Обеспечение информационной безопасности комплексных очистных сооружений: методология сбора данных

Е.В. Федорченко

Лаборатория проблем компьютерной безопасности, СПб ФИЦ РАН

Санкт-Петербург - **2024**

Содержание

Актуальность

- Планомерный рост уровня автоматизации систем водоподготовки и водоотведения.
- Рост атак на промышленные кибер-физические системы:
  - 2021 г. – атака на водоочистную станцию Oldsmar в США[1].
  - 2022 г. – атака на компанию South Staffs Water в Великобритании с использованием программы-вымогателя Clop[2].

[1] https://pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant
[2] https://www.computerweekly.com/news/252523856/South-Staffs-Water-is-victim-of-botched-Clop-attack

Постановка задачи исследования

Научная проблема

- *Рост атак на промышленные кибер-физические системы и как следствие – интерес к обнаружению кибератак и аномалий для таких систем.*
- *Применение методов глубокого обучения для выявления кибератак и аномалий, для которых необходимы большие наборы данных.*
- *...*

Релевантные исследования

Ref.	Набор данных:
[Inoue et al., 2015]	Secure Water Treatment (SWaT)
[Elnour et al., 2020]	SWaT, Water Distribution (WADI) – расширение SWaT
[Li et al., 2019]	SWaT, WADI
[Shalyga et al., 2018]	SWaT
[Wang et al., 2020]	SWaT
[Audibert et al., 2020]	SWaT, WADI
[Hundman et al., 2018]	SWaT, WADI, SMAP (Soil Moisture Active Passive satellite)
[Su et al., 2019]	SMAP (Soil Moisture Active Passive satellite) and MSL (Mars Science Laboratory rover), Server Machine Dataset
[Neshenko et al., 2021]	SWaT
[Lin et al., 2018]	SWaT
[Goetz et al., 2023]	Own dataset from rotary table dispenser system with limited access upon the request
[Xu et al., 2023]	SMAP, MSL (Mars Science Laboratory rover), Server Machine Dataset
[Oliveira et al., 2021]	SWaT
[Boateng et al., 2022]	SWaT

Постановка задачи исследования

Научная проблема

- *Рост атак на промышленные кибер-физические системы и как следствие – интерес к обнаружению кибератак и аномалий для таких систем.*
- *Применение методов глубокого обучения для выявления кибератак и аномалий, для которых необходимы большие наборы данных.*
- *Недостаток реалистичных наборов данных для кибер-физических систем, особенно данных, связанных с кибератаками. Отсутствие такого набора данных в РФ.*
- *Необходимость в формировании таких наборов данных и отсутствие единой методологии их формирования*[1].
- *Необходимость в методологии формирования наборов данных*[1].

[1] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2248–2294, 2021.

Требования к набору данных

1. Набор данных должен быть собран от физических и цифровых компонентов киберфизической системы, т. е. он должен включать в себя как данные сетевого трафика, так и журналы событий от датчиков/актуаторов.

2. Набор данных должен быть размечен и включать как нормальные, так и аномальные записи.

3. Набор данных должен быть максимально приближен к реальным данным.

Типы стендов и их ограничения

Типы: (1) *Виртуальные* стенды; (2) *физические* стенды; (3) гибридные стенды.

Ограничения:

- отсутствие единой методологии проектирования испытательного стенда и формирования наборов данных;
- необходимость представления реалистичного сценария как на технологическом уровне, так и на уровне атаки;
- сложность технологических процессов, и как следствие необходимость привлечения специалистов по АСУ ТП и моделируемому технологическому процессу;
- масштабируемость испытательного стенда;
- сбор данных, характеризующих нормальное и аномальное поведение;
- стоимость в случае физических стендов;
- проблемы безопасности (safety) в случае физических испытательных стендов;
- отсутствие документации;
- воспроизводимость испытательных стендов.

Постановка задачи исследования

Цель

Разработка методологии создания набора данных, применимого для исследований в области кибербезопасности промышленных киберфизических систем на примере систем очистки сточных вод.

