УДК 004.056.53

И.В. Котенко, И.Б. Саенко, О.В. Полубелова, А.А. Чечулин

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУРАХ

Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. **Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах.**

Аннотация. Применение *SIEM*-технологии (технологии управления информацией и событиями безопасности) является перспективным направлением в области защиты информации, особенно для критически важных инфраструктур. В статье приводятся общие положения по построению и функционированию систем, реализующих данную технологию, дается характеристика известных реализаций таких систем, а также обсуждаются особенности проекта *MASSIF* Седьмой рамочной программы Европейского Союза по созданию перспективных систем управления событиями и информационной безопасностью. Рассматриваются вопросы решения двух ключевых задач проекта, связанных с анализом событий безопасности на основе моделирования сетевых атак и построения репозитория.

Ключевые слова: информационная безопасность, события безопасности, критическая инфраструктура, мониторинг безопасности, моделирование сетевых атак, репозиторий.

Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A. **Application of security information and event management technology for information security in critical infrastructures.**

Abstract. Application of SIEM (Security Information and Event Management) technology is promising in the field of information protection, especially for critical infrastructures. The paper considers the general issues of construction and operation of systems that implement this technology. The known implementations of such systems are described. The paper also discusses the peculiarities of the MASSIF project of the seventh framework program of the European Union which is devoted to advanced SIEM systems. We outline two key tasks of the project associated with the analysis of security events, based on the modeling of network attacks, and building the SIEM repository.

Keywords: information security, security event, critical infrastructure, security monitoring, modeling of network attacks, repository.

1. Введение. В условиях интенсивного развития и внедрения информационных и телекоммуникационных технологий ведущими государствами мира уделяется особое внимание вопросам обеспечения безопасности критически важных объектов, к которым относятся крупные гидротехнические сооружения, сети атомных электростанций, вредные химические производства, транспортные узлы, аэродромы и другие. Выведение таких объектов из строя может привести к тяжелым и даже катастрофическим последствиям. Совокупность кри-

тически важных объектов составляет содержание понятия критически важной инфраструктуры (КВИ). В США в соответствии с «Законом о патриотизме» (*USA Patriot Act*), принятым Конгрессом 26 октября 2001 года, критическая инфраструктура определяется как «совокупность физических или виртуальных систем и средств, важных для США в такой мере, что их выход из строя или уничтожение могут привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации» [1].

Для успешной реализации мероприятий защиты КВИ необходимо решение ряда задач, основная из которых связана с созданием системы мониторинга угроз безопасности [2], главной целью создания которой является снижение до минимального уровня риска воздействия на объекты КВИ и минимизация возникающего ущерба.

2. Понятие *SIEM*-системы. Учитывая характер и содержание задач защиты КВИ, представляется целесообразным положить в основу построения системы мониторинга концепцию *SIEM*-системы. Для этого рассмотрим подробнее содержание этого понятия.

Основной целью построения и функционирования *SIEM*-систем, где *SIEM* означает управление информацией и событиями безопасности (*Security Information and Event Management*), является значительное повышение уровня информационной безопасности в информационно–телекоммуникационной инфраструктуре за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности.

«Проактивный» означает «действующий до того, как ситуация станет критической». Предполагается, что *проактивное управление* инцидентами и событиями безопасности основывается на автоматических механизмах, которые используют информацию об «истории» анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы [3, 4].

Для достижения данной цели *SIEM*-система КВИ должна обладать возможностью успешного решения следующего комплекса задач:

- сбора, обработки и анализа событий безопасности, поступающих в систему из множества гетерогенных источников;
- обнаружения в режиме реального времени атак и нарушений критериев и политик безопасности;
- оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов;

- анализа и управления рисками безопасности КВИ;
- проведения расследований инцидентов;
- обнаружения расхождения критически важных ресурсов и бизнес–процессов с внутренними политиками безопасности и приведение их в соответствие друг с другом;
- принятия эффективных решений по защите информации;
- формирования отчетных документов.

Основными исходными данными, которые используются *SIEM*-системой для решения указанных задач, являются записи различных журналов (*logs*), протоколирующие события в КВИ, называемые «событиями безопасности». Данные события отражают такие действия пользователей и программ, которые могут оказать влияние на безопасность. Из общего множества событий безопасности *SIEM*-система должна находить такие, которые свидетельствуют об атаках или иных нежелательных действиях в КВИ, причем традиционные методы поиска такой информации достаточно трудоемки.

3. Архитектура *SIEM* системы. Как правило, *SIEM*-система имеет архитектуру «агенты» — «хранилище данных» — «сервер приложений», которая разворачивается поверх защищаемой информационной инфраструктуры [5].

Агенты выполняют сбор событий безопасности, их первоначальную обработку и фильтрацию.

Собранная и отфильтрованная информация о событиях безопасности поступает в *хранилище данных* или *репозиторий*, где она хранится во внутреннем формате представления с целью последующего использования и анализа сервером приложений.

Сервер приложений реализует основные функции защиты информации. Он анализирует информацию, хранимую в репозитории, и преобразует ее для выработки предупреждений или управленческих решений по защите информации.

Таким образом, в *SIEM*-системе можно выделить следующие три архитектурных уровня ее построения (рис. 1) [6]: (1) сбора данных; (2) управления данными; (3) анализа данных.

На первом уровне сбор данных осуществляется от источников различных типов. К числу таковых относятся: файловые серверы, серверы баз данных, *Windows*-серверы, межсетевые экраны (МСЭ), рабочие станции, системы противодействия атакам (*IPS, intrusion prevention systems*), антивирусные программы и т.п.

На втором уровне осуществляется управление данными о событиях безопасности, которые хранятся в репозитории.

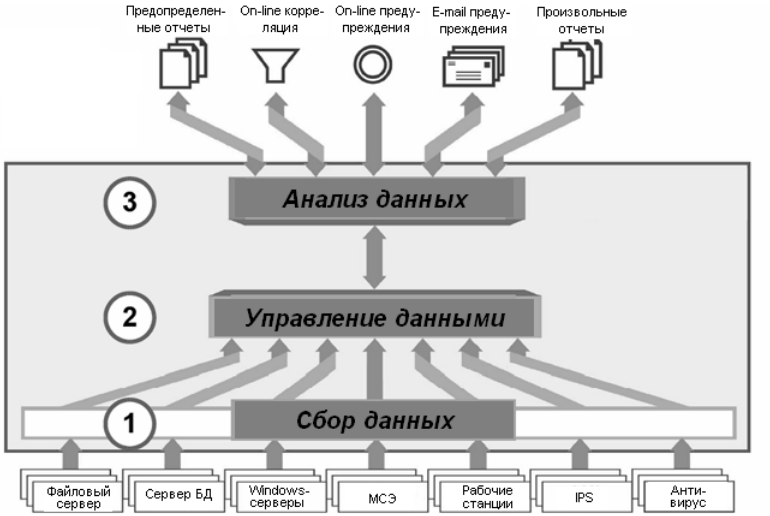

Рис. 1. Архитектура типовой *SIEM*-системы.

Данные, хранящиеся в репозитории, выдаются по запросам моделей анализа данных.

Результатами обработки информации в *SIEM*-системе, получаемыми на третьем уровне, являются отчеты в предопределенной и произвольной форме, оперативная (*on-line*) корреляция данных о событиях, а также предупреждения, вырабатываемые в режиме *on-line* и (или) передаваемые по электронной почте.

4. Функционирование *SIEM*-системы. *SIEM*-система сочетает функции двух других классов систем, относящихся к системам мониторинга и управления безопасностью информации — *SIM (Security Information Management)* и *SEM (Security Event Management).* По этой причине *SIEM*-система выполняет свойственные *SIM*- и *SEM*-системам функции. К группе функций *SIM*-системы относятся сбор, хранение и анализ записей журналов, а также формирование необходимой отчетности. К группе функций *SEM*-системы относится мониторинг событий безопасности в реальном времени, а также выявление и реагирование на инциденты безопасности.

