УДК 004.056.5

И.В. Котенко, И.Б. Саенко, Р.М. Юсупов

НОВОЕ ПОКОЛЕНИЕ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ ИНЦИДЕНТАМИ БЕЗОПАСНОСТИ

I.V. Kotenko, I.B. Saenko, R.M. Yusupov

NEW GENERATION OF SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEMS

Обоснована технологическая необходимость разработки нового поколения систем мониторинга и управления инцидентами безопасности, основанных на технологии управления информацией и событиями безопасности. Приведены типовая архитектура и основные решения по построению отдельных модулей таких систем, осуществляющих устойчивый сбор данных о событиях безопасности, их универсальную трансляцию, масштабируемую обработку, гибридное онтологическое хранение и многофункциональную визуализацию, а также межуровневую корреляцию событий, моделирование атак и прогностический анализ безопасности. Сформулированы предложения по применению таких систем в предметных областях, касающихся обеспечения безопасности в критических инфраструктурах.

МОНИТОРИНГ И УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ; КОМПЬЮТЕРНАЯ СЕТЬ; СОБЫТИЕ БЕЗОПАСНОСТИ; ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА.

The given paper justifies the technological necessity to develop a new generation of security monitoring and event management systems based on security information and event management technology. We have focused on the typical architecture and key solutions to design the individual modules of such systems collecting constant security data, their universal translation, scalable processing, hybrid ontological storage and rich visualization, as well as a cross-level correlation of events, attack modelling and predictive security analysis. We have also stated some proposals to use such systems in the domains related to security protection in critical infrastructures.

SECURITY MONITORING AND MANAGEMENT; COMPUTER NETWORK; SECURITY EVENT; INFORMATION INFRASTRUCTURE.

Технология управления событиями и информацией безопасности (Security Information and Events Management – SIEM) является новым, бурно развивающимся направлением в области информационной безопасности, обладающим достаточно большим потенциалом по обнаружению угроз и выработке контрмер по обеспечению требуемого уровня безопасности информационной инфраструктуры.

Функционирование SIEM-систем, или, как принято говорить в русскоязычной литературе, *систем мониторинга и управления инцидентами безопасности*, заключается в оперативном сборе, хранении и аналитической обработке данных о событиях безопасности, которые первоначально формируются и фиксируются в системных журналах различных аппаратных и программных элементов, образующих информационные ин-

фраструктуры: серверы, рабочие станции, маршрутизаторы, межсетевые экраны, системы управления базами данных, системы обнаружения атак, антивирусные средства и т. д. [1, 2]

SIEM-системы в настоящее время имеют большое количество коммерческих реализаций, выполненных ведущими разработчиками и интеграторами средств и систем защиты информации: компаниями IBM (система QRadar) [3], HP (ArcSight) [4], Symantec (Symantec Security Information Manager) [5], Novell (Novell Sentinel) [6] и др. Однако область применения данных систем, которые можно назвать *SIEM-системами первого поколения*, не выходит за рамки информационных процессов, протекающих в компьютерной сети.

В то же время при мониторинге безопасности становится все более актуальной задача выявления атак и прочих злонамеренных воздействий не только на основе анализа событий безопасности, зафиксированных в журналах сетевых инфраструктурных элементов, но и на уровне бизнес-процессов, а также на уровне физических датчиков. Кроме того, известные коммерческие SIEM-системы испытывают значительные затруднения при обеспечении безопасности компьютерных сетей большой размерности.

Эти и ряд других недостатков существующих коммерческих SIEM-решений обусловили необходимость исполнения международного проекта MASSIF [7], предназначенного для построения SIEM-систем, свободных от этих недостатков и определяемых как системы *нового поколения*.

Цель настоящей работы – обобщение основных результатов, полученных в рамках проекта MASSIF, связанных с построением нового поколения систем мониторинга и управления инцидентами безопасности.

Требования к SIEM-системам нового поколения

Появление нового поколения SIEM-систем связывается с рядом вполне конкретных предпосылок, которые определяются, с одной стороны, последними достижениями в области информационно-коммуникационных технологий (ИКТ), а с другой – новыми требованиями, предъявляемыми к современным информационным технологиям. Рассмотрим их подробнее.

Современные тенденции развития ИКТ тесно связываются с поддержкой распределенных информационных инфраструктур, ориентированных на широкое использование Интернета. К числу таких тенденций можно отнести, например, использование усовершенствованных протоколов передачи защищенных данных, сервис-ориентированных архитектур (Service-Oriented Architecture – SOA) [8], архитектур распределенных приложений, основанных на «передаче репрезентативного состояния» (Representational State Transfer), новых технологий взаимодействия с различными типами устройств.

Кроме того, специфическими технологиями, в настоящее время притягивающими к себе внимание разработчиков ИКТ, являются:

- применение методов виртуализации (Virtualization) для оптимизации информационной инфраструктуры;
- «облачные вычисления» (Cloud Computing) как основа для различных моделей обмена данными;
- контекстно-зависимые приложения (Context-aware Applications);
- семантические и контекстуальные глобальные сети (Semantic and Contextual Web);
- «зеленые» информационные технологии (Green IT);
- обработка сложных событий (Complex Event Processing);
- «социальные вычисления» (Social Computing), в т. ч. концепции Web 2.0 и Enterprise 2.0;
- усовершенствованные графические интерфейсы для человеко-машинного взаимодействия и др.

На вершине современной пирамиды ИКТ находятся парадигмы «Интернета будущего» (Future Internet) и «Интернета вещей» (Internet of Things), которые становятся реальностью по мере разработки упомянутых выше технологий.

