УДК 004.056

РАЗРАБОТКА ТИПОВОЙ МЕТОДИКИ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАБОТЫ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вернигорова А.А. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Михайличенко О.В. (ИТМО)

Введение. Развитие технологий, изменения в законодательстве и появление новых уязвимостей требуют от службы информационной безопасности (ИБ) постоянного совершенствования процессов, связанных с обеспечением безопасности информационных активов организации. В целях определения процессов, требующих осуществления корректирующих мероприятий и оптимизации расходов по обеспечению ИБ, необходимо осуществлять систематическое проведение оценки эффективности работы службы ИБ, позволяющее выявить слабые места в реализации процессов ИБ и определить эффективность внедряемых мер и средств защиты. При этом существующие методы оценки эффективности работы службы ИБ имеют недостатки, связанные с возможностью сотрудников влиять на значения показателей, узкой направленностью, субъективностью оценки и т.д., вследствие чего существует необходимость разработки типовой методики, позволяющей оперативно получить достоверные сведения о состоянии процессов ИБ и оценить эффективность работы службы ИБ.

Основная часть. В работе рассматривается процесс оценки эффективности работы службы ИБ, объединяющий контекст, свидетельства, критерии и модель оценки. Суть оценки заключается в выработке оценочного суждения относительно состояния процессов ИБ и целесообразности используемых защитных мер. В качестве возможных оценочных суждений предложено использовать следующие интерпретации результатов вычисления метрик: успех, тенденция и аномалия. В случае успеха измеренная величина оказывается лучше целевой, подтверждая эффективность рассматриваемого процесса. Тенденция предоставляет сведения о динамике процесса и указывает на направление изменения полученных значений по отношению к целевым в сравнении с данными, полученными ранее. Аномалия свидетельствует о том, что измеренная величина выходит за пределы допустимых пороговых значений, и указывает на некорректность проведения измерений или существующие проблемы в реализации процессов ИБ, которые требуют дальнейшего анализа и осуществления корректирующих действий.

Для оценки эффективности работы службы ИБ и поэтапного выявления аномалий в процессах ИБ предложена трехуровневая система взаимосвязанных метрик. Объективность и оперативность вычислений достигается за счет исключения субъективных экспертных оценок путем использования автоматизированных средств сбора свидетельств оценки, таких как SIEM, DLP, SOAR системы и др. для получения базовых количественных показателей, используемых в расчетах. Ввиду неравного влияния метрик на результаты вычислений вышестоящих уровней, каждой метрике назначается весовой коэффициент, который отражает ее вклад в производимые расчеты. Приведенная методика расчета метрик включает определение их функционального назначения, установление требований, предъявляемых к ним, выделение ключевых атрибутов и уровней измерения.

Процесс вычисления итоговых значений и выработки оценочного суждения описан в виде алгоритма и представляет собой последовательность операций от выбора

атрибутов объекта измерения и автоматизированных средств сбора исходных данных до формирования однозначных выводов о состоянии рассматриваемых процессов.

Выводы. В ходе проделанной работы проведен анализ существующих методов оценки эффективности работы службы ИБ и выявлены недостатки рассмотренных подходов. На основании результатов проведенного анализа разработана типовая методика оценки эффективности работы службы ИБ, представляющая собой унифицированное средство для оперативного и систематического анализа деятельности служб ИБ. Объективность и оперативность вычислений достигнута за счет исключения субъективных экспертных оценок путем использования автоматизированных средств сбора свидетельств оценки. Результаты оценки эффективности работы службы ИБ, проведенной с использованием предложенной методики, могут быть использованы для принятия решений по улучшению работы службы ИБ на основании вынесенных суждений относительно состояния процессов ИБ и целесообразности используемых защитных мер.

Список использованных источников:

1. Шаго Ф.Н. Методика оценки эффективности системы менеджмента информационной безопасности по времени реакции системы на инциденты информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – №4 (92) . – С. 115–123

2. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса // Альпина Паблишерз. – 2011. – 338 с.

3. Stoddard Martin, Bodeau Deb, Carlson Rolf, Glantz Cliff, Haimes Yacov, Lian Chenyang, Santos Joost, Shaw James Process Control System Security Metrics–State of Practice. – 2005. – 43 с.