Грант Российского научного фонда №15-11-30029
"Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах с учетом облачных сервисов и сетей Интернета вещей"
Описание выполненных работ и полученных в 2017 г. научных результатов

1. Разработана архитектура и программные прототипы компонентов сбора, предварительной обработки и корреляции информации и событий безопасности на основе применения комплекса распределенных интеллектуальных сенсоров и технологии больших данных.

Архитектура включает пять групп распределенных интеллектуальных сенсоров и сервисов, ответственных за: сбор данных; хранение данных; агрегацию данных; нормализацию и анализ данных; визуализацию данных. За реализацию каждой группы отвечает отдельный компонент общей архитектуры. Программные прототипы разработаны на базе вычислительного кластера обработки больших данных, сформированного в двух вариантах: на базе Hadoop и на базе Spark.

2. Разработана архитектура и программные прототипы надежной, доверенной шины данных и гибридного хранилища информации и событий безопасности.

Архитектура надежной, доверенной шины данных включает следующие уровни: кибернетический, физический и системный. Программный прототип шины данных разработан на основе протокола I2C. Архитектура гибридного хранилища информации и событий безопасности содержит: модуль загрузки информации безопасности из внешних источников; модуль нормализации данных; модуль анализа и формирования модели гибридного хранилища; модуль наполнения базы гибридного хранилища; модуль внешнего взаимодействия с другими компонентами разрабатываемой системы безопасности. Программный прототип гибридного хранилища содержит онтологические модели, позволяющие на основе логического вывода получать новые знания о безопасности и проводить автоматический выбор контрмер.

3. Разработана архитектура и программные прототипы компонентов обнаружения в реальном времени сложных многошаговых атак на основе технологий интеллектуального анализа информации и событий безопасности.

Архитектура имеет четырехуровневый механизм обработки данных. Программные прототипы позволяют обнаруживать отдельные атакующие действия за счет применения технологий интеллектуального анализа информации и событий безопасности, в том числе основанных на нейронных сетях.

4. Разработана архитектура и программные прототипы компонентов вычисления первичных и интегрированных метрик безопасности.

Архитектура включает модули, вычисляющие метрики в соответствии с предложенной ранее иерархической системой (топологического уровня, уровня атак, уровня атакующего, уровня событий, уровня контрмер и уровня системы). Программный прототип реализует следующие модели: зависимостей сервисов; Байесовского графа атак; событий; контрмер.

5. Разработана архитектура и программные прототипы компонентов анализа истории событий безопасности, прогнозирования действий нарушителей и их последствий.

Архитектура включает модуль анализа истории, который взаимодействует с базой данных инцидентов и передает результаты модулю вычисления метрик безопасности и прогнозирования действий нарушителей и их последствий. Программные прототипы реализуют модели, методики и алгоритмы анализа истории событий безопасности, прогнозирования действий нарушителей и их последствий (модель Байесовского графа атак, модель событий, методику анализа истории).

6. Разработана архитектура и программные прототипы компонентов автоматизированного реагирования на целевые информационно-программные и физические воздействия на основе гибридного хранилища информации и событий безопасности и основанного на экспертных знаниях логического вывода.

Архитектура охватывает следующие компоненты: обработки данных; оценки защищенности; выбора контрмер; моделирования атак; сбора входных данных. Разработаны методики использования программных прототипов для автоматизированного реагирования на целевые информационно-программные и физические воздействия на основе гибридного хранилища информации и событий безопасности и основанного на экспертных знаниях логического вывода.

7. Разработана архитектура и программные прототипы компонентов проактивного, динамического и многоаспектного управления инцидентами безопасности критически важных объектов с учетом облачных сервисов и сетей Интернета вещей.

Архитектура включает три уровня: 1) внешние источники данных (сенсоры), надежная и доверенная шина данных, компонент обработки и корреляции событий безопасности, гибридное хранилище данных, компонент интеллектуального анализа событий безопасности, компонент расчета метрик безопасности; компонент выбора контрмер и внешние системы, реализующие выбранные контрмеры; 2) компоненты, отвечающие за конкретные предметные области; 3) сервисы традиционных телекоммуникационных сетей, анализируемые с использованием системы управления инцидентами безопасности (СУИБ) , сервисы сетей Интернета вещей и облачные сервисы.

8. Разработаны научно-технические предложения по применению разработанных методов, моделей, методик, алгоритмов, архитектур и программных прототипов системы управления инцидентами безопасности для комплексной защиты элементов «умного дома».

Реализация обобщенной архитектуры перспективной системы управления инцидентами безопасности критически важных объектов для комплексной защиты элементов Умного дома состоит из нескольких основных частей: аппаратных источников информации; программных источников информации; концентраторов; сервера Умного дома; модуля аналитической обработки данных и визуализации (АОДВ); а также модуля интеграции с системами управления информацией и событиями безопасности (СУИСБ). Автоматизированное реагирование на целевые информационно-программные и физические воздействия осуществляются за счет следующих операций: 1) уведомление оператора об обнаруженных инцидентах, сценариях атак и аномальной активности; 2) уведомление оператора о необходимости усиления физического контроля инфраструктуры системы или её отдельных элементов; 3) уведомление о необходимости изменения правил доступа к сервисам системы. Для подтверждения корректности предложенного подхода спроектирован прототип системы Умного дома, а также осуществлён ряд экспериментов с ним.