Реализация указанных выше функций в *SIEM*-системе осуществляется на основе выполнения комплекса различных механизмов функционирования. В *SIEM*-системах первого поколения к числу таких механизмов, как правило, относятся нормализация, фильтрация, класси-

фикация, агрегация, корреляция и приоритезация событий, а также генерация отчетов и предупреждений [5]. В *SIEM*-системах нового поколения к их числу следует добавить также анализ событий, инцидентов и их последствий, а также принятие решений и визуализацию. Распределение указанных механизмов по уровням иерархии *SIEM*-системы показано на рис. 2.

Рис. 2. Обобщенная иерархическая модель *SIEM*-системы.

Раскроем содержание основных механизмов функционирования *SIEM*-системы. *Нормализация* означает приведение форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки. *Фильтрация* событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков. *Классификация* позволяет для атрибутов событий безопасности определить их принадлежность определенным классам. *Агрегация* объединяет события, схожие по определенным признакам. *Корреляция* выявляет взаимосвязи между разнородными событиями, что позволяет обнаруживать атаки на КВИ, а также нарушения критериев и политик безопасности. *Приоритезация* определяет значимость и критичность событий безопасности на основании правил, определенных в системе.

Анализ событий, инцидентов и их последствий включает процедуры моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушите-

лей, оценки риска, прогнозирования событий и инцидентов. *Генерация отчетов и предупреждений* означает формирование, передачу, отображение и (или) печать результатов функционирования. *Принятие решений* определяет выработку мер по реконфигурированию средств защиты с целью предотвращения атак или восстановления безопасности инфраструктуры. *Визуализация* предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой КВИ и ее элементов.

Следует отметить, что при переходе к механизмам более высокого уровня модели, показанной на рис. 2, количество обрабатываемых событий уменьшается, а сложность их обработки увеличивается.

Взаимосвязь механизмов функционирования *SIEM*-системы нового поколения наглядно демонстрирует функциональная модель, представленная на рис. 3.

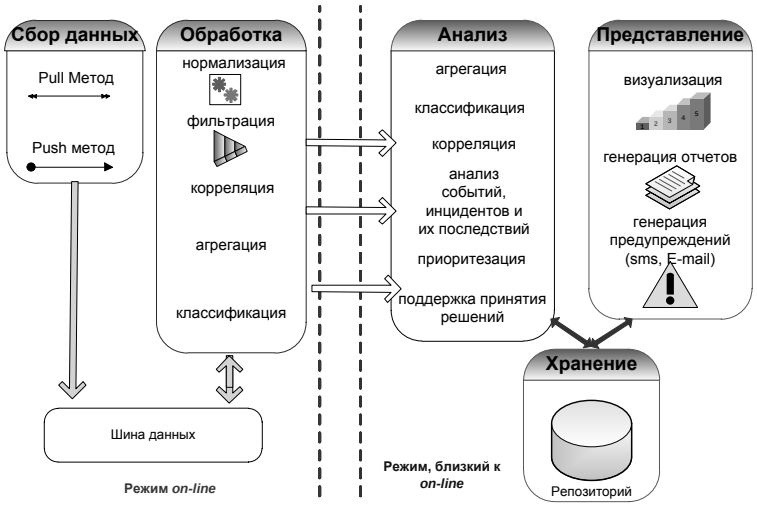

Рис. 3. Функциональная модель *SIEM*-системы.

Как видно из рис. 3, в *SIEM*-системе можно выделить пять основных функциональных подсистем: (1) сбора данных; (2) обработки; (3) хранения; (4) анализа; (5) представления. Причем первые две функционируют в режиме *on-line*, остальные — в близком к нему. Дадим краткую характеристику этим подсистемам.

Подсистема сбора данных. Для получения информации от источников используются два основных метода: *Push* и *Pull*. Суть метода *Push* заключается в том, что источник сам посылает данные записей своих журналов в *SIEM*-систему. В методе *Pull* система сама осуществляет процесс получения данных из журналов.

Сбор данных осуществляется от источников различных типов. Перечень примеров возможных источников данных о событиях безопасности схематично представлен на рис. 4 [6].

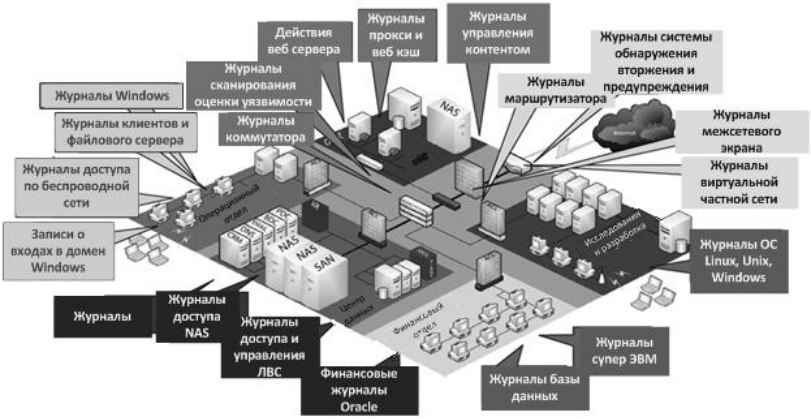

Рис. 4. Примеры источников данных о событиях безопасности.

Подсистема обработки. Обработка информации включает в себя нормализацию, фильтрацию, корреляцию, агрегацию и классификацию.

Подсистема хранения. Отфильтрованные данные в нормализованном виде помещаются для хранения в репозиторий. Репозиторий может быть создан на основе реляционной СУБД (наиболее распространенное решение), *XML*-ориентированной СУБД и (или) хранилища триплетов. Хранилище триплетов — это специально созданная база данных, оптимизированная для хранения и поиска *триплетов*, т.е. утверждений вида «субъект–предикат–объект».

Подсистема анализа. Анализ данных включает в себя следующие функции: корреляцию данных, классификацию, агрегацию, приоритезацию и анализ событий, инцидентов и их последствий (в том числе посредством моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров

нарушителей, оценки риска, прогнозирования событий и инцидентов), а также поддержку принятия решений. Анализ данных может основываться на качественных и количественных оценках. Количественная оценка является более точной, но требует заметно больше времени, что не всегда допустимо. Чаще всего бывает достаточно быстрого качественного анализа, задача которого заключается в распределении факторов риска по группам. Шкала качественного анализа может различаться в разных методах оценки, но все сводится к тому, чтобы выявить самые серьезные угрозы.

Подсистема представления. Представление включает в себя несколько функций: визуализацию, генерацию отчетов и генерацию предупреждений.

5. Обзор современных *SIEM*-систем. В настоящий момент существует множество коммерческих *SIEM*-решений, которые имеют возможность собирать и идентифицировать события безопасности, а также выполнять корреляцию событий и инцидентов.

Компания *Gartner* ежегодно производит оценку разработанных *SEIM*-систем различных производителей. Согласно отчетам компании *Gartner* [7] в число лидеров вошли следующие *SIEM*-системы: *Arc Sight, RSA (EMC), Q1 Labs, IBM, Symantec, Log Logic* и *Novell*(рис. 5). Приведем их краткую характеристику.

Компанией *Arc Sight* разработан ряд *SIEM*-систем. Система *Enterprise Security Manager* ориентирована на крупномасштабное применение [8], а система *Arc Sight Express* — на организации среднего размера с предопределенными процедурами мониторинга и отчетности [9]. Система *Arc Sight Logger* осуществляет сбор данных как в структурированных, так и в неструктурированных форматах [10, 11]. Структурированные данные собираются с помощью интерфейса, поддерживающего более 275 продуктов от 100 производителей. Неструктурированные данные собираются через *Syslog* или через доступ к *log*-файлам указанного устройства. Входная информация для данных систем представляется в специально разработанном едином формате *CEF* (*Common Event Format*) [12].

