УДК 004.89

ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ВОЗНИКНОВЕНИИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Спиридонов Д.Л. (Национальный исследовательский университет ИТМО)

Аннотация. В представленной работе проведен анализ систем поддержки принятия решений (СППР), анализ системы выявления инцидентов информационной безопасности. Приведен сценарий совместного использования обозначенных систем, который сокращает время устранения инцидента, что в свою очередь позволяет сократить возможные финансовые потери от реализации угрозы информационной безопасности.

Введение. В настоящее время немаловажную роль в функционировании организации играет сохранение конфиденциальности, целостности и доступности информации, которая курсирует на предприятии. Нарушение перечисленных свойств информации приводит к экономическим и репутационным потерям для организации, а также препятствует ее росту. По данным исследования Positive Technologies за первый квартал 2020 года, количество киберинцидентов стремительно растет (по сравнению с концом 2019 года), причем доля целенаправленных атак составляет 67% от их общего числа. В связи с этим возникает необходимость в формировании системы защиты информации на предприятии. Существующие системы информационной безопасности способны анализировать информацию о событиях безопасности и выявлять инциденты информационной безопасности, но к их устранению привлекаются специалисты. В данной работе предлагается применять подход по применению системы поддержки принятия решений при возникновении инцидентов информационной безопасности. Это позволит ускорить время устранения инцидента информационной безопасности и тем самым снизить экономический ущерб, принесенный предприятию.

Основная часть. СППР решает две основные задачи. Во-первых, выбор наилучшего решения из множества возможных (оптимизация). Во-вторых, упорядочение возможных решений по предпочтительности (ранжирование). СППР в области информационной безопасности применялись для оптимизации процесса размещения средств защиты информации, а также в области кибербезопасности. Так же существует подход, при котором пользователь вводит в СППР сведения об инциденте и в зависимости от наличия соответствующих данных в базе знаний, система предлагает решение.

В настоящее время крупные организации могут обратиться в специализированные центры (SOC или Security Operation center) для мониторинга событий и обнаружения инцидентов ИБ в своей организации. SOC в свою очередь, применяют для этого SIEM или «управление событиями и информацией о безопасности» — класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности.

SIEM-системы служат для отслеживания в реальном времени сигналов тревоги, поступающих от сетевых устройств и приложений, обработки полученных данных и поиска взаимосвязей между ними, выявления отклонений от нормального поведения контролируемых систем, а также оповещение операторов об обнаруженных инцидентах. Здесь стоит отметить, что SIEM не способна устранить инцидент самостоятельно, для устранения инцидентов привлекаются специалисты.

Сформируем новую область применения СППР – использование такой системы совместно с SIEM. Такая коллаборация позволит сократить время реакции специалистов на инцидент и поспособствует его оперативному устранению. Таким образом, применительно к задаче в данной предметной области получим наиболее предпочтительное разрешение инцидента информационной безопасности.

Реализация такого взаимодействия может быть обеспечена благодаря открытому API, например, в MaxPatrol SIEM – благодаря этому выгрузка информации из SIEM возможна на любом этапе работы системы. В других SIEM возможно выгружать данные из UI. Далее, выгруженные данные об инциденте путем, например, syslog-транспорта, передаются в СППР, база знаний которой снабжена различными сведениями об инцидентах и способах их устранения. СППР, основываясь на имеющихся экспертных знаниях, предлагает специалисту наилучшее решение возникшего инцидента.

Выводы. В результате проведенной работы была проанализирована возможность применения СППР при возникновении инцидентов информационной безопасности в составе SIEM-системы. Использование такого подхода позволит повысить уровень безопасности информационной системы предприятия за счет снижения времени устранения возникающих инцидентов. К тому же это позволит автоматизировать процесс устранения однотипных инцидентов, что в свою очередь, положительно скажется на экономике организации, так как вероятное время простоя предприятия (время на устранение инцидента), будет снижено.