9. Разработаны научно-технические предложения по применению разработанных методов, моделей, методик, алгоритмов, архитектур и программных прототипов системы управления инцидентами безопасности для комплексной защиты объектов РЖД.

Реализация обобщенной архитектуры перспективной системы управления инцидентами безопасности критически важных объектов для комплексной защиты объектов РЖД состоит из нескольких основных частей: модуля сбора данных; модуля управления данными; центрального процессора и информационной панели. Применение полученных результатов позволит реализовать динамический подход к управлению инцидентами за счет применения распределенных облачных сервисов, которые позволяют поддерживать в актуальном состоянии следующие базы знаний: 1) базы знаний правил процесса корреляции событий безопасности; 2) базы знаний шаблонов многошаговых атак; 3) базы знаний возможных конфликтов между элементами системы.

10. Разработаны научно-технические предложения по применению разработанных методов, моделей, методик, алгоритмов, архитектур и программных прототипов системы управления инцидентами безопасности для комплексной защиты объектов системы энерго- и водоснабжения.

Полученные в проекте результаты могут применяться для построения системы управления инцидентами безопасности для объектов системы энерго- и водоснабжения, где в качестве целевых процессов реализуются процессы накопления, распределения, передачи, учета объемов водного ресурса. Основные объекты инфраструктуры включают резервуары и каналы передачи воды между источниками и потребителями воды, а также энергогенерирующие мощности. Разработанные предложения учитывают разновидности физических сенсоров и активирующих элементов, в т.ч. сенсоров уровня воды, сенсоров величины потока воды, датчиков давления воды, электромеханических затворов (моделируемые посредством шаровых кранов с энергоприводом) и других элементы.

11. Разработаны научно-технические предложения по применению разработанных методов, моделей, методик, алгоритмов, архитектур и программных прототипов системы управления инцидентами безопасности для комплексной защиты инфраструктуры телекоммуникационной системы мобильной коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях.

Полученные в проекте результаты могут применяться для построения системы управления инцидентами безопасности кинфраструктуры телекоммуникационной системы мобильной коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях. Разработанные предложения учитывают разновидности имеющихся в наличии коммуникационных интерфейсов, физических сенсоров и активирующих элементов.

12. Проведена теоретическая и экспериментальная оценка эффективности методов, моделей, методик, алгоритмов и архитектур аналитической обработки больших данных для управления инцидентами и противодействия целевым кибер-физическим атакам в критически важных распределенных системах с учетом облачных сервисов и сетей Интернета вещей.

Экспериментальная оценка времени обработки данных показала, что применение параллельных вычислений позволяет реализовать требования по выполнению этого процесса в реальном или близком к реальному времени. Для задач корреляции событий безопасности было достигнуто ускорение более чем в 1.5 раза при помощи OpenMP и более чем в 1000 раз при помощи Cuda.

Время построения и анализа моделей атак не превысило 1 минуты для сети из 1000 хостов. Эксперименты показали, что поставленные функциональные и нефункциональные требования выполняются. Показано, что наибольший выигрыш достигается в случае реализации контрмер после первого инцидента. Средний выигрыш для тестовых компьютерных сетей составил 80% по сравнению с ситуацией отсутствия контрмер.

13. Получены 8 свидетельств о государственной регистрации программ для ЭВМ, и опубликовано 17 статей в научных изданиях, индексируемых в базах данных «Сеть науки» (Web of Science) и «Скопус» (Scopus), а также 11 публикаций в научных изданиях, индексируемых в РИНЦ.

14. Подготовлена и сдана в издательство одна монография. Также по результатам работы по проекту подготовлен к изданию материал еще двух монографий.

15.Организована и проведена 25-я юбилейная Международная конференция по параллельной, распределенной и сетевой обработке информации (PDP 2017), 6-8 марта 2017г., г. Санкт-Петербург, Российская Федерация, в том числе подготовлен сайт конференции https://www.pdp2017.org/, сформирован состав сопредседателей, программного и организационного комитетов конференции, проведены восемь специальных секций конференции, труды конференции опубликованы в сотрудничестве с Conference Publishing Services (CPS) международной ассоциации IEEE, труды конференции проиндексированы в международных базах цитирования Scopus и Web of Science.

16. Организована третья школа молодых ученых с приглашением в качестве лекторов ведущих российских и зарубежных ученых по тематике проекта . Название школы - "Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах" ("Incident management and countering targeted cyber-physical attacks in distributed large-scale critical systems", IM&CTCPA 2016). Даты проведения школы - 18 - 21 декабря 2017 г. Место проведения – СПИИРАН и Университет ИТМО, Санкт-Петербург. В школе принимает участие 150 участников, из них: 13 российских и 11 зарубежных ученых-лекторов (в том числе из Франции, Украины, Италии, Германии и Чехии).

17. Сделаны выступления на 20 международных и российских научных конференциях, где обсуждались вопросы по теме проекта.

Информационные ресурсы в сети Интернет, посвященные проекту:

- информация о проекте РНФ:

http://www.comsec.spb.ru/ru/projects

http://www.comsec.spb.ru/en/projects/

- информация об очной международной научной конференции:

https://www.pdp2017.org/

http://www.comsec.spb.ru/ru/pdp2017/

http://www.comsec.spb.ru/pdp2017/

- информация о школе молодых ученых (с презентациями лекций):

http://www.comsec.spb.ru/ru/imctcpa17/

http://www.comsec.spb.ru/imctcpa17/