Подразделение *RSA* компании *EMC* распространяет приложение *enVision*, обеспечивающее одновременную реализацию функций *SIM*- и *SEM*-компонентов [13].

Для небольших инсталляций система включает функции сбора данных о событиях безопасности, управления ими и генерации отчетов. Для более крупных применений система может быть сконфигурирована для выполнения специальных функций сбора данных, манипу-

лирования событиями, выполнения аналитических вычислений и имеет возможность горизонтального масштабирования.

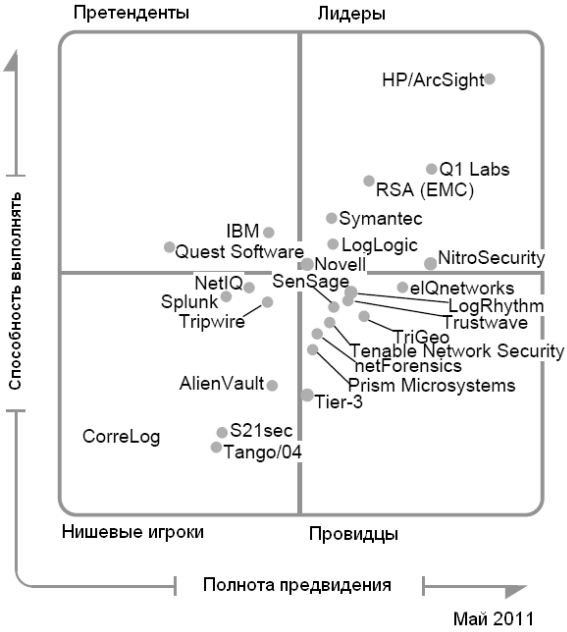

Рис. 5. Сравнение *SIEM*-систем согласно отчету *Gartner*.

SIEM-системы компании *Q1 Labs* обеспечивают управление записями журналов и событиями, отчетность и поведенческий анализ. Продукты семейства *QRadar* [14] могут быть установлены как решения «все в одном» для небольших организаций или могут быть внедрены в больших организациях с использованием специализированного коллектора событий, модуля обработки событий и консоли. Отличительной характеристикой *SIEM*-систем компании *Q1 Labs* является эффективная реализация сбора и обработки потоков сетевых данных для обеспечения анализа поведения сети и приложений.

Компания *IBM* предлагает комплексное решение в области *SIEM*-систем, которое называется *Tivoli Security Information and Event Manager* (*TSIEM*) [15, 16]. *TSIEM* позволяет, с одной стороны, проводить аудит событий безопасности на соответствие внутренним политикам и различным международным стандартам, а с другой стороны — осу-

ществлять обработку инцидентов, связанных с информационной безопасностью, и обнаруживать атаки и другие угрозы для элементов инфраструктуры.

В области представления и хранения событий *TSIEM* использует запатентованную методику *W7 (Who, did What, When, Where, Where-from, Where to and on What),* в соответствии с которой все события трансформируются в единый формат, понятный администраторам безопасности, аудиторам и управленцам. Также *TSIEM* обладает развитыми возможностями по формированию отчетов и мониторингу активности пользователей.

Компания *Symantec* обычно распространяет своим конечным пользователям собственные *SIEM*-технологии [17]. Система *Symantec Security Information Manager (SSIM)* разработана как программное приложение и обеспечивает возможности *SIM* и *SEM.*

Продукты компании *LogLogic* объединяют возможности *SEM,* управления конфигурацией механизмов защиты и мониторинга активности баз данных [18]. Возможности продуктов *LogLogic* могут быть объединены с широким множеством продуктов этого класса прочих разработчиков, включая *Oracle, SQL Server* и *Sybase*. С другой стороны, требуется улучшение интеграции между приложениями по управлению событиями безопасности и *LogLogic*, чтобы не возникало необходимости изменения интерфейса пользователя.

Приложение *Novell Sentinel Log Manager* компании *Novell* предназначено для сбора, хранения, представления и поиска данных аудита [19]. Основными компонентами *Novell Sentinel Log Manager* являются *Log Manager Server, Web* сервер, сервер отчетов и база данных. *Novell Sentinel Log Manager* может собирать и обрабатывать данные о событиях, которые генерируются журналами *Syslog*, журналами событий *Windows*, файлами, базами данных, *SNMP, Novell Audit, SDEE (Security Device Event Exchange), Check Point OPSEC* и другими механизмами хранения и протоколами.

Приложения *Sentinel* предпочтительны для крупномасштабных разработок, ориентированных на *SEM*. Они основываются на шинной событийной архитектуре, которая обеспечивает достаточно высокую гибкость и масштабируемость для больших разработок. Эти приложения просты в инсталляции, когда необходимо объединение управления событиями и простота отчетности, а также для организаций, которые используют другие продукты *Novell* в области управления доступом и идентификации.

Таким образом, по итогам отчета компании *Garter* на май 2011года компания *Arc Sight* является наиболее успешным и прогрессирующим производителем продуктов класса *SIEM*, которые обладают достаточно широким набором функций. По сравнению с конкурентами, у компании *Arc Sight* имеется самое большое число внедрений продуктов класса *SIEM*. В то же время, организации, которым нужны только основные функции управления событиями безопасности, могут использовать более простые и менее дорогие продукты, которые фокусируются на сборе данных и формировании базовой отчетности. При этом следует отметить, что программные продукты с открытым кодом традиционно являются также хорошим решением, не требующим больших затрат на программное обеспечение.

6. Цели и задачи проекта *MASSIF*. В связи с тем, что, с одной стороны, ни одна из существующих *SIEM*-систем не может считаться полностью пригодной для управления безопасностью, а, с другой, в связи с постоянно увеличивающейся значимостью и предполагаемым эффектом от применения *SIEM*-систем в различных инфраструктурах, возникает необходимость разработки решений по построению компонентов *SIEM*-систем нового поколения, способных эффективно функционировать в различных гетерогенных инфраструктурах, включая КВИ.

Проект с данными целями выполняется в настоящее время в рамках Седьмой рамочной программы Европейского Союза и носит название *MASSIF(Management of Security in formation and events in Service InFrastructure* — Управление информацией и событиями безопасности в инфраструктурах услуг) [20].

В проекте участвуют 12 организаций–партнеров: *ATOS* (Испания), *CINI* (Италия), *EPSILON* (Италия), *FRANCETELECOM* (Франция), Институт безопасных информационных систем Фраунхофера (Германия), Лиссабонский университет (Португалия), Санкт-Петербургский институт информатики и автоматизации РАН, Лаборатория проблем компьютерной безопасности (Россия), *Institut Telecom* (Франция), *ALIENVAULT* (Испания), *T-SYSTEMS* (ЮАР), Мадридский политехнический университет (Испания), *6CURE* (Франция).

Основной целью проекта *MASSIF* является достижение значимых результатов в области управления информацией и событиями безопасности. На базе надлежащей многоуровневой корреляции событий безопасности *MASSIF* должен предоставить инновационные методы для обнаружения возникающих угроз безопасности и инициирования дей-

ствий, направленных на восстановление безопасности до непосредственного возникновения возможных инцидентов.

SIEM-платформа уровня сервисов, разрабатываемая в проекте, затрагивает моделирование и формальную проверку безопасности, включая концепции доверенных вычислений, архитектуру надежного и отказоустойчивого сбора событий приложений, поддерживаемую масштабируемой и производительной платформой сбора и обработки событий в контексте моделей атак.

В документах проекта отмечается, что разрабатываемые решения призваны преодолеть следующие недостатки, присущие существующим *SIEM*-системам:

- ограничения на функции, накладываемые целевой инфраструктурой;
- неспособность согласованной интерпретации инцидентов и событий на различных уровнях;
- неспособность обеспечить высокую степень надежности и отказоустойчивости в распределенной среде сбора данных о событиях;
- низкая масштабируемость.

