УДК 004.056 **DOI** 10.15622/ia.25.3.9

И.Б. Саенко , Е.С. Новикова , А.В. Мелешко , В.Е. Садовников

ОНТОЛОГИЧЕСКИЙ ПОДХОД К УПРАВЛЕНИЮ РИСКАМИ В СИСТЕМЕ УПРАВЛЕНИЯ ОЧИСТНЫМИ СООРУЖЕНИЯМИ

Саенко И.Б., Новикова Е.С., Мелешко А.В., Садовников В.Е. **Онтологический подход к управлению рисками в системе управления очистными сооружениями.**

Аннотация. Современные системы управления технологическими процессами на критически важных объектах инфраструктуры, включая очистные сооружения, всё чаще становятся мишенью сложных кибератак, способных нарушить экологическую безопасность и устойчивость работы. Особенность задачи управления рисками в промышленных киберфизических системах (КФС) заключается в необходимости учитывать высокий уровень разнородности устройств, наличие данных об уязвимостях в программно-аппаратном обеспечении промышленного оборудования. Возникает необходимость в определении подхода, который учитывает поведение сложных КФС, особенности атакующих воздействий на КФС и последствия нарушения технологических процессов КФС. В статье предлагается подход к моделированию киберугроз КФС на примере очистных сооружений, в основе которого лежит онтологическая модель, ориентированная на оценку киберугроз для КФС. Модель связывает данные об уязвимостях и атаках со спецификой технологических процессов, включая экологические последствия нарушения целостности процесса очистки воды. Ее применение позволяет анализировать киберриски путем определения возможных информационные угроз с учетом последствий их реализации. Применение разработанной онтологии демонстрируется путем исследования атак, определенных для макета системы управления очистки воды флотационным методом.

Ключевые слова: информационная безопасность, семантическое моделирование угроз, матрица угроз MITRE ATT&CK, системы управления технологическими процессами, водоочистные сооружения.

1. Введение. Современные системы управления технологическими процессами на критически важных объектах инфраструктуры, к которым относятся комплексы очистных сооружений, всё чаще подвергаются киберугрозам, способным нарушить их стабильную работу и привести к серьёзным последствиям экологического характера [1]. В условиях растущей цифровизации и интеграции промышленных систем с корпоративными сетями и облачными платформами традиционные методы защиты, основанные на периметровой безопасности и сигнатурном обнаружении, оказываются недостаточными для противодействия сложным, многоэтапным и целенаправленным атакам. Это требует перехода к более гибким и адаптивным подходам к обеспечению информационной безопасности и киберустойчивости. В системах очистных сооружений, где используются датчики, контроллеры, исполнительные механизмы и программные комплексы автоматизации, каждое звено может стать точкой проникновения для злоумышленника. При этом нарушение работы даже одного компонента, например,

системы дозирования реагентов или насосной станции, может привести к сбоям в процессе очистки, превышению нормативов сброса загрязняющих веществ или полной остановке объекта. Для построения эффективной системы управления информационными рисками необходима систематизация знаний о возможных угрозах безопасности КФС, последствиях от реализации данных угроз и о существующих мерах противодействия им. Одним из подходов к систематизации знаний предметной области является онтологическое моделирование. Онтологии позволяют интегрировать разнородную информацию о киберугрозах, уязвимостях, технических активах, мерах защиты и инцидентах, создавая единое информационное пространство для анализа киберрисков и принятия решений по противодействию им. Особенно актуальна такая интеграция в сложных промышленных системах, где необходимо учитывать как кибербезопасность, так и функциональную устойчивость, надёжность и безопасность технологических процессов с учетом их динамической природы [2, 3].

В данной статье предлагается подход к управлению рисками информационной безопасности в автоматизированных системах управления водоочистными сооружениями, отличающийся построением семантической модели, которая определяет ключевые сущности системы управления водоочистными сооружениями, связывает их с возможными атаками и позволяет формализовать возможные последствия нарушения ее кибербезопасности. Данная модель позволяет исследовать риски информационной безопасности, выявляя критические (уязвимые) элементов системы и обосновывая выбор контрмер с учетом возможных последствий, в т.ч. экологических. Кроме того, анализ релевантных исследований показал, что задача построения подобной семантической модели для систем управления водоочистными сооружениями другими исследователями ранее не решалась.

Работа структурирована следующим образом. В разделе 2 проанализированы релевантные работы в области применения онтологий для решения задач информационной безопасности, включая задачи управления киберрисками. В разделе 3 дана общая схема системы управления очистными сооружениями, приводится описание с точки зрения технической реализации подобных сооружений, включающее описание возможных датчиков и других важных подсистем, таких как подсистема сбора данных для мониторинга состояния объекта и подсистема обновлений программного обеспечения. В разделе 4 представлена разработанная онтология, в разделе 5 приведен сценарий практического применения онтологии для анализа рисков на примере

макета системы очистки воды методом флотации. В разделе 6 даны выводы и определено дальнейшее направление работ.

2. Анализ релевантных работ. В последние годы наблюдается рост исследований, связанных с применением онтологий для решения задач в области информационной безопасности и управления киберрисками. Широко применяются онтологии, обобщающие и систематизирующие знания в области кибербезопасности. Примером такой онтологии служит онтология UCO (Unified Cyber Ontology, UCO), цель которой – определить базу для стандартизированного представления информации об объектах кибербезопасности. В частности, она определяет такие понятия, как кибербразведка, защита компьютеров/сетей, анализ угроз, анализ вредоносных программ, исследование уязвимостей и т.д., устанавливая между ними связи. Определенные в ней абстрактные классы могут быть использованы для детализации каждой предметной области по отдельности. Например, онтология CASE (Cyber-investigation Analysis Standard Expression) [4], являющаяся расширением онтологии UCO, определяет область цифровой криминалистики и формирует основу для автоматизации процессов расследования киберпреступлений, формализуя такие понятия, как наблюдаемые события и артефакты, источники данных, позволяя ответить на вопросы расследования (кто, когда, как долго, где). В [5] предложена онтология, построенная на основе словаря языка STIX [6] и связывающая такие сущности, как атакующие техники и тактики, атака, кампания, инструменты, уязвимости, атакующие и т.д. Ее применение позволяет по используемым атакующим техникам и инструментам определить потенциальных злоумышленников и объединить их в кампанию.

Таксономия контрмер представлена в онтологии D3FEND [7], она связывает технические меры по обеспечению информационной безопасности с информационными ресурсами разного типа. В [8] представлена онтология, объединяющая знания, представленные в таких базах знаний, как MITRE ATT&CK [9], D3FEND [10], CWE [11] и CVE [12]. Таким образом, ее ключевыми элементами являются тактики и техники APT (MITRE ATT&CK), уязвимости (CVE), слабые места (CWE), контрмеры (D3FEND), инструменты анализа и сценарии угроз. Данная онтология предназначена для формирования целостного представления о киберугрозах и упрощения выбора соответствующих контрмер.

Дойникова Е., и др. [13] предложили онтологию метрик, используемых для оценки рисков нарушения информационной безопасности. Разработанная онтология определяет иерархию метрик

безопасности и задает связи между источниками данных для их расчета и применяемыми алгоритмами расчета. Калеги М., и др. [14] дополнили модель метрик контекстом их использования, который определяется через такие концепты, как решаемая задача, время, целевая аудитория, положение наблюдаемых событий и ресурсов в системе, а также вычислительные характеристики системы.

