УДК 004.56
DOI: http://dx.doi.org/10.21686/1818-4243-2020-1-69-79

В.А. Сизов, А.Д. Киров
Российского экономического университета им. Г.В. Плеханова, Москва, Россия

Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности

Целью исследования *является повышение эффективности управления информационной безопасностью субъектов экономической деятельности, которые используют SIEM-системы, за счет выявления и решения основных проблем внедрения этих систем в практику управления информационной безопасностью с учетом специфических особенностей и типовых характеристик последних [1–3].*

Материалы и методы исследования. *На основе анализа схемы типовой архитектуры SIEM-системы и типового процесса внедрения SIEM-системы в практику управления информационной безопасностью СЭД различного вида определяются основные проблемы процесса установки и настройки SIEM-системы, а также обосновываются пути их решения с использованием системного подхода. В процессе установки и настройки SIEM-системы у коллектива заказчиков и исполнителей могут возникнуть следующие типовые проблемы. Процесс установки и настройки SIEM-системы в рамках системного подхода рассматривается как совокупность взаимосвязанных ресурсообеспеченных процедур, реализующих установку и настройку отдельных компонентов SIEM-системы. Из всего множества этих процедур определяются процедуры, подлежащие автоматизации. Для определения рациональной структуры процесса автоматизированной установки и настройки SIEM-системы предложен метод сетевого планирования и управления [4–5], который позволяет также оценить эффективность внедрения SIEM-системы в практику управления информационной безопасностью СЭД на основе разработки и расчета сетевых графиков.*

Результаты. *В работе разработаны пути решения проблем внедрения SIEM-систем в практику управления информационной безопасностью: упрощение SIEM-системы, представляющее собой отказ от редко используемых модулей и перестройку архитектуры SIEM-системы; автоматизацию процесса типовой установки и общей настройки SIEM-системы, представляющую собой разработку методики автоматизации процедуры типовой установки и общей настройки SIEM-системы и программного модуля, реализующего разработанную методику; комбинированный подход, представляющий собой совместное применение двух вышеуказанных подходов, который позволяет максимально приблизить SIEM-систему как продукт к «коробочному» варианту. В работе представлены обоснованные предложения по совершенствованию процесса внедрения SIEM-системы в практику управления информационной безопасностью СЭД, основанные на разработке и применении автоматизированных процедур типовой установки и настройки SIEM-системы, что приводит к снижению временных затрат на внедрение SIEM-системы, повышает удобство выполнения данных процедур. В целом использование предложенного подхода направлено на разработку и производство «коробочного» варианта продукта – системы управления событиями информационной безопасности, т.к. частично решает задачи унификации и стандартизации систем данного класса.*

Заключение. *Предложенные пути решения проблем внедрения SIEM-систем в практику управления информационной безопасностью СЭД, основанные на оптимизации процесса установки и настройки SIEM-систем, позволяют ускорить процесс распространения и внедрения систем управления событиями информационной безопасности в СЭД и повысить его эффективность за счет автоматизации процедур типовой установки и настройки SIEM-систем.*

Ключевые слова: *управление информационной безопасностью, SIEM, система управления событиями информационной безопасности, проблемы внедрения, автоматизация*

Valeriy A. Sizov, Aleksey D. Kirov
Plekhanov Russian University of Economic, Moscow, Russia

Problems of implementing SIEM systems in the practice of managing information security of economic entities

The aim of the study *is to increase the efficiency of information security management of economic entities that use Security Information and Event Management (SIEM) systems by identifying and solving the main problems of introducing these systems into the management of information security practices of economic entities [1–3].*

Materials and research methods*. Based on the analysis of scheme of the typical architecture of the SIEM system and the standard process of introducing the SIEM system into practice of managing information security of various types of economic entities, the main problems of the installation and configuration of the SIEM system are determined, and ways to solve them are substantiated. During the installation and configuration of the SIEM system, the team of customers and contractors may experience the following typical problems. The process of installing and configuring the SIEM system as part of a systematic approach is considered as a set of interconnected resource-based procedures that implement the installation and configuration of individual components of the SIEM system. Out of the whole set of these procedures, the procedures to be automated are determined. To determine the rational structure of the process of automated installation and configuration of the SIEM system, a method of network planning and management is proposed [4-5], which also allows you to evaluate the effectiveness of implementing the SIEM system in the practice of managing information security of economic entities based on the development and calculation of network schedules.*

Results. *In this work, we developed ways to solve the problems of introducing SIEM systems into information security management practice: simplifying the SIEM system, which is a rejection of rarely used modules and rebuilding the architecture of the SIEM system; automation of the process of typical installation and general setup of the SIEM system, which represents the development of a methodology for automating the procedure of typical installation and general setup of the SIEM system and software module that implements the developed methodology; a combined approach, which is a joint application of the two above approaches, which allows you to bring the SIEM system closer as a product to the "box" option.*
The paper presents reasonable proposals for improving the implementation of the SIEM system, based on the development and application of automated procedures for the typical installation and configuration of the SIEM system, which reduces the time spent on the implementation of the SIEM system, increases the convenience of performing these procedures, and in general can lead to the "boxed" version of the solution for a product of this class of information security event management systems.
Conclusion. *The proposed ways to solve the problems of implementing SIEM systems in the practice of managing information security of economic entities based on the optimization of the installation and configuration of SIEM systems can accelerate the distribution and implementation of information security event management systems and increase efficiency by automating standard installation procedures and SIEM system settings.*

Keywords: *information security management, SIEM, information security event management system, implementation problems, automation*

Введение

В настоящее время одним из основных трендов в области информационной безопасности субъектов экономической деятельности (СЭД) является внедрение комплексных решений для защиты информации и управления информационной безопасностью. Как правило, ядром таких решений являются системы класса SIEM – Security Information and Event Management – Системы управления событиями безопасности [6–8]. Системы такого класса позволяют собирать, агрегировать и предоставлять в удобном для инженеров информационной безопасности виде информацию о событиях в информационных системах СЭД, прямо или косвенно связанных с безопасностью. Использование таких систем в практике управления информационной безопасностью СЭД позволяет в том числе сделать более эффективным обмен информацией об угрозах и рисках информационной безопасности СЭД, автоматизировать многие процессы получения аналитических оценок в сфере информационной безопасности СЭД. Однако, внедрение систем класса SIEM сопряжено с целым рядом проблем, особенно если система защиты информации состоит из большого количества функционально неоднородных механизмов и средств обеспечения информационной безопасности от различных производителей и вендоров. Для решения этих проблем целесообразно использовать системный подход и методы бенчмаркинга, применяемые в информационной безопасности [9].