Устранение данных недостатков предполагается достичь за счет формирования уведомлений в режиме, близком к реальному времени, а также за счет применения проактивного управления инцидентами и событиями. *SIEM*-система нового поколения ориентируется на инфраструктуру сервисов, в которой обработка событий безопасности отличается интеллектуальностью, высокой масштабируемостью, многоуровневостью и многодоменностью. При этом должно быть реализовано упреждающее управление безопасностью, а так же надежный и устойчивый сбор данных о событиях.

Учет современного состояния исследуемой области в проекте *MASSIF* обеспечивается: (1) участием в проекте компании *Alien Vault* как разработчика ведущего *SIEM*-продукта *OSSIM* с открытым исходным кодом; (2) интеграцией результатов проекта *MASSIF* в систему *Prelude* (являющуюся вторым по популярности *SIEM*-продуктом с открытым исходным кодом), которая будет выполнена *Institut Telecom* (Франция); (3) развертыванием и использованием ряда коммерческих *SIEM*-продуктов.

Система *OSSIM* [21, 22] (рис. 6) является комплексным решением по управлению безопасностью, позволяющим обнаруживать и классифицировать компьютерные атаки на основе анализа, оценки рисков и корреляции событий в реальном времени.

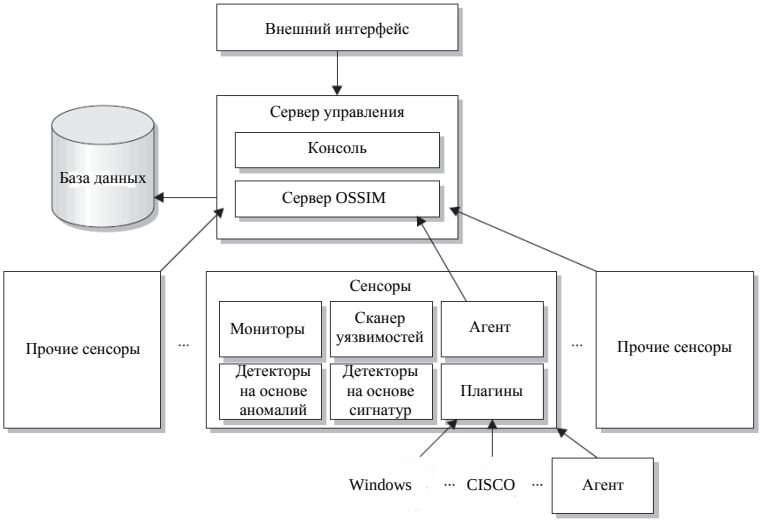

Рис. 6. Архитектура системы *OSSIM.*

Сенсоры являются низкоуровневыми компонентами, которые обеспечивают интерфейс между отдельными устройствами безопасности и сервером управления. Они включают множество агентов сбора данных, а также набор мониторов и детекторов.

База данных является *SQL*-ориентированной. Она хранит всю информацию, требуемую для функционирования *OSSIM*.

Сервер управления включает консоль, которая используется для контроля над остальными компонентами, и сервер *OSSIM*, который обрабатывает данные, поступающие от сенсоров.

Система *Prelude* имеет функциональную структуру, во многом схожую с *OSSIM* [23, 24]. Она состоит из следующих основных компонентов (рис. 7): менеджера, коррелятора, базы данных, интерфейсной подсистемы и подсистемы управления событиями безопасности (*Prelude Log Monitoring Lackey, Prelude-LML*).

Для обработки данных от источников система *Prelude* использует формат *IDMEF* [25]. Менеджер получает события от сенсоров, сохраняет их в постоянной памяти и сопоставляет события с другими менеджерами или корреляторами. Корреляционная логика может расширяться пользователем. Интерфейсная подсистема *Prewikka* обеспечивает сопряжение с базами данных *MySQL, PostgreSQL* и *SQLite3.*

Рис. 7. Функциональная структура системы *Prelude*.

Подсистема *Prelude-LML* позволяет использовать в качестве исходных данных записи журналов от различных устройств.

7. Тестовые области применения проекта *MASSIF* и общие требования к *SIEM*-системе нового поколения. В качестве тестовых областей применения (сценариев) в проекте *MASSIF* заданы следующие варианты инфраструктур:

1) сетевая инфраструктура большой размерности для информационного обеспечения Олимпийских игр;

2) инфраструктура сервисов по управлению «мобильными» деньгами (сервисы перечисления денежных средств на базе мобильного телефона);

3) распределенная сетевая инфраструктура сервисов управления крупными организациями;

4) критическая инфраструктура (на примере дамбы).

Наиболее характерным сценарием для рассмотрения вопросов применимости *SIEM*-систем к защите информации в КВИ является последняя тестовая область. Рассмотрим ее подробнее.

Управление процессами критической инфраструктуры должно обеспечить безопасность, надежность и устойчивость функционирования критического сервиса. В качестве примера КВИ в проекте рассматривается дамба (рис. 8).

Система управления дамбой содержит множество элементов разных типов — элементы системы защиты (например, МСЭ), системы

хранения данных, системы, предоставляющие удаленный доступ к данным (*Web*-сервера), беспроводные сети (сети управления сенсорами) и т.д.

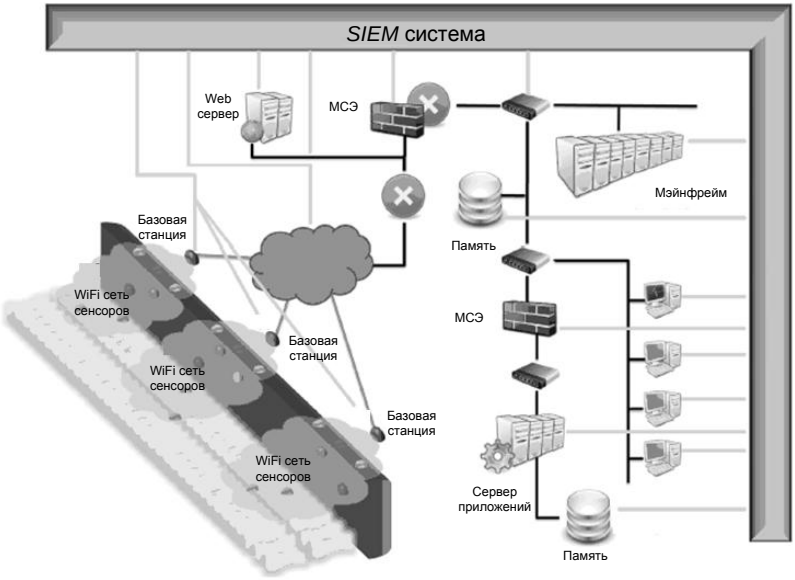

Рис. 8. Пример критической инфраструктуры (для дамбы).

Информация, получаемая из перечисленных элементов, собирается в *SIEM*-системе, что позволяет анализировать все необходимые аспекты безопасности в режиме реального времени.

Безопасность, надежность и устойчивость являются в данном сценарии ключевыми требованиями, так как последствия от их нарушений могут быть катастрофическими. Проблема безопасности определяется в данном сценарии следующими вопросами:

1) как распознать реальные угрозы среди множества предупреждений, появляющихся за день?

2) как гарантировать, что данные, поступившие от разных источников, заслуживают доверия?

3) как управлять данными, поступающими из разнородных устройств и сетей?

4) как коррелировать сильно разнородные данные с целью выявления угроз?

5) как сделать доступными экономические затраты принимаемых решений?

Вклад в решение данной проблемы видится в выполнении эффективных процедур корреляции событий, поступающих из различных слоев, а также в обеспечении требуемой полноты представления данных обо всех потенциальных критических событиях безопасности.

Анализируя требования к *SIEM*-системе, определяемые со стороны различных сценариев проекта *MASSIF*, а также решения, заложенные в системах *Prelude* и *OSSIM*, можно сформулировать цели, предъявляемые к разработке *SIEM*-системы. Эти цели можно считать дополнительными требованиями, которым должна удовлетворять *SIEM*-система нового поколения. Данные требования можно разделить на следующие три группы:

1) расширение уровней применения;
2) расширение возможностей по оценке и корреляции событий;
3) расширение технических возможностей.

