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 подходов к интеграции и анализу данных безопасности для получения обоснованных оценок защищенности и выбора защитных мер в системах индустриального Интернета вещей (ИИВ). Целью на весь срок выполнения проекта является повышение эффективности систем управления информационной безопасностью для ИИВ за счет разработки методик оценки защищенности и выбора защитных мер на основе онтологии метрик защищенности и методов интеллектуального анализа больших данных. Актуальность заявленной цели подтверждается развитием ИИВ с одной стороны, и ростом потерь в результате кибер преступлений в России, с другой.

Для достижения поставленной цели, на втором году выполнения проекта ставились следующие задачи: (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) разработка методики применения онтологии для решения задачи оценивания защищенности, включая выявление возможных угроз, прогнозирование атак и определение профилей атакующих; (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 ИИВ.

Выполнение перечисленных задач позволило получить следующие основные результаты: (1) усовершенствованная онтология метрик защищенности; (2) методика применения онтологии для оценки защищенности; (3) методика применения онтологии для выбора мер противодействия кибератакам. 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.

В рамках первого результата усовершенствована онтология метрик защищенности, включающая четыре основных группы концептов: источников данных, объектов данных безопасности, объектов инфраструктуры, участвующих в процессе управления безопасностью, и метрик защищенности. Усовершенствованная 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 ИИВ; 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. Данная онтология стала основой методик оценивания защищенности и выбора контрмер.

В рамках второго результата разработана методика применения онтологии для оценивания защищенности. Разработанная методика включает два основных этапа: формирование онтологии и оценивание защищенности с использованием разработанной онтологии. Первый этап включает заполнение онтологии на основе условно статической информации из открытых баз данных безопасности, и на основе динамической информации с применением подхода к ее динамическому формированию на основе анализа событий и сетевого трафика. Входными данными второго этапа выполнения методики являются: онтология, сформированная на первом этапе; список вопросов оценивания защищенности; метрики и алгоритмы для ответа на поставленные вопросы оценивания защищенности. Второй этап включает шаги: (1) определение доступных данных для ответа на вопрос оценивания защищенности (и соответствующих экземпляров онтологии); (2) расширение знаний с использованием отношений между концептами онтологии и вычисление интегральной метрики защищенности; и дополнительный шаг (3) анализ отдельных полей концептов онтологии, выделенных в группу для дополнительного анализа. Рассматриваемый на

втором шаге 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. Выходными данными второго этапа выполнения методики являются формула вычисления и значение интегральной метрики, отвечающей на вопрос оценивания защищенности.

Разработанная методика отличается новым подходом к формированию семантической модели 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.

Применение данной методики позволит 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. В итоговой реализации, методика позволит собирать информацию о внутренних и внешних атакующих и предотвращать достижение их целей по компрометации анализируемой системы.

В рамках третьего результата разработана методика выбора мер противодействия кибератакам на основе онтологии. Разработанная методика 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. Входными данными методики являются: онтология, сгенерированная на первом этапе выполнения методики оценивания защищенности; список вопросов, связанных с выбором мер противодействия кибератакам; метрики и алгоритмы для ответа на поставленные вопросы. Задействованные концепты онтологии и конкретные алгоритмы выбора контрмер зависят от выбранного вопроса. Методика включает следующие шаги: (1) определение набора доступных данных (и соответствующих экземпляров онтологии) для ответа на вопрос, связанный с выбором мер противодействия кибератакам; (2) выбор мер противодействия путем логического вывода с использованием отношений между концептами разработанной онтологии; (3) выбор оптимальной меры противодействия за счет оптимизации коэффициента выбора мер противодействия, рассчитанного для доступных мер. Выходными данными методики являются доступные меры противодействия и значения коэффициентов выбора, и оптимальная мера противодействия.

Разработанная методика отличается использованием оригинальной онтологии метрик защищенности, оригинальной методики прогнозирования инцидентов безопасности на основе корреляции событий безопасности, и оригинального интегрального показателя для выбора мер противодействия.

В следующем году планируется: завершить реализацию онтологии; разработать архитектуру компонента, предназначенного для интеграции с системами управления информационной безопасностью, и реализующего разработанные методики; реализовать методику динамического формирования онтологии и разработанные методики применения онтологии для решения таких задач, как оценивание защищенности и выбор защитных мер; проработать и реализовать входящие в методики алгоритмы. При реализации компонента, для использования системы управления информационной безопасностью как источника данных об инцидентах безопасности, событиях, происходящих в анализируемой системе и сетевом трафике, будут применяться методы интеллектуального анализа больших данных. Реализация разработанной онтологии и методик позволят провести их теоретическую и экспериментальную оценку, определить качество их влияния на принятие решений по реагированию и уровень защищенности систем ИИВ, и сравнить их с существующими аналогами. Полученные на втором этапе выполнения проекта результаты являются необходимой основой для успешной разработки компонента, реализующего методики применения онтологии для оценивания защищенности и выбора мер противодействия кибератакам, а также оценки эффективности разработанных методик и сравнения их с существующими аналогами на следующем этапе выполнения проекта.