В [15] описана семантическая модель безопасности приложений, которая формализует такие сущности, как сетевые настройки, конфигурации приложений, методы и инструменты тестирования и связывает их с показателями безопасности, что позволяет оценить степень защищенности критически важного приложения в контексте его положения в инфраструктуре организации.

В последнее время фокус исследований сместился на разработку онтологий, которые связывают в единое целое информационные системы, наблюдаемые инциденты безопасности и процессы реагирования для автоматизации данных процессов. В [3, 16] представлена онтология, которая определяет формальную базу для расчета уровня риска информационной безопасности в режиме, близком к реальному времени. В ее основе лежит онтологическое представление правил STIX и рекомендаций DRM (Disaster Risk Management), которые определяют такие понятия, как риск, оценка риска, вероятность риска и его критичность, контрмеры.

В [17—20] представлены онтологии, которые предназначены для управления рисками с учетом особенностей различных предметных областей. Например, представленная в [17] онтология разработана с учетом рекомендаций стандарта по кибербезопасности разработки дорожных транспортных средств ISO/SAE 21434:2021. Причем авторы показали, что стандарт не в полной мере учитывает практические особенности реализации контрмер. Ключевой задачей разработанной онтологии является устранение данного недостатка путем определения связей между компонентами процессов оценки рисков информационной безопасности, возникающих в процессе разработки транспортных средств, при взаимодействии различных его участников. В ее основе лежит формализованное представление методологии моделирования угроз и выбора контрмер TARA (Threat Analysis and Risk Assessment), сценариев ущерба в части нарушения физической безопасности, конфиденциальности пользователей, функциональных компонент транспортных средств и событий безопасности. В [18] предпринята попытка совместить риски нарушения кибербезопасности и физической безопасности, возникающие в промышленных информационных системах

на уровне построения гибридной онтологической модели оценки рисков, включающей элементы, относящиеся к киберрискам, физическому ущербу и функциональным элементам системы. Применимость разработанной модели была продемонстрирована на примере системы управления охлаждением резервуара с ядерным топливом.

В [19] обсуждаются особенности семантического моделирования информационных угроз, характерных для медицинских устройств. Разработанная К.С. Буджио и др. онтология отвечает на вопросы о типе медицинского устройства, его разработчике, используемом программном обеспечении, об уязвимостях, связанных с ним, а также о потенциально уязвимых группах пользователей и возможных последствиях реализованных атак. В [20] рассмотрены особенности атак на системы, использующие модели искусственного интеллекта, и механизмы, предложенные для повышения их уровня защищенности. Представленная онтология основана на базах знаний MITRE ATT&CK и ATLAS, тактики и техники MITRE ATT&CK дополнены новыми угрозами, связанными с уязвимостями машинного обучения.

Для полноты обзора релевантных работ следует отметить исследование [21], в котором представлена онтология, предназначенная для структурирования информации о наборах данных, которые могут быть использованы при обучении моделей машинного обучения для решения задач информационной безопасности. Данная онтология не только позволяет связать различные наборы данных, но и систематизирует типы атак, которые используются для их разметки.

Таким образом, в научной литературе представлены разнообразные онтологии для управления информационной безопасностью, однако отсутствуют решения, которые связывают описание разнородных киберфизических промышленных систем, наблюдаемых аномалий, включая инциденты безопасности, расчет рисков и выбор контрмер в зависимости от последствий их реализации. Также следует отметить, что в научной литературе не представлены решения для семантического моделирования угроз в системе управления очистными сооружениями. Таким образом, данная работа направлена решение выявленной проблемы и представляет онтологию, отличающуюся возможностью анализировать киберриски в контексте возможных экологических последствий.

3. Структура системы управления процессом очистки воды. Рассматриваемая в рамках данной работы система управления процессами очистки воды представляет собой автоматизированную технологическую платформу, объединяющую физические компоненты обработки воды

с цифровыми системами управления, мониторинга и внешними сервисами. Ее структура представлена на рисунке 1.

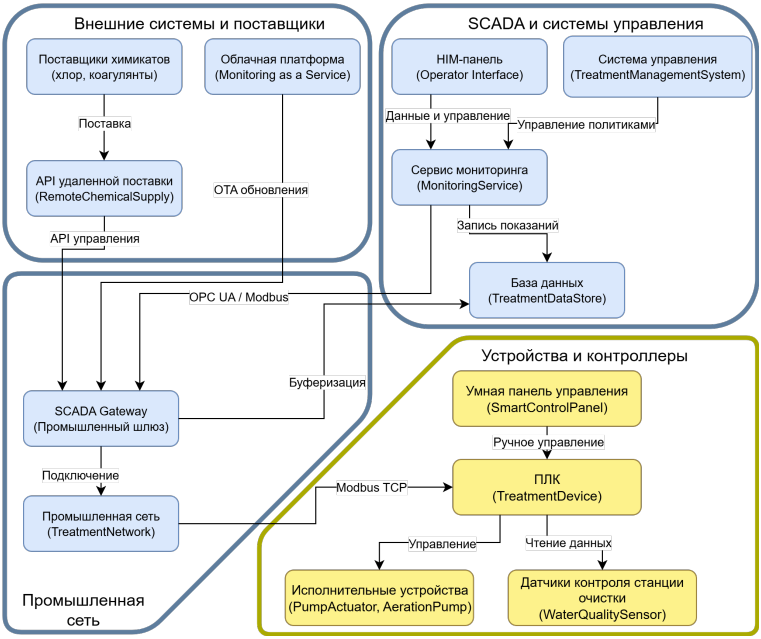

Рис. 1. Структурная схема системы управления водоочистными сооружениями

Центральным элементом системы является программируемый логический контроллер (ПЛК), который отвечает за выполнение алгоритмов управления процессами: запуск и остановку насосных станций, регулирование режимов аэрации, а также сбор данных с датчиков качества воды.

Для обеспечения точного контроля и автоматизации используется SCADA (Supervisory Control and Data Acquisition) система. Она включает в себя интерфейс оператора (HMI), через который осуществляется визуализация текущего состояния системы, а также программные управляющие сервисы, выполняющие сбор данных, их анализ и архивирование. Эта информация позволяет отслеживать ключевые показатели качества воды, выявлять отклонения и оптимизировать работу системы. База данных системы хранит всю историю работы: показания датчиков, параметры управления, события аварий и плановые операции, что позволяет проводить глубокий анализ производительности,

прогнозировать отказы оборудования и выстраивать стратегии технического обслуживания.

Связь между оборудованием и системой управления обеспечивается через промышленный шлюз (SCADA Gateway), который работает как мост между сетью оборудования и программными системами. Он поддерживает стандартные промышленные протоколы, такие как Modbus TCP и OPC UA, что гарантирует совместимость с различными типами оборудования. Шлюз также отвечает за безопасную передачу данных, буферизацию информации и защиту от перегрузок сети.

Современные системы управления водоочистными сооружениями также могут быть связаны с внешними поставщиками ресурсов, например, химикатов, необходимых для обеззараживания. Она может поддерживать OTA-обновления (over-the-air обновление) от облачной платформы, что обеспечивает постоянное совершенствование программного обеспечения без необходимости физического доступа к оборудованию.

4. Проектирование онтологии SecWat-O. Для управления рисками информационной безопасности разрабатываемая онтология должна уметь отвечать на следующие группы вопросов:

1. Какие атаки могут быть определены для системы управления очистными сооружениями?

2. Какие атакующие техники и тактики из базы знаний MITRE ATT&CK определены для заданной системы управления очистными сооружениями?

3. Для каких логических и физических компонентов заданной системы управления определены тактики и техники базы знаний MITRE ATT&CK?