Расширение уровней применения *SIEM*-системы означает, что эта область распространяется также и на уровень сервисов (*service layer*). Основной проблемой здесь является межуровневое (*cross-layer*) многодоменное управление информацией и событиями. Частными требованиями в данной группе являются:

- расширение применимости *SIEM*-системы, обеспечивающей реализацию в ней многодоменной точки зрения на высокоуровневые процессы и сервисы;
- реализация механизмов эффективной и действенной межуровневой корреляции событий.

Расширение возможностей системы по оценке и корреляции событий включает в себя:

- поддержку определения отношений между событиями и их автоматизированную корреляцию для принятия детальных решений в критических ситуациях;
- обеспечение эффективных методов (например, методов упреждающего мониторинга безопасности) для оценки событий безопасности и интеграции этих методов с *SIEM*-платформой и существующими средствами и (или) платформами;
- расширение выразительности процесса обработки событий для обеспечения сбора, фильтрации, корреляции и абстрагирования событий, а также предупреждающего оповещения и выработки эффективных контрмер.

Расширение технических возможностей системы обусловлено не только техническими потребностями других целевых категорий, но и такими возможностями, как высокая устойчивость системы. Основными требованиями здесь являются:

- обеспечение методов динамического абстрагирования, позволяющих адаптировать реальный уровень спецификаций к масштабу управляемой системы. Эти методы необходимы для учета масштаба, объема и частоты изменения имеющейся информации о событиях безопасности;
- увеличение минимум на два порядка количества событий безопасности, которые могут быть обработаны в системе за единицу времени, чтобы обеспечить возможность управления при экспоненциальном возрастании количества событий безопасности;
- достижение высокой доступности функционирования системы по обработке событий;
- обеспечение гибкости обработки событий, чтобы минимизировать пользовательские ресурсы, требуемые для загрузки входных событий;
- обеспечение устойчивого функционирования *SIEM*-системы при всех случайных и вредоносных воздействиях.

Дополнительными требованиями, предъявляемыми к процессу разработки *SIEM*-системы для КВИ, является получение ряда инноваций.

В области обеспечения безопасности такими инновациями являются:

- межуровневая корреляция событий безопасности и многоуровневое моделирование событий безопасности;
- интеллектуальный (упреждающий) мониторинг безопасности.

В области обработки событий:

- высоко масштабируемая обработка событий;
- гибкая («эластичная») масштабируемая обработка событий, которая позволит адаптировать вычислительные ресурсы к потребностям *SIEM*-систем.

В области надежности и достоверности:

- защита *SIEM*-системы от случайных отказов и воздействий, вызванных злоумышленными действиями с использованием передовых достижений в обеспечении высокой готовности и отказоустойчивости от потока отказов;

• возможность использования информации о сохраненных событиях в качестве доказательств при судебных разбирательствах против злоумышленников.

В области технологии компиляции основным требованием является использование передовых технологий автоматической генерации парсеров для «бесшовной» интеграции всех типов источников событий безопасности путем спецификации их языков и протоколов.

Подводя итоги рассмотрения содержания и требований выше указанных сценариев проекта *MASSIF*, можно сформулировать следующие общие функциональные требования к *SIEM*-системе нового поколения: высокая надежность; межуровневая корреляция; высокая масштабируемость; гибкость и динамичность механизмов реагирования; удобство пользователя; доверительность; экономичность; синергетичность; реализуемость; выполнение моделирования и оценки рисков; обратная связь и мониторинг.

8. Структура основных задач исследования в проекте *MASSIF*. Основные задачи проекта *MASSIF* как проекта создания *SIEM*-системы нового поколения разделяются на три блока (рис. 9):

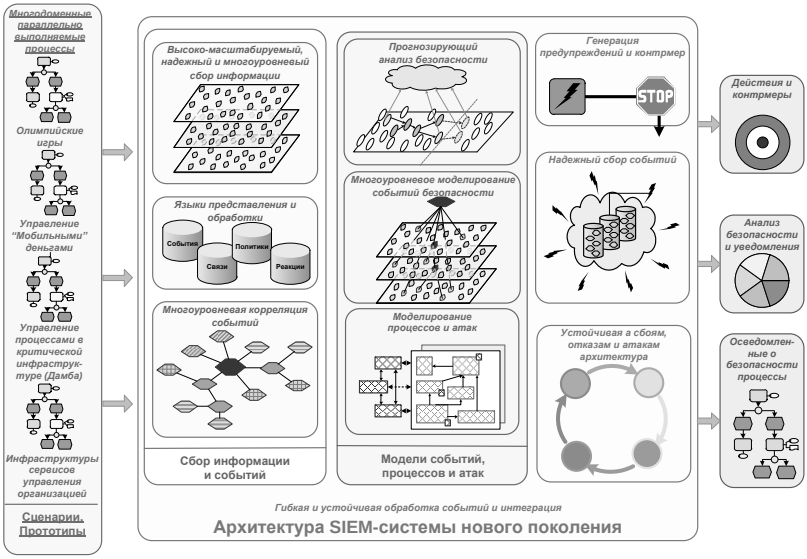

Рис. 9. Основные задачи исследования в проекте *MASSIF*.

1) блок задач сбора информации и событий;
2) блок моделирования событий, процессов и атак;
3) блок задач, обеспечивающих принятие решений.

Блок задач сбора информации и событий включает: высокомасштабируемый, надежный и многоуровневый сбор информации; формирование (выбор) языков внутреннего представления и обработки данных; многоуровневую корреляцию событий.

Блок задач по моделированию событий, процессов и атак включает следующие задачи: прогнозирующий анализ безопасности; многоуровневое моделирование событий безопасности; моделирование процессов и атак.

Блок задач, обеспечивающих принятие решений, состоит из задач выявления инцидентов безопасности, выбора контрмер и визуализации событий безопасности в удобном для оператора формате.

На рис. 10 представлена общая схема потоков данных в *SIEM*-системе, разрабатываемой в проекте *MASSIF*.

Рис. 10. Общая схема потоков в системе, разрабатываемой в проекте *MASSIF*.

На данной схеме представлен полный цикл обработки событий и информации безопасности в разрабатываемой системе. Поток данных начинается с внешних сенсоров, предоставляющих события безопасности в разных форматах. Затем через внешние (защищенные) инфор-

мационные коммутаторы (ИК) данные о событиях поступают на шину данных. Далее через внутренние ИК события безопасности поступают в систему корреляции и обработки, а затем в системы моделирования событий, процессов и атак и принятия решений.

Рассмотрим ниже примеры и текущее состояние исследований двух задач, решаемых в рамках проекта *MASSIF*: анализ событий безопасности на основе использования системы моделирования сетевых атак и построение репозитория *SIEM*-системы.

9. Анализ событий безопасности на основе использования системы моделирования сетевых атак. В проекте предлагается внедрить в существующие *SIEM*-системы дополнительную функциональность — подсистему моделирования атак, которая позволит расширить возможности и повысить точность выявления инцидентов, связанных с информационной безопасностью [26–34].

Поскольку результаты работы подсистемы моделирования атак часто не могут быть получены в реальном времени, их использование в процессах реального времени затруднено. Однако построенные графы атак сохраняют актуальность достаточное время (до значительных изменений в политике безопасности или физической топологии сети). Благодаря этому в рамках системы анализа событий предлагается использовать построенные заранее графы атак. Эти графы атак могут применяться для решения двух основных типов задач — для предсказания последующих действий нарушителя и для анализа и выявления его предыдущих действий, приведших систему к текущему состоянию. Также следует отметить, что для повышения эффективности в рамках моделирования атак используются не отдельные текущие события, а инциденты, распознанные с помощью корреляции отдельных событий. Таким образом, в подсистеме моделирования будут анализироваться не отдельные события вида «Хост *C* получил пакет на 80 порт от хоста *B*», а инциденты вида «производится сканирование хоста *C* хостом *B*», что позволит эффективнее обнаруживать графы атак, включающие в себя такие инциденты.