Для оценки основных проблем внедрения SIEM-систем в работе проанализированы основные особенности архитектуры типового процесса внедрения системы управления событиями безопасности. Выявленные проблемы связаны со сложностью построения SIEM-систем и, соответственно, требованиями наличия компетенций специалистов, которые в настоящее время могут быть только у производителя или вендора SIEM-системы. Кроме этого необходимость выделения зачастую неоднородных аппаратных платформ может ограничить внедрение SIEM-системы в существующую информационную инфраструктуру СЭД, а достаточно высокие требования к техническим характеристикам аппаратных платформ может приводить к удорожанию проекта внедрения SIEM-систем и требовать оптимизации функциональных и технических решений.

В качестве одной из основных проблем в данной статье рассматривается проблема невысокой степени автоматизации типового процесса внедрения SIEM-системы в практику управления информационной безопасностью СЭД, что сопряжено с увеличением временных, материальных, финансовых, кадровых и иных ресурсов на проведение данного процесса. Актуальность данной проблемы связана с растущими темпами разработки систем управления событиями безопасности различными производителями, а также внедрения этих систем в информационную инфраструктуру СЭД, и, как следствие, ростом расходов на их внедрение, поддержку и повышение эффективности использования. Современное состояние проблемы применительно к смежным областям характеризуется использованием ручного процесса внедрения с помощью пилотного проекта и «тонкой» настройки SIEM-системы в конкретном СЭД [10–11].

В работе разработаны пути решения проблем внедрения SIEM-систем в практику управления информационной безопасностью СЭД: упрощение SIEM-системы, представляющее собой отказ от редко используемых модулей и перестройку архитектуры SIEM-системы; автоматизацию процесса типовой установки и общей настройки SIEM-системы, представляющую собой разработку методики автоматизации процедуры типовой установки и общей настройки SIEM-системы и программного модуля, реализующего разработанную методику; комбинированный подход, представляющий собой совместное применение двух вышеуказанных подходов, который позволяет максимально приблизить

SIEM-систему как продукт к «коробочному» варианту.

Для автоматизации типового процесса внедрения SIEM-системы в практику управления информационной безопасностью СЭД в статье формализован процесс типовой установки и общей настройки SIEM-системы с использованием математического аппарата метода сетевого планирования и управления [9]. Суть этого метода состоит в моделировании процесса типовой установки и общей настройки SIEM-системы с помощью сетевого графика на базе применения теории графов, теории вероятностей и компьютерных технологий.

Решение этих проблем позволяет ускорить процесс внедрения SIEM систем в практику управления информационной безопасностью СЭД, расширить рынок для этого класса систем и в целом повысить эффективность управления информационной безопасностью СЭД.

Анализ схемы типовой архитектуры и процесса внедрения SIEM-системы

На сегодняшний день все больше компаний сталкивается с необходимостью обработки журналов событий, которые регистрируются в информационных системах, с целью выявления возможных атак. При этом даже в небольшой компании в журналах аудита может регистрироваться до нескольких десятков событий в секунду, что делает их анализ в ручном режиме длительным и крайне неэффективным. Для того, чтобы автоматизировать процесс сбора и анализа информации о событиях информационной безопасности могут использоваться специализированные системы мониторинга. Одним из классов таких систем являются системы управления событиями безопасности (SIEM-системы).

Системы управления событиями безопасности относятся к классу сложных систем [12–13]. Внедрение сложных систем, как правило, осуществляется путем двухэтапной реализации пилотного и основного проекта командой специалистов заказчика и исполнителя – поставщика продукта. Система мониторинга событий информационной безопасности (СМСИБ) предназначена для автоматизации процесса сбора и анализа информации о событиях безопасности, поступающих из различных источников. В качестве таких источников могут выступать средства защиты информации, общесистемное и прикладное ПО, телекоммуникационное обеспечение и др. СМСИБ включает в себя следующие компоненты:

- **программно-техническая часть** – реализуется на основе продуктов по мониторингу событий безопасности класса SIEM (Security Information and Event Management);
- **документационная часть** – включает в себя набор документов, описывающих основные процессы, связанные с выявлением и реагированием на инциденты безопасности;
- **кадровая составляющая** – подразумевает выделение сотрудников, ответственных за работу с СМСИБ.

Программно-техническая часть СМСИБ включает следующие компоненты:

- агенты мониторинга, предназначенные для сбора информации, поступающей от различных источников событий, включающих в себя средства защиты, общесистемное и прикладное ПО, телекоммуникационное обеспечение и др.;
- сервер событий, обеспечивающий централизованную обработку информации о событиях безопасности, которая поступает от агентов. Обработка осуществляется в соответствии с правилами, которые задаются администратором безопасности;
- хранилище данных, содержащее результаты работы системы, а также данные, полученные от агентов;
- консоль управления системой, позволяющая в реальном масштабе времени просматривать результаты работы системы, а также управлять её параметрами.

Документационная часть СМСИБ предполагает разработку пакета нормативных документов по управлению инцидентами безопасности. Как правило, для этого формируется политика управления инцидентами ИБ, которая определяет классификацию инцидентов, общий порядок реагирования, ответственность за реализацию данного документа и др. На основе данной политики для каждого из видов инцидентов безопасности разрабатывается отдельный регламент, описывающий детальный порядок реагирования на различные виды инцидентов.

