Проект РФФИ 19-07-01246 А
«Методики оценки защищенности и противодействия кибератакам в системах индустриального Интернета вещей на основе онтологии метрик безопасности и методов интеллектуального анализа больших данных»

Проект посвящен разработке новых методик интеграции и анализа данных безопасности для получения обоснованных оценок защищенности и выбора защитных мер в системах индустриального Интернета вещей (ИИВ) на основе выявления взаимосвязей и природы взаимосвязей между разнородными данными безопасности. Целью на весь срок выполнения проекта являлось повышение эффективности систем управления информационной безопасностью для ИИВ за счет разработки методик оценки защищенности и выбора защитных мер на основе онтологии метрик безопасности и методов интеллектуального анализа больших данных. Актуальность заявленной цели подтверждается развитием ИИВ с одной стороны, и ростом потерь в результате киберпреступлений в России, с другой.

Для достижения поставленной цели в Проекте были поставлены и решены следующие задачи:

1. Разработка онтологии метрик, ориентированной на задачи оценки защищенности и поддержки принятия решений по противодействию кибератакам, и связывающей первичные данные безопасности, получаемые из событий безопасности и открытых источников данных, с метриками безопасности и уровнем защищенности системы. Данная задача была разбита на подзадачи: (1.1) анализ объектов, журналов событий и особенностей индустриального Интернета вещей (ИИВ); (1.2) классификация метрик безопасности и последующее формирование иерархического набора метрик, на основе анализа взаимосвязей между целями оценки защищенности, объектами процесса оценки защищенности, источниками данных безопасности, и предоставляемыми ими характеристиками; (1.3) формирование онтологии метрик, ориентированной на задачи оценки защищенности и поддержки принятия решений по противодействию кибератакам.

2. Разработка методик оценки защищенности и выбора контрмер на основе разработанной онтологии. Данная задача была разбита на подзадачи: (2.1) усовершенствование онтологии метрик, разработанной на первом году выполнения проекта, ориентированной на задачи оценивания защищенности и поддержки принятия решений по противодействию кибератакам, и связывающей первичные данные безопасности, получаемые из событий безопасности и существующих эксплойтов, с метриками защищенности и уровнем защищенности системы; (2.2) разработка методики применения онтологии для решения задачи оценивания защищенности, включая выявление возможных угроз, прогнозирование атак и определение профилей атакующих; (2.3) разработка методики применения онтологии для решения задачи выбора защитных мер, то есть определения наилучших способов противодействия различным профилям атакующих, в интересах своевременного принятия адекватных решений по противодействию событиям, нарушающим безопасность индустриального Интернета вещей.

3. Экспериментальная оценка предложенных методик и сравнение их с существующими аналогами. Данная задача была разбита на подзадачи: (3.1) построение архитектуры системы, реализующей предложенные методики; (3.2) разработка прототипа программного средства, реализующего предложенные методики, в том числе, разработка онтологии на языке OWL, реализация методик применения онтологии для решения задач оценивания защищенности и выбора контрмер на языке Python, тестирование прототипа и доработка методик и онтологии; (3.3) проведение экспериментов для оценки эффективности предложенных методик и сравнение их с существующими аналогами, в том числе, разработка моделей и методов оценки эффективности разработанных методик.

Выполнение перечисленных задач позволило получить следующие основные результаты:

1. Определены основные объекты оценки защищенности и характеристики ИИВ, в том числе объектов, данных и протоколов их передачи, а также требования к системам управления безопасностью таких систем. В рамках результата введена оригинальная классификация устройств ИИВ; выделены требования и ограничения систем управления безопасностью ИИВ, и как следствие, требования к разработанной онтологии метрик; систематизированы существующие исследования по оцениванию защищенности ИИВ.

2. Проведен анализ журналов событий объектов ИИВ, способов представления событий и их характеристик, и существующих средств мониторинга безопасности ИИВ на предмет предоставляемых ими данных, а также первичные признаки событий, конфигураций и инцидентов. Разработана методика анализа журналов событий на основе структурного анализа, новизна которой заключается в возможности выделения характеристик событий из неформализованных журналов безопасности, в том числе типов событий и объектов-источников событий, а также взаимосвязей между событиями. Предложена классификация событий безопасности.

