УДК 004.056.5

Цветков Алексей Александрович
ФГБОУ ВПО «Ивановский государственный университет»
Шуйский филиал
Россия, Шуя[1]
Аспирант кафедры информационных систем и технологий
E-Mail: Tsvetkov.a.a@yandex.ru

Задачи обработки данных мониторинга ресурсов распределенной вычислительной сети

Аннотация. В работе представлены результаты изучения особенностей данных мониторинга ресурсов распределенной вычислительной сети. Проведение активного мониторинга является необходимым условием поддержания работоспособности сети, при этом обработка результатов мониторинга информационных ресурсов должна проводиться на высоком технологическом уровне, поскольку от качества проведенного анализа данных зависит обоснованность принимаемых решений по управлению рисками информационной безопасности. В статье выявлены и структурированы ключевые задачи обработки данных, проанализированы имеющиеся особенности такой обработки и охарактеризованы инструментальные программные средства аналитической поддержки мониторинга. К основным задачам обработки данных мониторинга отнесены: оценка качества собранных данных, ввод данных в различные информационные системы, анализ данных, наглядное представление данных, хранение накопленных данных и осуществление доступа к данным. Качественная обработка данных мониторинга позволяет решать такие основные задачи мониторинга, как: выявление реального состояния информационных и вычислительных ресурсов в интересах управления ими при изменении нагрузки; количественная оценка защищённости ресурсов от деструктивных факторов и информационное обеспечение механизмов управления рисками информационной безопасности. Так называемые SIEM-системы призваны осуществлять поставленные задачи, они позволяют консолидировать множество разрозненных решений по мониторингу безопасности, предоставляя возможности корреляции событий и выявления угроз со стороны инсайдеров.

Ключевые слова: активный мониторинг; распределенная вычислительная сеть; компьютерная сеть; информационные ресурсы; обработка данных; данные мониторинга; информационная безопасность; выявление инсайдеров; SIEM-системы; корреляция событий.

Идентификационный номер статьи в журнале 81TVN414

[1] 155908, Ивановская область, г. Шуя, ул. Кооперативная, д.24

Современные распределенные вычислительные сети объединяют в себе большое количество различных ресурсов, имеющих ключевое значение в деятельности организации. Во многих случаях информационные ресурсы содержат конфиденциальные данные, детализирующие особенности функционирования фирмы. В информационном обществе информация становится одним из самых значимых факторов инновационного развития, поэтому защите сетевых информационных ресурсов (ИР) в настоящее время уделяется повышенное внимание. Согласно статистическим данным именно ИР чаще всего становятся объектами информационных атак различного рода и потому требуют постоянного наблюдения в рамках выбранной политики безопасности. Отсюда следует, что мониторинг ресурсов сети является необходимым условием поддержания работоспособности распределенной вычислительной сети (РВС).

В ряде научных публикаций [2, 3, 4, 5, 6] отмечается, что обработка результатов мониторинга ИР играет ключевую роль в процессе администрирования РВС и должна проводиться на высоком технологическом уровне. От характеристик мониторинга ИР и степени автоматизации задач анализа данных зависит обоснованность принимаемых решений по управлению рисками информационной безопасности. Однако не производилось детального исследования вопроса обработки данных мониторинга, задачи и средства такой обработки не были проанализированы.

Настоящая статья имеет целью изучение особенностей данных мониторинга ИР РВС, обоснование и анализ ключевых задач обработки данных и поддерживающих их инструментальных программных средств.

Под термином «*мониторинг ресурсов сети*» будем понимать комплекс процедур, которые предусматривают целенаправленное автоматизированное или автоматическое прямое или косвенное дистанционное «наблюдение» за состоянием ресурсов сети в интересах своевременного обнаружения попытки или факта нарушений установленных прав доступа, других несанкционированных действий пользователей либо обнаружения иных пробелов в безопасности и обеспечивают сбор информации об изменении состояния ресурсов сети. Иначе, результатом проведения мониторинга ресурсов РВС является набор данных, характеризующих изменение выбранных системным администратором параметров за определенный промежуток времени.