4. Каковы последствия от реализации заданной угрозы?

5. Что является последствием компрометации заданного устройства?

6. Какая атака может привести к его компрометации?

Данные вопросы представляют собой вопросы компетентности онтологии SecWat-O. Они обуславливают необходимость формализовать следующие компоненты системы:

1. Физические и логические элементы системы управления водоочистных сооружений;

2. Информационно-коммуникационную среду, с помощью которой SCADA взаимодействует с системой очистных сооружений;

3. Атакующие техники и тактики, определенные для промышленных киберфизических систем;

4. Угрозы и последствия, возникающие в результате их реализации.

При проектировании онтологии был применен модульный подход, который позволяет импортировать и повторно использовать созданные ранее онтологии, и, как следствие, повышает совместимость разрабатываемой онтологии с существующими решениями в данной предметной области. Кроме того, такое решение дает возможность вести дальнейшую проработку компонентов независимо друг от друга и повторно использовать разработанную онтологию и/или ее отдельные компоненты в других проектах. На рисунке 2 представлена упрощенная схема основных компонент (модулей) разработанной онтологии SecWaT-O и связей между ними. Цветом выделены модули, отвечающие за моделирование физических и логических элементов системы управления водоочистных сооружений, атакующих воздействий и их последствий, и информационно-коммуникационную среду. Далее эти модули рассмотрены более подробно.

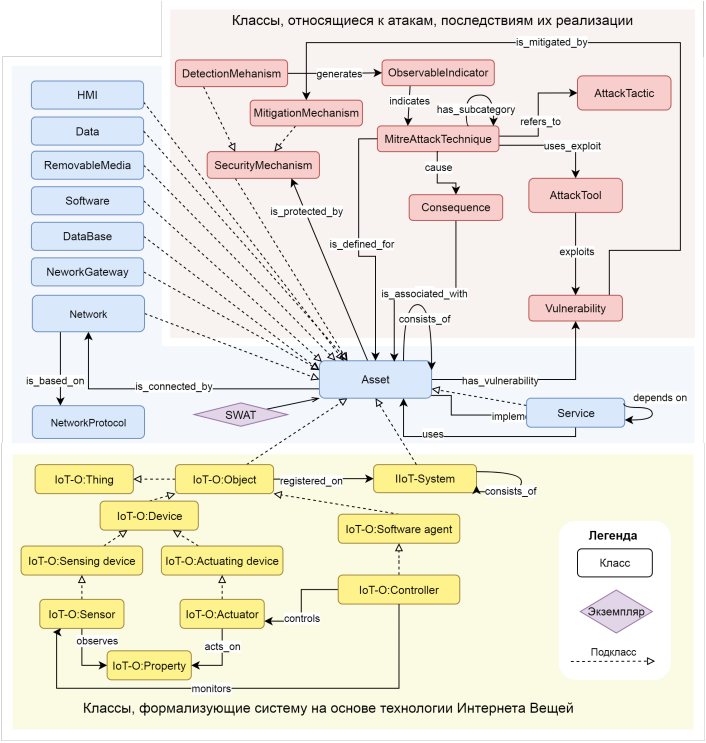

Рис. 2. Основные концепты онтологии SecWaT-O и связи между ними

4.1. Моделирование функционирования системы очистки воды. В качестве базы для моделирования устройств системы очистных сооружений была выбрана онтология IoT-O [22], которая определяет киберфизические системы через совокупность взаимодействующих устройств и выполняемые ими функции. Она определяет ключевые классы *Устройство* (Device) и *Программный агент* (Software Agent), которые формализуют понятия физических и логических элементов киберфизической системы. Класс "*Устройство*"(Device) имеет два подкласса, характеризующие два типа устройств:

– датчики (Sensing_Device) – устройства, которые собирают данные;

– актуаторы (Actuating_device) – устройства, взаимодействующие с системой.

Данные устройства управляются контроллером и в совокупности они формируют некоторую программно-аппаратную систему, выполняющую некоторую функцию или предоставляющую некоторый сервис.

В рамках общей онтологии SecWat-O (Рис. 2) реализуется импортирование онтологии IoT-O, классы которой формализуют систему на физическом уровне (на рис. 2 выделены желтым цветом).

В ходе построения онтологии для системы управления процессом флотационной очистки воды было специфицировано следующее аппаратное технологическое оборудование:

– датчики контроля состояния воды, к которым относятся датчики потока воды, датчики мутности воды, датчики уровня воды, датчики уровня pH, датчики взвешенных частиц, манометры;

– актуаторы, к которым относятся насосы подачи воды, краны, также регулирующие подачу воды, насосы подачи реагентов, мешалки, мотор скребка для шлама, компрессор для аэрации.

Координация данных устройств осуществляется с помощью общего контроллера управления всей станцией. На рисунке 3 представлена онтологическая модель компонентов технологического процесса флотационной очистки воды. Были определены следующие классы устройств:

– класс DensityMeter – датчик мутности воды, измеряющий плотность взвеси в воде;

– класс WaterLevelMeter – датчик уровня воды;

– класс WaterFlowMeter – датчик скорости потока;

– класс PHMeter – датчик уровня кислотности воды;

– класс PressureGauge – манометр;

– класс PumpActuator – исполнительный механизм насоса для подачи воды или подачи реагентов;

– класс VentActuator – управляемый кран насоса подачи воды;

– класс StirerActuator – исполняющий механизм мешалок, выполняющих перемешивание загрязненной воды;

– класс AirCompressor – компрессор для аэрации загрязненной воды;

– класс ScrapperMotor – мотор скребка для удаления шлама;

– класс WaterTreatmentNode – технологическое звено процесса, выполняющее определенную функцию, например, флотацию или флокулляцию.

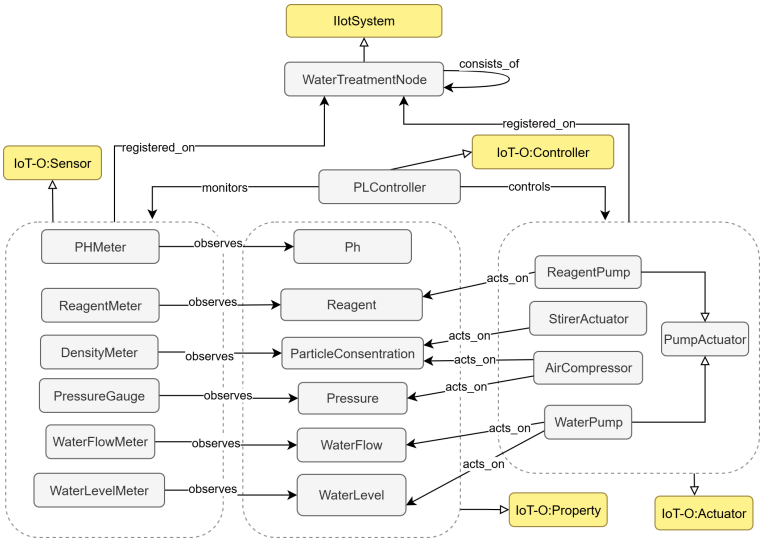

Рис. 3. Классы онтологии SecWaT-O, отражающие связи между технологическим оборудованием

Технологическая часть системы управления очисткой воды обычно интегрирована в информационную систему предприятия. Ресурсы информационной системы описываются через абстрактный класс *Ресурс* (Asset). Данный класс имеет такие подклассы, как *Сеть* (Network), *Хранилище данных* (DataBase), *Программное обеспечение* (Software), *Данные* (Data), *Человеко-машинные интерфейсы* (HMI), *Съемные носители данных* (Removable Media), *Механизм защиты* (Security Mechanism). Технологическая часть системы, состоящая

из промышленных датчиков и актуаторов, также является подклассом данного класса и представлена классом IoTSystem.