3. Определены источники входных данных безопасности и набор протоколов унифицированного представления исходных данных для их последующей автоматической обработки. В рамках результата определен и систематизирован набор источников данных безопасности, полнота которого подтверждается покрытием всех объектов, участвующих в оценке защищенности. Новизна заключается в выявлении взаимоотношений между источниками и между данными безопасности, для представления которых выбраны форматы унифицированного представления данных, для последующей автоматической обработки.

4. Введена классификация подзадач оценки защищенности и выбора защитных мер, классификация метрик безопасности на основе анализа выделенных метрик безопасности ИИВ, предложенных исследователями метрик безопасности компьютерных сетей и выделенных классов задач оценки защищенности и выбора контрмер. Новизна и оригинальность результата заключается во введении классификации метрик по нескольким признакам, в том числе, по типу задач оценки защищенности и выбора защитных мер (целям), по типу объекта, участвующего в оценке защищенности, по порядку вычисления метрик, и определении набора метрик и их источников.

5. Определен набор иерархически связанных метрик безопасности, позволяющих оценивать защищенность инфраструктур систем ИИВ на разных этапах их функционирования и с разной степенью точности. Введенная иерархия основана на разработанной классификации метрик, и отличается тем, что уровни метрик выделяются в зависимости от порядка их вычисления: от первичных метрик безопасности, получаемых от источников данных, до вторичных метрик, выделенных в соответствии с объектами процесса оценивания защищенности, и до интегральных метрик, выделенных в соответствии с целями оценивания защищенности, и отвечающих на вопросы оценивания защищенности и выбора защитных мер. Связи между метриками определены на основе связей между целями, объектами оценки, и самими метриками.

6. Разработана онтология метрик безопасности, в том числе представление верхнего уровня абстракции, и детальное представление онтологии, связывающей «сырые» (исходные) данные, первичные и интегрированные метрики, и уровень защищенности системы. Разработанная онтология включает четыре основных группы концептов: источников данных, объектов данных безопасности, объектов инфраструктуры, участвующих в процессе управления безопасностью, и метрик. Отличительной особенностью онтологии является определение метрик как отдельного концепта онтологии, связанного с другими концептами через объектные свойства, а не свойства данных. Таким образом, связи между метриками формируются как на основе родительских отношений между ними, так и на основе связей между концептами

онтологии, с которыми метрики связаны объектными свойствами. Это позволяет формировать связи от источников данных до интегральных метрик безопасности, и впоследствии определить алгоритм вычисления метрик, отвечающих на вопросы информационной безопасности. Другим отличием онтологии является введение класса концептов, соответствующего объектам инфраструктуры, что позволяет связать онтологию с любым типом киберфизических систем, в том числе, системами ИИВ. Также оригинальность результата состоит в разработанной методике интеграции данных безопасности из различных источников данных одного типа и одного источника данных, имеющего разные представления. Кроме того, предложенная онтология отличается новым подходом к ее динамическому формированию на основе анализа событий и сетевого трафика; детализацией концептов, связанных с источниками данных об атаках и контрмерах в рамках индустриального Интернета вещей; применением нового подхода к анализу исходного кода эксплойтов для выделения низкоуровневых признаков выполнения эксплойта, характеризующих используемые уязвимости; введением набора низкоуровневых метрик атакующего, извлеченных из сетевого трафика. Онтология реализована с использованием языка OWL.

7. Разработана методика применения онтологии для оценки защищенности, отличающаяся новым подходом к формированию онтологии на основе динамической информации; использованием онтологии для вывода формулы вычисления интегральной метрики защищенности на основе связей между объектами инфраструктуры, данными безопасности, первичными и интегральными метриками; и новым алгоритмом оценивания защищенности, учитывающим веса, сопоставленные отношениям между объектами онтологии, для получения оценок защищенности. Методика включает два основных этапа: формирование онтологии и оценивание защищенности с использованием разработанной онтологии. Второй этап, в свою очередь, включает определение доступных данных для ответа на вопрос оценивания защищенности; расширение знаний с использованием отношений между концептами онтологии; и вычисление интегральной метрики защищенности. Рассматриваемый набор экземпляров онтологии и отношения, учитываемые при расширении знаний и формировании формулы вычисления интегральной метрики для ответа на вопрос оценивания защищенности, зависят от вычисляемой метрики и конкретного алгоритма оценивания защищенности, которые, в свою очередь, зависят от вопроса оценивания защищенности.