Как правило, есть необходимость вести журналы мониторинга, в которых фиксируются ошибки и сообщения прикладной системы и заносится информация обо всех действиях пользователей. Также важно фиксировать все подозрительные события за время работы системы, такие как попытки проникновения в систему извне, подбора пароля, запуска приложений из закрытых каталогов, попытки доступа к ИР пользователями с заведомо недостаточными на то правами и т.д. Таким образом, администратором сети должно быть определено какие сведения о состоянии системы необходимо заносить в журналы мониторинга, исходя из особенностей выбранной политики безопасности [7].

Обработка данных представляет собой систематизированную последовательность операций, совершаемых с данными, с целью извлечения новой конструктивной и полезной информации посредством вычислений, пересмотра и анализа имеющейся информации, а также представления ее в качественно новой форме. При этом постоянно увеличивается количество источников информации о текущем состоянии защищенности, усложняя администраторам информационной безопасности задачу контроля над общей картиной происходящего. Суть процесса обработки данных мониторинга заключается в обнаружении необходимых на практике знаний в большом количестве необработанного материала, который делает эти знания неочевидными. Так, например, во всей совокупности данных о действиях пользователей и состоянии ресурсов РВС в журналах мониторинга информацию о

несанкционированных действиях ряда пользователей, приведших к сбою в работе какого-либо приложения, возможно получить лишь путем анализа действий всех пользователей и сопоставления их с изменениями состояния вышедшего из строя ресурса.

Таким образом, целью обработки данных мониторинга ресурсов РВС является отделение существенной информации от несущественной и представление первой в удобном для последующего применения виде. С одной стороны, сами данные должны отвечать требованиям актуальности, достаточности, достоверности и неизбыточности, чтобы на их основе было возможно произвести оценку состояния защищенности ИР и выявить необходимость проведения мер по корректировке используемых механизмов защиты информации. С другой стороны, детальная обработка данных позволяет извлечь действительно ценную информацию из всего имеющегося комплекса собранных данных, качество обработки данных определяет уровень надежности принимаемых решений в области информационной безопасности.

Обеспечение поставленной цели обработки данных мониторинга ресурсов сети достигается путем выполнения следующих прикладных задач:

1. Оценка качества собранных данных.

Собранная информация должна быть оценена с точки зрения ее достоверности, полноты, актуальности, неизбыточности и понятности для того, чтобы на ее основе можно было делать истинные выводы.

2. Ввод данных в различные информационные системы.

Для осуществления процесса обработки данных мониторинга и управления рисками информационной безопасности системный администратор должен располагать набором инструментальных программных средств, поддерживающих процедуры анализа состояния защищённости сетевых ресурсов на основе данных мониторинга. Как правило, такие программы собирают всю необходимую для них информацию автоматически, однако при необходимости возможен и ручной ввод данных.

3. Интеллектуальный анализ данных.

Обработка данных мониторинга состояния ресурсов сети подразумевает анализ собранных данных различными средствами, к примеру, с помощью решения задач классификации, кластеризации, поиска ассоциативных правил, нахождения последовательностей и прочих. Классификация представляет собой обнаружение признаков, характеризующих группы объектов исследуемого набора данных, по которым в дальнейшем каждый новый объект может быть отнесен к какой-либо группе. В задаче кластеризации в отличие от классификации классы объектов изначально не предопределены, поэтому результатом кластеризации является разбиение объектов на группы. Решение задачи поиска ассоциативных правил предусматривает отыскание закономерностей между связанными событиями, происходящими одновременно. Целью решения задачи последовательности является установление закономерностей между событиями, связанными во времени. В любом случае анализ данных проводится в интересах обнаружения качественно новых знаний, полученных из имеющегося набора данных.

4. Представление данных.

Различные информационные системы могут поддерживать различные форматы представления данных. Как правило, анализируемые данные могут быть представлены в текстовом, табличном, графическом (в виде гистограмм), рейтинговом (с выделением критических звеньев), аналитическом (с построением многофакторной модели уязвимости

сегмента сети) или ином визуальном виде, что способствует повышению уровня информативности материала за счет его наглядности.

5. Хранение накопленных данных.

Данные мониторинга состояния ресурсов сети требуют анализа во времени для отслеживания динамики их изменений, поэтому необходимо хранить накопленные данные в течение некоторого временного периода. При этом различные информационные системы могут предоставлять возможность хранения данных с разной степенью надежности, длительности, могут по-своему проводить учёт и инвентаризацию, упаковку и маркировку данных.