С ресурсами информационной системы связано понятие выполняемой функции, которое в разработанной онтологии определяется через класс *Функция* (Service). Примером такой функции может служить контроль мутности воды или очистка воды методом флотации, или удаленное обновление ПО. Для ее реализации может быть использован один и более ресурсов. Объекты класса *Ресурс* могут иметь некоторую уязвимость, которая может быть использована для реализации атакующего воздействия. Также ресурсы могут быть связаны с другими ресурсами с помощью коммуникационных сетей, которые, в свою очередь, также относятся к ресурсам. Таким образом, формально класс ресурс (Asset) определяется следующим образом:

$$\begin{aligned} Asset \sqsubseteq (&Thing \\ &\sqcap \forall implements.Service \\ &\sqcap \forall has\_vulnerability.Vulnerability \\ &\sqcap \forall is\_connected\_by.Network \\ &\sqcap \forall is\_protected\_by.SecurityMechanism \\ &\sqcap \forall consists\_of.Asset) \end{aligned} \tag{1}$$

На рисунке 2 показаны классы, относящиеся к информационно-коммуникационной части системы управления, отмечены синим цветом.

4.2. Моделирование кибер угроз и атак на систему очистных сооружений. В основе семантической модели угроз и атак лежит база знаний MITRE ATT&CK, которая систематизирует практические знания об атаках, техниках их выполнения, включая используемые уязвимости, а также возможные контрмеры. На основе данной базы знаний была разработана отдельная онтология MITRE-ATTACK, которая в дальнейшем импортируется в онтологию SecWat-O. Были выделены следующие классы:

– класс AttackTactic – цели атакующего;

– класс AttackTechnique – конкретные атакующие техники, которые использует злоумышленник для достижения своих целей, данный класс связан с абстрактным классом *Ресурс* (Asset), что позволяет учитывать техники, специфические для промышленных систем управления;

– класс Vulnerability – уязвимости, определенные для ресурса;

– класс AttackTool – инструменты, используемые для выполнения атакующего воздействия, включая эксплойты;

– класс ObservableIndicator – наблюдаемые индикаторы, которые сигнализируют о выполнении атаки;

– класс SecurityMechanism – механизм обеспечения кибербезопасности, он имеет два подкласса – механизм предотвращения атаки (MitigationMechanism) и механизм обнаружения атаки (Detection Mechanism), который генерирует наблюдаемые индикаторы атаки.

Для описания возможных последствий, возникающих вследствие выполнения атаки на заданный информационный ресурс, был определен класс *Последствия* (Consequence). Последствия задаются для скомпрометированных ресурсов. Поскольку ресурсы связаны между собой семантическими связями, имеется возможность построить цепочку связанных устройств, которые могут быть косвенно затронуты в результате выполняемых деструктивных действий. Классы и функциональные связи между ними, относящиеся к моделированию действий атакующего (на рис. 2 выделены красным цветом.

В результате разработанная онтология SecWat-O определяет элементы, связывающие две предметные области Интернета Вещей и атаки, показывая инфокоммуникационные связи между объектами, формализует понятие ресурс и бизнес-процессы. При ее построении осуществляется импортирование онтологий MITRE-ATTACK и IoT-O, а также их объединение в единую онтологию, что реализует модульный принцип построения.

В качестве инструмента разработки онтологии SecWat-O был выбран Protege. Проверка онтологии на непротиворечивость и наличие циклов была выполнена с помощью машины логического вывода HermiT 1.4.3. Проверка на полноту осуществлялась путем построения логических запросов на языке SPARQL, цель которых получить ответы на вопросы компетентности данной онтологии, определенных в начале раздела. Процесс построения запросов описан в следующем разделе.

5. Пример использования: моделирование атак на систему флотационной очистки воды. Для проверки полноты разработанной онтологии SecWaT-O была построена семантическая модель для макета системы управления очистки воды флотационным методом, представленного учебным стендом CE 587 (G.U.N.T., GmbH) [23].

Он оснащен следующими датчиками и исполнительными устройствами (Рис. 4):

– насос P1, установленный перед резервуаром для флокуляции, используемый для подачи неочищенной воды;

– датчик уровня воды LM1 в резервуаре для флотации;

– циркуляционный насос P2 перед воздушным барабаном, используемый для реализации системы аэрации резервуара для флотации;

– расходомер воды FM1, установленный после насоса P1;

– управляемый кран VA1, установленный после насоса P1;

– манометр PG1, установленный после воздушного компрессора AirC1;

– датчик скорости подачи воздуха FM2 перед воздушным барабаном, используемый для контроля подачи воздуха в барабан;

– датчик уровня воды LM2 в воздушном барабане для контроля работы система аэрации;

– манометр PG2 перед резервуаром флотации для контроля системы аэрации;

– датчик потока FM3 перед резервуаром флотации для контроля потока водно-воздушной смеси системы аэрации резервуара;

– датчик контроля уровня кислотности pH: датчик кислотности PH1;

– насосы подачи регентов P4, P4, P5, и механизмы для перемешивания воды в резервуаре флокуляции R1-R4.

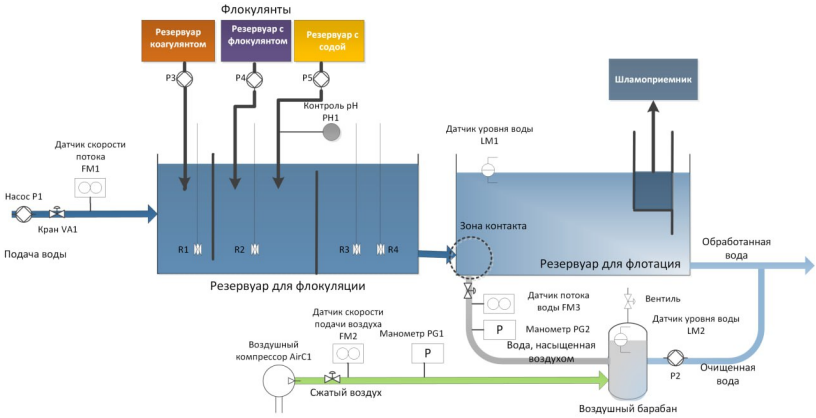

Рис. 4. Схема учебного стенда CE 587 с указанием установленных датчиков и актуаторов [23]

Рассматриваемый стенд не имеет подключения к сети Интернет, поэтому были рассмотрены сценарии атак с внутренним нарушителем:

– подключение съемного диска с вредоносным ПО к рабочей станции;

– сотрудник настроил систему таким образом, что процесс очистки нарушен;

– злоумышленник подключился к внутренней сети напрямую.

Нарушение целостности технологического процесса осуществляется путем подмены передаваемых значений сенсоров и/или команд актуаторов или путем их модификации. Согласно таксономии MITRE ATT&CK, атакующие техники, манипулирующие данными от таких устройств, относятся к тактикам *Ухудшение контроля технологического процесса* (Impair Process Control, ID: TA0106) и *Подавление ответной функции* (Inhibit Response Function, ID: TA0107).