Реализация этих парадигм приведет к значительному возрастанию информационных потоков, а также типов и количества сенсоров и устройств, распространяющих данные о событиях безопасности через Интернет. Интернет станет более интеллектуальным, т. к. он будет обрабатывать намного большее количество разнородной информации, необходимой для построения обоснованных решений, поддержки моделирования, прогнозирования, выработки рекомендаций, что в конечном итоге значительно повысит эффективность процесса принятия решений в целом.

Системы мониторинга и управления инцидентами безопасности в ближайшем будущем будут увеличивать свою значимость, поскольку они наиболее близки к этим событийно-ориентированным парадигмам и направлены на решение новых проблем безопасности. Однако в этом случае мониторинг и управление инцидентами безопасности становятся более сложными, т. к. они должны затрагивать распределенные бизнес-процессы в условиях недоступности и/или возможного несанкционированного изменения передаваемых и обрабатываемых данных.

Хотя традиционные SIEM-системы (т. е. системы первого поколения) уже нашли применение в корпоративных инфраструктурах, сценарии их будущего развертывания должны учитывать возможность того, что связи между управляемыми устройствами и поставщиками услуг будут проходить по общедоступным путям в Интернете. Кроме того, SIEM-системы нового поколения могут быть развернуты как «облачные» службы. В этом случае актуальным становится обеспечение доверия и конфиденциальности.

Таким образом, SIEM-системы нового поколения должны быть ориентированы на решение следующих проблем [1, 2, 7, 9]:

- разработку надежных и устойчивых средств обеспечения осведомленности пользователей о безопасности инфраструктуры;
- совершенствование механизмов распределенного управления безопасностью для адаптивного конфигурирования политик безопасности;
- улучшенную масштабируемость, обеспечивающую требуемое увеличение производительности при увеличении количества обрабатываемых данных;
- использование инновационных моделей прогнозирования безопасности, обеспечивающих проактивную обработку инцидентов и событий безопасности;
- децентрализацию сбора и обработки событий безопасности между центральными механизмами и удаленными коллекторами.

Тогда в качестве основных требований, предъявляемых к SIEM-системам нового поколения, следует указать возможность реализации следующего перечня новых функциональных возможностей:

- межуровневой корреляции событий безопасности, поступающих из неоднородных источников;
- адаптивной и высокомасштабируемой обработки событий, обеспечивающей управление большими объемами данных о безопасности в реальном или близком к реальному времени;
- прогностического анализа безопасности, позволяющего осуществлять проактивное обнаружение и предотвращение атак путем принятия соответствующих контрмер;
- высокой доступности и отказоустойчивости сбора данных о событиях безопасности в условиях территориально-распределенного построения информационной инфраструктуры и активного вредоносного и/или непреднамеренного воздействия на элементы инфраструктуры.

Обобщенная архитектура SIEM-системы нового поколения

Обобщенная архитектура SIEM-системы нового поколения представлена на рис. 1. В ней можно выделить четыре уровня: сети, данных, событий и приложений. Уровень сети является внешним и охватывает сетевые элементы, являющиеся источниками данных о событиях безопасности. На уровне данных происходит предварительная обработка поступивших данных, выделение из них событий безопасности и преобразование их в единый внутренний формат.

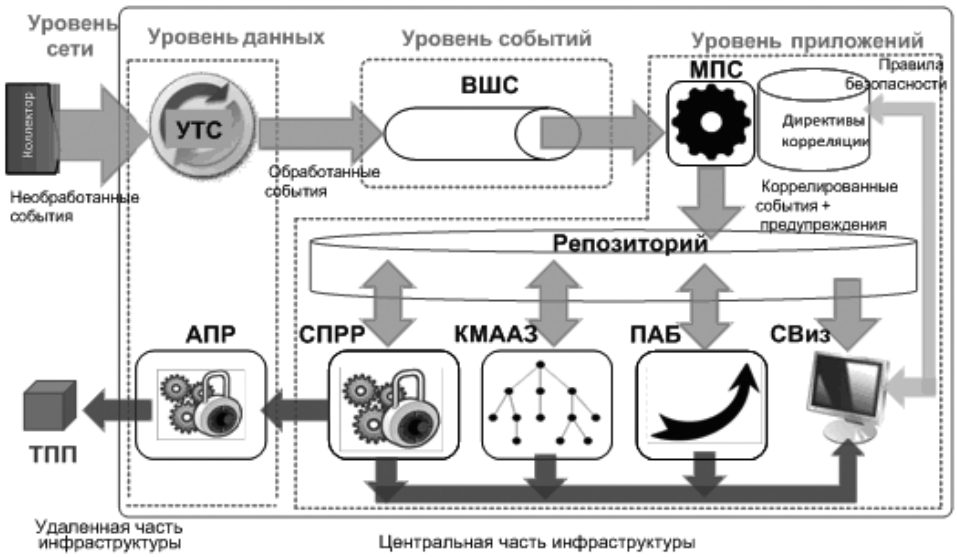

Рис. 1. Архитектура SIEM-системы нового поколения

На уровне событий осуществляется обмен событиями между всеми компонентами системы. На уровне приложений производится хранение и аналитическая обработка событий.

