A.V. Kuznetcov

The Method of Event Determination Registered into Audit Trails

Keywords: event source, audit trail, event, incident.
In this article the method of event determination registered into audit trails on the event source based on solution of linear programming task is described. This method allows to optimize the event management process within an information security management system by quantity of incidents. This method considers restrictions related to performance of the event source.

А.В. Кузнецов

СПОСОБ ОПРЕДЕЛЕНИЯ СОБЫТИЙ, РЕГИСТРИРУЕМЫХ В ЖУРНАЛАХ АУДИТА

Введение

Проблема защиты информации не только не теряет своей актуальности на протяжении ряда десятилетий, но и стремительно развивается и выходит на один из первых планов в научно-практической деятельности в последние годы. При этом в работе специалистов по защите информации на первое место выходит не столько возможность предотвращения инцидентов информационной безопасности (ИБ), сколько готовность их своевременного выявления (детектирования) и расследования. Данное обстоятельство требует обеспечить однозначное прослеживание действий любого субъекта доступа в автоматизированных информационных системах, т.е. подотчётность в рамках процесса управления событиями [1]. Стоит отметить, что на практике при реализации процесса управления событиями специалистами по защите информации основной акцент делается на популярные и активно развивающиеся технические решения класса Security Information and Event Management (SIEM) [2], а не на источники событий (средства защиты информации, средства контроля и анализа защищенности, общесистемное и прикладное программное обеспечение и т.п.), которые осуществляют непосредственную регистрацию событий (ведение журнала регистрации событий (журнала аудита)) и, как следствие, выступают основой для инфраструктуры управления событиями. Под событием будем понимать изменение или сохранение состояния, которое имеет значение для безопасности, управления и (или) работоспособности компонента(ов) автоматизированных информационных систем предприятия, а также зарегистрированная в журнале (файле, таблице базы данных или ином месте) информация о данном событии. С учетом вышесказанного задача определения событий, регистрируемых в журналах аудита на источниках событий, является актуальной.

Существующие способы определения регистрируемых событий

На сегодняшний день существует несколько способов решения поставленной задачи, но им присущ ряд недостатков [3–5].

1. Регистрировать события, определённые на источнике событий «по умолчанию», – зачастую производители источников событий «по умолчанию» регистрируют минимальный набор событий (вплоть до полного отсутствия регистрации каких-либо событий), в связи с этим данный способ может не отражать потребности конкретного предприятия и, как следствие, приводить к пропуску ценных для ИБ предприятия событий, несмотря на это, данный способ самый популярный.

2. Регистрировать абсолютно все события – данный способ может приводить к перерасходу ресурсов источника событий (вплоть до полного отказа в работе), а также зашумляет работу SIEM-системы и усложняет выявление действительно ценных для ИБ предприятия событий.

3. Регистрировать события, выявленные по результатам опытной эксплуатации SIEM-системы, – данный способ наиболее предпочтителен, но, учитывая ограниченность периода опытной эксплуатации SIEM-системы (обычно не более нескольких месяцев) и нестатистическую природу возникновения событий, он может приводить к пропуску ценных для ИБ предприятия событий, которые не были зафиксированы на этапе опытной эксплуатации SIEM-системы.

Стоит отметить, что ни один из существующих подходов не вводит каких-либо ограничений или критериев для определения событий, подлежащих регистрации на источниках событий, в том числе отсутствует количественный учет влияния факта регистрации событий на работоспособность самого источника событий, т.е. деградации производительности источника событий.

Таким образом, возникает противоречие между потребностями практики в выявлении максимального количества инцидентов ИБ с использованием SIEM-систем на базе зарегистрированных событий и минимизации влияния регистрации событий на работу источника событий, т.е. уменьшения количества регистрируемых событий, другими словами, необходимость поиска баланса между защищённостью автоматизированной информационной системы предприятия, доступностью источника событий и подотчетностью.

Предлагаемый способ определения регистрируемых событий

Предварительно необходимо определить, что будет представлять собой событие в рамках математической постановки задачи. В настоящей публикации событие представляется в виде двух переменных:

1) лингвистическая переменная – E_i (например, E_1 = {*Успешный вход в систему*}), где $i \in [1; n]$.