Методология

1. Определение и спецификация технологического процесса
2. Определение типа тестового стенда и его реализация
3. Генерация данных, соответствующих нормальному функционированию системы
4. Разработка модели атак для рассматриваемого технологического процесса с учетом их возможных последствий
5. Разработка сценариев реализации атак с учетом используемого технологического стека, используемого для моделирования технологического процесса
6. Реализация сценариев угроз и сбор данных о поведении технологического процесса
7. Оценка и валидация сформированного набора данных

Методология

1 Определение и спецификация технологического процесса

(1) Определение технологического процесса,
(2) построение его технологической схемы,
(3) определение сенсоров и актуаторов, используемых для мониторинга и контроля процесса,
(4) определение математической модели технологического процесса, в случае, если будет использоваться виртуальный или гибридный стенд.

2 Определение типа тестового стенда и его реализация

(1) Определяется тип создаваемого стенда,
(2) определяются ограничения стенда и особенности его построения,
(3) определяется ПО, необходимое в случае виртуального или гибридного стенда, и ПО и АО в случае физического стенда,
(4) формируется список сенсоров и актуаторов,
(5) определяются протоколы,
(6) формируется список инструментов управления и сбора данных,
(7) определяются формат собираемых данных и интервал их получения,

Методология

3. Генерация данных, соответствующих нормальному функционированию системы

(1) Формируется набор данных, характеризующих нормальное поведение системы.

4. Разработка модели атак для рассматриваемого технологического процесса с учетом их возможных последствий

(1) Разрабатывается модель атакующего, (2) атак, (3) определяется набор атак.

5. Разработка сценариев реализации атак с учетом используемого технологического стека, используемого для моделирования технологического процесса

(1) С учетом технологического стека, разрабатываются сценарии выполнения атак,
(2) определяется набор инструментов, необходимых для реализации разработанных сценариев,
(3) определяется набор инструментов, необходимых для сбора данных об атаках.

Методология

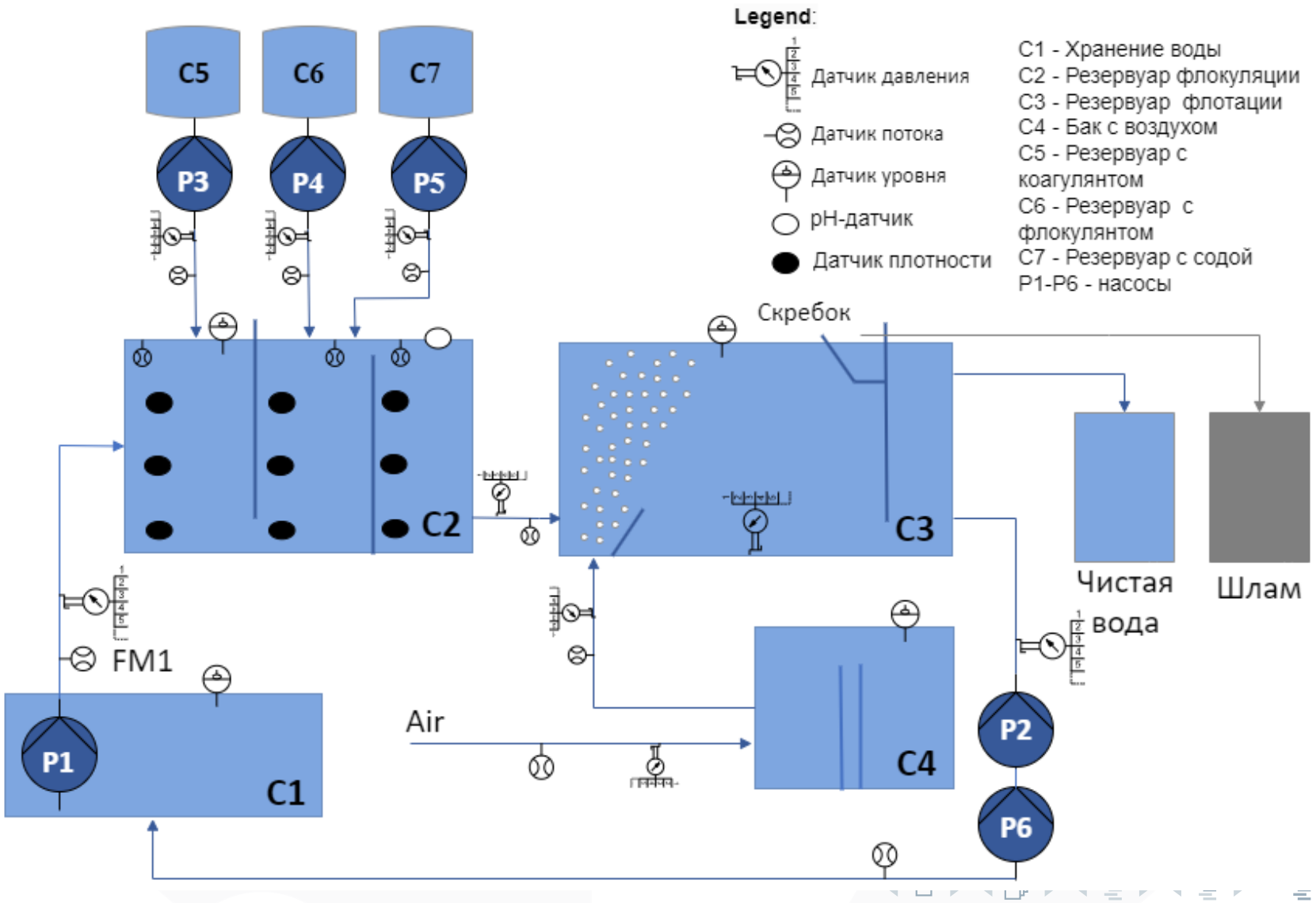
6. Реализация сценариев угроз и сбор данных о поведении технологического процесса