Основными компонентами SIEM-системы нового поколения являются:

коллектор, под которым понимаются источники данных о событиях безопасности, такие как сетевые устройства, серверы, рабочие станции, базы данных, межсетевые экраны, антивирусы, сенсоры и т. д. (уровень сети);

универсальный транслятор событий (УТС), предназначенный для первичной обработки данных о событиях безопасности, поступающих в SIEM-систему (уровень данных);

высоконадежная шина событий (ВШС), предназначенная для распространения данных о событиях безопасности и их гарантированной доставки требуемым компонентам SIEM-системы (уровень событий);

масштабируемый процессор событий (МПС), обеспечивающий адаптивную поддержку всех задач по обработке событий и их решение в реальном времени (уровень приложений);

репозиторий (хранилище) данных о безопасности (уровень приложений);

система принятия решений и реагирования (СПРР), предназначенная для верификации и управления политиками безопасности, обеспечивающими защиту инфраструктурных элементов (уровень приложений);

компонент моделирования атак и анализа защищенности (КМААЗ), обеспечивающий дополнительные аналитические возможности SIEM-системы за счет реализации функций моделирования атак и анализа защищенности (уровень приложений);

прогностический анализатор безопасности (ПАБ), обеспечивающий расширенные возможности мониторинга безопасности, заключающиеся в моделировании состояния элементов информационной инфраструктуры в ближайшей перспективе и предсказании возможных нарушений безопасности (уровень приложений);

система визуализации (СВиз), предназначенная для представления информации о безопасности в графическом виде, обеспечивающем ее наибольшую степень восприятия и визуального анализа (уровень приложений);

агент принятия решений (АПР), обеспечивающий доведение решений по безопасности до инфраструктурных элементов (уровень данных);

точки применения политик безопасности (ТПП), под которыми понимаются логические сущности или оборудование, реа-

лизующие по запросам пользователей команды управления доступом и решения по безопасности.

Характеристика компонентов

Приведем характеристику перечисленных компонентов, подробнее останавливаясь на решениях, полученных учеными Санкт-Петербургского института информатики и автоматизации РАН (СПИИ РАН).

Компонент УТС является программной системой, осуществляющей сбор событий и информации безопасности. Он обеспечивает управление неоднородными данными и их конфиденциальность за счет реализации процедур межуровневого сбора данных, расширенной обработки форматов, многоуровневой корреляции, агрегации, шифрования полей событий и анонимизации. Кроме того, он генерирует форматы выходных событий, пригодные для некоторых известных коммерческих SIEM-систем, например, систем OSSIM [10] и Prelude [11], основанных на открытом исходном коде.

Компонент ВШС, по сути, является телекоммуникационной подсистемой, пригодной для распределенных приложений, в которых обмен данными должен обладать высокой устойчивостью. Этот компонент в реальном масштабе времени осуществляет поиск оптимальных путей, учитывая, с одной стороны, избыточную доступность физической сети, а с другой – воздействие компьютерных атак и других негативных факторов. Для восстановления пропущенных пакетов применяются процедуры повышения достоверности, позволяющие минимизировать повторную передачу пакетов и тем самым максимально снизить временные задержки.

Компонент МПС обеспечивает адаптивную вычислительную поддержку в реальном масштабе времени всех задач обработки событий. Он способен обрабатывать несколько сотен тысяч событий в секунду, не требуя каких-либо корректировок правил или управления событиями. Благодаря постоянному хранению выбранных событий в памяти, становится возможным проведение анализа событий. Обработка событий может выполняться в распределенной среде, в которой высокая масштабируемость МПС обеспечивает достаточно высокую эффективность фильтрации, преобразования, агрегации, абстрагирования и корреляции событий. Вычислительная адаптивность МПС означает, что он может управлять входной нагрузкой. В случае резкого возрастания нагрузки компонент автоматически инициирует выполнение задач на новых узлах, что позволяет убрать пиковые нагрузки и равномерно распределить задания. Аналогично, в случае недоиспользования ресурсов происходит завершение функционирования всех ненужных узлов.

Компонент ПАБ использует в качестве входных данных различные модели обработки событий, политики безопасности, требования безопасности и события, поступающие в систему в реальном масштабе времени. Целью его функционирования является оказание помощи в принятии важнейших решений, касающихся выработки контрмер по противодействию атакам и угрозам безопасности, которые воздействуют на компьютерную сеть в текущий момент времени.

Компонент СПРР ориентирован на модель доступа организационного типа OrBAC [12]. Он осуществляет конфигурирование политик безопасности внешних систем, вызываемых соответствующими средствами. При этом не требуется знания правил конфигурирования других средств, достаточно правил конфигурирования самого компонента.

Репозиторий данных является средством кроссплатформенной интеграции различных компонентов SIEM-системы [13–15]. В качестве основы для его реализации положена архитектура SOA (рис. 2). Как видно из рисунка, архитектура репозитория разделяется на два уровня: уровень хранения и уровень веб-сервисов.

Уровень хранения включает в себя реляционную базу данных (РБД), базу XML-данных и базу данных в формате RDF, называемых «триплетами», т. к. они отражают отношения «субъект – предикат – объект». Тем самым обеспечивается гибридный подход к хранению данных о событиях безопасности, сочетающий достоинства всех