Предсказание последующих действий нарушителя производится на основе анализа следующих элементов:

1) возможных целей, специфицированных в графах атак;

2) моделей нарушителя, на основе которых были построены наиболее близкие к реальным графы атак [35];

3) классов атак и уязвимостей, использованных нарушителем [36].

Таким образом, на основе анализа инцидентов, с учетом данных полученных от подсистемы моделирования атак, становится возможным делать выводы о том, что существует большая вероятность того, что инциденту «производится сканирование хоста *C* хостом *B*» предшествовал не обнаруженный инцидент «хост *B* был атакован хостом *A*», и что последующим действием нарушителя будет «хост *C* подвергается атаке со стороны хоста *B*».

Кроме того, результатом работы подсистемы моделирования атак могут быть следующие характеристики:

1) слабые места в топологии сети (хосты, через которые проходит наибольшее число графов атак) [37];

2) выбранные контрмеры, позволяющие снизить вероятность максимального количества графов атак [38];

3) возможные последствия реализации контрмер, учитывающие зависимости сервисов [39–41].

В настоящее время продолжаются теоретические исследования применения различных стандартов [42–44], способов построения графов атак, учитывающих существующие уязвимости и уязвимости нулевого дня [45], политики безопасности, зависимости сервисов [46,47], динамического моделирования [48, 49] и т.д., и осуществляется разработка подсистемы моделирования атак как базового компонента общей *SIEM*-системы, разрабатываемой в рамках проекта *MASSIF* .

10. Построение репозитория *SIEM*-системы. Центральным компонентом *SIEM*-системы является репозиторий или информационное хранилище, в котором хранятся данные о событиях, правилах и инцидентах безопасности [50, 51].

Задача построения репозитория является ключевой для *SIEM*-системы. Особую значимость данная задача приобретает в критической информационной инфраструктуре, где учитываются не только традиционные события безопасности компьютерной инфраструктуры, но также параметры безопасности физического уровня.

Для разработки архитектуры репозитория *SIEM*-системы был проведен анализ стандартов в области управления событиями (*Common Event Expression* [52], *Common Base Event* [53], *XDAS* [54], *CIM* [55] и других), наиболее известных реализованных *SIEM*-систем (*OSSIM, AccelOps, Qradar, Splunk, Prelude, Arc Sight* и др.), а также требований в части состава и структуры хранимых данных и механизмов их обработки, выдвигаемых со стороны отдельных сценариев применения *SIEM*-системы. В результате был сделан вывод, что наиболее прием-

лемым стандартом является стандарт *CIM*. Данный стандарт может быть положен в основу создания модели данных верхнего уровня.

Для обоснования выбора языка внутреннего представления данных, содержащихся в репозитории, был проведен обзор ряда *XML*-ориентированных языков, которые можно использовать для доступа, обработки и логического вывода данных в репозитории. К числу таких языков были отнесены: *Web Ontology Language* (*OWL*) [56], *Semantic Web Rule Language*(*SWRL*) [57], *SPARQL Protocol and RDF Query Language* (*SPARQL*) [58], *Event calculus* [59], *SPIN* [60, 61] и др. Данный анализ привел к выводу, что эти языки могут быть использованы при применении онтологического подхода.

Для построения архитектуры репозитория предлагается метод, базирующийся на использовании сервис-ориентированной архитектуры (*SOA*). Основными принципами *SOA*, применяемыми для построения репозитория, являются множественное использование сервисов, однородная безопасность, интеграция с процессом программирования, использование открытых стандартов, независимость от местоположения компонентов, высокая управляемость.

Согласно принципам *SOA*, архитектура репозитория может быть разделена на три базовых уровня: уровень доступа к данным, уровень презентации данных и уровень реализации сервисов. Уровень доступа к данным интерпретирует запросы на поиск данных от клиентских приложений во внутренний язык, используемый СУБД. Уровень презентации данных охватывает все, что связано с взаимодействием с системой. Уровень реализации сервисов позволяет абстрагировать взаимодействие между двумя и более объектами, потоками и сервисами через промежуточный интерфейс *API*.

В предлагаемой архитектуре репозитория выделяются два типа баз данных: кратковременного хранения и длительного хранения. В базе данных кратковременного хранения содержится детальная информация обо всех событиях безопасности, поступивших в репозиторий. В базе данных долговременного хранения содержатся обобщенные данные, а также формализованное представление на внутреннем языке правил политик и инцидентов безопасности, которые используются для получения логического вывода.

Вместе взятые, эти базы образуют слой хранения данных репозитория. Другой функциональный слой представляет собой набор различных услуг, которые выполняются по отношению к хранимым данным.

Для выбора программно–инструментальных средств построения репозитория был проведен анализ СУБД следующих классов: традиционного класса реляционных СУБД, *XML*-ориентированных СУБД (*Base X* [62], *Apache X Indice* [63] и др.) и хранилищ триплетов (*4store* [64], *Big Data* [65], *Big Owlim* [66], *TDB* [67] и *Virtuoso* [68]). В результате был сделан выбор в пользу сервера программной системы *Virtuoso*, которая рационально сочетает в себе возможности всех трех классов СУБД.

Программный макет репозитория, выполненный с использованием *Virtuoso*, был протестирован для хранения и обработки данных, используемых в модуле анализа и моделирования атак на критически важную информационную инфраструктуру. Результаты тестирования подтвердили правомерность принятых решений по выбору и использованию методов и средств построения репозитория *SIEM*-системы.

11. Заключение. Обеспечение безопасности КВИ предполагает применение новых подходов к построению средств и систем защиты информации, которые способны осуществлять проактивный мониторинг событий безопасности, данные о которых могут собираться от различных сенсоров и источников и на основании межуровневой корреляции данной информации в режиме времени, близком к реальному, вырабатывать предупреждения и решения по обеспечению информационной безопасности.

В качестве системообразующей технологии, реализующей указанные функциональные возможности, представляется целесообразным применение технологии *SIEM*. Однако систему защиты КВИ, созданную на ее основе, следует относить к *SIEM*-системам нового поколения, разработке которых посвящен проект *MASSIF*. Сценарии применения *SIEM*-системы, определенные в *MASSIF*, в полной мере задают функциональные и реализационные требования к данной системе.

Разработка методов и моделей в области представления, сбора, хранения и обработки информации о событиях безопасности, позволяющих реализовать требования, предъявляемые к *SIEM*-системе нового поколения, является актуальной научной задачей, имеющей большое государственное и народнохозяйственное значение и определяющей новые направления научных исследований в области информационной безопасности.