(1) Выполнение сценариев атак,
(2) формирование набора данных, характеризующих поведение системы при проведении атаки.

7. Оценка и валидация сформированного набора данных

(1) Оценка соответствия модели технологического процесса реальному процессу,
(2) статистический анализ полученных данных,
(3) выполнение сравнительного анализа сформированных данных и реальных данных путем оценки разницы между распределениями вероятностей реальных данных и синтетических.

Определение технологического процесса

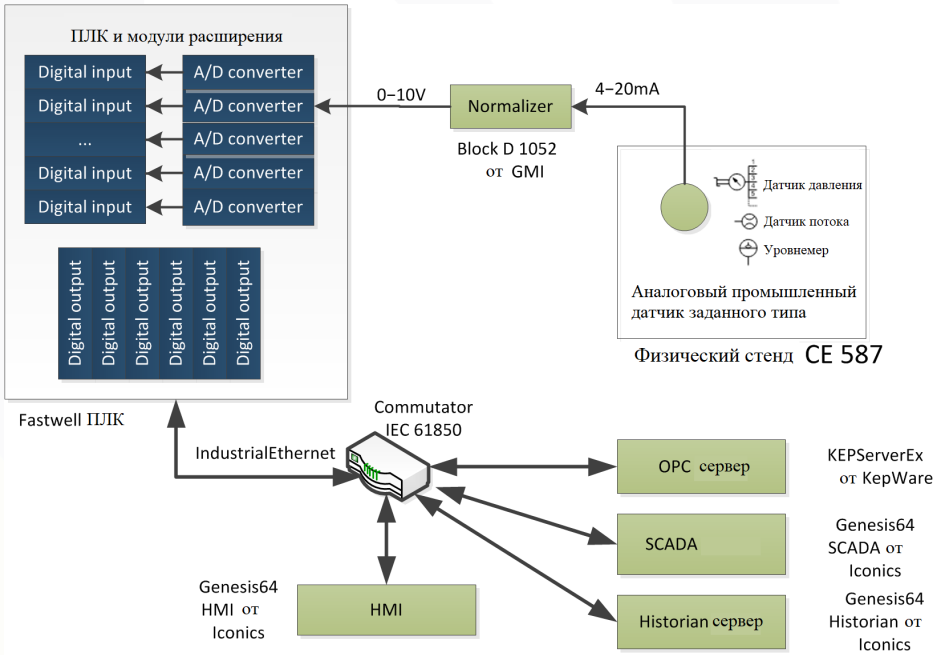


Модель киберфизического стенда

Разработана модель киберфизического стенда технологического процесса очистных сооружений для моделирования кибератак и выявления киберрисков. Основана на расширении физического стенда физическими, кибер- и логическими элементами.

