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 в 2015 году работ и полученных научных результатов

1. Разработана концепция построения и архитектура системы управления инцидентами безопасности критически важных объектов. Проведен анализ условий реализации целевых информационно-программных и физических воздействий в облачных системах и сетях Интернета вещей. Рассмотрены различные подходы к пониманию термина «целевые атаки», которые предлагаются со стороны различных разработчиков средств защиты, определяющие особенности проявления данного класса атак. Приведены примеры и дана характеристика целевых атак. В соответствии с формированными критериями целевых атак, выполнено их сравнение с массовыми атаками. По результатам проведенного сравнения сформирован перечень отличительных признаков целевых атак и раскрыто их содержание. Определена последовательность и содержание этапов проведения целевых атак. Проведен анализ векторов направленности целевых атак. Обоснована необходимость создания системы управления инцидентами безопасности (СУИБ) для успешной реализации мероприятий защиты критически важных объектов (КВО). Выделены задачи, решаемые СУИБ для защиты КВО. Определены цель и основные принципы построения СУИБ для КВО – проактивность, динамичность и многоаспектность. Обоснован комплекс задач, который должна решать СУИБ для реализации заявленных принципов. Выявлены недостатки существующих СУИБ, не позволяющие реализовать указанные принципы. Сформирована концепция построения СУИБ КВО на основе принципов проактивности, динамичности и многоаспектности, включающая: общие положения; принципы управления инцидентами безопасности; цели и задачи СУИБ; особенности КВО как объектов защиты; механизмы управления инцидентами безопасности; общее описание архитектуры СУИБ КВО.

2. Разработан общий подход и требования, предъявляемые к компонентам сбора, предварительной обработки, корреляции информации и событий безопасности на основе применения комплекса распределенных интеллектуальных сенсоров и концепции больших данных. Обоснованы место и роль компонентов сбора, предварительной обработки и корреляции информации и событий безопасности в СУИБ КВО. Расположение данных компонентов предполагается на конечных и промежуточных узлах инфраструктуры КВО, а также в центре сбора и обработки информации. Выделены два типа основных элементов, которые составляют основу рассматриваемых компонентов на конечных и промежуточных узлах – интеллектуальные сенсоры и агрегаторы. Определен общий подход и требования к построению компонентов сбора данных на основе использования распределенных интеллектуальных сенсоров. Предложена общая схема размещения интеллектуальных сенсоров в СУИБ КВО. Обоснована необходимость реализации процедуры нормализации в ходе сбора данных. Сформированы требования, предъявляемые к компонентам сбора информации в СУИБ КВО. Определен общий подход и требования к построению компонентов предварительной обработки данных на основе использования распределенных интеллектуальных сенсоров. Показано, что компонентами СУИБ КВО, занимающимся непосредственной предварительной обработкой данных, являются агрегаторы. Сформирована общая схема размещения агрегаторов в СУИБ КВО, позволяющая продемонстрировать принципы их размещения с учетом концепции обработки больших потоков данных. Сформулированы требования, предъявляемые к компонентам предварительной обработки данных в СУИБ КВО, необходимые для корректной работы в режиме реального времени с учетом концепции

больших данных. Определен общий подход и требования к построению компонентов корреляции данных на основе использования распределенных интеллектуальных сенсоров. Определены функции компонентов корреляции. Показано, что основным компонентом корреляции является центр обработки данных, который может быть представлен одним или несколькими связанными хостами соответствующего уровня. Сформированы требования к компонентам корреляции событий безопасности СУИБ КВО.

3. Разработан общий подход и требования, предъявляемые к надежной, доверенной шине данных и гибридному хранилищу информации и событий безопасности. Обоснованы требования, предъявляемые к надежной, доверенной шине данных, которыми являются: высокая надежность шины; высокая достоверность обработки информации; высокая оперативность обработки информации. Определены особенности, которыми обладают облачные системы и сети Интернета вещей как среды для распространения по шине данных. Определено место шины данных в СУИБ КВО и установлены ее связи с другими системными компонентами. Обоснован общий подход к построению надежной, доверенной шины данных. Для этой цели, прежде всего, был проведен анализ и дана характеристика воздействующих на шину атак. Для повышения надежности функционирования шины данных в условиях наличия рассмотренных видов атак предложен подход, ориентированный на использование не только упреждающих способов защиты, но и стратегий апостериорной защиты информации. Обоснованы требования, предъявляемые к гибридному хранилищу информации и событий безопасности, для чего, в первую очередь, было определено место хранилища в структуре СУИБ. При этом требования к хранилищу были разделены на две группы: требования со стороны пользователей и требования со стороны остальных компонентов СУИБ. Обоснован общий подход к построению гибридного хранилища информации и событий безопасности. При этом, в первую очередь, были выделены наиболее перспективные и широко используемые стандарты для представления данных по безопасности (событий, инцидентов, атак и т.д.). Была обоснована необходимость дополнения реляционного формата данных в хранилище XML-форматом и RDF-форматом. Для реализации такой необходимости была предложена архитектура онтологического хранилища данных в СУИБ КВО.