Кадровая составляющая СМСИБ предполагает выделение различных ролей, ответственных за сопровождение центра. Как правило, выделяют следующие роли в составе СМСИБ:

- **системный администратор**, отвечающий за поддержку общесистемного аппаратного обеспечения СМСИБ;
- **администратор безопасности**, обеспечивающий управление настройку параметров функционирования СМСИБ;
- **оператор**, выполняющий задачи просмотра результатов работы СМСИБ и реализации базовых функций реагирования на типовые инциденты;
- **аналитик**, обеспечивающий анализ и реагирования на сложные виды инцидентов. [14]

Для оценки основных проблем внедрения SIEM-систем целесообразно проанализировать основные особенности архитектуры типового процесса

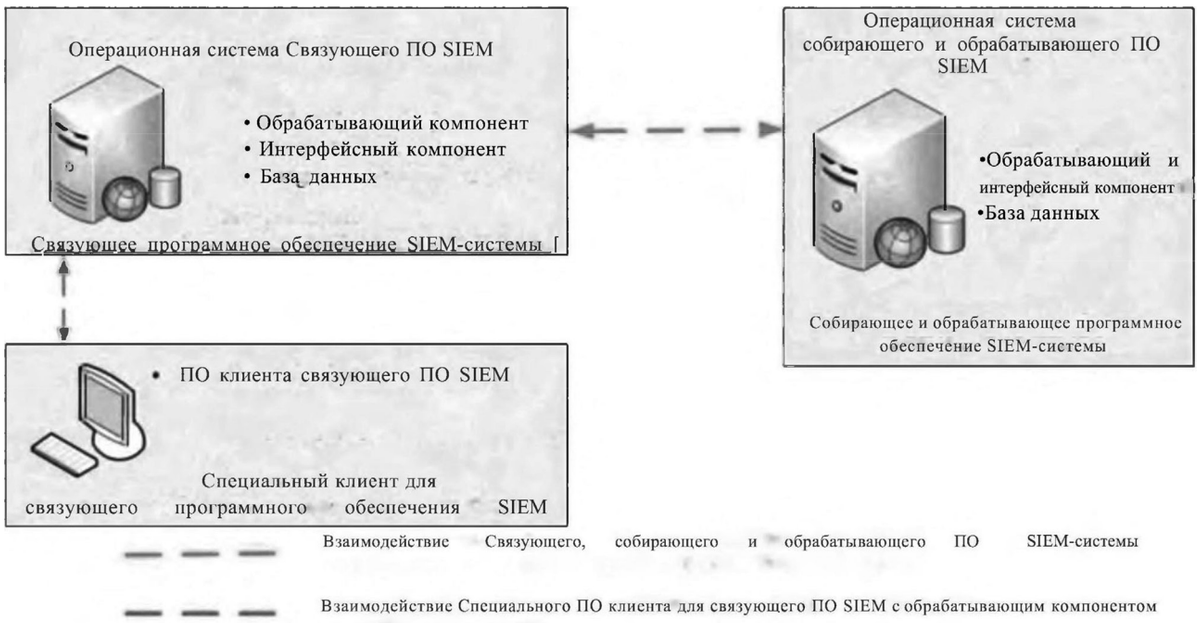

Рис. 1. Схема типовой архитектуры SIEM-системы

внедрения системы управления событиями безопасности. Схема типовой архитектуры SIEM-системы представлена на рис. 1.

Типовая SIEM-система обычно включает

– собирающее и обрабатывающее программное обеспечение;

– связующее программное обеспечение;

– специальный клиент для связующего программного обеспечения.

Собирающее и обрабатывающее программное обеспечение SIEM-системы предназначено для сбора информации из баз данных средств и систем обеспечения информационной безопасности и преобразования собранных записей баз данных в формат, использующийся внутри SIEM-системы. Как правило, оно состоит из следующих компонентов:

• коннекторов для средств и систем обеспечения информационной безопасности, поставляющихся отдельно, собирающих информацию о событиях информационной безопасности из баз данных средств и систем обеспечения информационной безопасности и отправляющих её в обрабатывающий и интерфейсный компонент;

• обрабатывающего и интерфейсного компонента, осуществляющего непосредственное преобразование информации о событиях информационной безопасности из баз данных средств и систем обеспечения информационной безопасности во внутренний формат SIEM-системы и предоставляющего доступ к преобразованной информации в виде унифицированных записей о событиях информационной безопасности;

• базы данных, хранящей унифицированные записи о событиях информационной безопасности.

Связующее программное обеспечение SIEM-системы предназначено для связи нескольких экземпляров собирающего и обрабатывающего программного обеспечения SIEM-системы и специального клиента для связующего программного обеспечения и предоставление единого интерфейса к ним. Как правило, оно состоит из следующих компонентов:

• обрабатывающего компонента, обращающегося к базам данных экземпляров собирающего и обрабатывающего программного обеспечения SIEM-системы и отправляющего копии событий информационной безопасности в свою базу данных;

• интерфейсного компонента, предоставляющего доступ к событиям безопасности, хранящимся во внутренней базе данных связующего программного обеспечения SIEM-системы специальному клиенту для связующего программного обеспечения;

• базы данных, хранящей записи о событиях безопасности, полученные от всех экземпляров собирающего и обрабатывающего программного обеспечения SIEM-системы.

Специальный клиент для связующего программного обеспечения взаимодействует с интерфейсным компонентом связующего программного обеспечения и предоставляет данные о событиях информационной безопасности непосредственно пользователю.

Анализ процесса внедрения типовой системы класса SIEM

показал, что такой процесс состоит из следующих этапов [15].

1. Установка (развёртывание) SIEM-системы.

2. Первоначальная настройка SIEM-системы.

3. Сопряжение SIEM-системы с системами обеспечения информационной безопасности, применяющимися в СЭД.

4. Тестирование работы SIEM-системы.

5. Опытная эксплуатация SIEM-системы.