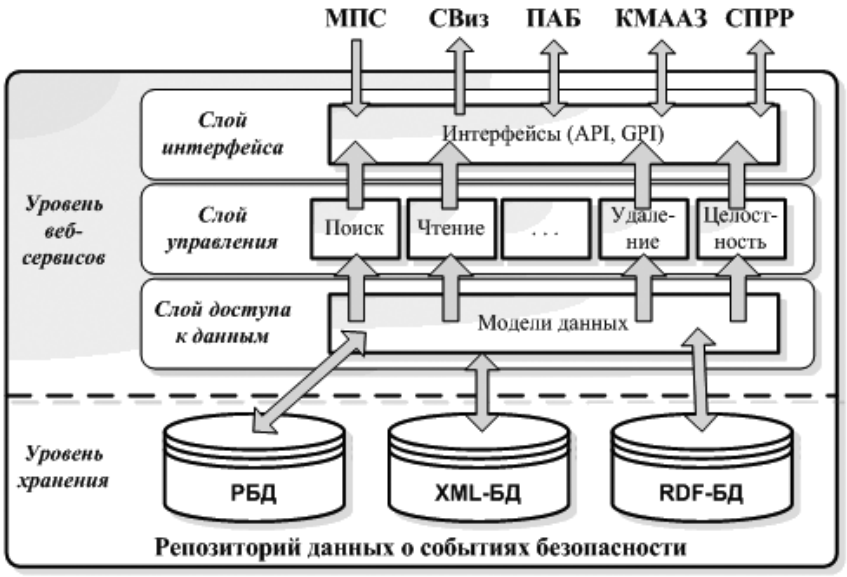

Рис. 2. Архитектура репозитория данных

базовых моделей представления данных и обеспечивающий, с одной стороны, задание моделей предметной области в виде онтологий, а с другой – использование логического вывода для выработки решений.

Уровень реализации веб-сервисов делится на три основных слоя: доступа к данным, управления и интерфейса. Слой доступа обеспечивает обращение к базам данных с помощью моделей данных. Слой управления реализует операции над данными. Слой интерфейса реализует различные виды взаимодействия с компонентами SIEM-системы.

Компонент КМААЗ способен генерировать графы атак, вычислять метрики защищенности, оценивать защищенность сети посредством анализа графов атак, генерировать отчеты с рекомендациями по повышению безопасности и анализировать события безопасности для обнаружения атакующих действий, что позволяет распознавать модели поведения возможного злоумышленника и его последующие шаги [16–22]. Входными данными для КМААЗ являются: конфигурация компьютерной сети (системы); политики безопасности, определяемые множеством полномочий или правил доступа; формируемые предупреждения; внешние базы данных уязвимостей, атак, платформ и т. д.; профили нарушителей; требуемые значения метрик безопасности. Основными результатами работы компонента КМААЗ являются: обнаруженные уязвимости; возможные маршруты (графы) атак и целей атак; зависимости между сервисами; «узкие места» в безопасности компьютерной сети; скорректированные деревья атак, основанные на изменениях, произошедших в сети; предсказания дальнейших шагов нарушителя; метрики безопасности, которые могут использоваться для оценки общего уровня безопасности; последствия атак и контрмер; предложения по увеличению уровня безопасности; решения, основанные на мерах, политиках и средствах безопасности.

Архитектура компонента КМААЗ показана на рис. 3 [23].

Загрузчик репозитория, обращаясь через Интернет к внешним базам данных, загружает информацию об уязвимостях, атаках, конфигурации, «узких местах», платформах и контрмерах. *Генератор спецификаций* преобразует информацию о сетевых событиях, конфигурации и политиках безопасности, полученную от других компонентов или от пользователя, во внутреннее представление. *Модуль моделирования нарушителя* определяет индивидуальные характеристики нарушителей, их начальное местоположение, пол-

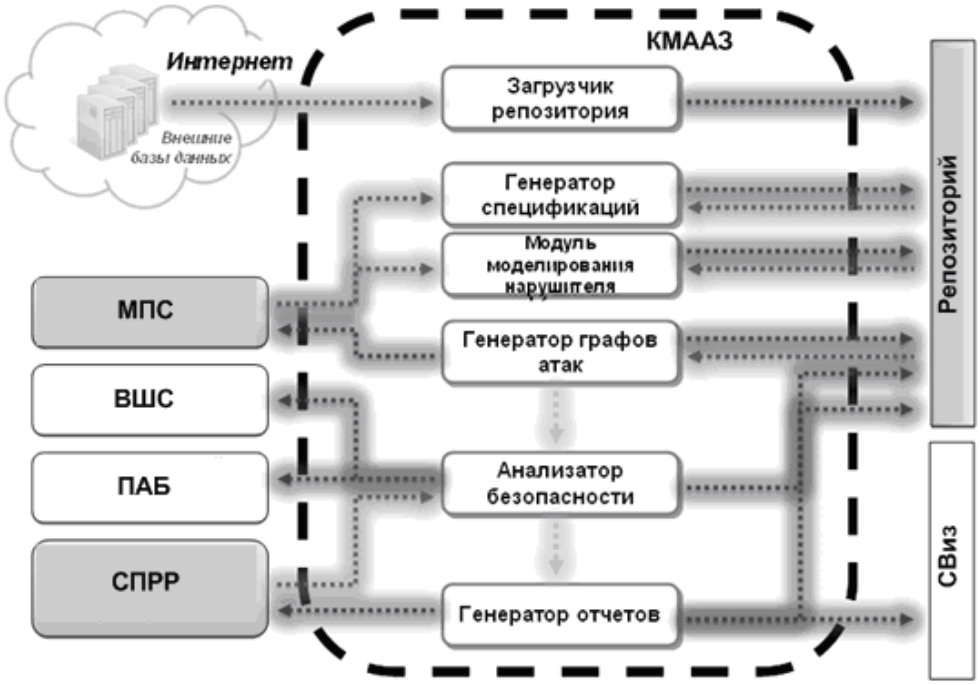

Рис. 3. Архитектура компонента КМААЗ

номочия, уже осуществленные и возможные действия, которые могут быть предсказаны, и знания об анализируемой сети. *Генератор графов атак* строит графы (деревья) атак путем моделирования последовательностей атакующих действий нарушителя в анализируемой компьютерной сети, используя информацию о различных типах возможных атак, зависимостях сервисов, конфигурации сети и использованных политиках безопасности. *Анализатор безопасности* имитирует многошаговые атаки, вычисляет метрики безопасности и оценивает эффективность контрмер. *Генератор отчетов* выдает информацию об обнаруженных уязвимостях и «узких местах», рекомендации по повышению уровня защищенности и другую релевантную информацию.