4. Разработан общий подход и требования, предъявляемые к компонентам обнаружения в реальном времени сложных многошаговых атак на основе технологий интеллектуального анализа информации и событий безопасности. Для определения требований к системе обнаружения многошаговых целевых атак проведен анализ существующих реализаций подобных систем. На основе проведенного анализа были сформулированы основные функциональные и нефункциональные требования к компонентам обнаружения многошаговых целевых атак. В процессе разработки общего подхода к построению компонентов обнаружения целевых атак проанализированы различные стратегии, применяемые компаниями для защиты от целевых атак и рассмотрены специализированные методы обнаружения таких атак, позволяющие обнаружить их проявления как на этапе проведения атак, так и при расследовании уже произошедшего инцидента. Рассмотрены стандартные компоненты защиты, которые составляют основу для систем обнаружения сложных многошаговых целевых атак. В том числе были рассмотрены: межсетевые экраны; системы обнаружения вторжений; системы предотвращения вторжений; интернет-шлюзы; шлюзы электронной почты; ложные информационные системы; анализаторы сетевого трафика. Кроме компонентов защиты, которые принимают непосредственное участие в процессе обнаружения целевых атак, выделены компоненты, оказывающие косвенное влияние на обнаружение, но позволяющие повысить эффективность стандартных и комплексных компонентов защиты. Так, для противодействия использованию уязвимостей были проанализированы

следующие компоненты защиты: компонент автоматического обновления установленного программного обеспечения; компонент автоматического тестирования установленного программного обеспечения; компонент анализа сетевой инфраструктуры; компонент контроля доступа к сети. Выделены основные принципы, отличающие предлагаемый подход к построению компонентов защиты от существующих аналогов: принцип многоуровневости и принцип разнородности. Сделан вывод, что использование таких компонент позволит значительно повысить вероятность обнаружения и снизить возможные риски.

5. Разработан общий подход и требования, предъявляемые к компонентам вычисления первичных и интегрированных метрик безопасности.

Для разработки данного научного результата проведен развернутый анализ метрик, применяемых для оценки защищенности и поддержки принятия решений, и методик их вычисления. Указанный анализ позволил выявить основные результаты и направления в данной области, достоинства и недостатки существующих решений, а также дал возможность предложить основные требования к первичным и интегрированным метрикам безопасности. Данные требования были сформулированы с учетом стандартных требований к метрикам, требований к метрикам безопасности на основе проведенного обзора и требований со стороны анализируемой системы. Предложена классификация метрик безопасности, сформированная согласно данным, применяемым для вычисления метрик безопасности, и позволившая определить многоуровневый подход к вычислению первичных и интегрированных метрик безопасности. Разработан общий подход к вычислению метрик безопасности, включающий три этапа: сбор входных данных; вычисление метрик безопасности; определение уровня защищенности и выбор контрмер. Особенностью предлагаемого подхода является возможность определения уровня защищенности и выбора контрмер на различных уровнях функционирования защищаемой системы и с учетом доступных на момент анализа входных данных.

6. Разработан общий подход и требования, предъявляемые к компонентам анализа истории событий безопасности, прогнозирования действий нарушителей и их последствий. В процессе получения данного научного результата были сформулированы основные требования к функциональным и нефункциональным характеристикам компонентов анализа истории событий безопасности, прогнозирования действий нарушителей и их последствий. Разработан подход, основанный на оперативном построении, модификации и анализе моделей атак, который позволяет в режиме близком к реальному времени прогнозировать действия нарушителей и их последствия. Данный подход, за счет комплексного анализа многошаговой атаки, позволяет выявить группы событий, среди которых был возможно не обнаружен элемент многошаговой атаки. Это дает возможность выявлять эксплуатацию уязвимостей нулевого дня и другие скрытые действия нарушителя.

7. Проведена 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 2015). Даты проведения школы - 26-28 ноября 2015 г. Место проведения - Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург. В школе приняло участие 12 российских и 6 зарубежных ученых-лекторов (в том числе из Германии, Италии, Финляндии и Белоруссии), а также 37 слушателей - российских молодых ученых в возрасте до 35 лет включительно, аспирантов и студентов.

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.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/imctcpa15/
  http://www.comsec.spb.ru/imctcpa15/