УДК 004.056.57

МЕТОДОЛОГИЯ СБОРА ДАННЫХ ДЛЯ АНАЛИЗА БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Котенко И.В. [1], Федорченко Е.В.[2], Новикова Е.С.[3], Саенко И.Б.[4], Данилов А.С.[5]

Цель исследования: *формирование методологии сбора и формирования наборов данных, используемых для разработки и тестирования эффективности подходов к выявлению аномалий и кибератак на основе машинного обучения, в т.ч. с применением моделей глубокого обучения.*

Методы исследования: *методы системного анализа и моделирования, машинное обучение, статистический анализ данных.*

Полученные результаты: *исследованы и систематизированы подходы к формированию обучающих наборов данных, используемых для разработки методов обнаружения аномалий и кибератак. Разработана методология сбора данных для анализа безопасности промышленных киберфизических систем, ключевые этапы проиллюстрированы на примере построения тестового стенда системы водоочистных сооружений, предназначенного для исследования ее защищенности от кибератак.*

Научная новизна: *представленная в работе методология специфицирует последовательность взаимосвязанных этапов, которые определяют действия, начиная от формализации промышленного процесса, заканчивая валидацией полученных данных. Последовательное выполнение этих этапов позволяет создавать наборы данных, которые содержат как сетевые данные, так и показания датчиков и актуаторов киберфизических систем, имеют четкую схему аннотирования и валидированы относительно реальных данных, обрабатываемых в подобных системах.*

Вклад: *Котенко И.В. и Федорченко Е.В. – общая концепция методологии сбора данных для исследования безопасности киберфизических систем; Котенко И.В., Федорченко Е.В. и Новикова Е.С. – проработка этапов методологии; Новикова Е.С. и Федорченко Е.В. – анализ положения дел по созданию обучающих наборов данных для разработки и тестирования аналитических моделей выявления аномалий и кибератак; Данилов А.А. и Саенко И.Б. – формализация флотационного процесса очистки воды и разработка тестового стенда в соответствии с формулированными требованиями к обучающему набору данных.*

Ключевые слова: *кибербезопасность, автоматизированные системы управления, выявление аномалий и кибератак, обучающие наборы, тестовый стенд, системы водоочистных сооружений.*

DOI:10.21681/2311-3456-2023-5-69-79

Введение

Анализ положения дел в области формирования наборов данных, используемых для оценки кибербезопасности промышленных систем показал, что в настоящее время отсутствует единая комплексная методология сбора данных и их валидации для тестирования методик обнаружения аномалий и кибератак на основе машинного обучения.

В настоящее время задача обнаружения аномалий и кибератак в промышленных киберфизических системах хорошо исследована [1, 2], и в научной литерату-

1 Котенко Игорь Витальевич, заслуженный деятель науки РФ, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: ivkote@comsec.spb.ru

2 Федорченко (Дойникова) Елена Владимировна, кандидат технических наук, старший научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: doynikova@comsec.spb.ru

3 Новикова Евгения Сергеевна, кандидат технических наук, доцент, старший научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: novikova@comsec.spb.ru

4 Саенко Игорь Борисович, доктор технических наук, профессор, ведущий научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: ibsaen@comsec.spb.ru

5 Данилов Александр Сергеевич, кандидат технических наук, доцент кафедры геоэкологии, Санкт-Петербургский Горный университет, старший научный сотрудник ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) г. Санкт-Петербург, Россия. E-mail: aleksandrsdanilov@gmail.com

ре представлено большое число различных подходов к ее решению. Предложены методы на основе статистического анализа данных, анализа временных рядов [3, 4], на основе классического машинного обучения [5], и в последнее время активно исследуется применимость методов глубокого обучения [6-8]. Например, в [6] предложен подход к обнаружению и прогнозированию аномалий в потоках данных от промышленных систем с помощью рекуррентной сверточной нейронной сети с блоками долгой краткосрочной памяти (Long Short Term Memory, LSTM). В [7] был выполнен анализ различных архитектур глубоких нейронных сетей для обнаружения аномалий на примере реальных данных от датчиков промышленного лифта. Проведенные эксперименты показали, что эффективность обнаружения аномалий на несбалансированных данных достигает 0,899% для случая, когда в обучающем наборе содержится 3% аномальных данных, и 0,984% для случая, когда в тестовом наборе данных содержится 20% аномальных данных. В [8] представлена нейронная сеть с механизмом внимания, она состоит из энкодера, который кодирует входные многомерные данные временного ряда с помощью многослойных связанных модулей внимания, и двух декодеров, выполняющих операции по прогнозированию и реконструкции временных рядов. Исчерпывающий обзор подходов глубокого обучения к обнаружению атаки аномалий в киберфизических системах (КФС) можно найти в [9, 10].

Однако эффективное применение методов глубокого обучения для обнаружения аномалий связано с выполнением двух практических условий: наличие значительных вычислительных ресурсов и наличие больших объемов хорошо подготовленных данных. Под хорошо подготовленными данными подразумевается данные большого объема, которые имеют достоверную разметку. Разметка включает информацию об аномалиях или об их отсутствии.