2) булевая переменная – e_i, удовлетворяющая соответствующим значениям:

$$e_i = \begin{cases} 1, \text{ событие зарегистрировано,} \\ 0, \text{событие не зарегистрировано.} \end{cases} \quad (1)$$

С учетом вышесказанного, поставлена следующая математическая задача (2): определение набора регистрируемых событий ($E_1, \ldots, E_n$), при заданном в SIEM-системе наборе правил выявления инцидентов ИБ ($I_1, \ldots, I_m$) и ограничений на производительность источника событий P, который по возможности обращал бы в максимум показатель рациональности организации процесса управления событиями – W:

$$W = W(I_1, \ldots, I_m; E_1, \ldots, E_n; P) \rightarrow max. \quad (2)$$

В настоящей публикации автор развивает предложенный им ранее способ решения поставленной задачи [0].

При решении задачи необходимо удовлетворить следующие условия, представленные в виде системы из m уравнений:

$$\begin{cases} \sum_{i=1}^{n} a_{i1} \times e_i \le P; \\ \sum_{i=1}^{n} a_{ij} \times e_i \le P; \\ \sum_{i=1}^{n} a_{im} \times e_i \le P, \end{cases} \quad (3)$$

где m – количество правил выявления инцидентов ИБ для SIEM-системы, используемой на предприятии, получаемое путем визуального анализа данных в интерфейсе конкретной SIEM-системы;

$a_{ij} \in [0;+\infty)$ и $a_{ij} \in N$ – коэффициент, отражающий количество зарегистрированных событий e_i, получаемый из эксперимента путем имитации действий нарушителя в соответствии с разработанной на предприятии моделью угроз безопасности информации; $e_i \in \{0;1\}$ – дискретная величина, соответствующая данным из набора событий (E_1, ..., E_n), которые могут быть зарегистрированы источником событий; $P \in [0;+\infty)$ и $P \in N$ – пороговое значение количества зарегистрированных событий.

Стоит отметить, что величина P для каждого источника событий определяется из эксперимента путем определения порогового значения количества регистрируемых событий в секунду, соответствующего верхней границе оптимального уровня загрузки (утилизации) центрального процессора источника событий. На рис. 1 и 2 представлены примеры определения данной величины для оборудования Mikrotik с процессором CPUAR9344-DC3A-R (тактовая частота 600 МГц) и с процессором QCA8511-AL1C (тактовая частота 400 МГц).

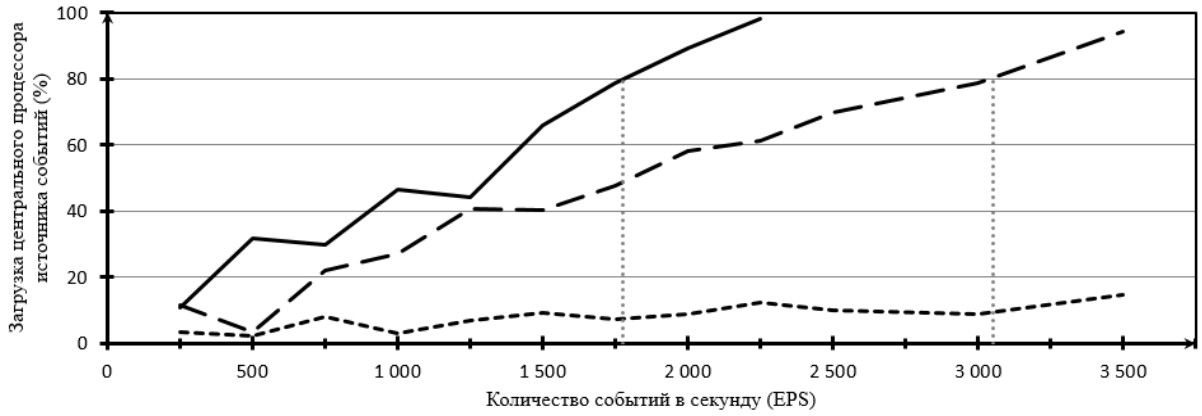

Рис. 1. Значения загрузки центрального процессора CPUAR9344-DC3A-R (тактовая частота 600 МГц) в трёх режимах работы