6. Доступ к данным.

Для создания условий безопасного хранения собранных данных необходимо осуществлять контроль доступа и защиту этих данных, кроме того, должна быть организована возможность поиска нужных данных в накопленных массивах.

Задачи обработки данных мониторинга не лишены ряда проблем. Во-первых, собранная информация может быть противоречивой или неопределённой, что является необходимым и достаточным условием риска информационной безопасности, то есть может не представляться возможным сделать однозначный вывод о сложившейся ситуации, а необходимо выбирать наиболее вероятный вариант из некоторого числа возможных вариантов. Во-вторых, допустимое время обработки данных весьма ограничено, поскольку зачастую приходится принимать решения по управлению системой защиты информации практически в реальном времени [4]. Заметим, что проблема неопределенности информации в частности вызвана ограниченностью времени обработки данных, так как по мере возникновения новой уточняющей информации может быть снята неопределенность, однако, это недостижимо в условиях реального времени.

Как упоминалось выше, задачи обработки данных мониторинга могут быть решены посредством специализированных инструментальных программных средств, их называют системами класса Security Information and Event Management (SIEM), что в переводе означает «Система Сбора и Корреляции Событий». SIEM призваны анализировать информацию, собранную от различных источников, таких как антивирусы, DLP-системы, IDS/IPS-системы, маршрутизаторы, межсетевые экраны, операционные системы серверов и пользовательских компьютеров, сканеры уязвимостей, системы веб-фильтрации и др. [9], и в результате анализа выявлять отклонения от норм по каким-либо критериям. На базе собранных данных SIEM-решение выявляет подозрительные действия, которые внешне могут выглядеть безобидно, но в совокупном анализе с рядом других событий представлять угрозу. Например, однократный ввод неверного пароля не представляет опасности и, скорее всего, является результатом случайной ошибки, в случае же, если такой ввод повторяется некоторое количество раз, это уже может свидетельствовать о попытках взлома системы злоумышленником. Или, например, пользователь, имеющий доступ к конфиденциальным данным, отправляет часть из них по e-mail, если на базе накопленной статистики SIEM выявит, что данный email-адрес расположен вне обычного круга адресатов, то будет сгенерирован инцидент.

На сегодняшний день все большее число предприятий признают значимость SIEM-систем в качестве ИТ-инструмента, и рынок инструментальных программных средств такого рода достаточно широк, многие фирмы-производители предлагают свои решения, например, ArcSight (фирмы HP), Q1 Radar (IBM), Security Information Manager (Symantec) и другие.

Система ArcSight (http://www8.hp.com/) предоставляет возможность собирать и обрабатывать данные о событиях, поступающих от различных средств защиты информации, операционных систем, телекоммуникационного оборудования, аппаратного обеспечения,

прикладных сервисов и других источников. Она обладает уникальным механизмом интеграции с любым бизнес-приложением, моментально реагирует на инциденты путем анализа информации, при этом все события информационной безопасности собираются на единой консоли. Система генерирует отчеты о работе сетевых устройств, по антивирусной защите, об устройствах виртуальной частной сети, отчеты баз данных, отчеты по системам обнаружения и предотвращения вторжений, отчеты операционной системы, отчеты об управлении доступом, отчеты межсетевого экрана.

LogRhythm (http://www.logrhythm.com/) производит сбор сведений из разных источников (события Windows, системный журнал, файл, база данных и т.д.). Журналы организуются централизованно, в масштабируемой и безопасной форме, по всем журналам возможен быстрый и гибкий поиск, производится автоматическая классификация журналов, нормализация, агрегация и корреляция. Программа определяет аномалии в приложениях, базах данных, системе и устройствах в режиме реального времени посредством применения передовых методов интеллектуального анализа данных. В решении LogRhythm работает гибкая ролевая система оповещения с расстановкой приоритетов, осуществляется комплексное управление инцидентами, а также имеются широкие возможности по созданию отчетов.