В работе [11] авторы проанализировали наиболее часто используемые наборы данных, применяемые в исследованиях по обнаружению аномалий в киберфизических системах, и сформулировали основные требования к наборам данным, которые могут быть использованы в исследованиях кибербезопасности таких систем:

- набор данных должен включать данные от физических и цифровых компонентов киберфизической системы, т.е. включать данные сетевого трафика и журналы датчиков и актуаторов;
- набор данных должен иметь разметку, схема аннотации должна включать метки «норма» и/или «аномалия», аномалии и атаки должны быть описаны;
- набор данных должен быть максимально приближен к реальным данным, как с точки зрения моделируемых технологических процессов, так и выполняемых кибератак на систему.

Для исследования безопасности киберфизических систем и формирования соответствующих наборов данных, могут быть использованы следующие типы тестовых стендов [12]: виртуальные, аппаратные и гибридные.

Виртуальные стенды используют только методы программного моделирования и аппаратной эмуляции для моделирования работы промышленных устройств и сетевого взаимодействия между ними. Очевидным преимуществом таких стендов является низкая стоимость их разработки. Однако моделирование сложных процессов представляет собой нетривиальную задачу, и в результате программные имитаторы технологических процессов могут быть менее точными и надежными, чем их физические реализации. Пример такого стенда – виртуальный стенд, описанный в [13]. В ней моделируется небольшая электрическая сеть, состоящая из одной основной питающей ветви и трех подветвей – A, B и C. Данные от системы автоматизированного контроля и сбора данных (Supervisory Control and Data Acquisition, SCADA-системы) создаются с помощью специализированной “песочницы” SCADA-системы, кибератаки выполняются в реальности и имитируют кибератаки, совершенные на энергосистему Украины в декабре 2015 года.

Физические стенды разрабатываются с использованием реальных аппаратных и программных средств, применяемых в промышленных системах. Генерируемые с их помощью данные отличаются реалистичностью, кроме того, уязвимости конкретных устройств могут быть использованы для реализации кибератак. Примером такого стенда является стенд водоочистных сооружений SWaT [14].

Гибридные стенды представляют собой комбинацию программно-эмулируемых компонентов и физических устройств. Такой подход является компромиссным решением между дорогостоящими физическими стендами и более дешевыми, но иногда недостаточно реалистичными виртуальными стендами. Примером такого стенда является стенд HAI [15], в котором моделируются четыре различных процесса, три из которых реализуются с помощью программно-аппаратных средств, а четвертый является полностью программной моделью.

УДК 004.056.57

Разработка тестового промышленного стенда и, соответственно, формирование набора данных является сложной практической задачей [12, 16] в связи с наличием следующих проблем и ограничений:

- отсутствием единых рекомендаций по проектированию стендов площадок и формированию наборов данных;
- необходимостью реализацией реальных сценариев как на технологическом уровне, включающем программные и аппаратные средства, так и на уровне атак, заключающемся в моделировании атак, характерных для заданного промышленного процесса/системы;
- сложностью современных технологических процессов, что обусловливает необходимость участия в разработке стенда как специалистов в области промышленной автоматизации, в области моделируемых технологических процессов, так и в области кибербезопасности;
- масштабируемостью тестового стенда, поскольку, как правило, тестовые площадки моделируют некоторую упрощенную версию технологического процесса;
- сбором данных, включающем сбор как нормальных, так и аномальных данных;
- стоимостью в случае физических стендов;
- физической безопасностью в случае физических стендов, поскольку не все технологические процессы могут быть безопасно смоделированы в лабораториях в уменьшенном варианте;
- отсутствием документации;
- возможностью воспроизвести разработанные стенды, которая практически невозможна для физических стендов и очень ограничена для гибридных стендов.

В данной работе решается проблема, связанная с отсутствием единых рекомендаций по проектированию. Таким образом, новизна статьи и вклад авторов заключается в представленной методологии создания наборов данных, применимых для исследований в области кибербезопасности промышленных систем. В качестве примера авторы представляют макет стенда, разработанного для анализа защищенности системы управления водоочистными сооружениями.

Методология формирования набора данных

Предлагаемая методология создания наборов данных основывается на выполнении следующих этапов:

- определение технологического процесса;
- разработка соответствующего тестового стенда;
- формирование набора данных, соответствующих нормальному функционированию системы;
- разработка модели атак на рассматриваемый технологический процесс;
- разработка сценариев атакующих действий с учетом технологического стека, используемого для развертывания тестовой площадки;
- реализация атаки и сбор массива данных для атакуемой системы;
- валидация набора данных.

Рассмотрим данные этапы более подробно.

Определение технологического процесса. Данный этап предполагает определение технологического процесса и набора параметров, которые будут собираться во время экспериментов.

Технологический процесс может быть представлен в виде технологической схемы, которая описывает выполняемую последовательность технологических операций, в т.ч. графически в виде мнемосхем. На этом этапе определяются, какие параметры значимы для безопасного и эффективного выполнения заданного технологического процесса, а какими можно пренебречь. На их основе формируется перечень датчиков и актуаторов, необходимых для построения тестовой системы, и данные от этих устройств будут описывать технологический процесс на физическом уровне.

На этом этапе также определяется математическая модель процесса, если планируется использовать виртуальный или гибридный тестовый стенд. Формализованная модель технологического процесса также позволит определить возможные последствия атакующих действий с учетом связей между датчиками и исполнительными устройствами.