6. Подготовка к сопряжению SIEM-системы с системами обеспечения информационной безопасности, находящимися в стадии развёртывания в СЭД.

В настоящее время основные проблемы внедрения SIEM-систем относятся к первым двум этапам, т.к. требуют одновременного учета необходимых параметров режима их функционирования и имеющихся ограничений на характеристики технического обеспечения, а также определения большого количества конфигурационных атрибутов разворачиваемой SIEM-системы.

Установка (развёртывание) SIEM-системы представляет собой копирование основных компонентов SIEM-системы на автоматизированные рабочие места либо специализированные серверы. Данная процедура производится согласно инструкции по установке SIEM-системы, предоставляемой производителем SIEM-системы либо сотрудниками компании-заказчика SIEM-системы, либо сотрудниками производителя SIEM-системы по согласованию с заказчиком.

Первоначальная настройка SIEM-системы представляет собой набор действий по редактированию конфигурационных файлов SIEM-системы или использование специальных программ – «мастеров конфигурации», выполняющих первоначальную настройку пошагово. Процедура первоначальной настройки SIEM-системы выполняется либо согласно инструкции по настройке SIEM-системы, либо согласно инструкции по установке SIEM-системы, если она содержит раздел настройки. Цель первоначальной настройки SIEM-системы – приведение установленной SIEM-системы в минимально работоспособное состояние, в котором она способна предоставлять базовый набор функций. Установка и настройка SIEM-системы производится либо для всей SIEM-системы в целом, либо для отдельных её компонентов.

В процессе установки и настройки SIEM-системы у коллектива заказчиков и исполнителей могут возникнуть следующие типовые проблемы.

1. Сложность построения SIEM-систем, связанная с необходимостью сбора и анализа событий от различных неоднородных агентов, требует с одной стороны высокой квалификации специалистов по установке для правильной конфигурации SIEM-системы в СЭД, с другой стороны, компетенции такого специалиста могут быть только у производителя или вендора SIEM-системы, что в значительной степени увеличивает сроки внедрения и делает невозможным пакетный вариант решения SIEM-системы.

2. Необходимость выделения зачастую неоднородных аппаратных платформ, что может ограничить внедрение SIEM-системы в существующую информационную инфраструктуру СЭД.

3. Достаточно высокие требования к техническим характеристикам аппаратных платформ, что может приводить к удорожанию проекта внедрения SIEM-систем и требовать оптимизации функциональных и технических решений.

4. Большая трудоемкость разработки технической документации на многокомпонентную SIEM-систему и, соответственно, наличие в ней возможных ошибок может приводить к увеличению сроков внедрения таких систем.

Разработка путей решения выявленных проблем внедрении SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности

Для решения выявленных проблем внедрения SIEM-систем целесообразно использовать следующие пути, основанные на применении системного подхода.

1. Упрощение SIEM-системы, представляющее собой отказ от редко используемых модулей и перестройку архитектуры SIEM-системы.

2. Автоматизация процедуры типовой установки и общей настройки SIEM-системы, представляющая собой разработку методики автоматизации процедуры типовой установки и общей настройки SIEM-системы и программного модуля, реализующего разработанную методику.

3. Комбинированный подход, представляющий собой совместное применение двух вышеуказанных подходов, который позволяет максимально приблизить SIEM-систему как продукт к «коробочной» версии.

Наиболее предпочтительным в настоящее время путём решения выявленных проблем внедрении SIEM-систем в практику управления информационной безопасностью СЭД является комбинированный подход, так как он позволяет как оптимизировать архитектуру SIEM-системы, так и упростить типовую установку и общую настройку SIEM-системы. В данной статье рассмотрена схема автоматизации процедуры типовой установки и общей настройки SIEM-системы на основе применения

метода сетевого планирования и управления [16]. Суть этого метода состоит в моделировании процесса типовой установки и общей настройки SIEM-системы с помощью сетевого графика на базе применения теории графов, теории вероятностей и компьютерных технологий.

Данный метод позволяет является не только моделировать весь комплекс работ, но и выявить те участки, от которых в наибольшей степени зависит выполнение всего проекта внедрения SIEM-системы в установленные сроки. Этот метод учитывает все многообразие связей между отдельными работами и позволяет оценить влияние отклонения от плана на дальнейший ход работы и способствует оптимизации процесса управления всем ходом работ по внедрению SIEM-системы в практику управления информационной безопасностью СЭД.

Система сетевого планирования и управления (СПУ) – совокупность научно обоснованных положений организации и управления производством, основанной на моделировании процесса с помощью сетевого графика на базе применения теории графов, теории вероятностей и компьютерных технологий.

Система СПУ позволяет формировать календарный план реализации сложного комплекса работ, определять и мобилизовать резервы времени, предупреждать возможные срывы в ходе работ, осуществлять оперативную корректировку планов.

Первоначально разработка СПУ вызывалась необходимостью обоснованного прогнозирования срока окончания крупных бизнес-проектов, однако по мере развития этих систем и компьютерных технологий они стали применяться для решения значительно более широкого круга задач. Будучи эффективным средством планирования и управления, сетевые методы вместе с тем отличаются простотой и доступностью, что в немалой степени способствовало их быстрому освоению на практике. В настоящее время возможно применение СПУ как в форме однократного использования сетевых методов и моделей, так и в форме постоянно действующей системы СПУ как составной части более сложных систем управления. В этом случае методы СПУ сочетаются с применением ряда экономико-математических методов, в первую очередь таких, в которых использование сетевых моделей особо показательно и результативно (теория массового обслуживания).

Преимущества СПУ весьма велики, поскольку система позволяет:

- сформировать календарный план реализации сложного бизнес-проекта;
- определить и мобилизовать резервы времени, материальных, финансовых, информационных, трудовых ресурсов;
- осуществить реализацию логистического принципа “точно в срок” с прогнозированием и предупреждением возможных срывов в ходе реализации проекта;
- производить оперативную реализацию бизнес-проекта;
- повышать эффективность менеджмента при четком распределении ответственности между руководителями разного уровня и исполнителями и необходимом делегировании полномочий.