Программный продукт GFI EventsManager фирмы GFI Software (http://www.GFI.com/) проводит централизованную обработку, мониторинг и архивацию лог-файлов формата Syslog, W3C и Windows, созданных брандмауэрами, серверами, маршрутизаторами, коммутаторами, телефонами, персональными компьютерами и др., осуществляет аудит баз данных SQL и Oracle, имеет систему обнаружения событий, поддерживающую обработку более шести миллионов событий в час. В программе настроены правила обработки различных типов лог-файлов, встроены функции мониторинга сервисов, имеются широкие возможности по созданию отчетов, при этом не требуется установка на управляемых компьютерах.

Система SIEM, реализованная компанией FSPro Labs, под названием Event Log Explorer (http://fspro.net/) предоставляет возможность группировать в дерево избранные компьютеры и их журналы для более быстрого и удобного доступа, причем возможен просмотр не только журналов, но и сохраненных файлов журналов. Предусмотрены развитые средства резервного копирования журналов, вожможна фильтрация событий по любому критерию, в том числе с поддержкой регулярных выражений, предусмотрен быстрый поиск по любому критерию, осуществляется быстрая навигация по журналу при помощи закладок, возможна интеграция с известными базами знаний по событиям, осуществлены возможности распечатки журналов и экспорта их в различные форматы, также не требует установки на управляемых компьютерах.

В системе Corner Bowl Software (http://www.cornerbowl.com/) консолидируются журналы событий, syslogs а также нестандартные файлы журналов приложений, производится резервное копирование, сжатие, шифрование и защита паролем журналов событий, существуют фильтры регулярных выражений, предусмотрено несколько типов оповещения, уведомления и действий, включая SNMP ловушки, как и предыдущие решения, не требует установки на управляемых компьютерах.

Netwrix Event Log Manager (http://www.netwrix.com/) консолидирует данные из нескольких журналов событий, производит оповещения о критичных событих в режиме реального времени, генерирует подробные отчеты с возможностью фильтрации и поиска о соответствии международным стандартам и нормативам информационной безопасности, а также пользовательские отчеты по заданным параметрам или из библиотеки стандартных отчетов (более 250 видов). Система проводит аудит устройств Cisco и веб-сервера IIS.

Системы SIEM, как правило, включают в себя следующие компоненты: агенты, устанавливаемые на исследуемую информационную систему и локально собирающие журналы событий; коллекторы на агентах, предназначенные для разбора конкретного журнала мониторинга; серверы-коллекторы, собирающие события от различных источников; сервер-коррелятор, собирающий информацию от коллекторов и агентов и производящий обработку данных; сервер баз данных и хранилища для размещения журналов событий [9].

Своевременное обнаружение и предотвращение угроз реализуется системами SIEM путем применения правил корреляции, индивидуально настраиваемых с учетом рисков конкретной организации. Правила представляют собой общее описание случаев отклонения от нормального поведения информационных систем и трафика, на базе которых генерируются инциденты. При этом корреляционными механизмами необходимо управлять, корректируя и обновляя их с появлением новых угроз, а также настраивая их на работу в конкретной организации с ее особенностями инфраструктуры и системными процессами. Поэтому отличительной чертой SIEM-систем является то, что они достаточно сложны в грамотной установке и эффективной эксплуатации, что требует, как правило, привлечения квалифицированных специалистов. Однако успешное внедрение такой системы привносит значительное число преимуществ, такие как автоматизация процессов обнаружения угроз и генерирования инцидентов, контроль над системой информационной безопасности в режиме реального времени, корреляция событий, составление отчетов и прочие.

Таким образом, основным инструментом SIEM является корреляционный анализ, средствами которого могут быть выявлены угрозы, описанные правилами корреляции, либо типовые угрозы на базе шаблона, а также отклонения от стандартных настроек конфигурации и политики безопасности, кроме того, могут быть определены причинно-следственные связи произошедших событий, имеющих отношение к информационной безопасности.

Существуют различные методы корреляции, которые подразделяют на две большие группы – сигнатурные и бессигнатурные. Первые подразумевают наличие неких правил, определяемых пользователем, по которым выявляется инцидент. А вторые – это методы с обучением, то есть такие методы настроены производителями SIEM на определенные действия согласно обучающему набору данных. Кроме того, есть возможность исключения из использования заданных правил корреляции и создания на их основе собственных правил [10].