Создание тестового стенда. На этом же этапе определяется тип тестового стенда: гибридный, виртуальный или физический. В зависимости от типа стенда прорабатываются детали его реализации: определяется программное обеспечение для моделирования и эмуляции оборудования в случае виртуальной и гибридной тестовой площадки, выбираются сенсоры, датчики и соответствующее программное обеспечение для их подключения в случае физического стенда. Определяются протоколы взаимодействия между устройствами, а также механизмы автоматизированного сбора данных и управления. Специфицируется формат собираемых данных и интервал их получения, исходя их технических характеристик используемого программного и аппаратного обеспечения.

Другой важной задачей является выявление ключевых отличий технологических процессов, реализуе-

мых на тестовом стенде, от реальной системы: в частности, определяется, как влияет масштабирование и упрощение системы на ее функционирование, какие критические моменты необходимо учитывать при разработке аналитических моделей безопасности, предназначенных для реальных систем.

На этом этапе готовится документация по моделируемому технологическому процессу и разработанной экспериментальной площадке, она включает схему технологического процесса, детали аппаратной и программной реализации, доступные источники данных и их формат. Для виртуального стенда подготавливаются рекомендации по его воспроизводимости.

Формирование набора данных, соответствующих нормальному функционированию системы. Этот этап заключается в сборе данных с датчиков и сетей за определенный промежуток времени. Интервал времени определяется специалистом предметной области с учетом переходного периода, необходимого для достижения системой нормального рабочего состояния. Сбор данных должен осуществляться с использованием инструментов и механизмов, определенных на предыдущем этапе. Подготавливается документация, касающаяся продолжительности функционирования стенда, его особенностей, например, переходного периода.

Разработка модели атак на рассматриваемый технологический процесс. Этот этап включает в себя определение модели атакующего, его возможностей. Таким образом, необходимо определить объем ресурсов, доступных злоумышленникам, и их осведомленность об атакуемой системе.

Кибератаки могут осуществляться как на сетевом, так и на физическом уровне и могут включать в себя различные типы атак. Однако они должны коррелировать с выбранным технологическим процессом и быть максимально похожими на реальные случаи. К наиболее распространенным сетевым атакам относятся атаки сбора данных (разведки), атака «человек посередине» (MitM), атака с вбросом ложных данных или команд (False Data Injection), атака повторного воспроизведения (Replay Attack) и атака “отказ в обслуживании” (DoS-атака). Атаки на физическом уровне направлены на физические устройства и имеют целью изменение их показаний (Device Manumission Attack) или их физическое повреждение (Direct Damage Attack). Учитывая многообразие возможных атакующих действий, рекомендуется сформировать упрощенную формальную модель, связывающую скомпрометированные датчики и ожидаемый результат атаки в виде изменений в функционировании системы. Такая формализация полезна при оценке эффективности атак. Информация о модели злоумышленника и атаках должна быть включена в документацию.

Разработка сценариев атакующих действий с учетом технологического стека экспериментального стенда. Технологический стек, включающий протоколы сетевого взаимодействия, систему SCADA и настройки контроля доступа на рабочей станции оператора, определяет выбор средств и методов атаки.

При использовании SCADA-систем рекомендуется проводить атаки непосредственно на инфраструктуру тестового стенда, что обеспечивает максимальную точность определения времени атаки и реакции системы на нее [13].

На этом этапе также необходимо определить, каким образом будет фиксироваться процесс выполнения атаки для получения размеченных данных, а также определен формат протокола фиксации атакующих действий. Обычно этот процесс реализуется вручную. В протокол необходимо включить следующую информацию об атаке: точка входа атаки (IP-адрес), цели атаки (атакующий IP-адрес, датчик), тип атаки, времени начала и окончания атаки, используемые программного-аппаратные средства, наблюдаемые изменения в работе системы. Для автоматизированного разбора протокола атак, рекомендуется хранить их в формате JSON[6].

Реализация атак и сбор массива данных для атакуемой системы. Данный этап заключается в проведении кибератак, фиксации их реализации и записи результатов. Частота выполняемых атакующих действий должна быть определена с учетом времени реакции системы на воздействие, поскольку это позволит избежать наложения реакции системы на разные виды атак, возникновению аномальных периодов функционирования системы, не связанных с выполнением атакующих действий.

Наблюдаемые изменения в работе стенда могут быть получены путем анализа данных с сервера-историка SCADA. Подготовленная на этом этапе документация включает заполненные протоколы атак.

Валидация набора данных по имеющимся реальным данным. В настоящее время не существует устоявшихся процедур проверки и валидации сгенерированных наборов данных. Однако проверка набора данных может быть проведена через проверку выбранного тестового стенда, т.е. на основе оценки

6 https://javaee.github.io/tutorial/jsonp001.html

Рис. 1. Основные этапы методологии сбора данных для анализа защищенности киберфизических систем

соответствия реализованной модели технологического процесса и реального процесса. В случае доступа к реальным данных от подобных систем валидация набора данных может быть осуществлена путем статистического анализа данных на основе оценки корреляции между параметрами искусственного и реального наборов данных, и относительной энтропии между двумя наборам.

На рис. 1 представлены этапы предложенной методологии и промежуточные результаты каждого этапа.

В следующем разделе представлена реализация двух этапов предлагаемой методологии.