Особенностью методов СПУ является не только моделирование всего комплекса работ, но и выявление тех участков, от которых в наибольшей степени зависит выполнение всего бизнес-проекта в установленные сроки. Этот метод учитывает все многообразие связей между отдельными работами, позволяет оценить влияние отклонения от плана на дальнейший ход работы и способствует оптимизации процесса управления всем ходом работ.

Основным элементом системы СПУ является сетевая модель, отображающая с любой степенью детализации план выполнения некоторого комплекса взаимосвязанных работ, заданного в специфической форме сети, наглядное изображение которой представляет собой сетевой график. Сетевым графиком называется наглядное изображение последовательности и взаимной логической связи всех работ, выполняемых в процессе разработки и получаемых при этом результатов, вплоть до достижения конечной цели. Различают системы СПУ с детерминированными и вероятностными моделями. Всем моделям свойственны общие принципы:

- по каждому объекту составляются сетевые графики – условные экономико-математические модели, отражающие весь ход выполнения работ от начала до завершения;
- сроки проведения работ по отдельным этапам определяются исходя из конечного срока;
- при составлении сетевого графика используются следующие исходные материалы: задание на проектирование, проектно-конструкторская документация, проекты производства работ, действующие технологические процессы, графики поставок ресурсов, оборудования, документации.

Главными элементами сетевого графика являются понятия ***событие*** и ***работа.*** Термином “работа” обозначается совокупность приемов и действий, необходимых для выполнения конкретной задачи или достижения определенной цели. Работа выражает сложное понятие и подразделяется на работу-действие, работу-ожидание и зависимость (фиктивную работу).

Работа-действие – процесс, происходящий во времени, и требующий затрат ресурсов (материальных, информационных, финансовых, трудовых). Каждая работа-действие конкретна, определенна, имеет ответственного исполнителя. Она переводит одно событие в другое и на сетевом графике изображается сплошной линией со стрелкой. Примеры подобной работы: закупка материальных ресурсов, изготовление конечной продукции, испытание конструкции.

Работа-ожидание – процесс, происходящий во времени, но не требующий ресурсных затрат. Работа-ожидание переносит событие во времени и на сетевом графике также изображается сплошной линией со стрелкой. К таким работам относятся процесс сушки изделия естественным путем после покраски, твердение бетона при строительных работах.

Зависимость (фиктивная работа) показывает логическую связь между двумя или несколькими событиями; не требует ресурсных и временных затрат, но указывает на то, что возможность начала одной работы непосредственно зависит от результатов другой. Ее продолжительность принимается равной нулю и на сетевом графике она изображается пунктирной линией со стрелкой.

Термином ***событие*** обозначается некоторый итог, результат, состояние, момент завершения процесса, которым закапчивается какая-либо работа. Событие отражает этап выполнения комплекса работ, причем этот результат должен быть достаточным для начала последующей работы. Иначе говоря, событие может свершиться только тогда, когда закончатся все работы, ему предшествующие, а последующие работы могут начаться только тогда, когда событие свершится. Для всех непосредственно следующих за ним работ событие является начальным или предшествующим, а для всех непосредственно предшествующих ему работ – конечным или последующим. Событие не имеет продолжительности, совершается как бы мгновенно; оно должно иметь точную формулировку, включающую в себя результат всех непосредственно предшествующих ему работ.

События могут быть простыми и сложными. Простое событие характеризуется результатом выполнения одной работы, а сложное событие – двух и более работ. Среди событий выделяют исходное и завершающее события. Исходное событие не имеет предшествующих работ и событий, относящихся к отраженному в сетевой модели комплексу работ. Завершающее событие не имеет последующих работ и событий.

Если в сетевой модели нет числовых оценок, то такая сеть называется структурной. Однако чаще всего используются сети, в которых заданы оценки продолжительности работ (указываемые в часах, неделях, месяцах и т.д. над соответствующими стрелками), а также оценки других показателей (трудоемкости, стоимости). Ориентация и размеры стрелок (топология сети) принципиального значения не имеют, так же как сетевой график не имеет масштаба. При построении сетевого графика необходимо соблюдать целый ряд общепринятых правил:

1) только исходные события не имеют входящих стрелок, т.е. не должно быть событий (кроме исходного), которым не предшествует хотя бы одна работа;

2) только конечные события не имеют выходящих стрелок, т.е. не должно быть событий, из которых не выходит ни одна работа, за исключением завершающего;

3) каждая работа должна иметь предшествующее и последующее события;

4) не должно быть контуров и петель, соединяющих события с ними же самими, так как это означает, что условием начала некоторой работы является ее же окончание;

5) любые два события должны быть непосредственно связаны не более чем одной работой. Нарушение этого условия приводит к появлению на сетевом графике параллельных работ, которые могут значительно отличаться по затрачиваемым ресурсам. Для устранения этого нарушения вводится фиктивное событие, фиктивная работа и одна из параллельных работ замыкается на это фиктивное событие.

Путь, имеющий наибольшую временную продолжительность, называется критическим. В нашем случае этот вариант пути таков: 1 – 2 – 3 – 7 – 8 – 9. Критическими называются также события и работы, расположенные на критическом пути. Пути, имеющие продолжительность, близкую к продолжительности критического пути, называются подкритическими, а остальные – ненапряженными.

Критический путь является центральным понятием СПУ. Важнейшей целью анализа сетевого графика по критерию времени является установление общей продолжительности всего комплекса работ. Общая продолжительность определяется не всеми работами сети, а лишь лежащими па критическом пути. Увеличение времени или задержка выполнения любой критической работы ведет к задержке завершения всего комплекса работ, в то время как отсрочка выполнения некритических работ может и не отразиться на сроке наступления завершающего события. Отсюда следует, что первоочередное внимание надлежит уделить своевременному выполнению критических работ, обеспечению их необходимыми материальными, информационны-

ми, финансовыми, трудовыми и пр. ресурсами с тем, чтобы выдержать срок выполнения всего комплекса работ. Если критический путь по первоначально составленному графику оказался продолжительней планового срока, то для его уменьшения необходимо выявить возможности сокращения именно критических, а не любых других работ. В этом и проявляется логистическое содержание метода СПУ.

