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 2016 г. научных результатов

1. Разработана общая архитектура перспективной системы управления инцидентами безопасности критически важных объектов. На основе проведенного анализа применимости принципов проактивности, динамичности и многоаспектности к управлению инцидентами безопасности критически важных объектов выделены следующие компоненты системы управления инцидентами безопасности: (1) внешние источники данных (сенсоры); (2) надежная и доверенная шина данных; (3) компонент обработки и корреляции событий безопасности; (4) гибридное хранилище данных; (5) компонент интеллектуального анализа событий безопасности; (6) компонент расчета метрик безопасности; (7) компонент выбора контрмер; (8) внешние системы, реализующие выбранные контрмеры.

2. Разработаны методы, модели, методики и алгоритмы сбора, предварительной обработки и корреляции информации и событий безопасности на основе применения комплекса распределенных интеллектуальных сенсоров и концепции больших данных. Разработаны методы, модели, методики и алгоритмы сбора и предварительной обработки информации и событий безопасности критически важных объектов. Сформулирована постановка задачи обеспечения агрегирования информации и событий безопасности, которая декомпозирована на две подзадачи: определения последовательности выполнения операторов потоковой обработки данных, реализующих требуемые запросы на агрегацию; распределения операторов по узлам транспортной сети, обеспечивающим параллельную обработку последовательностей операторов потоковой обработки данных. Для решения обеих задач предложено использовать подход, основанный на технологии Complex Event Processing. В качестве инструментальной платформы исследована и использована программная система Spark Streaming. Разработаны методы, модели, методики и алгоритмы корреляции информации и событий безопасности, которые основаны на комбинации нескольких подходов: машинах конечных состояний, правило-ориентированном подходе, методе рассуждения на основе прецедентов, Байесовских сетях, искусственных нейронных сетях.

3. Разработаны методы, модели, методики и алгоритмы функционирования надежной, доверенной шины данных и гибридного хранилища информации и событий безопасности. Заданы требования к шине данных, обусловливающие необходимость обеспечения надежности передачи данных в условиях воздействия компьютерных атак, достоверности передаваемых данных, исключающей возможность стороннего и (или) несанкционированного внедрения, и оперативности передачи данных в условиях, приближенных к реальному времени. На этой основе определены методы, модели, методики и алгоритмы функционирования надежной, доверенной шины данных. Определены методы, модели, методики и алгоритмы гибридного хранилища информации и событий безопасности, включающие методы представления информации и событий безопасности, методику построения гибридного хранилища, методику выбора инструментального средства для создания гибридного хранилища, а также модели и алгоритмы разграничения доступа к гибридному хранилищу.

4. Разработаны методы, модели, методики и алгоритмы обнаружения в реальном времени сложных многошаговых целевых атак на основе технологий интеллектуального анализа информации и событий безопасности. Предложены модели и методы обнаружения целевых атак, основанные на технологиях интеллектуального анализа данных и событий безопасности: модель двухслойной нейронной сети в качестве бинарного классификатора для обнаружения целевых атак; модель нейро-нечеткого классификатора на основе нечеткого вывода Такаги-Сугено; метод обнаружения атак, основанный на машине опорных векторов. Для обнаружения в реальном времени сложных многошаговых целевых атак разработана методика, основанная на аналитическом моделировании, которая использует информацию об инцидентах безопасности, получаемую от предложенных моделей, методов и алгоритмов обнаружения целевых атак.

5. Разработаны методы, модели, методики и алгоритмы вычисления первичных и интегрированных метрик безопасности. Предложены методы, методики и алгоритмы расчета различных метрик (топологического уровня, уровня графа атак, уровня атакующего, уровня событий, уровня контрмер и интегрального уровня). Разработаны модели (в том числе модель атак в виде Байесовского графа атак, модель зависимостей между сервисами сети, модель сервиса, модель атакующего, модель события и модель контрмеры), методики и алгоритмы вычисления показателей защищенности, включенных в таксономию.

6. Разработаны методы, модели, методики и алгоритмы анализа истории событий безопасности, прогнозирования действий нарушителей и их последствий. Обработанные события поступают от подсистемы корреляции и указывают на компрометацию хоста сети (то есть нарушение свойств конфиденциальности/ целостности/ доступности или нелегитимное получение прав доступа). Для анализа событий применяются разработанные модели атак, атакующего и события. Изменение элементов состояния данных моделей позволяет прогнозировать дальнейшие шаги нарушителя. Модель события определяет момент, в который было зафиксировано событие, хост, на котором оно было зафиксировано, и тип события (то есть последствия для системы). Для фиксации изменения состояний модели атак (Байесовского графа атак) и атакующего вводится связь между этими моделями и моделью события. Связь осуществляется через хост и последствия (тип компрометации хоста). На основе этих данных и разработанной методики определяется текущая позиция нарушителя в системе. Кроме того учитывается информация о предыдущих зафиксированных событиях с учетом их временных и пространственных характеристик, для отнесения событий к одной атаке или нескольким различным многошаговым атакам.