Разработка тестового стенда для моделирования процессов очистки воды

Определение технологического процесса. В качестве примера технологического процесса очистки воды был выбран процесс флотации. Данный процесс является одним из наиболее современных и безопасных методов очистки сточных вод и относится к механическим процессам очистки воды. Для него характерна высокая способность удалять жировые отложения из воды, что исключает необходимость устранения засоров в трубах на выходе очищенной воды. Он недорог в эксплуатации и надежен, поскольку все элементы флотационной установки представляют собой простые механизмы. Флотационный процесс также обладает высокой скоростью очистки воды от органических загрязнений (по сравнению с отстаиванием воды) и эффективно снижает количество болезнетворных бактерий, ПАВ и легко окисляемых веществ и микропластика [17]. Благодаря этим факторам данный процесс водоочистки часто используется в составе городских систем водоподготовки.

Процесс флотационной очистки воды состоит из двух основных этапов: 1) процесс флокуляции; 2) про-

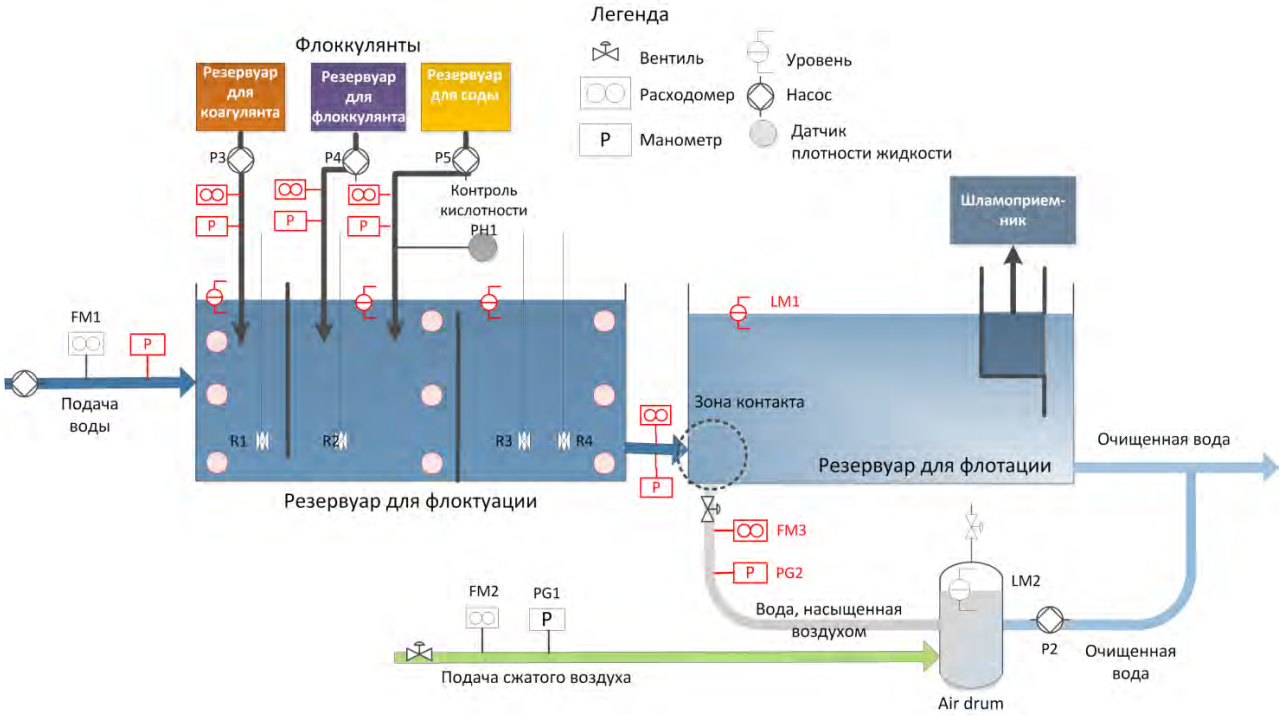

Рис. 2. Технологическая схема процесса флотации

цесс флотации. Упрощенная схема технологического процесса представлена на рис. 2.

Флокуляция является предварительным этапом флотации. Она заключается в объединении тонкодисперсных твердых частиц в более крупные агломераты. Такие агломераты более эффективно удаляются из воды, чем мелкие частицы. Процесс флокуляции происходит в трехкамерном резервуаре для флокуляции (рис. 2) и включает несколько подпроцессов: коагуляцию, непосредственно флокуляцию и созревание флокулы и регулирование уровня кислотности (pH).

Процесс коагуляции инициируется коагулянтами, объем добавляемых реагентов контролируется насосами для их подачи, четыре погружные мешалки перемешивает воду с коагулянтами. В первой камере резервуара формируются микрофлокулы. Во второй камере подается флокулянт и сода, которые перемешиваются с водой и микрофлокулами, постоянно увеличивающимися в размерах. Необходимая эффективная концентрация коагулянта – флокулянта и соды – зависит от соотношения скорости подачи воды, определяемой насосом P1, и скорости дозирования коагулянтов, которые контролируются насосами-дозаторами (P3, P4, P5). Затем суспензия с крупными флокулами поступает в третью камеру резервуара для флокуляции. В этой камере мешалки R3 и R4 препятствуют осаждению флокулы, постоянно перемешивая воду. Скорость их вращения должна быть несколько ниже скорости вращения мешалок в первых двух камерах, чтобы предотвратить разрушение флокулы. Коагулянт имеет низкое значение кислотности, что может снизить эффективность флокуляции. По этим причинам необходимо контролировать уровень pH в емкости для флокуляции.