Если длительности работ не являются детерминированными величинами, то каждая работа оценивается следующими возможными сроками исполнения:

t_{min} – оптимистическая оценка – минимальный срок, в течение которого будет выполнена работа в наиболее благоприятных условиях;

t_{max} – пессимистическая оценка – максимальный срок," необходимый для выполнения работы при наиболее неблагоприятных условиях;

$t_{вер}$ – наиболее вероятная продолжительность времени, показывающая время выполнения работы в нормальных условиях;

$t_{ож}$ – ожидаемая продолжительность работы; определяется на основании вышеуказанных оценок по одной из формул:

$$t_{ож} = \frac{\left(t_{\min} + 4t_{вер} + t_{\max}\right)}{6}$$

или

$$t_{ож} = \frac{\left(3t_{\min} + 2t_{\max}\right)}{5}.$$

Исходной информацией сетевой модели являются:

– сеть с единственным исходным событием 1 и единственным завершающим событием 9, которое является единственным целевым в модели;

– продолжительность каждой из комплекса работ, представленных в сети, при этом фиктивным работам соответствует нулевая продолжительность.

Кроме того, исходная информация содержит момент начала выполнения комплекса работ, т.е. момент наступления исходного события, а также плановый срок наступления завершающего события, т.е. всего комплекса работ.

Любой план однозначно определяет момент завершения комплекса работ и если задан плановый срок, то критический путь модели не должен превышать этого срока. Если продолжительность критического пути не превышает плановый срок или в исходной информации таковой отсутствует, то допустимый план существует и выполнение его реально. При этом момент наступления событий, начала и окончания работ определяются исходной информацией не обязательно однозначно: они могут варьироваться в определенных диапазонах. При анализе сетевого графика определяются параметры, ограничивающие этот диапазон. При анализе сетевого графика определяются параметры, ограничивающие эти диапазоны.

Для каждого события определяются:

Тр – ранний срок наступления события – минимальный из возможных моментов наступления данного события при заданных продолжительностях работ и начальном моменте без учета планового срока завершения комплекса работ. Ранний срок наступления события определяется продолжительностью максимального пути, предшествующего этому событию, так как событие не может свершиться до наступления всех предшествующих ему событий и выполнения всех предшествующих работ. Наступление события может быть задержано до тех пор, пока срок его наступления и продолжительность максимального из последующих за ним путей не превысит длины критического пути;

Т" – поздний срок наступления события – максимальный из допустимых моментов наступления данного события, при которых еще возможно выполнение всех последующих работ с соблюдением планового срока наступления завершающего события. Поздний срок наступления события определяется разностью между длительностью критического пути и продолжительностью максимального пути, следующего за этим событием до завершающего события сети;

К – резерв времени события – допустимый срок, на который можно задержать наступление этого события, не вызывая при этом увеличения срока выполнения всего комплекса работ. Резерв времени события определяется как разность между поздним и ранним сроками его наступления [17].

В обобщенном виде весь комплекс работ можно разбить на этапы, которые представлены в табл. 1 и на рис. 2.

Процесс установки и настройки SIEM-системы включает в себя следующие этапы:

1. Типовая установка SIEM-системы;
2. Установка дополнительных компонентов SIEM-системы;
3. Общая настройка SIEM-системы;
4. Тонкая настройка SIEM-системы.

Этап типовой установки SIEM-системы представляет собой копирование основных компонентов SIEM-системы на автоматизированные рабочие места, либо специализированные серверы. Данная процедура производится согласно инструкции по установке SIEM-системы, предоставляемой производителем SIEM-системы либо сотрудниками компании-заказчика SIEM-системы, либо сотрудниками производителя SIEM-системы по согласованию с заказчиком.

Этап установки дополнительных компонентов

Таблица 1

Технологическая таблица этапов установки и настройки SIEM-системы

Этап	Предшествующие этапы	Последующие этапы	Исходное состояние	Конечное состояние
Этап 1	–	Этап 3	Начало	1
Этап 2	Этап 3	Этап 4	2	3
Этап 3	Этап 1	Этап 2	1	2
Этап 4	Этап 2	–	3	Конец

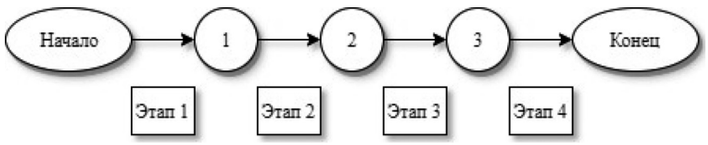

Рис. 2. Граф этапов установки и настройки SIEM-системы

Таблица 2

Технологическая таблица этапов установки и настройки SIEM-системы с применением автоматизированного решения задачи

Этап	Предшествующие этапы	Последующие этапы	Исходное состояние	Конечное состояние
Этап 1	–	Этап 2	Начало	1
Этап 2	Этап 1	Этап 3	1	2
Этап 3	Этап 2	–	2	Конец

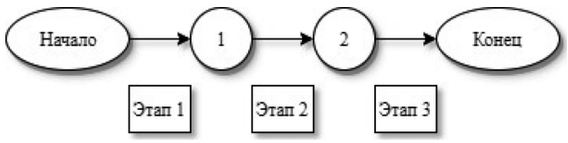

Рис. 3. Граф этапов установки и настройки SIEM-системы с применением автоматизированного решения задачи

SIEM-системы представляет собой копирование дополнительных компонентов SIEM-системы (коннекторов для средств и систем обеспечения информационной безопасности, систем тестирования и т.д.) на автоматизированные рабочие места либо специализированные серверы.