Тактика *Ухудшение контроля технологического процесса* (ID: TA0106) состоит из методов, целью которых является нарушение логики управления и оказания определяющего воздействия на процессы, выполняемые системой. Ключевым объектом атак становится программно-логический контроллер, который непосредственно взаимодействуют с объектами физического процесса и определяет логику их функционирования. В группу техник, относящихся к тактике *Подавление ответной функции* (ID: TA0107), входят методы, целью которых является отключение функций обеспечения безопасности, защиты, контроля качества или предотвращение вмешательства оператора. Они направлены на активное выявление и предотвращение ожидаемых аварийных сигналов и ответных мер, возникающих в ответ на получаемые данные или команды от исполнительных устройств.

В таблице 1 предоставлены возможные последствия, определенные для учебного стенда CE 587 и возникающие в результате манипуляций с его датчиками.

Наиболее критичным узлом учебного стенда является контроллер. На текущий момент для атак, модифицирующих логику контроллера, специфических контрмер нет (объект онтологии – Mitigation Limited or Not Effective, ID: M 0816). Таким образом, защита таких ресурсов должна включать такие контрмеры, как контроль доступа к ресурсам информационно-коммуникационной системы в целом, применение механизмов аутентификации, формирование списков доступа, сегментацию компьютерной сети и т.д.

Таблица 1. Атаки на датчики и их возможные последствия на технологический процесс

Компонент стенда	**Датчик**	**Последствия**
Резервуар флокуляции	Кран подачи воды VA1	– повреждение насоса P1 (работа в сухом режиме); – переполнение/осушение резервуара флокуляции; – утечка загрязненной воды в результате переполнения резервуара флокуляции; – попадание неочищенной воды в водоемы.
	Насос P1	– переполнение/осушение резервуара флокуляции; – утечка загрязненной воды в результате переполнения резервуара флокуляции; – попадание неочищенной воды в водоемы.
	Расходомер воды FM1	– переполнение/осушение резервуара флокуляции; – утечка загрязненной воды в результате переполнения резервуара флокуляции; – попадание неочищенной воды в водоемы.
	Насосы подачи регентов P4, P4, P5	– избыточное/недостаточное количество флокулянтов и каугулянтов нарушает процесс очистки воды; – очищамая вода загрязняется флокулянтами/каугулянтами; – загрязненная вода попадает в водоемы.

Продолжение таблицы 1. Атаки на датчики и их возможные последствия на технологический процесс

Компонент стенда	**Датчик**	**Последствия**
	Механизмы перемешивания R1-R4	– нарушение процесса флокуляции, образуется меньшее число флокулянтов; – ухудшается качество очищаемой воды; – загрязненная вода попадает в водоемы.
	Датчик уровня кислотности PH1	– изменяются параметры процесса флокуляции, зависящие от уровня кислотности воды; – ухудшается качество очищаемой воды; – загрязненная вода попадает в водоемы.
Резервуар флотации	Датчик уровня воды LM1	– переполнение/осушение резервуара флотации; – утечка загрязненной воды в результате переполнения резервуара флокуляции; – попадание неочищенной воды в водоемы.
	Манометр PG1	– нарушение работы системы аэрации; – избыточная/недостаточная подача воздуха; – недостаточное удаление шлака из очищаемой воды, переполнения резервуара флокуляции; – попадание неочищенной воды в водоемы.

Продолжение таблицы 1. Атаки на датчики и их возможные последствия на технологический процесс

Компонент стенда	**Датчик**	**Последствия**
	Датчик уровня воды LM2	– нарушение работы системы аэрации; – избыточная/недостаточная подача воды; – недостаточное удаление шлака из очищаемой воды, переполнения резервуара флокуляции; – попадание неочищенной воды в водоемы; – выдавливание воды из воздушного барабана.
	Насос P2	– нарушение работы системы аэрации; – избыточная/недостаточная подача воды; – недостаточное удаление шлама из очищаемой воды; – переполнение резервуара флотации; – попадание неочищенной воды в водоемы; – выдавливание воды из воздушного барабана.
	Манометр PG2	– нарушение работы системы аэрации; – избыточная/недостаточная подача воды; – недостаточное удаление шлама из очищаемой воды; – переполнение резервуара флотации; – попадание неочищенной воды в водоемы.

Продолжение таблицы 1. Атаки на датчики и их возможные последствия на технологический процесс

Компонент стенда	**Датчик**	**Последствия**
	Датчик потока FM3	– нарушение работы системы аэрации; – избыточная/недостаточная подача воды; – недостаточное удаление шлама из очищаемой воды; – переполнение резервуара флотации; – попадание неочищенной воды в водоемы.

На рисунке 5 представлены экземпляры онтологии SecWat-O, которые описывают датчики и актуаторы учебного стенда CE 587, используемые обозначения сенсоров и актуаторов представлены выше. На рисунке 6 представлены экземпляры классов части онтологии, относящаяся к MITRE ATT&CK, в частности показаны индивиды, имеющие класс *Тактики*, *Техники*, *Противодействия*, а также указаны связи между ними. Идентификаторы индивидов совпадают с идентификаторами объектов базы знаний MITRE ATT&CK.

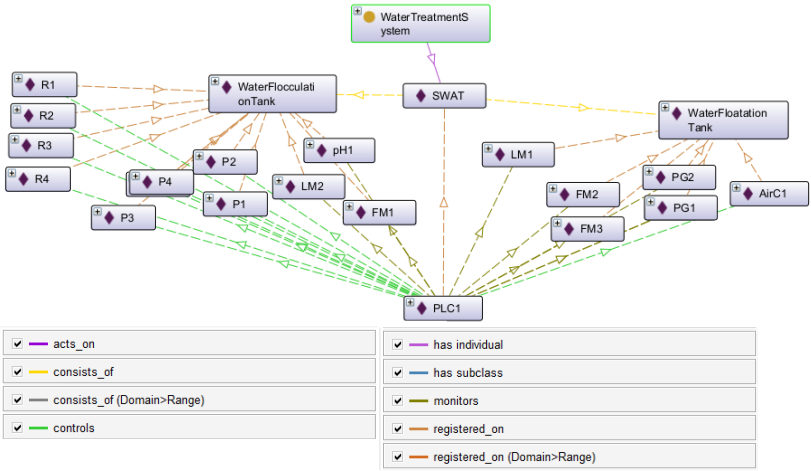

Рис. 5. Экземпляры онтологии, представляющие структурные компоненты учебного стенда CE 587