Из резервуара для флокуляции грязная вода через зону контакта поступает в резервуар для флотации. Смесь воды и пузырьков воздуха подается в резервуар для флотации через три отверстия в зоне контакта. Образование мелких воздушных пузырьков является важной составляющей процесса флотации. Мелкие пузырьки получаются за счет снижения давления: воздух, растворенный в воде под высоким давлением, переходит в газообразное состояние за счет быстрой декомпрессии. Для образования пузырьков используется чистая вода, получаемая на выходе, и которая подается обратно в систему под давлением с помощью насоса P2.

Время контакта флокулы с воздухом зависит от соотношения скоростей подачи загрязненной и очищенной воды. Пузырьки воздуха обволакивают флокулу, в результате плотность агломератов, связанных с воздухом, становится меньше плотности воды во флотационном резервуаре, и они всплывают на поверхность воды. Грязная пена с поверхности резервуара

для флотации удаляется скребком в шламоприемник, а очищенная вода выходит через правый нижний угол резервуара.

Математическое описание этого процесса достаточно сложно, оно требует рассмотрения гидродинамических процессов с большим числом управляющих, и контролируемых переменных с учетом физико-химического взаимодействия [18], поэтому в данном случае было решено разрабатывать физический стенд.

Создание экспериментального стенда. Основой для экспериментального стенда послужил учебный стенд CE 587 (G.U.N.T., GmbH, Германия). Он оснащен следующими датчиками:

- подача воды на установку - датчики используются в реальной системе водоочистки для контроля объема воды: расходомер воды FM1, устанавливаемый после насоса P1, расходомер давления внутри насоса P2, расходомер перед входным резервуаром (после насосов P2 и P6);
- коагуляция — расходомер воды FM1 перед резервуаром флокуляции;
- флокуляция - нет датчиков;
- созревание флокул - расходомер воздуха FM2 и манометр PG1 перед воздушным барабаном, измеритель уровня воды LM2 устройства генерации пузырьков, измеритель давления внутри насоса P2;
- контроль уровня кислотности pH: датчик кислотности PH1.

На рис. 2 эти датчики отмечены черным цветом.

Учебный стенд CE 587 имеет весьма ограниченные возможности контроля и управления технологическим процессом. Блок управления стенда достаточно прост, он позволяет включать/выключать насосы P1, P2, P3, P4 и P5, мешалки R1-R4 (см. рис. 2), задавать параметры скорости вращения мешалок, однако настройки управления всех задаются непосредственно на устройства. Централизованный модуль управления процессом и модуль сбора данных отсутствуют. С целью автоматизации процесса управления и сбора информации было предложено: 1) расширить набор датчиков; 2) дополнить учебный стенд SCADA-системой, осуществляющей управление компонентами стенда и сбор данных.

Для дальнейшего анализа данных авторы предлагают расширить набор датчиков следующими датчиками:

- подача воды на установку - датчик уровня, измеритель давления после водохранилища;
- коагуляция — датчики плотности жидкости на разных уровнях резервуара для флокуляции в первой камере (верхний, нижний, средний), расходомер и манометр после насоса P3, расходомер в первой камере резервуара для флокуляции, датчик уровня;
- флокуляция — датчики плотности на разных уровнях резервуара для флокуляции во второй камере (сверху, снизу, посередине), расходомер и измеритель давления после насоса P4, расходомер во второй камере резервуара для флокуляции;
- созревание флокул — уровнемер, измеритель давления в резервуаре для флокуляции, расходомер и измеритель давления перед резервуаром для флокуляции;
- контроль pH — датчики плотности на разных уровнях резервуара для флотации в третьей камере (верхний, нижний, средний), расходомер и измеритель давления после насоса P5, расходомер в третьей камере резервуара для флокуляции.

На рис. 2 новые датчики выделены красным цветом.

Расширение тестового стенда включает в себя не только добавление новых датчиков, но и компонентов, которые объединяют их в единую систему: нормализаторов сигналов для аналоговых датчиков, программируемого логического контроллер (ПЛК) и всех необходимых модулей его расширения для подключения датчиков и актуаторов, OPC сервера (Open Platform Communication, OPC), базы данных архив и пульта управления оператора.

Программируемый логический контроллер – это микропроцессорные электронные устройства реального времени, которые соединяют между собой датчики и исполнительные механизмы, реализуют логику технологического процесса, передают данные и получают команды от оператора процесса. Датчики и исполнительные устройства могут подключаться непосредственно к цифровым или аналоговым входам/выходам ПЛК, обычно ПЛК поддерживает различные модули расширения, позволяющие подключать различные типы устройств и использовать различные протоколы связи, такие как RS-232, CAN, Modbus и Industrial Ethernet. В качестве ПЛК может выступать отладочная плата Arduino Mega 2560 R3, однако для приближения тестового стенда к реальным системам управления водоочистными сооружениями будет использован промышленный контроллер.