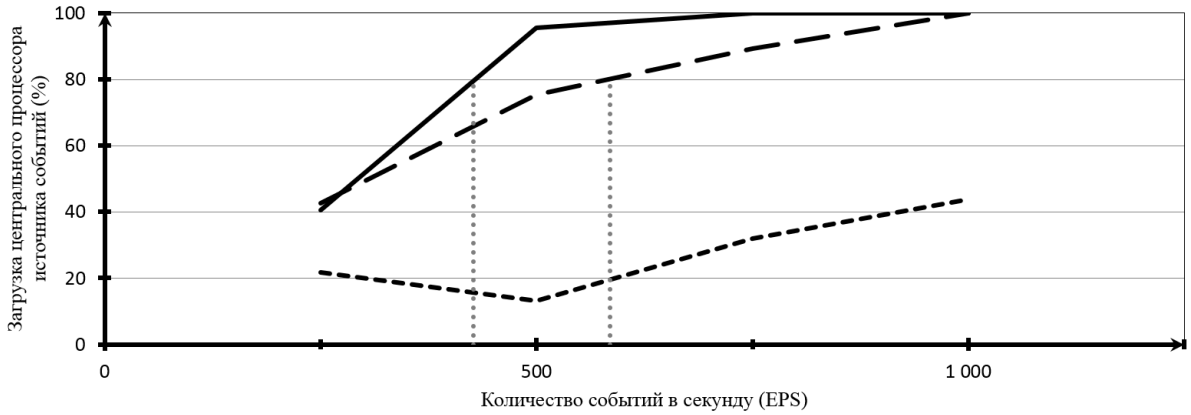

Рис. 2. Значения загрузки центрального процессора QCA8511-AL1C (тактовая частота 400 МГц) в трёх режимах работы

Для каждого правила выявления инцидентов ИБ (I_1, …, I_m) из SIEM-системы справедливо уравнение, отражающее связь конкретного правила с зарегистрированными событиями:

$$I_j = \sum_{i=1}^{n} b_{ij} \times e_i, \quad (4)$$

$$I_j = \begin{cases} 1, \text{ инцидент выявлен;} \\ 0, \text{инцидент не выявлен,} \end{cases} \quad (5)$$

где $b_{ij} \in [0;1]$ и удовлетворяет условию

$$\sum_{i=1}^{n} b_{ij}|_{j=\text{const}} = 1. \quad (6)$$

Значение коэффициента b_{ij} для соответствующего j-го правила выявления инцидентов ИБ получают по результатам визуального анализа данных в интерфейсе конкретной SIEM-системы.

Таким образом, необходимо максимизировать показатель W:

$$W = \sum_{j=1}^{m} I_j = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{ij} \times e_i \rightarrow \max, \quad (7)$$

где max = m.

В итоге поставленная задача сводится к решению задачи линейного программирования. Для её решения могут использоваться любые из доступных методов [6], которые в рамках настоящей публикации не рассматриваются.

Полученный в результате решения набор булевых переменных e_i необходимо сопоставить со значениями лингвистических переменных E_i, которые уже используются в последующей работе специалистами по защите информации.

С учетом вышесказанного, способ определения событий, регистрируемых на источнике событий, включает в себя:

определение начального набора событий (E_1, …, E_n) путем анализа документации на конкретный источник событий;

определение количества правил выявления инцидентов ИБ для конкретной SIEM-системы – m, путем визуального анализа данных в интерфейсе SIEM-системы;

экспериментальное определение коэффициентов a_{ij} для каждого правила выявления инцидентов ИБ;

экспериментальное определение величины P для конкретного источника событий;

определение коэффициентов b_{ij} для каждого правила выявления инцидентов ИБ путем визуального анализа правил в интерфейсе SIEM-системы;

составление систем уравнений с использованием коэффициентов a_{ij} и b_{ij};

определение необходимого набора переменных (e_1,…,e_n) путем решение задачи линейного программирования с использованием доступных методов [6];

сопоставление полученного набора булевых переменных (e_1,…,e_n) с лингвистическими переменными (E_1,…,E_n).

По результатам применения способа определения событий, регистрируемых на источнике событий, специалисту по защите информации необходимо активировать параметры ведения журнала регистрации событий (журнала аудита), соответствующие значениям (E_1, …, E_n), и обеспечить передачу зарегистрированных данных в SIEM-систему с использованием одного из следующих протоколов (способов):

1. Syslog, Security Device Event Exchange (SDEE), Simple Network Management Protocol (SNMP) – актуально для операционных систем семейства Linix/Unix, систем-

ного программного обеспечения, активного сетевого оборудования, гипервизоров, и т.п.