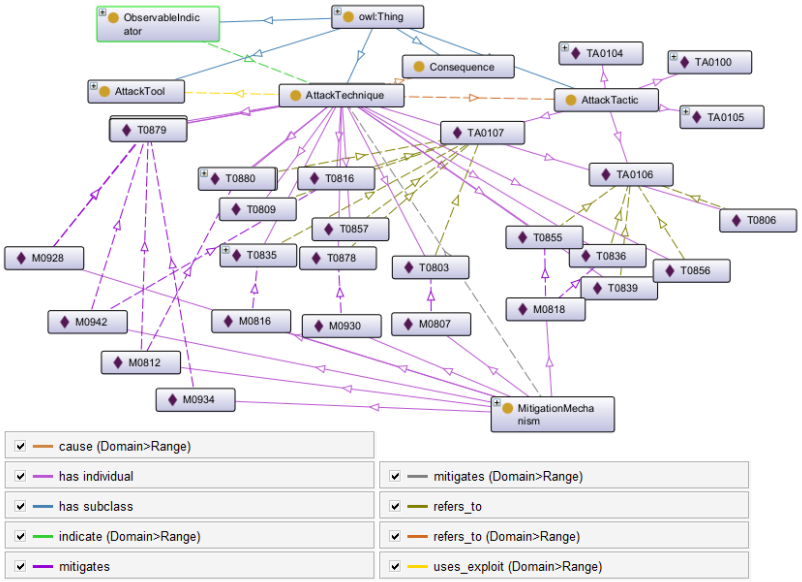

Рис. 6. Экземпляры онтологии, относящиеся к базе знаний MITRE ATT&CK

Для проверки полноты разработанной онтологии был разработан ряд запросов, построенных с учетом вопросов компетентности данной онтологии, сформулированных в разделе 4. Запросы позволяют ответить на вопросы о связях между устройствами, наличии атакующих тактик и техник, возможных для данного стенда, каковы возможные меры по их устранению и каковы возможные последствия успешной реализации атак. Например, запрос, показанный в листинге 1, возвращает список устройств, функционирование которых связано с показаниями датчика уровня воды LM1, а на рисунке 7 представлен результат запроса для учебного стенда. Нарушение целостности функционирования одного из этих устройств, например, путем подмены значений, потенциально может вызвать неисправности в функционировании связных устройств.

```
PREFIX IoT-O: <http://www.semanticweb.org/eve/ontologies/2025/8/IoT-O#>
SELECT ?actuator ?property  WHERE {
            ?actuator IoT-O:acts_on ?property.
            IoT-O:LM1 IoT-O:observes ?property}
```

Листинг 1. Поиск устройств, функционирование которых взаимосвязано через заданное свойство системы

actuator	property
P1	flotation_water_level
P2	flotation_water_level

Рис. 7. Результат SPARQL запроса, представленного в листинге 1

Запрос, представленный в листинге 2, возвращает перечень возможных атакующих техник, определенных для контроллера. На рисунке 8 представлен результат запроса для текущей версии онтологии.

```
PREFIX SecWat-O: <http://www.semanticweb.org/eve/ontologies/2025/8/SecWat-O#>
PREFIX MITRE-ATTACK: <http://www.semanticweb.org/eve/ontologies/2025/8/
     MItreAttack#>
PREFIX IoT-O: <http://www.semanticweb.org/eve/ontologies/2025/8/IoT-O#>
SELECT ?attack_tech ?description ?device ?device_type   WHERE {
        ?attack_tech rdfs:comment ?description.
    ?attack_tech SecWat-O:is_defined_for ?device.
        ?device rdf:type  ?device_type.
        ?device_type rdfs:subClassOf  IoT-O:Controller}
```

Листинг 2. Запрос, возвращающий список возможных атакующих техник для устройства типа Controller

attack_tech	description	device	device_type
T0803	"Block Command Message"	PLC1	PLController
T0806	"Brute Force I/O"	PLC1	PLController
T0856	"Spoof Reporting Message"	PLC1	PLController
T0836	"Modify Parameter"	PLC1	PLController
T0878	"Alarm Suppresion"	PLC1	PLController
T0804	"Block Reporting Message"	PLC1	PLController

Рис. 8. Результат SPARQL запроса, показанного в листинге 2

Запрос, показанный в листинге 3 возвращает список устройств, для которых определены уязвимости в CVE, инструменты, которые их эксплуатируют. Для учебного стенда примером такой уязвимости служит уязвимость CVE-2020-15782, определенная для контроллера приводов семейства SIMATIC компании Siemens AG. Результат запроса дан на рисунке 9, из него следует, что для эксплуатации уязвимости CVE-2020-15782 может быть использован червь PLC-Blaster. Запрос, представленный на листинге 4, возвращает перечень возможных последствий, определенных для заданного устройства, а именно насоса P1, который управляет подачей воды в резервуар флокуляции. Список последствий формируется на основе анализа последствий, заданных как для заданного устройства, так и для устройств, с которыми он связан

физически: резервуар флокуляции и сама система очистки воды в целом. Результат запроса представлен на рисунке 10.

```
PREFIX SecWat-O: <http://www.semanticweb.org/eve/ontologies/2025/8/SecWat-O#>
PREFIX MITRE-ATTACK: <http://www.semanticweb.org/eve/ontologies/2025/8/
     MItreAttack#>
PREFIX IoT-O: <http://www.semanticweb.org/eve/ontologies/2025/8/IoT-O#>

SELECT ?vulnerability ?tool ?device ?technique WHERE {
    ?technique SecWat-O:is_defined_for ?device.
    ?technique MITRE-ATTACK:uses_exploit ?tool.
    ?tool   MITRE-ATTACK:exploits ?vulnerability.
    ?vulnerability rdf:type MITRE-ATTACK:Vulnerability }
```

Листинг 3. Запрос, возвращающий список устройств, для которых определены уязвимости в MITRE ATT&CK

vulnerability	tool	device	technique
CVE-2020-15782	PLC-Blaster	PLC1	T0835

Рис. 9. Результат SPARQL запроса, показанного в листинге 3

```
PREFIX SecWat-O: <http://www.semanticweb.org/eve/ontologies/2025/8/SecWat-O#>
PREFIX MITRE-ATTACK: <http://www.semanticweb.org/eve/ontologies/2025/8/
     MItreAttack#>
PREFIX IoT-O: <http://www.semanticweb.org/eve/ontologies/2025/8/IoT-O#>
SELECT * WHERE {
    {   SELECT ?id ?desc WHERE {
           ?id rdfs:comment ?desc.
           ?id SecWat-O:is_associated_with ?system.
           ?system IoT-O:consists_of ?node.
           IoT-O:P1 IoT-O:registered_on ?node. }
    }   UNION
    {   SELECT ?id ?desc WHERE {
         ?id rdfs:comment ?desc.
         ?id SecWat-O:is_associated_with ?node.
         IoT-O:P1 IoT-O:registered_on ?node. }
    }
}
```

Листинг 4. Запрос, возвращает возможные последствия для заданного устройства и связанных с ним компонентов

id	
con001_SWAT	"Leakage of the waste water"
Con000_SWAT	"Malfunction of water treatment system"
Con00_Flocculation_tank	"OVerfiiling or drying of the tank reservour"
Con01_Floculation_tank	"Leackage of waste water"

Рис. 10. Результат SPARQL запроса, представленного в листинге 4

6. Заключение. В статье был предложен подход к управлению рисками информационной безопасности в системе управления водоочистными сооружениями, в основе которого лежит онтология SecWat-O. Онтология представляет собой семантическую модель, объединяющую данные о системе управления технологическим процессом и атакующими воздействиями на киберфизические системы. Многими исследователями [13] отмечается, что применение подходов, в основе которых лежат семантические модели, актуально ввиду растущей сложности таких систем и наличию множества зависимостей между ее элементами. Таким образом, онтология является эффективным инструментом анализа информационных рисков, позволяющим моделировать логические зависимости между компонентами системы, анализировать возможные угрозы и интерпретировать их последствия в контексте технологического процесса.

Предложенная в статье онтология SecWat-O объединяет в себе ключевые знания о предметной области очистки воды, представленные в виде описания технических и логических активов системы управления процессом очистки и определения связей между ними, типов киберугроз, уязвимостей и атакующих воздействий, представленных в виде тактик и техник базы знаний MITRE ATT&CK.

Одной из ключевых особенностей разработанной онтологии является учет специфики технологии очистки воды, что позволяет использовать ее для задач оценки рисков, мониторинга безопасности, в т.ч. экологической безопасности, и принятия решений в условиях кибератак.