OPC-технология – это набор принятых во всем мире спецификаций, обеспечивающих универсальный механизм обмена данными в промышленных

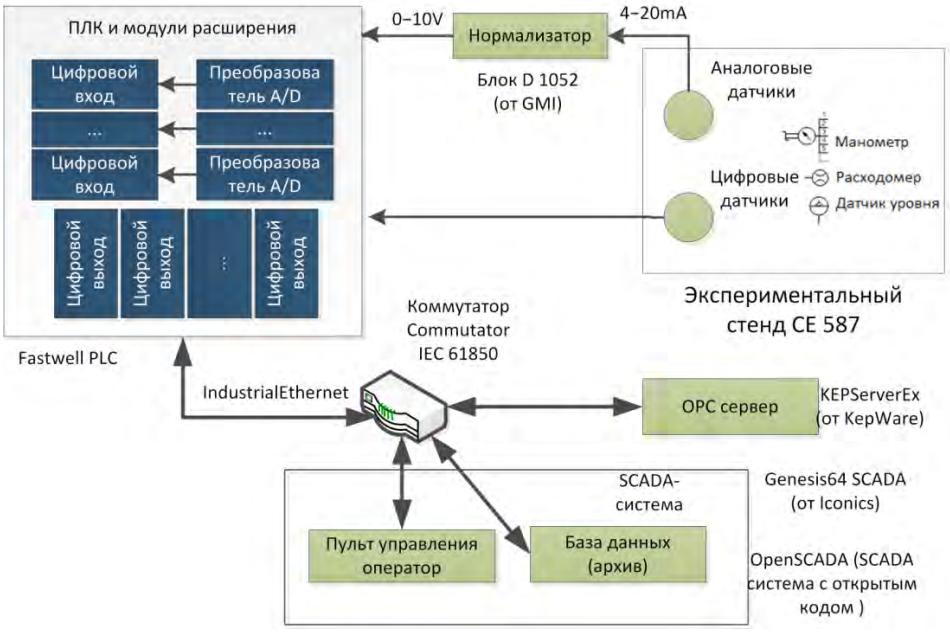

Рис. 3. Программно-аппаратное расширение учебного стенда CE 587 (G.U.N.T., GmbH, Германия)

системах управления, OPC-сервер – это программа, которая получает данные во внутреннем формате устройства или системы и преобразует их в формат OPC. Таким образом, OPC-сервер – это своего рода универсальный драйвер физического оборудования, который обеспечивает взаимодействие с любым OPC-клиентом, причем любые изменения в программных решениях на уровне OPC-клиентов не приводят к изменениям в контролируемом оборудовании.

Для организации хранения данных и мониторинга состояния тестового стенда естественным решением является использование SCADA-системы, которая собирает, обрабатывает и хранит данные, поступающие от ПЛК; предоставляет текущую и архивную информацию в удобной для оператора форме (мнемосхемы, графики, тренды, журналы сообщений); предоставляет утилиты для ввода команд оператора и передачи их в ПЛК; поддерживает отчетность по результатам технологического процесса. На рис. 3 показано предлагаемое расширение флотационного стенда CE 587 с соответствующими программными и аппаратными решениями.

Заключение

В последнее время для обнаружения атак и аномалий в промышленных киберфизических системах было предложено большое число методов, в основе которых лежат модели машинного обучения, включая глубокие нейронные сети. Однако их применение требует наличия реалистичных размеченных обучающих наборов данных. Формирование подобных наборов данных представляет собой сложную практическую задачу, и одной из причин, обуславливающих ее сложность, является отсутствие единых рекомендаций по их созданию.

В данной статье авторы решают эту проблему и предлагают методологию создания размеченных наборов данных для исследования кибербезопасности промышленных систем. Для иллюстрации разработанной методологии подробно рассмотрены первые два этапа - проектирование и создание тестового стенда водоочистных сооружений.

Будущие работы включают реализацию дальнейших этапов методики и создание самого набора данных.

Благодарность. *Работа выполнена при поддержке гранта Российского научного фонда № 23-11-20024, https://rscf.ru/project/23-11-20024/, и Санкт-Петербургского научного фонда.*

Рецензент: *Лаута Олег Сергеевич, доктор технических наук, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, Санкт-Петербург, Россия.*

