотек управления
CORYS INDISS PLUS / OTS	Учебные и инженерные симуляторы для энергетики, транспорта, процесса [17]	Более 35 лет поставок симуляторов [17]	Отраслевые сценарии с учетом регламентов и физики объекта

Сопоставление платформ показывает, что OTS не следует рассматривать как готовую систему защиты. Его ценность состоит в создании достоверного технологического окружения, где средство обнаружения проверяется вместе с оператором, регламентом и динамикой объекта. Поэтому при выборе платформы для кибериспытаний важны API, экспорт журналов, повторяемость сценариев, возмож-

ность включения сетевого сенсора и изолированное развертывание.

Моделирование угроз и обнаружение аномалий

Сценарий моделирования должен описывать не вредоносный инструмент, а наблюдаемое киберфизическое воздействие: изменение уставки, задержку данных, подавление тревоги, деградацию доступности или изменение логики на стенде. Это снижает риск и делает испытание воспроизводимым. Один и тот же сценарий можно запускать многократно, меняя амплитуду воздействия, длительность и момент относительно технологического перехода.

Минимальный цикл включает формирование базовой линии, выбор техники MITRE ATT&CK for ICS, запуск управляемого воздействия, сбор данных HMI/SCADA, historian, сетевого мониторинга и контроллеров, затем сравнение с эталоном. Для медленной подмены уставки полезно варьировать изменение от 0,5 до 5% шкалы и длительность от 30 с до 10 мин, чтобы найти границу обнаружения раньше технологической тревоги.

На рисунке 2 показана временная логика сценария. Важна не только точка срабатывания правила, но и поведение персонала: переход на нужный экран, проверка тренда, связь с полевым оператором, выбор безопасного режима и отсутствие лишних ручных команд.