Физический учебный стенд CE 587 (G.U.N.T., GmbH, Германия), реализующий процесс флотации, включающий стадии флокуляции и флотации.

Модель киберфизического стенда.[a]



[a] Таким образом расширен учебный стенд для решения задач мониторинга.

Модель атак

Разработана модель атак для очистных сооружений (основа для разработки сценариев атак).

За основу взята абстрактная модель атак[a]: $AM = (M, I, D, P, S_0, S_e)$,
M—техники проведения атак (на основе MITRE ATT&CK),
I—намерения (цели) атакующего,
D—модель объекта системы,
$D = (Cm, Pr, Pe)$, где
Cm—компоненты системы;
Pr—свойства системы;
Pe—показатели производительности системы.
$P \subseteq Cm$—объекты атаки,
S_0 и S_e—множества состояний системы.

Модель атакующего: $At = (I, D)$.

[a] https://ieeexplore.ieee.org/document/7552024

Определены следующие цели атакующего I:

- нарушение процесса перемешивания сырой воды;
- нарушение работы расходомера сырой воды, насоса подачи реагентов или pH-датчика;
- отсутствие коагулянта/флокулянта/соды в резервуаре или отказ насоса его подачи, или нарушение подачи сжатого воздуха в систему;
- повышение уровня воды в резервуарах флокуляции и флотации;
- заполнение резервуара чистой воды/шлама;
- забивка фильтра;
- выход из строя циркуляционных насосов/ скребков/ смесителей/ насоса сырой воды;
- утечка жидкости из системы.

Выделены следующие объекты атаки P.

Точка атаки	Тип компонента	Класс компонента		
		Физический	Кибер	Логический
Насосы	Испонительные механизмы	+	Связь с контроллером	-
Датчики давления	Сенсоры			
Датчики потока воды	Сенсоры			
Датчики потока воздуха	Сенсоры			
Датчики уровня воды	Сенсоры			
pH-датчики	Сенсоры			
Датчики плотности	Сенсоры			
Сервер Historian	Хранилище	+	-	+
ПЛК и модули	Контроллер	+	-	+
Нормализаторы для аналоговых датчиков	Преобразователь	+	-	+
OPC сервер	Преобразователь	+	-	+
SCADA	Контроллер	+	-	+
HMI	Контроллер	+	-	+

Сценарии атак (внешние)

Название начального вектора атаки	Описание	Предусловия	Связь с MITRE ICS
Подбор пароля к веб-порталу одного из компонентов АСУ ТП (например, SCADA)	Позволит злоумышленнику управлять АСУ ТП, предоставляя доступ к системе с правами того пользователя, к которому подобрал пароль.	Доступ в Интернет, статический IP. Зависит от установленного ПО (возможно, пароли по умолчанию не изменены), а также от того есть ли 2FA (двухфакторная аутентификация).	Internet Accessible Device https://attack.mitre.org/techniques/T0883/
Получение доступа к одному из компонентов при эксплуатации уязвимости (например, типа RCE – Remote Code Execution)	Позволит злоумышленнику получить доступ к внутренней сети, соответственно, развить атаку применяя всевозможные другие методы и средства. Пример: получение доступа к внутренней сети → ARP spoofing между рабочей станцией инженера и SCADA → получение пароля в открытом виде.	Компоненты выходят в Интернет. Зависит от того, каким образом компоненты взаимодействуют с другими, существует ли сегментация сети, названий и версий ПО (для проверки в базах уязвимостей).	Exploit Public-Facing Application https://attack.mitre.org/techniques/T0819/
DDOS	Телекоммуникационное оборудование и/или другие компоненты АСУ ТП могут иметь статический IP в Интернете – существует вероятность, что в час «Ч» иностранное государство либо террористические организации могут провести распределенную атаку типа «отказ в обслуживании».	Доступ в Интернет, статический IP.	Internet Accessible Device https://attack.mitre.org/techniques/T0883/
Атака на Wi-Fi	Если компоненты АСУ ТП управляются по беспроводным сетям (Wi-Fi), возможны атаки: перехват handshake и дальнейший брутфорс (перебор пароля), деаутентификация Wi-Fi (не позволит устройствам обмениваться данными до тех пор, пока пакеты деаутентификации не перестанут появляться в эфире) приведет к отказу в обслуживании и ряд других.	Зависит от протокола безопасности (WEP, WPA, WPA2, WPA3), наличия пароля, того, скрытая ли сеть, какие компоненты взаимодействуют при помощи Wi-Fi.	*Wireless Compromise* https://attack.mitre.org/techniques/T0860/
Атака на телекоммуникационное оборудование (коммутаторы)	Для организации сети используется всевозможное сетевое оборудование зарубежного производства, например, Cisco, Juniper и другие – это создает возможность реализации вредоносных воздействий со стороны зарубежных специальных служб на критическую информационную инфраструктуру Российской Федерации. Неоднократно исследователями находились различные недокументированные возможности, а также уязвимости в программном обеспечении сетевого оборудования.	Зависит от используемого ТКО, версий прошивок, способа подключения к сети, конфигурации оборудования.	MITRE ICS
Атака на VPN	Если для доступа к промышленной или корпоративной сети используется VPN, то злоумышленники могут получить файл конфигурации VPN и подбирать пароль для получения доступа к внутренней сети, либо используя особенности некоторых протоколов (например, IPSec IKE VPN) и реализаций проводить bruteforce атаку.	Используется VPN, зависит от названия и версии ПО, протокола, наличия защиты от брутфорса (например, OpenVPN + fail2ban).	External Remote Services https://attack.mitre.org/techniques/T0822/
Доставка и запуск вредоносного ПО	Вредоносное ПО может быть доставлено на рабочую станцию различными методами – социальной инженерии (фишинговое письмо), watering hole атакой (например, часто посещаемый сотрудниками сайт (портал) был заражен вредоносным ПО) и другими.	Использует почта, посещаются сторонние Интернет-ресурсы.	Spearphishing Attachment https://attack.mitre.org/techniques/T0865/ Drive-by Compromise https://attack.mitre.org/techniques/T0817/

