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 является 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, на первом году ставилась задача разработки 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 безопасности, с метриками безопасности и уровнем защищенности системы. Данная задача была разбита на ряд подзадач, включая (1) анализ объектов, журналов событий и особенностей ИИВ; (2) классификация метрик безопасности и последующее формирование иерархического набора метрик, с учетом классификации характеристик и задач оценки защищенности и выбора защитных мер, исходных данных безопасности, и связей между ними, позволяющего оценивать защищенность систем ИИВ 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; (3) формирование онтологии метрик, ориентированной на задачи оценки защищенности и поддержки принятия решений по противодействию кибератакам, связывающей «сырые» данные, первичные и интегрированные метрики, и уровень защищенности системы, на основе выявления взаимосвязей между исходными данными безопасности, их источниками, а также введенными концептами объектов предметной области оценки защищенности.

Выполнение перечисленных задач позволило получить следующие основные результаты: (1) 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; (2) 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 и инцидентов; (3) источники входных данных безопасности и набор протоколов унифицированного представления исходных данных для их последующей автоматической обработки; (4) 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; (5) набор иерархически связанных метрик безопасности, позволяющих оценивать защищенность инфраструктур систем ИИВ на разных этапах их функционирования и с разной степенью точности; (6) онтология метрик безопасности, в том числе представление верхнего уровня абстракции, и детальное представление онтологии, связывающей «сырые» данные, первичные и интегрированные метрики, и уровень защищенности системы. Для достижения заявленных результатов использовались методы классификации, методы теоретического и системного анализа, методы статистического, структурного и семантического анализа, методы логического вывода, методы интеллектуального анализа данных.

В рамках первого результата была введена оригинальная классификация компонентов ИИВ: на верхнем уровне выделены классы аппаратного обеспечения (АО), программного обеспечения (ПО) и протоколов взаимодействия. На нижнем уровне классификации каждый из этих классов включает подклассы, выделенные по следующим признакам: стандартные или специфичные для ИИВ АО/ПО/протоколы; наличие/отсутствие функций управления; наличие/отсутствие ограничений по ресурсам. Данная классификация необходима для определения концептов разрабатываемой онтологии, соответствующих объектам, входящим в конфигурацию анализируемой системы, и выделения метрик ИИВ. Кроме того, она позволит определять уровень критичности различных компонентов ИИВ. Требования к системам управления безопасностью ИИВ (и, как следствие, разрабатываемой онтологии и методикам) были определены на основе анализа особенностей систем ИИВ (таких как большие размеры и распределенность, динамичность, использование специфичного АО, ПО, и протоколов, и др.), и включают, например, возможность обработки больших объемов данных за ограниченное время, высокие требования к точности оценки, скорости обнаружения и предотвращения инцидентов, и живучести системы, и др.

В рамках второго результата разработана методика анализа журналов событий на основе структурного анализа, включающая этапы: (1) анализ множеств значений свойств в журнале событий для определения типов свойств; (2) анализ свойств, входящих в отдельные записи событий для выявления событий одного типа; (3) анализ отношений между свойствами разных событий для определения отношений между событиями (определения последовательностей событий для выявления инцидентов); (4) выявление

событий, относящихся к одному типу объектов. Новизна разработанной методики заключается в том, что она позволяет выделять характеристики событий из неформализованных журналов безопасности, в том числе типы событий и объектов-источников событий, и определять взаимосвязи между разнородной информацией безопасности. Данная методика и введенная классификация событий безопасности (по типам источника и типам события) стали основой для формирования динамической онтологии, в зависимости от характеристик зафиксированных в анализируемой системе событий. На следующем этапе выполнения проекта она будет использоваться как основа методики обнаружения и оценки инцидентов безопасности.

В рамках третьего результата определен и систематизирован набор источников данных безопасности, полнота которого подтверждается покрытием всех объектов, участвующих в процессе оценки защищенности, и предоставляющих данные безопасности, для представления которых выбраны соответствующие форматы унифицированного представления данных, для последующей автоматической обработки. Отличительной особенностью результата является тщательный анализ и выявление характеристик, предоставляемых разными источниками, и взаимосвязей между источниками и характеристиками, что является необходимой основой для разработанной онтологии.

Предложенная классификация метрик отличается тем, что она основана на нескольких признаках, выбранных исходя из требований построения онтологии метрик. В том числе, на классах подзадач оценки защищенности и выбора защитных мер (конфиденциальность, целостность, доступность, аутентичность, приватность, прозрачность, надежность, аудит, и индекс выбора контрмер), типах объектов, участвующих в процессе оценки защищенности (инфраструктура, уязвимость, слабое место, эксплойт, атака, атакующий, инцидент безопасности, защитная мера), порядке вычисления метрик (первичные, вторичные, интегральные), и включает набор метрик для оценки защищенности ИИВ и источники данных для их вычисления.

Предложенная иерархия метрик основана на разработанной в рамках предыдущего результата оригинальной классификации, и предполагает выделение уровней метрик в зависимости от порядка их вычисления от первичных метрик безопасности до вторичных и интегральных метрик, отвечающих на вопросы оценки защищенности и выбора защитных мер. Поскольку процесс вычисления метрик предполагается начинать с изначально доступных данных безопасности, соответствующих первичным метрикам, иерархия предназначена для оценки защищенности на разных этапах функционирования систем и с разной степенью точности в зависимости от доступных данных безопасности. Поскольку верхний уровень иерархии соответствует интегральным метрикам, выделенным в соответствии с целями оценки защищенности, иерархия позволяет оценивать защищенность в соответствии с выделенными целями. Поскольку средний уровень иерархии составляют метрики, выделенные в соответствии с объектами, участвующими в процессе оценки защищенности, к которым относятся, в том числе, компоненты ИИВ, она подходит для оценки защищенности и выбора защитных мер в системах ИИВ.

Разработанная онтология метрик безопасности является основным результатом первого этапа выполнения проекта. Она связывает «сырые» данные безопасности с интегральными метриками, необходимыми для ответов на вопросы информационной безопасности. Отличительной особенностью онтологии является определение метрик как отдельного концепта онтологии, связанного с другими концептами (информацией безопасности и объектами инфраструктуры) 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 сформировать механизм вычисления интегральных метрик, отвечающих на вопросы информационной безопасности. Онтология основана на оригинальной иерархии метрик (результат 5), позволившей определить связи между метриками, а также метриками и информацией безопасности и объектами инфраструктуры. Кроме того, отличием онтологии является введение отдельного класса концептов, соответствующего объектам инфраструктуры, что позволяет связать онтологию с любым типом киберфизических систем, в том числе, системами ИИВ (типы учитываемых объектов выделены в рамках результата 1). Также оригинальность данного результата состоит разработанной методике интеграции данных безопасности из различных источников данных одного типа и одного источника данных, имеющего разные представления.

В следующем году планируется продолжить работу над усовершенствованием разработанной онтологии, а также над разработкой методик оценки защищенности и выбора защитных мер на ее основе. Полученные на первом этапе выполнения результаты по определению значимых для оценки защищенности и принятия решений количественных метрик безопасности и связей между ними, объектами оценки, первичными данными безопасности и источниками данных, являются необходимой основой для успешной разработки методик оценки защищенности и выбора защитных мер на основе онтологического подхода и методов интеллектуального анализа больших данных на следующем этапе выполнения проекта.