Проверка полноты разработанной онтологии SecWat-O была выполнена путем моделирования функционирования упрощенной системы управления водоочистными сооружениями, представленного учебным стендом флотационной очистки воды CE 587. Были подробно описаны основные элементы данного стенда, датчики, исполнительные устройства. Определены атакующие сценарии, такие как подключение съемного диска с вредоносным ПО к рабочей станции, настройка системы

с нарушением процесса очистки и подключение злоумышленника к внутренней сети. Были разработаны SPARQL запросы, реализующие компетентностные вопросы онтологии. С их помощью было показано, что наиболее критичными атаками являются атаки, направленные на изменение логики функционирования контроллера, для которых в настоящее время нет эффективных контрмер.

Задачи дальнейших исследований связаны с автоматизацией синхронизации с базами MITRE ATT&CK, обновлением информации о самой системе водоочистных сооружений, а также уточнением классов онтологии, связанных с наблюдаемыми событиями и выбором контрмер. Последнее позволит строить адаптивную систему противодействия атакам в режиме, близком к реальному, с учетом последствий нарушения безопасности технологического процесса.

Литература

1. 11 recent cyber attacks on the water and wastewater sector // Wisdiam. 2024. URL: https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/ (дата обращения: 17.09.2025).
2. Almoabady T.A., et al. Protecting digital assets using an ontology based cyber situational awareness system // Frontiers in Artificial Intelligence. 2024. vol. 7. DOI: 10.3389/frai.2024.1394363.
3. Sanchez-Zas C., et al. A methodology for ontology-based interoperability of dynamic risk assessment frameworks in IoT environments // Internet of Things. 2024. vol. 27. 101267 p. DOI: 10.1016/j.iot.2024.101267.
4. Getting Started just the basics // CASE Ontology. 2025. URL: https://caseontology.org/ontology/start.html (дата обращения: 17.09.2025).
5. STIX 2.1 ontology model POC with Stardog using knowledge graphs and RDF // Smart City Cyber Security. 2024. URL: https://smartcitysecurity.net/stix-2-1-ontology-model-poc-with-stardog-using-knowledge-graphs-and-rdf/ (дата обращения: 17.09.2025).
6. Introduction to STIX // GitHub. 2024. URL: https://oasis-open.github.io/cti-documentation/stix/intro.html (дата обращения: 17.09.2025).
7. D3FEND Analytic Technique Taxonomy // MITRE. 2024. URL: https://d3fend.mitre.org/acf/ (дата обращения: 17.09.2025).
8. Akbar K.A., et al. The Design and Application of a Unified Ontology for Cyber Security / In: Muthukkumarasamy V., Sudarsan S.D., Shyamasundar R.K. (eds) // Information Systems Security. Lecture Notes in Computer Science. Springer. 2023. vol. 14424. pp. 23–41.
9. MITRE ATTCK. 2025. URL: https://attack.mitre.org/ (дата обращения: 17.09.2025).
10. D3FEND. A knowledge graph of cybersecurity countermeasures // MITRE. 2025. URL: https://d3fend.mitre.org/ (дата обращения: 17.09.2025).
11. CWE: Common Weakness Enumeration // MITRE. 2025. URL: https://cwe.mitre.org/ (дата обращения: 17.09.2025).
12. CVE: Common Vulnerabilities and Exposures // MITRE. 2025. URL: https://www.cve.org/ (дата обращения: 17.09.2025).
13. Doynikova E., et al. Ontology of Metrics for Cyber Security Assessment // Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). DOI: 10.1145/3339252.3341496.

14. Khaleghi M., et al. Context-Aware Ontology-based Security Measurement Model // Journal of Information Security and Applications. 2022. vol. 67. 103199 p. DOI: 10.1016/j.jisa.2022.103199.
15. Mozzaquatro B.A., et al. An Ontology-Based Cybersecurity Framework for the Internet of Things // Sensors. 2018. vol. 18. no. 9. 3053 p. DOI: 10.3390/s18093053.
16. Sanchez-Zas C., et al. Ontology-based approach to real-time risk management and cyber-situational awareness // Future Generation Computer Systems. 2023. vol. 141. pp. 462–472. DOI: 10.1016/j.future.2022.12.006.
17. Khalil K., et al. CyberROAD: A cybersecurity risk assessment ontology for automotive domain aligned with ISO/SAE21434:2021 // Journal of Information Security and Applications. 2025. vol. 90. 104015 p. DOI: 10.1016/j.jisa.2025.104015.
18. Alanen J., et al. Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems // Reliability Engineering System Safety. 2022. vol. 220. 108270 p. DOI: 10.1016/j.ress.2021.108270.
19. Bughio K.S., et al. Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring // Sensors. 2024. vol. 24. no. 9. 2804 p. DOI: 10.3390/s24092804.
20. Preuveneers D., et al. An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Applications // Future Internet. 2024. vol. 16. no. 3. 69 p. DOI: 10.3390/fi16030069.
21. Dash S., et al. From Data to Defense: How Ontology Fuels AI in Cyber Threat Detection // Proceedings of the 8th International Conference on Advances in Artificial Intelligence (ICAAI '24). 2025. pp. 121–133. (ICAAI '24). DOI: 10.1145/3704137.3704176.
22. Seydoux N., et al. IoT-O, a Core-Domain IoT Ontology to Represent Connected Devices Networks / In: Blomqvist E., Ciancarini P., Poggi F., Vitali F. (eds) // Knowledge Engineering and Knowledge Management. Lecture Notes in Computer Science. Springer. 2016. vol. 10024. pp. 561–576.
23. Novikova E., et al. Dataset Generation Methodology: Towards Application of Machine Learning in Industrial Water Treatment Security // SN Computer Science. 2024. vol. 5. 373 p. DOI: 10.1007/s42979-024-02704-9.

Саенко Игорь Борисович — д-р техн. наук., профессор; главный научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук». Область научных интересов: автоматизированные информационные системы, информационная безопасность, искусственный интеллект, машинное обучение, теория моделирования и математическая статистика, теория информации. Число научных публикаций — свыше 500. ibsaen@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., д. 39, Санкт-Петербург, 199178, Российская Федерация; тел.: +7(812)328-7181, факс: +7(812)328-4450.

Новикова Евгения Сергеевна — канд. техн. наук, старший научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук». Область научных интересов: безопасность информационных систем, обнаружение аномалий методами машинного обучения, обеспечение конфиденциальное машинное обучение. Число научных публикаций — более 150. novikova@comsec.spb.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Российская Федерация; р.т.: +7(812)328-7181; факс: +7(812)328-4450

Мелешко Алексей Викторович — младший научный сотрудник, Международный центр цифровой криминалистики, Федеральное государственное бюджетное учреждение науки

«Санкт-Петербургский Федеральный исследовательский центр Российской академии наук». Область научных интересов: обнаружение атак методами машинного обучения, безопасность беспроводных сенсорных сетей, безопасность аддитивных производств. Число публикаций - 55. meleshko.a@iias.spb.su; 14-я линия В.О., 39, 199178, Санкт-Петербург, Российская Федерация; р.т.: +7(812)328-7181; факс: +7(812)328-4450

Садовников Владимир Евгеньевич — аспирант, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук». Область научных интересов: обнаружение компьютерных атак, машинное обучение. Число научных публикаций — 25. bladimir1998@mail.ru; 14-я линия В.О., д. 39, Санкт-Петербург, 199178, Российская Федерация; тел.: +7(812)328-7181, факс: +7(812)328-4450.

Поддержка исследований. Работа выполнена при поддержке гранта Российского научного фонда № 23-11-20024 (https://rscf.ru/project/23-11-20024/) и Санкт-Петербургского научного фонда в СПб ФИЦ РАН.