7. Разработаны методы, модели, методики и алгоритмы, архитектуры 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 и логическом выводе. Компонент реагирования на основе гибридного хранилища информации и событий безопасности использует для логического вывода исчисление событий и темпоральную логику. Компонент реагирования, основанный на экспертных знаниях, использует показатели защищенности и реализует основанный на их анализе метод выбора контрмер. Компонент реагирования, основанный на нечетком логическом выводе, обеспечивает принятие решений о наличии аномального поведения системы, используя метод нечеткого вывода Мамдани.

8. Разработаны методы, модели, методики и алгоритмы, архитектуры и программные прототипы компонентов проактивного, динамического и многоаспектного управления инцидентами безопасности критически важных объектов с учетом облачных сервисов и сетей Интернета вещей.

Предложенные результаты реализованы на примере системы контроля и управления доступом в офисное здание, построенной с использованием программируемого микроконтроллера Arduino Yun, цифровых датчиков RFID, рабочих станций, серверного и связующего сетевого оборудования.

9. Разработаны модели конкретных предметных областей (умный дом, РЖД, система энерго- и водо-снабжения, мобильная коммуникационная сеть поддержки и оперативного управления в чрезвычайных ситуациях) как объектов управления инцидентами безопасности.

Предложенная комплексная модель системы Умного дома содержит три уровня представления. Нижний уровень представлен моделями программных и аппаратных источников информации, предназначенных для моделирования отдельных аспектов концепции Интернета вещей. На промежуточном уровне осуществляется моделирование сетевой инфраструктуры, объединяющей отдельные программные и аппаратные источники информации в единую систему сбора, хранения и предобработки информации и событий безопасности. Верхний уровень содержит модель Умного дома как объекта управления инцидентами безопасности.

Физическая модель системы централизации, сигнализации и блокировки РЖД состоит из четырех уровней. Первый (операторский) уровень представлен графическим пользовательским интерфейсом, который служит для отображения информации о состоянии объектов железнодорожной автоматики, диспетчерского контроля и централизации. Второй (вычислительный) уровень представлен в модели персональным компьютером, служащим для выполнения функций сбора, хранения, обработки и передачи информации о текущем состоянии объектов централизации, а также диагностики системы централизации. Третий уровень (уровень управления и контроля состояния напольного оборудования) моделируется в виде системы контроллеров на базе Arduino. Для моделирования четвертого уровня (уровня физических устройств железнодорожной автоматики) используется модель железной дороги под цифровым управлением от компании Piko.

Разработанная физическая модель дамбы включает ряд гидротехнических приспособлений – емкостей для воды, сенсоров, переключателей, шлангов, работающих в связке с микроконтроллером Arduino Yun, которые на физическом уровне позволяют моделировать процессы протекания воды, открытие и закрытие шлюзов, превышение уровня воды установленных ограничений и т.п., а также программно-информационную часть системы, ответственную за сбор, обработку, анализ и отображение пользователю основных и критически-важных событий и инцидентов безопасности дамбы.

В качестве основы для прототипа мобильной коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях были выбраны встроенные устройства XBee s2, позволяющие организовать беспроводные коммуникации по протоколу ZigBee. Программно-аппаратная реализация данного протокола на физических устройствах сети обеспечивает свойства ее самоорганизации и самовосстанавливаемости после отказа одного из узлов или в случае ухудшения качества связи.

Для данных систем построены модели инцидентов безопасности. Рассмотрены возможные атаки на все уровни систем, а также получены примеры моделируемых инцидентов безопасности.

10. Получены три свидетельства о государственной регистрации программ для ЭВМ, и опубликовано шесть статей в научных изданиях (и одна статья принята для публикации),

индексируемых в базах данных «Сеть науки» (Web of Science) и «Скопус» (Scopus), а также десять публикаций в научных изданиях, индексируемых в РИНЦ.

11. Проведены подготовительные работы по организации 25-й юбилейной Международной конференции по параллельной, распределенной и сетевой обработке информации (PDP 2017), 6-8 марта 2017 г., г. Санкт-Петербург, Российская Федерация, в том числе подготовлен сайт конференции (http://pdp2017.org), сформирован состав сопредседателей, программного и организационного комитетов конференции, проведено рецензирование и отбор научных статей на конференцию из более чем 20 различных стран, заключено соглашение и начато сотрудничество с Conference Publishing Services (CPS) международной ассоциации IEEE для опубликования трудов конференции и др.

12. Проведена вторая школа молодых ученых с приглашением в качестве лекторов ведущих российских и зарубежных ученых по тематике проекта (первая школа была в 2015 г.). 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 - 31 октября - 2 ноября 2016 г. Место проведения - СПИИРАН, Санкт-Петербург. В школе приняло участие 79 участников, из них: 13 российских и 6 зарубежных ученых-лекторов (в том числе из Франции, Швеции, Финляндии, Белоруссии и Украины), а также 9 слушателей - российских молодых ученых в возрасте до 35 лет включительно, 51 аспирантов и студентов.

13. Сделаны выступления на 13 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:

http://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/imctcpa16/

http://www.comsec.spb.ru/imctcpa16/