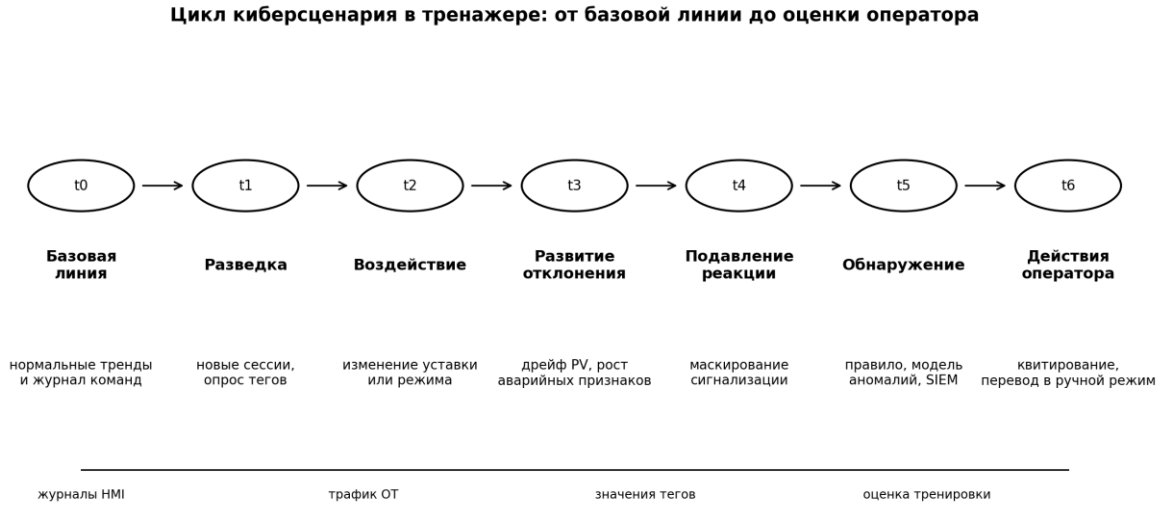

Рис. 2. Цикл моделирования киберсценария на тренажере оператора

Таблица 3. Сценарии киберугроз, моделируемые в тренажере АСУ ТП

Сценарий	MITRE ATT&CK for ICS	Воздействие на процесс	Признаки обнаружения	Метрики
Нештатный удаленный доступ	Initial Access: External Remote Services [3]	Команды вне окна обслуживания	Новая сессия, чтение множества тегов, необычное время входа	Tdet; число команд до срабатывания
Медленное изменение уставки	Execution / Impair Process Control [3]	Дрейф PV на 1-5% шкалы	Расхождение SP с технологическим заданием, частые ручные коррекции	Амплитуда обнаружения; задержка реакции
Подмена датчика или задержка HMI	Adversary-in-the-Middle, Spoof Reporting Message [3]	Оператор видит норму при развитии отклонения	Несовпадение расчетного и отображаемого PV, задержка тренда	Время до выявления расхождения
Изменение логики контроллера на стенде	Modify Controller Tasking, Program Download [3]	Нарушение блокировок или последовательности	Смена контрольной суммы, новые блоки логики	Точность выявления и время восстановления
Подавление сигнализации	Inhibit Response Function [3]	Нет ожидаемой тревоги при опасном отклонении	Аварийная переменная без тревоги, разрыв SIS-HMI	Доля найденных подавлений
Деградация доступности SCADA/OPC	Impact: Denial of View / Denial of Control [3]	Задержки управления и обновления экранов	Задержка более 250 мс, потери пакетов, останов обновления	Доля сохраненных функций

Детектирование должно быть двухслойным. Первый слой фиксирует сетевые и системные признаки: новые сессии, команды, изменения конфигурации, задержки, ошибки протоколов. Второй слой проверяет физическую согласованность: соответствуют ли расход, давление, температура, положение клапана и состояние насоса законам процесса. Несогласованность слоев является сильным индикатором киберфизической аномалии.

Активные проверки в OT-среде ограничены, поэтому предпочтителен пассивный мониторинг. В тренажере допустимо безопасно отрабатывать и более агрессивные режимы, но только при подтвержденной изоляции. Результатом каждого прогона должен быть не просто факт срабатывания, а протокол: причина, затронутые теги, первое наблюдаемое событие, технологическое последствие, действия оператора и восстановление режима.

Метрики и условия внедрения

Основная метрика – время обнаружения Tdet, измеряемое от запуска сценария до первого достоверного сигнала детектора или правильной диагностической команды оператора. Tdet нельзя оценивать вне динамики объекта: для быстрых приводов допустимы секунды, для инерционных химических процессов – минуты. Поэтому каждая тренировка должна задавать технологически допустимое время реакции Tmax.

Вторая метрика - полнота реконструкции события. По журналам должно быть возможно восстановить не менее 90% контрольных точек сценария: старт, затронутый тег, команда, изменение PV/SP/MV, тревога или ее отсутствие, действие оператора и момент восстановления. Третья метрика – доля ложных срабатываний на нормальных возмущениях: смена сырья, запуск резерва, калибровка датчика, плановое обслуживание.

Оценка оператора включает время перехода на нужный экран, проверку тренда, связь с полевым персоналом, корректность квитирования, отсутствие опасных ручных действий и достижение безопасного состояния. Быстрота не должна считаться единственным критерием, поскольку слишком резкое ручное действие может устранить один симптом и создать другое технологическое нарушение.

Организационно тренажер-киберстенд внедряется поэтапно: инвентаризация критичных сценариев, валидация модели по историческим данным, настройка журналирования, проведение 5-7 базовых киберсценариев, корректировка правил SOC и регламентов смены. Модели, перечни тегов и аварийные границы должны защищаться как чувствительная инженерная информация.

Заключение

Тренажер оператора АСУ ТП при расширении средствами мониторинга и сценарного управления становится безопасным инструментом моделирования киберугроз. Он позволяет связать сетевые события, системные журналы и технологические последствия в единую проверяемую картину, не воздействуя на действующий объект.

Наибольшую практическую ценность дают сценарии малых скрытых отклонений: подмена датчика, медленный дрейф уставки, подавление тревоги, задержка HMI и деградация доступности. Именно они проверяют не только качество детектора, но и зрелость операторских действий, регламентов и межфункционального взаимодействия.

Промышленные платформы Siemens SIMIT, Yokogawa OmegaLand, Honeywell UniSim, Emerson DeltaV Mimic, AVEVA Dynamic Simulation, ABB 800xA Simulator и CORYS INDISS PLUS демонстрируют достаточную технологическую основу для таких задач. При условии изоляции, валидации модели и строгого управления доступом OTS целесообразно включать в программу промышленной киберустойчивости как стенд для обучения, проверки изменений, настройки детекторов и расследования киберфизических инцидентов.