Используются следующие основные методы корреляции: статистический, на основе правил, на основе матрицы, метод моделирования, на основе графа зависимости, байесовский метод, на основе нейронных сетей [5, 6, 10]. Статистический метод (Statistical) – бессигнатурный метод, основанный на вычислении степени статистической связи между двумя и более событиями. Метод на основе правил (RBR – Rule-based) подразумевает выявление связей между событиями аналитиками на основе заданных правил. Правила обычно определяют отношения вида «условие-действие». Преимуществом данного метода является простота его понимания в связи со сходством с привычной конструкцией «если–то», а недостатками – субъективность заданных правил, сформированных экспертом, неспособность автоматически обучаться на опыте его применения и невозможность сохранять эффективность своей работы при переходе к новой нестандартной ситуации.

Метод на основе матрицы (CBR – Codebook based) подразумевает, что по заданной матрице событий определяется подходящий вектор. При этом заданная матрица содержит в себе степени связей между событиями, то есть каждому вектору событий (*A, B*) поставлено в соответствие некоторое значение, расположенное на пересечении строки *A* и столбца *B* матрицы. Например, причинами проблемы *A* являются события *Y* и *Z*, проблема *B* вызывается событиями *X* и *Y, C* возникает в следствие причины *Y*, события *X, Y* и *Z* влекут проблему *D*.

События могут происходить в произвольном порядке. Тогда матрица корреляции будет выглядеть следующим образом (см. рис. 1, составленный автором).

	A	*B*	*C*	*D*
X	0	1	0	1
Y	1	1	1	1
Z	1	0	0	1

Рис. 1. *Матрица корреляции*

Элементами матрицы являются нули, если отсутствует зависимость между причиной и появлением события, и единицы, если такая зависимость имеется. Если произойдут, например, события *X* и *Z*, выбирается вектор с наименьшим расстоянием Хэмминга, то есть будет идентифицирована проблема *D*. Решение может быть неопределено, как в случае, если наблюдаются только *X* и *Y* или только *Y* и *Z*. Отметим, что *Y* можно не учитывать, так как данная причина вызывает все события. Корреляция на основе матриц является сравнительно быстрым в применении методом, обладающим высокой устойчивостью к потерянным событиям и помехам, проблемные векторы могут генерироваться автоматически на основании обучающего набора данных. Недостатками данного метода являются отсутствие информации о времени происхождения событий и отсутствие свойств у событий.

Метод моделирования (MBR – model based reasoning) подразумевает наблюдение за абстрактными объектами в рамках заданных виртуальных интеллектуальных моделей, программно представляющих реальные объекты домена в MBR-системе. Типы моделей для различного рода физических и логических объектов применяются в качестве шаблонов для создания моделей реальных объектов. Каждый тип модели содержит базовый набор атрибутов, отношений и поведений. В процессе моделирования необходимо распознавать объекты реальной системы и моделировать их, заполняя обобщенные характеристики реальными данными. Затем осуществляется их мониторинг в реальном времени, при этом модели взаимодействуют друг с другом согласно предопределенным правилам поведения для выполнения задачи корреляции событий.

Метод на основе графа зависимости (Dependency graph based) заключается в построении графа на основе выявленных зависимостей между системными компонентами, который используется для поиска причины возникновения инцидента. Граф зависимости – это направленный граф, узлами которого в случае исследования компьютерной сети являются сетевые элементы (хосты), а наличие ребра, соединяющего узлы *A* и *B*, указывает, что сбои узла *A* могут вызвать неудачи в узле *B*. Метод позволяет определить вероятную первопричину возникновения события, начиная анализ в узлах, которые произвели начальные события, и отыскивая узлы, от которых начальные события зависят. Длина пути между узлом-первопричиной и начальными узлами может использоваться как метрика по качеству корреляции. При использовании такого подхода может не представляться возможным определить все первопричины событий при возникновении множественных проблем почти одновременно.

Байесовский метод (Bayesian network based) основан на определении по формуле Байеса вероятности какого-либо события при условии, что произошли другие взаимозависимые с данным события. Байесовская сеть представляет собой направленный нециклический граф, который моделирует вероятностные отношения между сетевыми элементами, представленными случайными величинами.