Компонент СВиз предназначен для визуального анализа информации о безопасности [24, 25]. Архитектура этого компонента включает три слоя (рис. 4): интерфейс пользователя; управляющие сервисы; графические элементы. *Интерфейс пользователя* поддерживает различные виды графических интерфейсов, начиная от простой командной строки и заканчивая сложным многооконным интерфейсом с панелями управления. *Слой управляющих сервисов* рассматривается как модуль управления визуализацией. Исходя из выполняемых функций, в данном слое можно выделить контроллер графических элементов и менеджер сервисов. *Контроллер графических элементов* предоставляет стандартный интерфейс по работе с потоками визуализации, обеспечивающий создание и остановку графического потока, реализуемого на уровне графических элементов. *Менеджер сервисов* обеспечивает подключение сервисов мониторинга и управления безопасностью. *Слой графических элементов* включает библиотеку необходимых графических примитивов: графов, лепестковых диаграмм, гистограмм, карт деревьев, географических карт и т. д. *Графические элементы* реализуют обработку входных данных, их отображение и взаимодействие пользователя с входными данными.

Рассмотренные особенности построения и функционирования компонентов SIEM-системы нового поколения позволяют выработать предложения по ее применению в различных инфраструктурах.

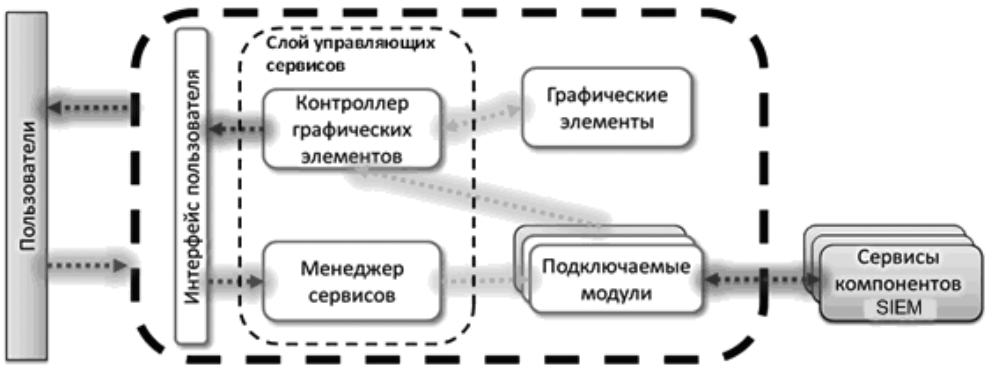

Рис. 4. Архитектура компонента визуализации

Предложения по применению

В качестве примеров областей использования, демонстрирующих преимущества SIEM-систем нового поколения, использованы следующие сценарии:

компьютерная инфраструктура высокой производительности, применяющаяся для поддержки проведения Олимпийских Игр, в которой циркулируют потоки, равные сотням тысяч / миллионам событий в секунду;

распределенная компьютерная инфраструктура, в которой доставка данных о событиях безопасности от периферии к центру и передача решений по применению контрмер от центра к периферии осуществляется через коммуникационную среду, подвергающуюся многочисленным воздействиям;

критическая инфраструктура (например, дамба), в которой необходимо проведение совместной обработки данных, поступающих как от традиционных для SIEM-систем источников событий, так и от инфраструктурных датчиков (сенсоров), фиксирующих параметры состояния элементов инфраструктуры;

информационная инфраструктура для проведения мобильных денежных платежей, в которой угрозы информационной безопасности коррелируются с угрозами финансового мошенничества.