Библиографический список

1. NIST Special Publication 800-82 Revision 3. Guide to Operational Technology (OT) Security // National Institute of Standards and Technology, 2023. – [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/pubs/sp/800/82/r3/final.

2. ISA/IEC 62443 Series of Standards // International Society of Automation. – [Электронный ресурс]. – Режим доступа: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

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

4. ENISA Threat Landscape 2024 // European Union Agency for Cybersecurity, 2024. – [Электронный ресурс]. – Режим доступа: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

5. Dragos's 8th Annual OT Cybersecurity Year in Review Is Now Available // Dragos, 2025. – [Электронный ресурс]. – Режим доступа: https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available.

6. The Global State of CPS Security 2024: Business Impact of Disruptions // Claroty, 2024. – [Электронный ресурс]. – Режим доступа: https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions.

7. SIMIT Simulation Platform // Siemens. – [Электронный ресурс]. – Режим доступа: https://www.siemens.com/en-gb/products/simit/.

8. SIMIT Simulation Platform. Overview Infographic // Siemens, 2022. – [Электронный ресурс]. – Режим доступа: https://assets.new.siemens.com/siemens/assets/api/uuid:741f3149-ea21-43e8-9636-f052a3cda1d1/220803-simit-overview-infographic.pdf.

9. Operator Training Simulator // Yokogawa United Kingdom Ltd. – [Электронный ресурс]. – Режим доступа: https://www.yokogawa.com/uk/solutions/products-and-services/information/qhsse-management/operator-training-simulator/.

10. OmegaLand Trainer. Operator Training Simulator. – Yokogawa, 2025. – [Электронный ресурс]. – Режим доступа: https://web-material3.yokogawa.com/13/39086/files/OmegaLand%20Trainer.pdf.

11. Honeywell UniSim Design Suite. – Honeywell. – [Электронный ресурс]. – Режим доступа: https://process.honeywell.com/us/en/products/industrial-software/process-optimization/unisim-design-suite.

12. Honeywell UniSim Tutor. – Honeywell. – [Электронный ресурс]. – Режим доступа: https://process.honeywell.com/us/en/initiative/unisim-competency-suite/unisim-tutor.

13. DeltaV Mimic. – Emerson. – [Электронный ресурс]. – Режим доступа: https://www.emerson.com/en/automation-systems/operations-business-management/deltav-mimic.

14. DeltaV Mimic Field 3D. Product Data Sheet. – Emerson, 2024. – [Электронный ресурс]. – Режим доступа: https://www.emerson.com/is/content/emerson/en/systems-and-software/deltav-mimic/product-data-sheets/deltav-mimic-field-3d.pdf.

15. AVEVA Dynamic Simulation // AVEVA. – [Электронный ресурс]. – Режим доступа: https://www.aveva.com/en/products/dynamic-simulation/.

16. ABB Ability System 800xA Simulator // ABB. – [Электронный ресурс]. – Режим доступа: https://new.abb.com/control-systems/service/customer-support/800xA-services/800xa-training/800xa-simulator.

17. CORYS. Dynamic Simulation // CORYS. – [Электронный ресурс]. – Режим доступа: https://www.corys.com/en/.

OPERATOR TRAINING SIMULATORS OF INDUSTRIAL CONTROL SYSTEMS AS A TOOL FOR DETECTING AND MODELLING CYBER THREATS IN INDUSTRIAL AUTOMATION SYSTEMS

G.G. Dominyak[1], *Head of Information Technology Department*
A.V. Borzov[2], *Deputy Director General for Information Security*
[1]Sibgazpolymer JSC – managing organization of Poliom LLC (Omsk Polypropylene Plant)
[2]JSC "TGK-11"
[1,2](Russia, Omsk)

Abstract. *The paper examines operator training simulators for industrial control systems as a safe environment for cyber-threat modelling, detection testing and operator response assessment. A simulator based on a dynamic process model, PLC/DCS/SIS emulation, HMI screens, an instructor station and event logging can be expanded into a cyber-physical testbed without affecting the real plant. The paper provides numerical parameters, examples of industrial platforms and attack scenarios mapped to MITRE ATT&CK for ICS. The main metrics are detection time, false-positive rate, completeness of event reconstruction and quality of operator actions.*

Keywords: *industrial control system; operator training simulator; cyber threats; industrial automation; digital twin; MITRE ATT&CK for ICS; anomaly detection.*