Метод на основе нейронных сетей (Neural network based) основан на построении нейронной сети, являющейся прототипом биологических нейронов человеческого мозга, которая обучается для обнаружения отклонений.

Процесс обработки данных мониторинга ресурсов РВС крайне важен для создания общей картины ИТ-безопасности. Основными задачами такой обработки являются оценка качества собранных данных, ввод данных в различные информационные системы, анализ данных, наглядное представление данных, хранение накопленных данных и осуществление доступа к данным. Причем, как правило, решения по управлению системой безопасности и настройке механизмов защиты информации приходится принимать в условиях неопределенности и в крайне сжатые сроки. Качественная обработка данных мониторинга позволяет решать такие основные задачи мониторинга, как: выявление реального состояния информационных и вычислительных ресурсов в интересах управления ими при изменении нагрузки; количественная оценка защищённости ресурсов от деструктивных факторов и информационное обеспечение механизмов управления рисками информационной безопасности. Существует большое количество программных продуктов, призванных осуществлять поставленные задачи. Так называемые SIEM-системы позволяют консолидировать множество разрозненных решений по мониторингу безопасности, предоставляя возможности корреляции событий и выявления угроз со стороны инсайдеров. Таким образом, поставленная цель данной работы достигнута, выявлены задачи обработки данных с имеющимися особенностями и охарактеризованы существующие инструментальные программные средства обработки данных мониторинга.

ЛИТЕРАТУРА

1. Андрианов, В. В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев; под ред. А. П. Курило. – М. : Издательство Альпина Паблишерз, 2011. – 373 с.
2. Надеждин, Е.Н. Математические основы моделирования и анализа интегрированных систем защиты информации: учебное пособие / Е.Н. Надеждин, Е.Е. Смирнова, Т.Л. Шершакова. – Тула: НОУ ВПО «Московский институт комплексной безопасности»; Изд-во ТулГУ, 2013. – 206 с.
3. Надеждин, Е.Н. Методы моделирования и оптимизации интегрированных систем управления организационно-технологическими процессами в образовании: монография / Е.Н. Надеждин, Е.Е. Смирнова.- Тула: Изд-во ТулГУ, 2013. – 250 с.
4. Надеждин, Е.Н. Научно-методические основы автоматизации процессов обеспечения информационной безопасности в сфере образования // Учёные записки ИИО РАО. – 2012. – № 41.– С.56-74.
5. Hanemann, A., Marcu, P. Algorithm design and application of service-oriented event correlation. [Электронный ресурс] URL: http://www.researchgate.net/publication/221033552_Algorithm_design_and_application_of_service-oriented_event_correlation (дата обращения 25.05.2014).
6. Muller, A. Event Correlation Engine. [Электронный ресурс] URL: ftp://ftp.tik.ee.ethz.ch/pub/students/2009-FS/MA-2009-01.pdf (дата обращения 25.05.2014).
7. Цветков, А.А. Модель активного мониторинга пользователей корпоративной информационной сети вуза // Информационная среда образования и науки, 2012. Выпуск 9. [Электронный ресурс] URL: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2012/num_9_2012/Cvetkov.pdf (дата обращения 03.03.2014).
8. Цветков, А.А. Сетевая модель активного мониторинга рабочих станций распределенной информационно-вычислительной сети // Информационная среда образования и науки [Электронный ресурс]: Электронное периодическое издание. – М.: ИИО РАО, 2013. Вып. 15. – URL: http://www.iiorao.ru/iio/pages/izdat/ison/pu blication/ison_2013/ num_15_2013/
9. Перкунов, А., Коростелев, П. Эффективная защита в режиме реального времени / Storage News. № 3 (55). 2013. – С. 12–14.
10. Шелестова, О. Корреляция SIEM – это просто. Сигнатурные методы. [Электронный ресурс] URL: http://www.securitylab.ru/analytics/431459.php (дата обращения 30.03.2014).

Рецензент: Шварев Евгений Анатольевич, ФГБОУ ВПО Ивановский институт государственной противопожарной службы МЧС России, старший преподаватель кафедры высшей математики и информатики, капитан внутренней службы, кандидат технических наук.