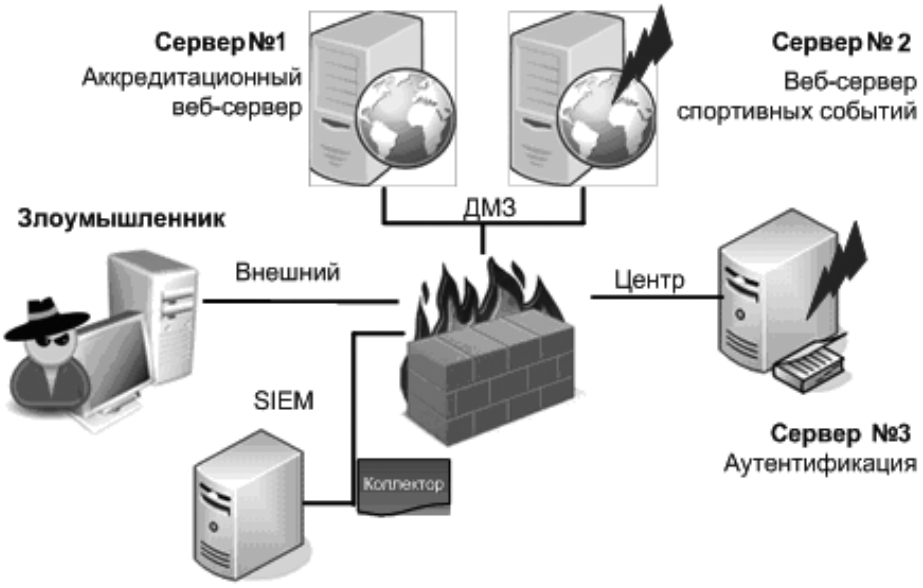

Рис. 5. Пример применения SIEM-системы в инфраструктуре Олимпийских Игр

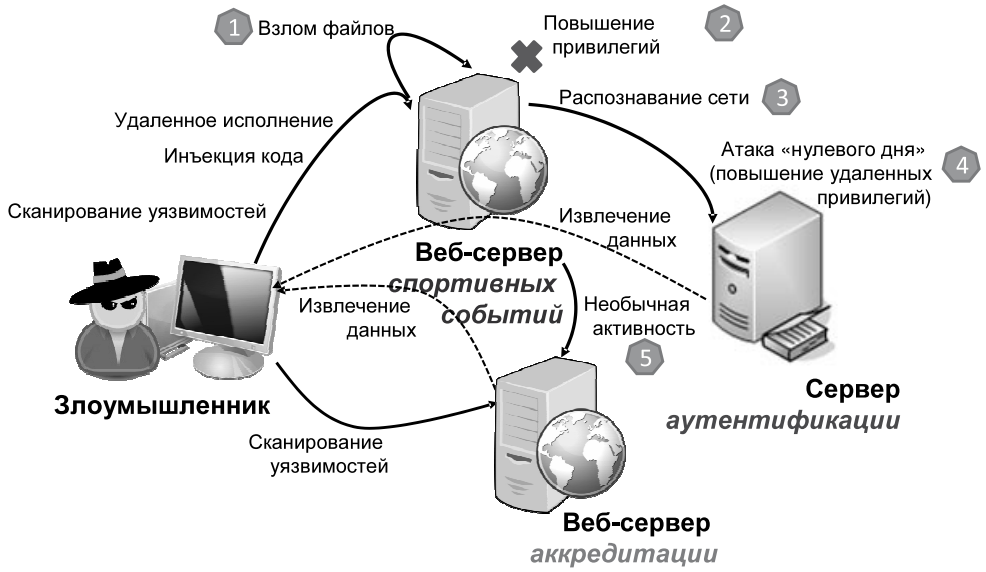

Рис. 6. Схема действий нарушителя в инфраструктуре Олимпийских Игр

Для примера остановимся на особенностях только первого сценария. С особенностями других сценариев можно ознакомиться в [1, 7].

Логическая модель примера сценария компьютерной инфраструктуры Олимпийских Игр представлена на рис. 5. Демилитаризованную зону (ДМЗ) образуют два веб-сервера: сервер аккредитации и сервер спортивных событий. К центральной части защищаемой инфраструктуры относится сервер аутентификации. В центральную часть поступают данные от периферии (удаленной части) инфраструктуры. Атакующий злоумышленник, как предполагается, также является внешним пользователем.

Схема проведения атаки злоумышленником представлена на рис. 6. Она включает пять этапов. Целью первого этапа является установление удаленного контроля над сервером спортивных событий. В ходе первого этапа злоумышленником выполняются следующие действия: сканирование уязвимостей, инъекция кода (внедрение вредоносной программы), удаленное исполнение кода и взлом файлов на сервере спортивных событий.

На втором этапе осуществляется повышение привилегий (полномочий), которыми наделяется злоумышленник. Целью этого этапа является атака «грубой силы» на пароль локальной административной учетной записи. На третьем этапе производится исследование компьютерной сети на предмет наличия уязвимостей. Цель этого этапа заключается в определении открытых портов на сервере аутентификации. На четвертом этапе осуществляется проведение атаки «нулевого дня» (направленной на ранее неизвестную уязвимость), целью которой является удаленное повышение полномочий. Благодаря выполнению этой атаки злоумышленник получает возможность выполнения произвольных команд на удаленном сервере. Наконец, пятый этап заключается в нахождении учетной записи, обеспечивающей доступ к приложениям сервера аккредитации. Проявлением таких действий злоумышленника может быть наблюдаемая необычная активность сервера аутентификации и аккредитации.

Особенность и основная задача применения SIEM-системы в этом сценарии заключается в обеспечении ее способности выявить «необычную активность», обусловленную деятельностью злоумышленника, на фоне огромного количества прочих событий, обрабатываемых в системе.

В статье представлены основные решения по построению и функционированию нового поколения систем мониторинга и

управления безопасностью. Рассмотренные компоненты SIEM-системы нового поколения расширяют ее возможности в направлении высокой масштабируемости, возможности межуровневой корреляции событий безопасности, высокоустойчивого сбора и передачи данных в распределенной вычислительной среде и повышения безопасности информационных инфраструктур.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт №2.2), проекта ENGENSEC программы Европейского Сообщества TEMPUS и госконтракта № 14.BBB.21.0097.

СПИСОК ЛИТЕРАТУРЫ

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

2. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2012. № 2. С. 57–68.

3. QRadar SIEM [электронный ресурс] / URL: http://q1labs.com/Products/QRadar–SIEM.aspx (дата обращения 25.01.2014).

4. ArcSight ESM Enterprise Security Manager [электронный ресурс] / URL: http://www.arcsight.com/products/products-esm (дата обращения 25.01.2014).

5. Symantec Security Information Manager [электронный ресурс] / URL: http://www.symantec.com/ business/security–information–manager (дата обращения 25.01.2014).

6. Sentinel Log Manager Review [электронный ресурс] / URL: https://www.sans.org/reading-room/analysts-program/novell-whitepaper (дата обращения 25.01.2014).

