УДК 004.046

АНАЛИЗ И ОЦЕНКА ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ SIEM СИСТЕМОЙ

Медведев Н. В.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. Представлен подход к разработке методик проверки выполнения требований безопасности информации в SIEM-системах с учетом результатов разработки предложений по техническим требованиям к таким системам.

Ключевые слова: SIEM – система, требования безопасности, технологические требования, метрики испытаний.

ANALYSIS AND EVALUATION OF THE TECHNOLOGICAL PROCESS OF INFORMATION PROCESSING BY THE SIEM SYSTEM

Medvedev N.

Bauman Moscow State Technical University
Moscow, Russian Federationn Federation

Abstract. An approach to the development of methods for verifying compliance with information security requirements in SIEM systems is presented, taking into account the results of the development of proposals for technical requirements for such systems.

Key words: SIEM system, safety requirements, technological requirements, test metrics.

Адрес для переписки: Медведев Н. В., ул. Вторая Бауманская, 5, г. Москва 107005, Российская Федерация
e-mail: medvedevnick54@yandex.ru

SIEM (Security information and event management) – объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) – управление информационной безопасностью, и SEM (Security event management) – управление событиями безопасности. Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, приборами и сервисами, и используется также для журналирования данных и генерации отчетов в целях совместимости с прочими бизнес-данными.

Оценка технологического процесса обработки информации SIEM системой в части противодействия несанкционированному доступу (НСД). В качестве субъектов доступа могут рассматриваться лица и процессы (программы пользователей), имеющие возможность доступа к объектам штатными средствами объекта ВТ. Субъекты доступа обязаны иметь официальное разрешение (допуск) к информации определенного уровня конфиденциальности.

Под штатными средствами доступа к информации SIEM системы на объекте информатизации понимаются общесистемные и прикладные аппаратные средства и программы, предоставляющие субъектам документированные возможности доступа к объектам доступа. Комиссия проверяет соответствие описания технологического процесса обработки и хранения конфиденциальной информации реальному процессу. Особое внимание уделяется выявлению возможностей переноса информации большего уровня конфиденциальности на информационный носитель меньшего уровня [6].

Проводится анализ разрешенных и запрещенных связей между субъектами и объектами доступа с привязкой к конкретным СВТ и штатному персоналу, оценка их соответствия разрешительной системе доступа персонала к защищаемым ресурсам на всех этапах обработки.

Модели и метрики испытаний при проверке выполнения требований безопасности информации к SIEM системам. Методика испытаний SIEM системы на соответствие требованиям защиты информации от НСД уточняется на основании результатов анализа технологического процесса обработки информации в АС. Методика испытаний должна включать в себя перечень инструментальных средств, используемых при испытаниях и проверках данного объекта информатизации. Методика испытаний может дополняться, уточняться и корректироваться в процессе испытаний руководителем сертификационного органа по согласованию с заявителем.

При выполнении оценки соответствия по требованиям безопасности информации используются полуколичественные и количественные показатели. Полуколичественными показателями обычно выступают частные показатели, оцениваемые по некоторой бальной шкале. Например, при сертификационных испытаниях на соответствие традиционным РД используются частные показатели положительного результата проверок, принимающие значения, скажем, {0, 1}.

Количественные показатели могут принимать различные точные числовые значения. Примером использования таких показателей является проведение тематических исследований и сертификационных испытаний на соответствие ТУ, сертификационных испытаний по надежности обработки информации, обеспечению полноты, безошибочности, актуальности и защищенности информации в процессе функционирования информационных систем. Значения показателей могут быть, например, определены экспертным, регистрационным или расчетным путем.

В таблице 1 приведены примеры показателей качества, регламентированные национальными стандартами для программных и автоматизированных систем, к которым относятся и SIEM системы: ГОСТ 28195–89 «Оценка качества программных средств» и ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» [7].

Таблица 1 – Частные показатели «технологической безопасности» по ГОСТ 28195

Наименование	Метод оценки
Показатель устойчивости к искажающим воздействиям	$P(Y) = 1 - D/K$, где D – число экспериментов, в которых искажающие воздействия приводили к отказу; K – число экспериментов, в которых имитировались искажающие воздействия
Вероятность безотказной работы	$P = 1 - Q/N$, где Q – число зарегистрированных отказов, N – число экспериментов
Оценка по среднему времени восстановления	$Q_B = \begin{cases} 1, \text{если } T_B \le T_B^{\text{доп}} \\ \frac{T_B^{\text{доп}}}{T_B}, \quad \text{если } T_B > T_B^{\text{доп}} \end{cases}$, где $T_B = \frac{1}{N}\sum_i^N T_{B_i}$ – среднее время восстановления, где: N – число восстановлений; T_{B_i} – время восстановления после i-го отказа
Оценка по продолжительности преобразования входного набора данных в выходной	$Q_{\pi_i} = \begin{cases} 1, \text{если } T_{\pi_i} \le T_{\pi_i}^{\text{доп}} \\ \frac{T_{\pi_i}^{\text{доп}}}{T_{\pi_i}}, \quad \text{если } T_{\pi_i} > T_{\pi_i}^{\text{доп}} \end{cases}$, где T_{π_i} – допустимое время π_i преобразования i-го входного набора данных; π_i – фактическая продолжительность преобразования i-го входного набора данных

Следует отметить, что в области тестирования ПО измеряемые количественные частные показатели принято называть метриками. Это в полной мере относится и к SIEM системам [8].

Вывод. Метрики позволяют получить идентификационный профиль конкретных программ при статическом анализе. На практике это позволяет решить задачи аутентификации ПО, оценить сложность ПО, и, как следствие, уровень безошибочности программного проекта, трудоемкость анализа и доработок ПО, стоимость и сроки работ, эффективность технологии разработки и внедрения и др. Часто метрики являются параметрами моделей планирования испытаний [9].

Литература

1. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2011 г. / В. А. Матвеев [и др.] // Вестник МГТУ им. Баумана. Сер. «Приборостроение». 2011. Спецвыпуск «Технические средства и системы защиты информации». – С. 3–6.

2. Нормативные и методические документы по технической защите информации. Специальные нормативные документы: официальный сайт ФСТЭК России [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_razd/_karto.htm.

3. Специальные требования и рекомендации по технической защите информации (СТР-К). –Гостехкомиссия России. – Москва, 2001.

4. ГОСТ 28195. Оценка качества программных средств. – М.: Издательство стандартов, 1989.

5. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. – М.: Издательство стандартов, 1995.

6. Темнов О. Д. Анализ и исследование методов и средств обнаружения недекларированных возможностей / О. Д. Темнов // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2007. – № 39. – С. 45–50.

7. Grusho, A. Strictly consistent tests for detection of statistical covert channels / A. Grusho, A. Knyazev, E. Timonina // Journal of Mathematical Sciences. – 2007. – Т. 146, № 4. – P. 5984–5991.

8. Kostogryzov, A. Mathematical Models and Software Tools to Support an Assessment of Standard System Processes / A. Kostogryzov, G. Nistratov, N. Kleshchev // Proceedings of the 6th International SPICE Conference on Process Assessment and Improvement (SPICE-2006), Luxembourg, 2006. – P. 63–68.