Этап общей настройки SIEM-системы представляет собой набор действий по редактированию конфигурационных файлов SIEM-системы или использование специальных программ – «мастеров конфигурации», выполняющих первоначальную настройку пошагово.

Этап тонкой настройки SIEM-системы представляет собой набор действий по внесению в конфигурационные файлы SIEM-системы дополнительных параметров и их значений, специфичных для конкретной системы обеспечения информационной безопасности и других информационных систем заказчика.

Анализ содержания работ, входящих в рассмотренные этапы установки и настройки SIEM-системы показывает, что целесообразно рассмотреть задачу автоматизации процедур типовой установки и общей настройки SIEM-системы на этапах 1 и 3, так как они не зависят от системы обеспечения информационной безопасности и других информационных систем заказчика [18]

В результате решения этой задачи автоматизированный процесс установки и настройки SIEM-системы включает в себя следующие этапы:

запуск программы автоматизированной типовой установки и общей настройки SIEM-системы;

установка дополнительных компонентов SIEM-системы;

тонкая настройка SIEM-системы.

Обобщенный комплекс работ по установке и настройке SIEM-системы с применением автоматизированного решения задачи представлен в табл. 2 и на рис. 3.

Заключение

Проведенный анализ схемы типовой архитектуры и процесса внедрения SIEM-системы показал, что в настоящее время вышеуказанный процесс является во многом ручным, требует от специалиста, проводящего установку и настройку SIEM-системы, высокой квалификации и занимает достаточно продолжительное время [19–20].

Разработанные предложения по совершенствованию процесса внедрения SIEM-системы основаны на применении автоматизированных процедур типовой установки и настройки SIEM-системы, что приводит к снижению временных затрат на внедрение SIEM-системы, повышает удобство выполнения данных процедур и в целом может привести к «коробочному» варианту решения продукта данного класса систем управления событиями информационной безопасности, что является существенным экономическим фактором для производителей и вендоров этих систем.

Литература

1. Riesco R., Villagrá, VA Int. J. Инф. Secur. 2019. 18: 715. DOI: 10.1007/s10207-019-00433-2.

2. ОАЗИС: «Технические характеристики STIX ™ 2.0». URL: https://oasisopen.github.io/cti-documentation/resources#stix-20-specification. (дата обращения: 7.08.2018)

3. ОАЗИС: «Белая книга STIX ™». URL: https://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf (дата обращения: 15. 06. 2018).

4. Новицкий Н.И. Сетевое планирование и управление производством. М.: Новое знание, 2004. 159 с.

5. Методы сетевого планирования и управления. URL: https://studme.org/1633082614268/logistika/metody_setevogo_planirovaniya_upravleniya. (дата обращения: 15. 12. 2019)

6. ОАЗИС: «TTP (Техника, тактика и процедуры» от STIX ™. URL: https://stixproject.github.io/getting-started/whitepaper/#tactics-techniques-and-procedures-ttp. (дата обращения: 7.08.2018)

7. ОАЗИС: «Кампании STIX ™». URL: https://stixproject.github.io/getting-started/whitepaper/#campaigns. (дата обращения: 7.08.2018)

8. ОАЗИС: «Инциденты от STIX ™». URL: https://stixproject.github.io/getting-started/whitepaper/#incidents. (дата обращения: 7.08.2018)

9. Сизов В.А. Разработка метода многокритериального бенчмаркинга информационной безопасности организации. Инжиниринг предприятий и управление знаниями (ИП&УЗ-2019). Сборник научных трудов XXII Международной научной конференции. 25–26 апреля 2019 г. под науч. ред. Ю. Ф. Тельнова: в 3 т. Москва: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2019. Т. 2. С. 97–100.

10. SIEM. Что это такое? URL: https://www.itbsgroup.ru/news/blog/siem-security/. (дата обращения: 15.12.2019)

11. SIEM (Security information and event management) URL: https://ru.bmstu.wiki/SIEM_(Security_information_and_event_management). (дата обращения: 15.12.2019)

12. VM Cotenescu. SIEM (Security Information and Event Management Solutions) Implementations in Private or Public Clouds. J. Lee, Y.S. Kim, J.H. Kim, I.K. Kim. Toward the SIEM architecture for cloud-based security services // Naval Academy Scientific Bulletin. 2016. Volume XIX. Issue 2. DOI: 10.21279/1454-864X-16-I2-058.

13. 6 типичных ошибок при внедрении SIEM-решений и как их избежать. URL: https://rvision.pro/blog-posts/6-tipichnyh-oshibok-pri-vnedrenii-siem-reshenij-kak-ih-izbezhat/. (дата обращения: 15.12.2019)

14. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5. С. 54–65.

15. Рыболовлев Д.А., Карасёв С.В., Поляков С.А. Классификация современных систем управления инцидентами безопасности // Вопросы кибербезопасности. 2018. № 3 (27). С. 47–53.

16. Будникова И.К., Приймак Е.В. Моделирование управляемых процессов с применением методов сетевого планирования // Вестник технологического университета. Казань.: Изд-во: Казанский национальный исследовательский технологический университет, 2018. Т. 21. № 1. с. 115–118.

17. Допира Р.В., Кордюков Р.Ю., Беглецов А.А., Сергиенко С.В. Метод сетевого планирования разработки сложных технических систем // Программные продукты и системы. 2014, № 2, с. 22–25.

18. Киров А.Д. Автоматизация процесса общей настройки автоматизированной системы защиты от утечек данных «InfoWatch Traffic Monitor 6.9».

19. M. Nabil, Soukainat S., Lakbabi A., Ghizlane O. SIEM selection criteria for an efficient contextual security // 2017 International Symposium on Networks, Computers and Communications (ISNCC), 2017. DOI: 10.1109/ISNCC.2017.8072035.