7. MASSIF FP7 Project [электронный ресурс] / URL: http://massif-project.eu (дата обращения 25.01.2014).

8. Service-oriented Architecture [электронный ресурс] / URL: http://en.wikipedia.org/wiki/Service-oriented_architecture (дата обращения 25.01.2014).

9. **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. 2009. № 1. С. 37–42.

10. OSSIM [электронный ресурс] / URL: http://www.alienvault.com/community (дата обращения 25.01.2014).

11. Prelude [электронный ресурс] / URL: http://www.prelude–ids.com (дата обращения 25.01.2014).

12. OrBAC: Organization Based Access Control [электронный ресурс] / URL: http://orbac.org (дата обращения 25.01.2014).

13. **Kotenko I., Polubelova O., Saenko I.** Data Repository for Security Information and Event Management in Service Infrastructures // Internat. Conf. on Security and Cryptography. Rome, Italy, 2012. Pp. 308–313.

14. **Полубелова О.В., Полубелова О.В., Котенко И.В., Саенко И.Б., Чечулин А.А.** Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. 2012. № 2. Т. 8. С.100–108.

15. **Kotenko I., Polubelova O., Saenko I.** The Ontological Approach for SIEM Data Repository Implementation // IEEE Internat. Conf. on Internet of Things. Bezanson, France, 2012. Los Alamitos, California. IEEE Computer Society, 2012. Pp. 761–766.

16. **Kotenko I., Stepashkin M.** Network Security Evaluation Based on Simulation of Malefactor's Behavior // Internat. Conf. on Security and Cryptography. Proceedings. Portugal, 2006. Pp. 339–344.

17. **Kotenko I., Ulanov A.** Agent Teams in Cyberspace: Security Guards in the Global Internet // Internat. Conf. on Cyber Worlds. Lausanne, Switzerland, 2006. Proceedings. IEEE Computer Society, 2006. Pp.133–140.

18. **Котенко И.В., Степашкин М.В.** Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Изв. вузов. Приборостроение. 2006. Т. 49. № 3. С. 3–8.

19. **Ruiz J.F., Harjani R., Maca A., Desnitsky V., Kotenko I., Chechulin A.** A Methodology for the Analysis and Modelling of Security Threats and Attacks for Systems of Embedded Components // Proc. of 20th Euromicro Internat. Conf. on Parallel, Distributed and Network-Based Processing. Garching, 2012. Pp. 261–268.

20. **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 // Труды СПИИ РАН. СПб.: Наука, 2012. Вып. 1(20). С. 27–56.

21. **Котенко И.В., Степашкин М.В., Котенко Д.И., Дойникова Е.В.** Оценка защищенности информационных систем на основе построения деревьев социоинженерных атак // Изв. вузов. Приборостроение. 2011. Т. 54. № 12. С. 5–9.

22. **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.

23. **Kotenko I., Chechulin A., Novikova E.** Attack Modelling and Security Evaluation for Security Information and Event Management // Internat. Conf. on Security and Cryptography. Rome, Italy, 2012. Pp. 391–394.

24. **Новикова Е.С., Котенко И.В.** Механизмы визуализации в SIEM-системах // Системы высокой доступности. 2012. № 2. С. 91–99.

25. **Новикова Е.С., Котенко И.В.** Технологии визуализации для управления информацией и событиями безопасности // Труды СПИИ РАН. СПб.: Наука, 2012. Вып. 4(23). С. 7–29.

REFERENCES

1. **Kotenko I.V., Saenko I.B.** SIEM-sistemyi dlya upravleniya informatsiey i sobyitiyami bezopasnosti [SIEM-system for security information and events management], *Zaschita informatsii. Insayd* [*Protection of the information. Inside*], 2012, No. 5, Pp. 54–65. (rus)

2. **Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A.** Tehnologii upravleniya informatsiey i sobyitiyami bezopasnosti dlya zaschityi kompyuternyih setey [Security information and events management technologies to protect computer networks], *Problemyi informatsionnoy bezopasnosti. Kompyuternyie sistemyi* [*The problems of information security. Computer systems*], 2012, No. 2, Pp. 57–68. (rus)

3. *QRadar SIEM*. Available: http://q1labs.com/Products/QRadar–SIEM.aspx (Accessed 25.01.2014).

4. *ArcSight ESM Enterprise Security Manager*. Available: http://www.arcsight.com/products/products-esm (Accessed 25.01.2014).

5. *Symantec Security Information Manager*. Available: http://www.symantec.com/ business/security-information-manager (Accessed 25.01.2014).

6. *Sentinel Log Manager Review*. Available: https://www.sans.org/reading-room/analysts-program/novell-whitepaper (Accessed 25.01.2014).

7. *MASSIF FP7 Project*. Available: http://massif-project.eu (Accessed 25.01.2014).

8. *Service-oriented Architecture*. Available: http://en.wikipedia.org/wiki/Service-oriented_architecture (Accessed 25.01.2014).

9. **Kotenko I.V., Vorontsov V.V., Chechulin A.A., Ulanov A.V.** Proaktivnyie mehanizmyi zaschityi ot setevyih chervey: podhod, realizatsiya i rezultatyi eksperimentov [Proactive security mechanisms against network worms: approach, implementation and results of experiments], *Informatsionnyie tehnologii* [*Information Technologies*], 2009, No. 1, Pp. 37–42. (rus)

10. *OSSIM*. Available: http://www.alienvault.com/community (Accessed 25.01.2014).

11. *Prelude*. Available: http://www.prelude-ids.com (Accessed 25.01.2014).

12. *OrBAC: Organization Based Access Control*. Available: http://orbac.org (Accessed 25.01.2014).