E-mail: laos-82@yandex.ru

Литература

1. Котенко И.В., Ушаков И.А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд, № 3, 2017. С. 23-33.
2. Котенко И.В., Левшун Д.С., Чечулин А.А., Ушаков И.А., Красов А.В. Комплексный подход к обеспечению безопасности киберфизических систем на системе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29-38. DOI: 10.21681/2311-3456-2018-3-29-38.
3. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6 (98). С. 64-71. DOI: 10.22184/2070-8963.2021.98.6.64.70.
4. Котенко В.И., Саенко И.Б., Коцыняк М.А., Лаута О.С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей // Труды СПИИРАН. 2017. № 6(55). С. 160-184. DOI: 10.15622/sp.55.7.
5. Branitskiy A., Kotenko I., Saenko I. Applying Machine Learning and Parallel Data Processing for Attack Detection in IoT // IEEE Transactions on Emerging Topics in Computing, 2021, vol. 9, no. 4, pp. 1642-1653. DOI: 10.1109/TETC.2020.3006351.
6. Wu Z., Guo Y., Lin W., Yu S., Ji Y. A weighted deep representation learning model for imbalanced fault diagnosis in cyber-physical systems // Sensors, vol. 18, no. 4, 2018, 1096. DOI: 10.3390/s18041096.
7. Canizo M., Triguero I., Conde A., Onieva E. Multi-head CNN–RNN for multi-time series anomaly detection: An industrial case study // Neurocomputing, vol. 363, pp. 246-260, 2019, pp. 246-260. DOI: 10.1016/j.neucom.2019.07.034.
8. Xia F., Chen X., Yu S., Hou M., Liu M., and You L. Coupled attention networks for multivariate time series anomaly detection // Arxiv. 2023. URL: https://arxiv.org/pdf/2306.07114.pdf (дата обращения: 29.08.2023).
9. Luo Y., Xiao Y., Cheng L., Peng G., Yao D. D., Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities // ACM Comput. Surv., 2021, vol. 54, no. 5, Article 106, 36 p. DOI: 10.1145/3453155.
10. Kotenko I., Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods // IEEE Access, 2022, vol. 10, pp. 43387-43420. DOI: 10.1109/ACCESS.2022.3168976.
11. Tushkanova O., Levshun D., Branitskiy A., Fedorchenko E., Novikova E., Kotenko I. Detection of cyber attacks and anomalies in cyber-physical systems: approaches, data sources, evaluation // Algorithms, vol. 16, no. 2, 2023, 85. DOI: 10.3390/a16020085.
12. Conti M., Donadel D., Turrin F. A survey on industrial control system testbeds and datasets for security research // IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2248–2294, 2021.
13. Lemay A., Fernandez J. M. Providing SCADA network data sets for intrusion detection research // 9th Workshop on Cyber Security Experimentation and Test (CSET 16). Austin, TX: USENIX Association, Aug. 2016.
14. Goh J., Adepu S., Junejo K. N., Mathur A. A dataset to support research in the design of secure water •treatment systems // Critical Information Infrastructures Security. Cham: Springer International Publishing, 2017, pp. 88–99. DOI: 10.1007/978-3-319-71368-7_8.
15. Shin H.-K., Lee W., Yun J.-H., Kim H. HAI 1.0: HIL-based augmented ICS security dataset // Proceedings of the 13th USENIX Conference on Cyber Security Experimentation and Test, 2020, pp. 1–1.
16. Dominguez M., Fuertes J.J., Prada M.A., Alonso S., Moran A., Perez D. Design of platforms for experimentation in industrial cybersecurity // Applied Sciences, vol. 12, no. 13, 2022, 6520. DOI: 10.3390/app12136520.
17. Kyzas G.Z., Matis K.A. Flotation in water and wastewater treatment // Processes, vol. 6, no. 8, 2018, 116. DOI: 10.3390/pr6080116.
18. Антонова Е.С. Моделирование процесса очистки сточных вод во флотационной установке с эжекционной системой аэрации с диспергатором // Безопасность в техносфере. 2017. №. 1. С. 43-50. DOI: 10.12737/article590199b9952dc2.23575176 (дата обращения: 29.08.2023).

DATA COLLECTION METHODOLOGY FOR SECURITY ANALYSIS OF INDUSTRIAL CYBER-PHYSICAL SYSTEMS

Kotenko I.V.[7], Fedorchenko E.V.[8], Novikova E.S.[9], Saenko I.D.[10], Danilov A.S.[11]

7 Igor V. Kotenko, Honored Worker of Science of the Russian Federation, Dr.Sc., Professor, Chief Scientist and Head of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: ivkote@comsec.spb.ru

8 Elena V. Fedorchenko, Ph.D., Senior researcher of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: doynikova@comsec.spb.ru

9 Evgenia S. Novikova, Ph.D., Associate Professor, Senior researcher of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: novikova@comsec.spb.ru

10 Igor B. Saenko, Dr.Sc., Professor, Leading researcher of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: ibsaen@comsec.spb.ru

11 Aleksandr S. Danilov, Ph.D., Associate Professor of Geoecology department at St. Petersburg Mining University, Senior researcher of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: aleksandrsdanilov@gmail.com

The purpose of the study: *formation of methodology for collecting and generating datasets used to develop and test the effectiveness of anomaly and cyber attack detection approaches based on machine learning, including deep learning models.*

Research methods: *methods of system analysis and modeling, machine learning, statistical data analysis.*

Results obtained: *approaches to the formation of training data sets used for the development of anomaly and cyber attack detection methods were investigated and systematized. The methodology of data collection for analyzing the security of industrial cyber-physical systems is developed, the key stages are illustrated on the example of building a test bench of a water treatment plant system designed to study its security against cyber attacks.*

Scientific novelty: *The analysis of the state of arts in the field of forming datasets used to assess the cyber security of industrial systems has shown that there is currently no unified methodology for data collection and validation for testing anomaly and cyber attack detection techniques based on machine learning. The methodology presented in this paper specifies a sequence of interrelated steps that define actions ranging from the formalization of the industrial process to the validation of the acquired data. The sequential execution of these steps will allow the creation of datasets that contain both network data and readings from sensors and actuators of the cyber-physical system, have a clear annotation scheme and are validated against real data from similar systems.*

Contribution: *Igor Kotenko and Elena Fedorchenko - general concept of data collection methodology for cyber-physical systems security research; Igor Kotenko, Elena Fedorchenko and Evgenia Novikova - elaboration of methodology stages; Evgenia Novikova and Elena Fedorchenko - analysis of the state of affairs on the creation of training data sets for the development and testing of analytical models of anomaly and cyber attack detection; Aleksandr Danilov and Igor Saenko - formalization of the flotation process of water treatment development and development of a test bench in accordance with the formulated requirements for the training data set.*