Литература

1. *Леваков А.* Информационная безопасность в США: проблемы и решения. http://freelance4.narod.ru/IS_USA.htm

2. *Котенко И.В., Юсупов Р.М.* Перспективные направления исследований в области компьютерной безопасности // Защита информации. Инсайд, № 2, 2006. С.46–57.
3. *Котенко И.В., Воронцов В.В., Чечулин А.А., Уланов А.В.* Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов // Информационные технологии, № 1, 2009. С.37–42.
4. *Котенко И.В.*Интеллектуальные механизмы управления кибербезопасностью// Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Т.41, Москва, URSS, 2009. С.74–103.
5. *Miller D.R., Harris Sh., Harper A.A., VanDyke S., Black Ch.* Security Information and Event Management (SIEM) Implementation. McGraw–Hill Companies. 2011. 430 p.
6. *Stevens M.* Security Information and Event Management (SIEM). Presentation // TheNEbraska CERT Conference, August 9–11, 2005. http://www.certconf.org/presentations/2005/files/WC4.pdf
7. *Nicolett M., Kavanagh K.M.* Magic Quadrant for Security Information and Event Management. Gartner, 12 May 2011. 20 p.
8. ArcSight ESM. http://www.arcsight.com/products/products–esm/
9. ArcSight Express. http://www.arcsight.com/products/products–esm/arcsight–express.
10. ArcSight Logger. http://www.arcsight.com/products/products–logger/
11. Shenk J.ArcSight Logger Review. A SANS Whitepaper. January 2009. http://www.arcsight.com/collateral/whitepapers/ArcSight_Combat_Cyber_Crime_ with_Logger.pdf.
12. Common Event Format. http://www.arcsight.com/solutions/solutions–cef.
13. RSA enVision. http://www.rsa.com/node.aspx?id=3170
14. QRadar SIEM. http://q1labs.com/Products/QRadar–SIEM.aspx
15. Tivoli Security Information and Event Manager. http://www–142.ibm.com/software/products/ru/ru/securityinformationandeventmanager/
16. *Buecker A., Amado J., Druker D., Lorenz C., Muehlenbrock F.,Tan R.* IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager. IBM Redbooks. 2010. 464 p.
17. Symantec Security Information Manager. http://www.symantec.com/ business/security–information–manager
18. Loglogic. http://loglogic.com
19. Novell Sentinel Log Manager 1.0.0.5. Installation Guide. March 31, 2010.
20. Проект MASSIF «Управление информацией и событиями безопасности в инфраструктурах услуг». Проект Седьмой рамочной программы Европейского Союза. http://www.massif–project.eu/
21. OSSIM. http://www.alienvault.com/community
22. AlienVaultUser's Manual, 2011. 225 p.
23. Prelude. http://www.prelude–technologies.com/
24. Prelude as a Hybrid IDS Framework. SANS Institute InfoSec Reading Room, 2009. 43 p.
25. The Intrusion Detection Message Exchange Format (IDMEF). RFC 4765. 2007.
26. *Котенко И.В., Степашкин М.В., Богданов В.С.* Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006, №. 2, С.7–24.
27. *Котенко И.В., Степашкин М.В., Богданов В.С.* Анализ защищенности компьютерных сетей на различных этапах их жизненного цикла // Изв. вузов. Приборостроение. Т.49, № 5, 2006, С.3–8.

28. *Котенко И.В., Степашкин М.В.* Метрики безопасности для оценки уровня защищенности компьютерных сетей на основе построения графов атак // Защита информации. Инсайд, № 3, 2006. С.36–45.
29. *Kotenko I., Stepashkin M.* Analyzing network security using malefactor action graphs // International Journal of Computer Science and Network Security, Vol.6 No.6, June 2006. P.226–235.
30. *Kotenko I., Stepashkin M.* Attack Graph based Evaluation of Network Security // Lecture Notes in Computer Science, Vol. 4237, 2006. P.216–227.
31. *Котенко И.В., Степашкин М.В.* Оценка защищенности компьютерных сетей на основе анализа графов атак // Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Т.31, Москва, URSS, 2007. С.126–207.
32. *Kotenko I., Stepashkin M., Doynikova E.* Security Analysis of Computer–aided Systems taking into account Social Engineering Attacks // Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network–based Processing (PDP 2011). IEEE Computer Society. 2011. P.611–618.
33. *Котенко И.В, Степашкин М.В., Дойникова Е.В.* Анализ защищенности автоматизированных систем с учетом социо–инженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011, № 3, С.40–57.
34. *Котенко И.В, Степашкин М.В., Котенко Д.И., Дойникова Е.В.* Оценка защищенности информационных систем на основе построения деревьев социо–инженерных атак // Изв. вузов. Приборостроение, Т.54, № 12, 2011. Р.5–9. ISSN 0021–3454.
35. *Leversage D., Byres E.* Estimating a system's mean time-to-compromise // IEEE Security and Privacy, Vol.6, No.1, 2008. P.52–60.
36. *Balzarotti D., Monga M., Sicari S.* Assessing the risk of using vulnerable components // Quality of protection: security measurements and metrics, Advances in Information Security 23. Springer, New York, 2006. P. 65–77.
37. *Mehta V., Bartzis C., et al.*Ranking Attack Graphs // Lecture Notes in Computer Science, Springer–Verlag, Vol.4219, 2006. P.127–144.
38. *Ingols K., Chu M., Lippmann R., Webster S., Boyer S.* Modeling modern network attacks and countermeasures using attack graphs // Proceedings of the 2009 Annual Computer Security Applications Conference (ACSAC '09), Washington, D.C., USA, IEEE Computer Society, 2009. P.117–126.
39. *Noel S., Jajodia S., O'Berry B., Jacobs M.* Efficient minimum–cost network hardening via exploit dependency graphs // Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC'03), 2003. P.86–95.
40. *Wang L., Noel S., Jajodia S.* Minimum–cost network hardening using attack graphs // Computer Communications, 29(18), 2006. P.3812–3824.
41. *Kheir N., Debar H., Cuppens–Boulahia N., Cuppens F., Viinikka J.* Cost evaluation for intrusion response using dependency graphs // IFIP International Conference on Network and Service Security (N2S), 2009. P.1–6.
42. *Котенко И.В., Дойникова Е.В.* Методы оценивания уязвимостей: использование для анализа защищенности компьютерных систем // Защита информации. Инсайд, 2011, № 4, С.74–81.
43. *Котенко И.В., Дойникова Е.В.* Система оценки уязвимостей CVSS и ее использование для анализа защищенности компьютерных систем // Защита информации. Инсайд, 2011, № 5, С.54–60.
44. *Котенко И.В., Дойникова Е.В.*Анализ систем оценки злоупотреблений и конфигураций (CMSS и CCSS) для унифицированного анализа защищенности компьютерных систем // Защита информации. Инсайд, 2011, № 6. С.52–60.

45. *Дойникова Е.В., Чечулин А.А., Котенко И.В., Котенко Д.И.* Расширение методики оценки информационных рисков для учета атак нулевого дня // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР–2011). 26–28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.71–72.
46. *Чечулин А.А., Котенко И.В.* Анализ происходящих в реальной сети событий на основе использования системы моделирования сетевых атак // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР–2011). 26–28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.97–98.
47. *Дойникова Е.В., Котенко И.В*. Расширение методики оценки информационных рисков за счет использования графов зависимостей сервисов // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно–технической конференции. 27 июня — 1 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета. 2011. С.131–132.
48. *Котенко И.В., Коновалов А.М., Шоров А.В.* Моделирование бот–сетей и механизмов защиты от них // Системы высокой доступности, № 2, 2011. С.107–111.
49. *Котенко И.В., Коновалов А.М., Шоров А.В.* Агентно-ориентированное моделирование бот-сетей и механизмов защиты от них // Вопросы защиты информации, № 3, 2011. С.24–29.
50. *Саенко И. Б., Полубелова О.В., Котенко И.В.* Разработка информационного хранилища системы управления информацией и событиями безопасности для гетерогенной инфраструктуры // Методы и технические средства обеспечения безопасности информации. Материалы XX Общероссийской научно-технической конференции. 27 июня — 1 июля 2011 года. Санкт-Петербург. Издательство Политехнического университета. 2011. С.41–42.
51. *Котенко И.В., Саенко И. Б., Полубелова О.В., Чечулин А.А.* Методы и средства построения репозитория системы управления информацией и событиями безопасности в критической информационной инфраструктуре // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР–2011). 26–28 октября 2011 г. Материалы конференции. СПб.: СПОИСУ, 2011. С.79–80.
52. Common Event Expression. White Paper. The MITRE Corporation. June 2008. 30 p.
53. *Ogle D., Kreger H., Salahshour A., Cornpropst J., Labadie E., Chessell M., Horn B., Gerken J., Schoech J., Wamboldt M.* Canonical Situation Data Format: The Common Base Event V1.0.1. International Business Machines Corporation, 2004. 73 p.
54. Open Group, the Distributed Audit Services. http://www.opengroup.org/projects/security/xdas
55. Common Information Model (CIM) Standards, DMTF. http://dmtf.org/standards/cim
56. OWL 2 Web Ontology Language Document Overview. W3C Recommendation 27 October 2009. http://www.w3.org/TR/owl2-overview/
57. SWRL: A Semantic Web Rule Language Combining OWL and RuleML. W3C Member Submission 21 May 2004. http://www.w3.org/Submission/SWRL/
58. SPARQL Query Language for RDF. W3C Recommendation, 15 January 2008. http://www.w3.org/TR/rdf–sparql–query
59. *Kowalski R.A., Sergot M.J.* A logic-based calculus of events. New Generation Computing, V.4, 1986. P.67–95.
60. ON–THE–FLY, LTL MODEL CHECKING with SPIN. http://spinroot.com/spin/whatispin.html

