Основные результаты Проекта “Разработка моделей, методик и алгоритмов автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности”.

Цель Проекта состояла в повышении эффективности систем управления информацией и событиями безопасности за счет разработки моделей, методик и алгоритмов автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов. Необходимость достижения цели объясняется ущербом, который несут различные организации из-за успешных атак на важные для их функционирования сервисы информационно-технологической инфраструктуры. Детальный анализ исследований в области автоматизированного реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов позволил выявить основные достоинства и недостатки существующих подходов, и сделать вывод о необходимости комплексного подхода, объединяющего ряд моделей, методик и алгоритмов, и позволяющего: получать адекватную и актуальную оценку защищенности системы; учитывать характеристики атакующего, взаимосвязи между сервисами сети, стоимостные характеристики атак и защитных мер; выявлять слабые места компьютерной сети; выявлять возможные атаки на сеть, и получать набор показателей защищенности, характеризующий их; учитывать инциденты безопасности и переоценивать ситуацию по защищенности в соответствии с полученной информацией; своевременно выбирать наиболее адекватное решение по реагированию.

Для достижения целей проекта была разработана система показателей защищенности, аналитические модели объектов оценки защищенности и реагирования на инциденты, методики автоматизированной оценки защищенности и реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов.

Для адекватной и актуальной оценки защищенности анализируемой системы, а также для своевременного выбора рациональных защитных мер на основе доступных входных данных, **разработана система показателей защищенности** для которой **введена иерархическая классификация показателей защищенности** на уровни на основе входных данных, применяемых для их вычисления (самый нижний топологический уровень включает показатели, вычисляемые на основе данных о составе и конфигурации анализируемой системы, следующий уровень атак – показатели, вычисляемые на основе данных об атаках, уровень атакующего – показатели, вычисляемые на основе данных об атакующем, уровень событий – показатели, вычисляемые на основе данных об инцидентах безопасности, поступающих от системы управления информацией и событиями безопасности, уровень выбора контрмер – показатели, характеризующие контрмеры, и верхний интегральный уровень объединяет показатели, вычисляемые на основе показателей предыдущих уровней), режимов оценки защищенности (топологический уровень, уровень атак и атакующего соответствуют статическому режиму, или режиму проектирования системы, а уровень событий – динамическому режиму, или режиму эксплуатации анализируемой системы), и типов показателей (базовые характеристики, стоимостные характеристики, и характеристики, учитывающие уязвимости нулевого дня). Система позволяет для каждой выделенной группы показателей (топологические, атак, атакующего и событий) получить оценку защищенности системы и выбрать защитные меры (с использованием показателей интегрального уровня).

Для последующего применения в рамках методик оценки защищенности и реагирования на инциденты безопасности **разработаны аналитические модели объектов оценки защищенности и реагирования на инциденты**. Основными являются модель атак (граф атак) и модель зависимостей сервисов системы (граф зависимостей сервисов). Модель зависимостей сервисов в виде направленного графа (узлы – сервисы, дуги – связи между ними, определяющие зависимость свойств безопасности сервиса предка от свойств безопасности сервиса потомка) введена для отслеживания распространения ущерба в системе взаимодействующих сервисов, и позволяет определять влияние атак и контрмер на активы

сети. Модель атак в виде байесовского графа атак (узлы графа – атакующие действия, дуги – связи между ними) введена для определения направления развития атак, их вероятностей, и влияния событий на вероятность успешной атаки. Все модели взаимосвязаны для совместного применения в рамках оценки защищенности и выбора контрмер. Для задания значений параметров моделей используются данные из различных источников, в том числе из открытых баз уязвимостей, атак и слабых мест (NVD, CAPEC, CWE). Для автоматизированной обработки данных с целью сокращения времени реагирования на инциденты определены форматы представления входных данных на основе открытых стандартов протокола SCAP (CVE, CWE, CPE, CAPEC, CRE, ERI).

Разработана иерархическая методика оценки защищенности на основе графов атак и зависимостей сервисов, определяющая применяемые на каждом уровне иерархии модели, показатели и алгоритмы их вычисления, и их взаимосвязи между разными уровнями. Основным отличием методики является то, что она позволяет получить оценку текущей ситуации по защищенности в форме адекватных количественных показателей на основе имеющихся в наличии входных данных из различных источников, и уточнять ее с появлением новых данных за счет постоянного мониторинга ситуации и перерасчета показателей защищенности на основе алгоритмов соответствующего уровня методики (в том числе алгоритмов определения вероятности атаки с использованием байесовского вывода, алгоритмов определения критичности ресурсов компьютерной сети с использованием логического вывода, алгоритмов определения уровня риска компрометации отдельных объектов сети, и др.).

Разработана методика выбора защитных мер для систем взаимодействующих сервисов, основанная на предложенной системе показателей, и позволяющая учитывать доступные данные безопасности от SIEM-системы, администраторов анализируемой системы, средств мониторинга анализируемой системы и из открытых источников, и требования бизнеса. Методика отличается выделением этапов статического и динамического уровней (на первом уровне выбирается набор средств защиты, позволяющих реализовать контрмеры, для повышения уровня защищенности анализируемой системы, на втором – конкретные контрмеры для противодействия обнаруженным атакам), совместным применением графов атак и зависимостей сервисов, и применимостью для SIEM-систем. Для определения влияния контрмер на успешную реализацию атак (с применением графа атак) и корректное функционирование анализируемой системы (с применением графа зависимостей сервисов), и последующего выбора контрмер, разработана аналитическая модель контрмер и определены ее связи с моделями атак, сети и зависимостей сервисов, а также разработаны алгоритмы выбора защитных мер в рамках предложенной методики. Алгоритмы выбора защитных мер основаны на оптимизации по области покрытия контрмеры (то есть объектам компьютерной сети или графа атак, которые охватываются контрмерой) и свойствам покрытия контрмеры (то есть свойствам безопасности, которые охватываются контрмерой). Окончательный выбор контрмер осуществляется на основе индекса, учитывающего эффективность, стоимость и побочный ущерб от реализации контрмер.

Проведено качественное сравнение разработанных методик с существующими аналогами, показавшее их превосходство. **Построена архитектура системы оценки защищенности и выбора защитных мер** для реагирования на инциденты в процессе управления информацией и событиями безопасности в системах взаимодействующих сервисов, основанная на предложенных методиках. **Разработан прототип системы оценки защищенности** в статическом и динамическом режимах работы анализируемой системы, **и выбора защитных мер** для повышения уровня защищенности анализируемой системы и реагирования на инциденты в процессе управления информацией и событиями безопасности, реализующий разработанные алгоритмы и методики. С его помощью **осуществлена экспериментальная оценка полученных результатов**, показавшая эффективность разработанной системы и достижение поставленной цели.