DOI 10.15622/ia.25.3.9

I.B. Saenko , E.S. Novikova , A.V. Meleshko , V.E. Sadovnokov

AN ONTOLOGICAL APPROACH TO RISK MANAGEMENT IN WASTEWATER TREATMENT SYSTEM

Saenko I.B., Novikova E.S., Meleshko A.V., Sadovnikov V.E. **An Ontological Approach to Risk Management in Wastewater Treatment System.**

Abstract. Modern process control systems at critical infrastructure facilities, including wastewater treatment plants, are increasingly becoming the target of sophisticated cyberattacks aimed at compromising environmental safety and operational sustainability. Risk management in industrial cyber-physical systems (CPS) requires taking into account the high level of device heterogeneity and the presence of vulnerabilities in the software and hardware of industrial equipment. This necessitates developing an approach that takes into account the behavior of complex CPS, the specifics of attack patterns against CPS, and the consequences of disrupting CPS processes. This article proposes an approach to modeling cyberthreats in CPS using the example of a wastewater treatment system. This approach is based on an ontological model focused on assessing cyberthreats to CPS. The model links vulnerability and attack data with the specifics of the process, including the environmental consequences of disrupting the integrity of the water treatment process. Its application enables cyber risk analysis by identifying potential information threats and considering their consequences. The application of the developed ontology is demonstrated by investigating attacks defined for a prototype of a flotation water treatment system.

Keywords: information security, semantic threat modeling, MITRE ATT&CK threat matrix, industrial control systems, water treatment facilities.

References

1. 11 recent cyber attacks on the water and wastewater sector. Wisdiam. 2024. Available at: https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/ (accessed 17.09.2025).
2. Almoabady T.A., et al. Protecting digital assets using an ontology based cyber situational awareness system. Frontiers in Artificial Intelligence. 2024. vol. 7. DOI: 10.3389/frai.2024.1394363.
3. Sanchez-Zas C., et al. A methodology for ontology-based interoperability of dynamic risk assessment frameworks in IoT environments. Internet of Things. 2024. vol. 27. 101267 p. DOI: 10.1016/j.iot.2024.101267.
4. Getting Started just the basics. CASE Ontology. 2025. Available at: https://caseontology.org/ontology/start.html (accessed 17.09.2025).
5. STIX 2.1 ontology model POC with Stardog using knowledge graphs and RDF. Smart City Cyber Security. 2024. Available at: https://smartcitysecurity.net/stix-2-1-ontologymodel-poc-with-stardog-using-knowledge-graphs-and-rdf/ (accessed 17.09.2025).
6. Introduction to STIX. GitHub. 2024. Available at: https://oasis-open.github.io/cti-documentation/stix/intro (accessed 17.09.2025).
7. D3FEND Analytic Technique Taxonomy. MITRE. 2024. Available at: https://d3fend.mitre.org/acf/ (accessed 17.09.2025).
8. Akbar K.A., et al. The Design and Application of a Unified Ontology for Cyber Security. In: Muthukkumarasamy V., Sudarsan S.D., Shyamasundar R.K. (eds). Information Systems Security. Lecture Notes in Computer Science. Springer. 2023. vol. 14424. pp. 23–41.

9. MITRE ATTCK. 2025. Available at: https://attack.mitre.org/ (accessed 17.09.2025).
10. D3FEND. A knowledge graph of cybersecurity countermeasures. MITRE. 2025. Available at: https://d3fend.mitre.org/ (accessed 17.09.2025).
11. CWE: Common Weakness Enumeration. MITRE. 2025. Available at: https://cwe.mitre.org/ (accessed 17.09.2025).
12. CVE: Common Vulnerabilities and Exposures. MITRE. 2025. Available at: https://www.cve.org/ (accessed 17.09.2025).
13. Doynikova E., et al. Ontology of Metrics for Cyber Security Assessment. Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). DOI: 10.1145/3339252.3341496.
14. Khaleghi M., et al. Context-Aware Ontology-based Security Measurement Model. Journal of Information Security and Applications. 2022. vol. 67. 103199 p. DOI: 10.1016/j.jisa.2022.103199.
15. Mozzaquatro B.A., et al. An Ontology-Based Cybersecurity Framework for the Internet of Things. Sensors. 2018. vol. 18. no. 9. 3053 p. DOI: 10.3390/s18093053.
16. Sanchez-Zas C., et al. Ontology-based approach to real-time risk management and cyber-situational awareness. Future Generation Computer Systems. 2023. vol. 141. pp. 462–472. DOI: 10.1016/j.future.2022.12.006.
17. Khalil K., et al. CyberROAD: A cybersecurity risk assessment ontology for automotive domain aligned with ISO/SAE21434:2021. Journal of Information Security and Applications. 2025. vol. 90. 104015 p. DOI: 10.1016/j.jisa.2025.104015.
18. Alanen J., et al. Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliability Engineering System Safety. 2022. vol. 220. 108270 p. DOI: 10.1016/j.ress.2021.108270.
19. Bughio K.S., et al. Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring. Sensors. 2024. vol. 24. no. 9. 2804 p. DOI: 10.3390/s24092804.
20. Preuveneers D., et al. An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Applications. Future Internet. 2024. vol. 16. no. 3. 69 p. DOI: 10.3390/fi16030069.
21. Dash S., et al. From Data to Defense: How Ontology Fuels AI in Cyber Threat Detection. Proceedings of the 8th International Conference on Advances in Artificial Intelligence (ICAAI '24). 2025. pp. 121–133. (ICAAI '24). DOI: 10.1145/3704137.3704176.
22. Seydoux N., et al. IoT-O, a Core-Domain IoT Ontology to Represent Connected Devices Networks. In: Blomqvist E., Ciancarini P., Poggi F., Vitali F. (eds). Knowledge Engineering and Knowledge Management. Lecture Notes in Computer Science. Springer. 2016. vol. 10024. pp. 561–576.
23. Novikova E., et al. Dataset Generation Methodology: Towards Application of Machine Learning in Industrial Water Treatment Security. SN Computer Science. 2024. vol. 5. 373 p. DOI: 10.1007/s42979-024-02704-9.

Saenko Igor Borisovich — Ph.D., Dr. Sci., Professor, Chief scientific officer, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: automated information systems, information security, artificial intelligence, machine learning, modeling theory and mathematical statistics, information theory. The number of publications — 500. ibsaen@comsec.spb.ru; 39, 14th line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-7181; fax: +7(812)328-4450.

Novikova Evgenia Sergeevna — Ph.D., Senior researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: information system security, anomaly detection using machine

learning methods, providing confidential machine learning. The number of publications — 150. novikova@comsec.spb.ru; 39, 14th line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-7181; fax: +7(812)328-4450.

Meleshko Aleksei Viktorovich — Junior research assistant, International Center for Digital Forensics, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: attack detection using machine learning, wireless sensor network security, additive manufacturing security. The number of publications — 55. meleshko.a@iias.spb.su; 39, , 199178, Saint-Petersburg, Russia; office phone: +7(812)328-7181; fax: +7(812)328-4450.

Sadovnokov Vladimir Evgenevich — Graduate student, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: detection of computer attacks, machine learning. The number of publications — 25. bladimir1998@mail.ru; 39, 14th line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-7181; fax: +7(812)328-4450.

Acknowledgements. The research is supported by the grant of Russian Science Foundation #23-11-20024, https://rscf.ru/project/23-11-20024/, and St. Petersburg Science Foundation.