2. Open Database Connectivity (ODBC), Java Database Connectivity (JDBC), запросы Structured Query Language (SQL) – актуально для систем управления базами данных.

3. Windows Management Instrumentation (WMI), Windows Remote Management (WinRM) – актуально для операционных систем семейства Microsoft Windows.

Выводы

Предложенный способ учитывает недостатки существующих подходов, в том числе принимает во внимание возможности конкретной SIEM-системы по выявлению инцидентов ИБ, а именно: предустановленные наборы правил выявления инцидентов ИБ (правил корреляции событий), и позволяет максимизировать число выявляемых инцидентов ИБ для конкретного предприятия, при этом сохранив производительность источника событий на заданном уровне.

Достоверность результатов подтверждается корректным использованием теоретических методов, а также тем, что предложенный способ получил практическое подтверждение на базе информационно-телекоммуникационной инфраструктуры научно-технического центра «Вулкан» (г. Москва) с использованием следующих SIEM-систем:

1. RSA Security Analytics.
2. IBM QRadar Security Intelligence Platform.
3. McAfee Enterprise Security Manager.

Данный способ является инвариантным к реализации источников событий и SIEM-систем, что позволяет применять его для различных информационно-телекоммуникационных инфраструктур предприятий, в том числе тех, которые появятся в ближайшие годы в результате развития информационных технологий. Стоит отметить, что данный способ может быть перенесен для решения аналогично поставленных задач в других научно-практических областях.

СПИСОК ЛИТЕРАТУРЫ:

1. Кузнецов А.В. Способ организации процесса управления событиями, в части их обработки, в рамках системы управления информационной безопасностью предприятия // Вопросы защиты информации. 2015. № 2. С. 57–62.
2. Кузнецов А.В., Федоров А.Ю. Современные тенденции развития SIEM-решений // Storage News. 2013. № 2 (54). С. 8–11.
3. Райс А., Рингольд Д. Защита от целенаправленных устойчивых угроз с помощью больших данных // Безопасность ИТ-инфраструктуры. 2015. № 4 (94). С. 6–7.
4. Чувакин А. SIEM: что делать, если некуда идти? // Безопасность ИТ-инфраструктуры. 2015. № 2 (92). С. 9–11.
5. БирюковА. Security Operation Center. Искусственный интеллект на службе ИБ // Системный администратор. 2013. № 9 (130). С. 42–45.
6. Кузнецов А.В. Способ определения регистрируемых событий // Вопросы кибербезопасности. 2015. № 5(13). С. 23–25.
7. Вентцель Е.С. Исследование операций. М: Советское радио, 1972. С. 59–119.

REFERENCES:

1. Kuznetcov A.V. Sposob organizatsii protsessa upravleniya sobytiyami, v chasti ikh obrabotki, v ramkakh sistemy upravleniya informatsionnoy bezopasnost'yu predpriyatiya // Voprosy zashchity informatsii. 2015. № 2. Pp. 57–62.
2. Kuznetcov A.V., Fedorov A.Yu. Sovremennye tendentsii razvitiya SIEM-resheniy // Storage News. 2013. № 2 (54). Pp 8–11.
3. Rays A., Ringol'd D. Zashchita ot tselenapravlennykh ustoychivykh ugroz s pomoshch'yu bol'shikh dannykh // Bezopasnost' IT-infrastruktury. 2015. № 4 (94). Pp. 6–7.
4. Chuvakin A. SIEM: chto delat', esli nekuda idti? // Bezopasnost' IT-infrastruktury. 2015. № 2 (92). Pp. 9–11.
5. Biryukov A. Security Operation Center. Iskusstvennyy intellekt na sluzhbe IB // Sistemnyy administrator. 2013. № 9 (130). Pp. 42–45.
6. Kuznetcov A.V. Sposob opredeleniya registriruemykh sobytiy // M: Voprosy kiberbezopasnosti. 2015. № 5(13). Pp. 23–25 p.
7. Venttsel' E.S. Issledovanie operatsiy. M: Sovetskoe radio, 1972. Pp. 59–119.