13. **Kotenko I., Polubelova O., Saenko I.** Data Repository for Security Information and Event Management in Service Infrastructures, *International Conference on Security and Cryptography*. Rome, Italy, 2012, Pp. 308–313.

14. **Polubelova O.V., Kotenko I.V., Saenko I.B., Chechulin A.A.** Primenenie ontologiy i logicheskogo vyivoda dlya upravleniya informatsiey i sobyitiyami bezopasnosti [The use of ontologies and inference for security information and events management], *Sistemyi vyisokoy dostupnosti* [*High-availability systems*], 2012, No. 2, Vol. 8, Pp. 100–108. (rus)

15. **Kotenko I., Polubelova O., Saenko I.** The Ontological Approach for SIEM Data Repository Implementation, *IEEE International Conference on Internet of Things*. Bezanson, France, 2012, Los Alamitos, California, IEEE Computer Society, 2012, Pp. 761–766.

16. **Kotenko I., Stepashkin M.** Network Security Evaluation based on Simulation of Malefactor's Behavior, *International Conference on Security and Cryptography. Proceedings*. Portugal, 2006, Pp. 339–344.

17. **Kotenko I., Ulanov A.** Agent Teams in Cyberspace: Security Guards in the Global Internet, *International Conference on Cyber Worlds*. Lausanne, Switzerland, 2006, Proceedings, IEEE Computer Society, 2006, Pp. 133–140.

18. **Kotenko I.V., Stepashkin M.V.** Sistemyi-imitatoryi: naznachenie, funktsii, arhitektura i podhod k realizatsii [Systems-imulators: purpose, functions, architecture and the approach to realization], *Izvestiya vuzov. Priborostroenie*, 2006, Vol. 49, No. 3, Pp. 3–8. (rus)

19. **Ruiz J.F., Harjani R., Maca A., Desnitsky V., Kotenko I., Chechulin A.** A Methodology for the Analysis and Modelling of Security Threats and Attacks for Systems of Embedded Components, *Pro-*

ceedings of 20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, Garching, 2012, Pp. 261–268.

20. **Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A.** Primenenie tehnologii upravleniya informatsiey i sobyitiyami bezopasnosti dlya zaschityi informatsii v kriticheski vazhnyih infrastrukturah [Application of securitzy information and events management technology to protect critical information infrastructures], *Trudyi SPII RAN*. St. Petersburg: Nauka Publ., 2012, Iss. 1(20), Pp. 27–56. (rus)

21. **Kotenko I.V., Stepashkin M.V., Kotenko D.I., Doynikova E.V.** Otsenka zaschischennosti informatsionnyih sistem na osnove postroeniya derevev sotsioinzhenernyih atak [Security assessment of information systems based on building socio-engineering attacktrees], *Izvestiya vuzov. Priborostroenie*, 2011, Vol. 54, No. 12, Pp. 5–9. (rus)

22. **Kotenko I.V., Stepashkin M.V., Bogdanov V.S.** Arhitekturyi i modeli komponentov aktivnogo analiza zaschischennosti na osnove imitatsii deystviy zloumyishlennikov [Architectures and components of active security analysis model based on simulating the action of hackers], *Problemyi informatsionnoy bezopasnosti. Kompyuternyie sistemyi* [*The problems of information security. Computer systems*], 2006, No. 2, Pp. 7–24. (rus)

23. **Kotenko I., Chechulin A., Novikova E.** Attack Modelling and Security Evaluation for Security Information and Event Management, *International Conference on Security and Cryptography*, Rome, Italy, 2012, Pp. 391–394.

24. **Novikova E.S., Kotenko I.V.** Mehanizmyi vizualizatsii v SIEM-sistemah [Visualization mechanisms in SIEM systems], *Sistemyi vyisokoy dostupnosti* [*High-availability systems*], 2012, No. 2, Pp. 91–99. (rus)

25. **Novikova E.S., Kotenko I.V.** Tehnologii vizualizatsii dlya upravleniya informatsiey i sobyitiyami bezopasnosti [Visualization technologies for security information and events management], *Trudyi SPII RAN*, St. Petersburg: Nauka Publ, 2012, Iss. 4(23), Pp. 7–29. (rus)

КОТЕНКО Игорь Витальевич – *заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН, доктор технических наук, профессор.*
199178, Россия, Санкт-Петербург, 14-я линия В.О., д. 39.
E-mail: ivkote@comsec.spb.ru

KOTENKO, Igor V. *St. Petersburg institute for information and automation of Russian academy of sciences.*
199178, Liniya 14, 39, St. Petersburg, Russia.
E-mail: ivkote@comsec.spb.ru

САЕНКО Игорь Борисович – *ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН, доктор технических наук, профессор.*
199178, Россия, Санкт-Петербург, 14-я линия В.О., д. 39.
E-mail: ibsaen@comsec.spb.ru

SAENKO, Igor B. *St. Petersburg institute for information and automation of Russian academy of sciences.*
199178, Liniya 14, 39, St. Petersburg, Russia.
E-mail: ibsaen@comsec.spb.ru

ЮСУПОВ Рафаэль Мидхатович – *директор Санкт-Петербургского института информатики и автоматизации РАН, член-корреспондент РАН.*
199178, Россия, Санкт-Петербург, 14-я линия В.О., д. 39.
E-mail: yusupov@iias.spb.su

YUSUPOV, Rafael M. *St. Petersburg institute for information and automation of Russian academy of sciences.*
199178, Liniya 14, 39, St. Petersburg, Russia.
E-mail: yusupov@iias.spb.su