61. *Holzmann G.J.* The Spin Model Checker // IEEE Transactions on Software Engineering, Vol. 23, No. 5, 1997. P.573–576.
62. BaseX. http://basex.org
63. XIndice. http://xml.apache.org/xindice
64. 4store. http://4store.org/
65. Berlin SPARQL Benchmark. http://www4.wiwiss.fuberlin.de/ bizer/BerlinSPARQLBenchmark/ results/V6/index.html
66. BigOWLIM. http://www.ontotext.com/owlim/big/
67. TDB. http://incubator.apache.org/jena/documentation/tdb/index.html
68. Virtuoso. http://virtuoso.openlinksw.com

Котенко Игорь Витальевич — д.т.н., проф., заведующий лабораторией проблем компьютерной безопасности Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Kotenko Igor Vitalievich — Ph.D., Professor, Head of Laboratory of Computer Security Problems, Institution of RAS St. Petersburg Institute for Informatics and Automation of RAS (SPIIRAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital rights' management, modeling, simulation and visualization of technologies for counteraction to cyber terrorism. The number of publications — more 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Саенко Игорь Борисович — д–р техн.наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: автоматизированные информационные системы, информационная безопасность, обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. Число научных публикаций — 240. ibsaen@comsec.spb.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of Laboratory of Computer Security Problems, Institution of RAS St. Petersburg Institute for Informatics and Automation of RAS (SPIIRAS). Research interests: automated information systems, information security, processing and transfer of data by data links, theory of modeling and mathematical statistics, information theory. The number of publications — 240. ibsaen@comsec.spb.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Полубелова Ольга Витальевна — младший научный сотрудник лаборатории проблем компьютерной безопасности Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, информационная безопасность в системах документооборота. Число научных публикаций — 26. ovp@comsec.spb.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Polubelova Olga Vitalievna —junior research scientist of Laboratory of Computer Security Problems, Institution of RAS St. Petersburg Institute for Informatics and Automation of RAS (SPIIRAS). Research interests: security of computer networks, information security in work-flow systems. The number of publications — 26. ovp@comsec.spb.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Чечулин Андрей Алексеевич — младший научный сотрудник лаборатории проблем компьютерной безопасности Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, обнаружение вторжений, анализ сетевого трафика, анализ уязвимостей. Число научных публикаций — 43. chechulin@comsec.spb.ru;СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Chechulin AndreyAlexeevich — junior research scientist of Laboratory of Computer Security Problems, Institution of RAS St. Petersburg Institute for Informatics and Automation of RAS (SPIIRAS). Research interests: computer network security, intrusion detection, analysis of the network traffic, analysis of vulnerability. The number of publications — 43. chechulin@comsec.spb.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Поддержка исследований. В публикации представлены результаты исследований, поддержанные Министерством образования и науки Российской Федерации (государственный контракт 11.519.11.4008), грантами РФФИ (проекты 10–01–00826–а, 11–07–00435–а), программой фундаментальных исследований ОНИТ РАН и проектами Седьмой рамочной программы Европейского Союза *SecFutur* и *MASSIF*.

Рекомендовано лабораторией криптологии, заведующий лабораторией Молдовян Н.А., д–р техн.наук, проф., заслуженный изобретатель РФ.
Статья поступила в редакцию 22.03.2012.

РЕФЕРАТ

Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. **Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах.**

Применение *SIEM*-технологии (технологии управления информацией и событиями безопасности) является перспективным направлением в области защиты информации, особенно для критически важных инфраструктур (КВИ). Для успешной реализации мероприятий защиты КВИ необходимо решение ряда задач, одна из которых связана с созданием системы мониторинга угроз безопасности, целью создания которой является минимизация уровня риска воздействия на объекты КВИ и, соответственно, возникающего ущерба.

Приводятся общие положения по построению и функционированию систем, реализующих *SIEM*-технологию. Рассматриваются уровни архитектуры типовой *SIEM*-системы и распределение по этим уровням ее основных механизмов функционирования. Дается характеристика основных функциональных подсистем, к числу которых относятся подсистемы сбора данных, обработки, хранения, анализа и представления.

Приводится обзор наиболее известных существующих *SIEM*-систем с указанием их достоинств и недостатков на основании исследований, проведенных компанией *Gartner*. Показано, что даже самая успешная реализация *SIEM*-системы, разработанная компанией *Arc Sight*, не в полной мере отвечает современным потребностям защиты информации в КВИ.

Обсуждаются особенности проекта Европейского Союза *MASSIF* по созданию перспективных систем управления событиями и информационной безопасностью, целью которого является устранение недостатков, присущих существующим *SIEM*-системам. Рассматриваются основные задачи проекта и тестовые области применения его результатов. Более подробно дается характеристика тестовой области критической инфраструктуры на примере дамбы. Для нее обосновывается проблема обеспечения безопасности информации, и формулируются основные требования к *SIEM*-системе нового поколения, предназначенной для применения в КВИ. К числу основных требований отнесены возможность межуровневой корреляции событий безопасности, высокая масштабируемость, высокая надежность и отказоустойчивость.

Рассматриваются аспекты решения двух ключевых задач проекта *MASSIF*, связанных с анализом событий безопасности на основе моделирования сетевых атак и построения репозитория. В рамках первой задачи предлагается внедрить в существующие *SIEM*-системы подсистему моделирования атак, которая позволит расширить возможности и повысить точность выявления инцидентов.

В рамках второй задачи предложена архитектура репозитория, выбрано средство его построения и выполнена экспериментальная оценка полученных результатов.

SUMMARY

Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A. **Application of security information and event management technology for information security in critical infrastructures.**

Application of SIEM technology (technology of security information and event management) is a promising one in the field of information protection, especially for critical infrastructures. For the successful implementation of protection measures in critical infrastructure it is necessary to solve a number of tasks, one of which involves creation of a security threat monitoring system, which goal is to minimize the level of risk exposure of objects and their damage.

The paper considers the general issues of construction and operation of systems that implement SIEM technology. It discusses the levels of a standard SIEM system architecture, and distribution of main operation mechanisms on these levels. It describes the major functional subsystems, i.e. systems of data collection, processing, storage, analysis and reporting.

The most well-known existing SIEM systems are reviewed. Their advantages and disadvantages pointed by Gartner are outlined. We show that even the most successful SIEM system developed by Arc Sight does not fully meet the needs of information security in critical infrastructures.

We also discuss the peculiarities of the European Commission project named MASSIF devoted to creation of advanced SIEM systems. The purpose of this project is to address the shortcomings of existing SIEM systems. The key objectives of the project and the main case studies are considered. A more detailed description of the dam case study is given. The information security problem is justified, and the basic requirements for the next-generation SIEM system, intended for use in critical infrastructures, are formulated. Key requirements include the possibility of interlayer correlation of security events, high scalability, high reliability and fault tolerance.

We discuss two key tasks of the MASSIF project associated with the analysis of security events, based on the modeling of network attacks, and with constructing the repository. The first task is to introduce into existing SIEM systems an attack modeling subsystem which can expand the incident detection opportunities and enhance their accuracy.

The second task is the development the repository architecture, and the tool for it’s constructing and performing is proposed.