Сценарии атак (внутренние)

Название начального вектора атаки	Описание	Предусловия	Связь с MITRE ICS
Подключение съемного диска с вредоносным ПО к рабочей станции	Сотрудник нашел или получил накопитель с вредоносным ПО (рассматриваются случаи как заведомо (случай со Stuxnet), так и из-за любопытства) и подключил к рабочей станции.	Зависит от того, установлены и работают ли СЗИ, есть ли доступные порты (разъемы) (USB, micro SD), того, к каким компонентам можно подключать накопители и как они взаимодействуют с другими.	Replication Through Removable Media https://attack.mitre.org /techniques/T0847/
Сотрудник изменил параметры датчиков и актуаторов	Сотрудник изменил параметры датчиков и актуаторов таким образом, что процесс был нарушен.	Зависит от наличия ограничений, «защиты от «дурака» в ПО, используемом в АСУ ТП,	-
Злоумышленник подключился к внутренней сети напрямую	Проникнув на объект или обнаружив коммуникации (провода, кабели) вне контролируемой зоны, злоумышленник имеет возможность подключиться к внутренней сети напрямую и развить атаку дальше.	Зависит от того, какие аппаратные СЗИ используются для обеспечения безопасности передаваемой информации.	-

Заключение

- Разработана мтодология сбора данных для выявления кибератак и аномалий в процессах очистки сточных вод.
- Разработана модель киберфизического стенда технологического процесса очистных сооружений для моделирования кибератак и выявления киберрисков, собран стенд.
- Разработана модель атак для систем очистки сточных вод.
- Разработаны сценарии атак для систем очистки сточных вод.

Следующие шаги

- Сбор данных в нормальном режиме функционирования стенда.
- Проведение атак (на основе модели на слайде 16 и сценариев на слайдах 17-18).
- Сбор данных в аномальном режиме функционирования стенда.
- Валидация данных.
  - Необходима для подтверждения, что собранный набор данных отражает реальное поведение систем очистки сточных вод и может использоваться для разработки методик выявления аномалий и кибератак.

Спасибо за внимание!

Контактная информация:

Елена Владимировна Федорченко: doynikova@comsec.spb.ru

Сайт лаборатории: http://comsec.spb.ru/

Финансовая поддержка проекта: Грант Российского научного фонда № 23-11-20024 и Санкт-Петербургского научного фонда.