20. Connolly J, Davidson M, Richard M, Skorupka C. "The Trusted Automated eXchange of Indicator Information (TAXIITM)" November 2012. URL: http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf

References

1. Riesco R., Villagrá, VA Int. J. Inf. Secur. 2019. 18: 715. DOI: 10.1007/s10207-019-00433-2.

2. OAZIS: «Tekhnicheskiye kharakteristiki STIX ™ 2.0» = OASIS: "STIX™ 2.0 Specifications.". URL: https://oasisopen.github.io/cti-documentation/resources#stix-20-specification. (cited: 7.08.2018). (In Russ.)

3. OAZIS: «Belaya kniga STIX ™». [Internet] = OASIS: STIX ™ White Paper. URL: https://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf. (cited: 15. 06. 2018). (In Russ.)

4. Novitskiy N.I. Setevoye planirovaniye i upravleniye proizvodstvom = Network planning and production management. Moscow: New knowledge; 2004. 159 P. (In Russ.)

5. Metody setevogo planirovaniya i upravleniya = Methods of network planning and management. URL: https://studme.org/1633082614268/logistika/metody_setevogo_planirovaniya_upravleniya. (cited: 15. 12. 2019). (In Russ.)

6. OAZIS: «TTP (Tekhnika, taktika i protsedury» ot STIX ™ = OASIS: "TTP (Technique, Tactics and Procedures" by STIX ™. URL: https://stixproject.github.

io/getting-started/whitepaper/#tactics-techniques-and-procedures-ttp. (cited: 7.08.2018). (In Russ.)

7. OAZIS: «Kampanii STIX ™» = OASIS: «STIX ™ Campaigns». URL: https://stixproject.github.io/getting-started/whitepaper/#campaigns. (cited: 7.08.2018). (In Russ.)

8. OAZIS: «Intsidenty ot STIX ™» = OASIS: «Incidents from STIX ™. URL: https://stixproject.github.io/getting-started/whitepaper/#incidents. (cited: 7.08.2018). (In Russ.)

9. Sizov V.A. Development of a multi-criteria benchmarking method for information security of an organization. Enterprise engineering and knowledge management (IP & UZ-2019). Sbornik nauchnykh trudov XXII Mezhdunarodnoy nauchnoy konferentsii. 25–26 aprelya 2019 g. pod nauch. red. YU. F. Tel'nova: v 3 t = Collection of scientific papers of the XXII International Scientific Conference. April 25–26, 2019 under the scientific ed. Yu. F. Telnova: in 3 tons. Moscow: Plekhanov Russian University; 2019; 2: 97–100. (In Russ.)

10. SIEM. Chto eto takoye? = SIEM. What it is? URL: https://www.itbsgroup.ru/news/blog/siem-security/. (cited: 15.12.2019). (In Russ.)

11. SIEM (Security information and event management) URL: https://ru.bmstu.wiki/SIEM_(Security_information_and_event_management). (cited: 15.12.2019). (In Russ.)

12. VM Cotenescu. SIEM (Security Information and Event Management Solutions) Implementations in Private or Public Clouds. J. Lee, Y.S. Kim, J.H. Kim, I.K. Kim. Toward the SIEM architecture for cloud-based security services. Naval Academy Scientific Bulletin; 2016; XIX; 2. DOI: 10.21279/1454-864X-16-I2-058.

13. 6 tipichnykh oshibok pri vnedrenii SIEM-resheniy i kak ikh izbezhat' = 6 typical mistakes in the implementation of SIEM-solutions and how to avoid them. URL: https://rvision.pro/blog-posts/6-tipichnyh-oshibok-pri-vnedrenii-siem-reshenij-kak-ih-izbezhat/. (cited: 15.12.2019). (In Russ.)

14. Kotenko I.V., Sayenko I.B. SIEM systems for managing information and security events. Zashchita informatsii. Insayd = Information Security. Insider. 2012; 5: 54–65. (In Russ.)

15. Rybolovlev D.A., Karasov S.V., Polyakov S.A. Classification of modern security incident management systems. Voprosy kiberbezopasnosti = Cybersecurity issues. 2018; 3 (27): 47–53. (In Russ.)

16. Budnikova I.K., Priymak Ye.V. Modeling of controlled processes using network planning methods. Vestnik tekhnologicheskogo universiteta = Bulletin of the Technological University. Kazan: Publishing House: Kazan National Research Technological University; 2018; 21; 1: 115–118. (In Russ.)

17. Dopira R.V., Kordyukov R.Yu., Begletsov A.A., Sergiyenko S.V. Network planning method for the development of complex technical systems. Programmnyye produkty i sistemy = Software products and systems. 2014; 2: 22–25. (In Russ.)

18. Kirov A.D. Avtomatizatsiya protsessa obshchey nastroyki avtomatizirovannoy sistemy zashchity ot utechek dannykh «InfoWatch Traffic Monitor 6.9» = Automation of the general setup process for the automated InfoWatch Traffic Monitor 6.9 data leak protection system. (In Russ.)

19. M. Nabil, Soukainat S., Lakbabi A., Ghizlane O. SIEM selection criteria for an efficient contextual security. 2017 International Symposium on Networks, Computers and Communications (ISNCC); 2017. DOI: 10.1109/ISNCC.2017.8072035.

20. Connolly J, Davidson M, Richard M, Skorupka C. "The Trusted Automated eXchange of Indicator Information (TAXIITM)" November 2012. URL: http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf

Сведения об авторах

Валерий Александрович Сизов
д.э.н., профессор, профессор кафедры прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: sizovva@gmail.com

Алексей Дмитриевич Киров
Специалист специализированной учебно-научной лаборатории по информационному противоборству в бизнесе кафедры прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В. Плеханова, Москва, Россия
E-mail: kirow.alesha@yandex.ru

Information about the authors

Valery A. Sizov
Dr. Sci. (Economics), Professor, Professor of the Department of applied Informatics and information security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: sizovva@gmail.com

Alexey D. Kirov
Specialist of the specialized educational and scientific laboratory on information confrontation in business of the Department of applied Informatics and information security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: sizovva@gmail.com