Keywords: *cyber security, automated control systems, anomaly and cyber attack detection, training sets, test bed, water treatment facilities.*

References

1. Kotenko I.V., Ushakov I.A. [Big data technologies for monitoring computer security] Технологии больших данных для мониторинга компьютерной безопасности. Information security. Inside [Защита информации. Инсайд], No. 3, 2017. pp. 23-33.
2. Kotenko I.V., Levshun D.S., Chechulin A.A., Ushakov I.A., Krasov A.V. [Integrated approach to provide security of cyber-physical systems based on microcontrollers] Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров. Cybersecurity issues [Вопросы кибербезопасности]. 2018. No 3 (27). pp.29-38. DOI: 10.21681/2311-3456-2018-3-29-38.
3. Kotenko I., Saenko I., Lauta O., Kribel. [A method for early detection of cyberattacks based on the integration of fractal analysis and statistical methods] Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов. Pervaya milya [Первая миля]. 2021. № 6 (98). pp. 64-71. DOI: 10.22184/2070-8963.2021.98.6.64.70
4. Kotenko V.I., Saenko I.B., Kotsynyak M.A., Lauta O.S. [Assessment of Cyber-Resilience of Computer Networks based on Simulation of Cyber Attacks by the Stochastic Networks Conversion Method] Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей. SPIIRAS Proceedings [Труды СПИИРАН]. 2017. No 6(55). pp.160-184. DOI: https://doi.org/10.15622/sp.55.7.
5. Branitskiy A., Kotenko I., Saenko I. Applying Machine Learning and Parallel Data Processing for Attack Detection in IoT // IEEE Transactions on Emerging Topics in Computing, 2021, vol. 9, no. 4, pp. 1642-1653. DOI: 10.1109/TETC.2020.3006351.
6. Wu Z., Guo Y., Lin W., Yu S., Ji Y. A weighted deep representation learning model for imbalanced fault diagnosis in cyber-physical systems. Sensors, vol. 18, no. 4, 2018, 1096. DOI: 10.3390/s18041096.
7. Canizo M., Triguero I., Conde A., Onieva E. Multi-head CNN–RNN for multi-time series anomaly detection: An industrial case study. Neurocomputing, vol. 363, pp. 246–260, 2019, pp. 246-260. DOI: 10.1016/j.neucom.2019.07.034.
8. Xia F., Chen X., Yu S., Hou M., Liu M., You L. Coupled attention networks for multivariate time series anomaly detection. Arxiv. 2023. URL: https: arxiv.org/pdf/2306.07114.pdf (accessed on: 29.08.2023).
9. Luo Y., Xiao Y., Cheng L., Peng G., Yao D.D., Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. ACM Comput. Surv., 2021. vol. 54, no. 5, Article 106, 36 p. DOI: 10.1145/3453155.
10. Kotenko I, Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods. IEEE Access, 2022, vol. 10, pp. 43387-43420. DOI: 10.1109/ACCESS.2022.3168976.
11. Tushkanova O., Levshun D., Branitskiy A., Fedorchenko E., Novikova E., Kotenko I. Detection of cyber attacks and anomalies in cyber-physical systems: approaches, data sources, evaluation. Algorithms, vol. 16, no. 2, 2023, 85. DOI: 10.3390/a16020085.
12. Conti M., Donadel D., Turrin F. A survey on industrial control system testbeds and datasets for security research. IEEE Communications

Surveys & Tutorials, vol. 23, no. 4, pp. 2248-2294, 2021.
13. Lemay A., Fernandez J.M. Providing SCADA network data sets for intrusion detection research. 9th Workshop on Cyber Security Experimentation and Test (CSET 16). Austin, TX: USENIX Association, Aug. 2016.
14. Goh J., Adepu S., Junejo K.N., Mathur A.A dataset to support research in the design of secure water treatment systems. Critical Information Infrastructures Security. Cham: Springer International Publishing, 2017, pp. 88-99. DOI: 10.1007/978-3-319-71368-7_8.
15. Shin H.-K., Lee W., Yun J.-H., Kim H. HAI 1.0: HIL-based augmented ICS security dataset. Proceedings of the 13th USENIX Conference on Cyber Security Experimentation and Test, 2020, pp. 1–1.
16. Dominguez M., Fuertes J.J., Prada M.A., Alonso S., Moran A., Perez D. Design of platforms for experimentation in industrial cybersecurity. Applied Sciences, vol. 12, no. 13, 2022, 6520. DOI: 10.3390/app12136520.
17. Kyzas G.Z., Matis K.A. Flotation in water and wastewater treatment. Processes, vol. 6, no. 8, 2018, 116. DOI: 10.3390/pr6080116.
18. Antonova E.S. [Modeling of wastewater treatment process in a flotation plant with an induction aeration system with dispersant] Моделирование процесса очистки сточных вод во флотационной установке с эжекционной системой аэрации с диспергатором. Bezopsnost' v technosphere [Безопасность в техносфере]. 2021. № 6 (98). p. 64-71. DOI: 10.22184/2070-8963.2021.98.6.64.70