8. Разработана методика применения онтологии для выбора мер противодействия кибератакам, отличающаяся использованием в рамках методики выбора контрмер оригинальной онтологии, методики прогнозирования инцидентов безопасности на основе корреляции событий безопасности, и оригинального интегрального показателя для выбора мер противодействия. Методика работает с учетом обнаруженных событий безопасности и различных профилей атакующих. Она использует объекты и отношения онтологии, взаимодействующие в процессе оценивания защищенности и выбора мер противодействия кибератакам, а также метрики защищенности, лежащие в основе методик оценивания защищенности и выбора мер противодействия. Методика включает определение набора доступных данных для ответа на вопрос, связанный с выбором мер противодействия кибератакам; выбор мер противодействия путем логического вывода с использованием отношений между концептами разработанной онтологии; и выбор оптимальной меры противодействия за счет оптимизации коэффициента выбора мер противодействия, рассчитанного для доступных мер. Задействованные концепты онтологии и конкретные алгоритмы выбора контрмер зависят от выбранного вопроса. Выходными данными методики являются доступные меры противодействия и значения коэффициентов выбора, и оптимальная мера противодействия.

9. Разработана архитектура системы оценивания защищенности и выбора контрмер, отличающаяся применением предложенных оригинальных методик,

разработанной онтологии, совместимостью с системами управления информационной безопасностью и возможностью обработки больших данных безопасности.

10. Разработан прототип программного средства, реализующего методику применения онтологии для оценки защищенности и выбора мер противодействия кибератакам.

11. Предложены модели и методы оценки эффективности разработанных методик, а также результаты оценки предложенных методик и сравнения их с существующими аналогами, демонстрирующие достижение поставленной цели повышения эффективности систем управления информационной безопасностью для индустриального Интернета вещей.

Таким образом, в рамках Проекта была разработана онтология метрик безопасности, ориентированная на задачи оценки защищенности и поддержки принятия решений по противодействию кибератакам, а также методики обработки данных безопасности, методики расчета метрик и их применения в задачах оценки защищенности и поддержки принятия решений по противодействию кибератакам в индустриальном Интернете вещей. Суть разработанного подхода заключается в том, что в основу процесса оценки защищенности ставится набор иерархически взаимосвязанных метрик безопасности, позволяющих оценивать защищенность инфраструктур подобных систем на разных этапах их функционирования и с разной степенью точности в зависимости от доступных данных безопасности, новых знаний, получаемых в процессе оценки защищенности, и целей оценки защищенности. Разработанная онтология формируется путем выявления взаимосвязей и природы взаимосвязей между первичными признаками исходных данных безопасности, набором иерархически взаимосвязанных метрик безопасности и текущим уровнем защищенности системы.

Для достижения заявленных результатов использовались методы классификации, методы теоретического и системного анализа, методы статистического и структурного анализа, методы семантического анализа, методы логического вывода, методы интеллектуального анализа данных, включая методы агрегации, нормализации и кластеризации данных, методы машинного обучения и методы оптимизации.

Эксперименты показали, что применение разработанных методик позволяет отслеживать изменения в уровне защищенности системы при изменениях конфигурации системы или новой информации об уязвимостях информационных систем, а также при добавлении новых средств защиты в систему, выделять из множества зафиксированных инцидентов безопасности те, на которые необходимо обратить внимание, расследовать и применить дополнительные контрмеры, собирать информацию о внутренних и внешних атакующих и предотвращать достижение их целей по компрометации анализируемой системы.

Полученные результаты также могут быть использованы при формировании и обработке новых знаний в других видах управленческих систем.