Aleksey Tsvetkov
Shuya branch of Ivanovo State University
Russia, Shuya
E-Mail: Tsvetkov.a.a@yandex.ru

The problems of monitoring resources' data processing in a distributed computer network

Abstract. In the paper the results of the studying of data monitoring features of the distributed computer network resources are presented. The active monitoring is a necessary condition of maintenance of network operability. Thus processing of information resources monitoring results have to be carried out at high technological level as validity of made decisions about risk management of information security depends on the quality of the carried-out data analysis. In the paper key problems of data processing with available features are identified and structured and software tools of analytical support of monitoring are characterized. The main problems of monitoring data processing are assessment of data quality, data input in different information systems, data analysis, visual data representation, data storage and access implementation. High-quality processing of monitoring data allows to solve such basically problems of monitoring as: detection of a real condition of information and computing resources to control them in case of loading change; the quantitative assessment of resources security from destructive factors and information support of mechanisms of information security's risk management. So-called SIEM systems are urged to realize the problems, they allow to consolidate a set of separate solutions about safety's monitoring, giving opportunities of events correlation and detection of threats from insiders.

Keywords: the active monitoring; the distributed computer network; computer network; information resources; data processing; monitoring data; information security; detection of insiders; SIEM systems; correlation of events.

Identification number of article 81TVN414

REFERENCES

1. Andrianov, V. V. Obespechenie informacionnoj bezopasnosti biznesa / V. V. Andrianov, S. L. Zefirov, V. B. Golovanov, N. A. Golduev; pod red. A. P. Kurilo. – M. : Izdatel'stvo Al'pina Pablisherz, 2011. – 373 s.
2. Nadezhdin, E.N. Matematicheskie osnovy modelirovanija i analiza integrirovannyh sistem zashhity informacii: uchebnoe posobie / E.N. Nadezhdin, E.E. Smirnova, T.L. Shershakova. – Tula: NOU VPO «Moskovskij institut kompleksnoj bezopasnosti»; Izd-vo TulGU, 2013. – 206 s.
3. Nadezhdin, E.N. Metody modelirovanija i optimizacii integrirovannyh sistem upravlenija organizacionno-tehnologicheskimi processami v obrazovanii: monografija / E.N. Nadezhdin, E.E. Smirnova.- Tula: Izd-vo TulGU, 2013. – 250 s.
4. Nadezhdin, E.N. Nauchno-metodicheskie osnovy avtomatizacii processov obespechenija informacionnoj bezopasnosti v sfere obrazovanija // Uchjonye zapiski IIO RAO. – 2012. – № 41.– S.56-74.
5. Hanemann, A., Marcu, P. Algorithm design and application of service-oriented event correlation. [Jelektronnyj resurs] URL: http://www.researchgate.net/publication/221033552_Algorithm_design_and_application_of_service-oriented_event_correlation (data obrashhenija 25.05.2014).
6. Muller, A. Event Correlation Engine. [Jelektronnyj resurs] URL: ftp://ftp.tik.ee.ethz.ch/pub/students/2009-FS/MA-2009-01.pdf (data obrashhenija 25.05.2014).
7. Cvetkov, A.A. Model' aktivnogo monitoringa pol'zovatelej korporativnoj informacionnoj seti vuza // Informacionnaja sreda obrazovanija i nauki, 2012. Vypusk 9. [Jelektronnyj resurs] URL: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2012/num_9_2012/Cvetkov.pdf (data obrashhenija 03.03.2014).
8. Cvetkov, A.A. Setevaja model' aktivnogo monitoringa rabochih stancij raspredelennoj informacionno-vychislitel'noj seti // Informacionnaja sreda obrazovanija i nauki [Jelektronnyj resurs]: Jelektronnoe periodicheskoe izdanie. – M.: IIO RAO, 2013. Vyp. 15. – URL: http://www.iiorao.ru/iio/pages/izdat/ison/pu blication/ison_2013/num_15_2013/
9. Perkunov, A., Korostelev, P. Jeffektivnaja zashhita v rezhime real'nogo vremeni / Storage News. № 3 (55). 2013. – S. 12–14.
10. Shelestova, O. Korreljacija SIEM – jeto prosto. Signaturnye metody. [Jelektronnyj resurs] URL: http://www.securitylab.ru/analytics/431459.php (data obrashhenija 30.03.2014).