N.G. Miloslavskaya, A.T. Makhmudova

The Actual Issues Of Big Data Appliance In Network Information Security Monitoring

Keywords: big data, network securitymonitoring, information security

Abstract: Network information security (IS) monitoring continues to be the essential part of security maintenance for many enterprises, and data collected during monitoring is considered to be Big Data. This technology has the properties that expand network infrastructure scope providing a higher performance and data security. Nevertheless, Big Data appliances pose serious challenges for IS monitoring formulated in this article. Based on the analysis of Big Data some recommendations for eliminating the existing problems are offered and briefly summarized in conclusion.

Н.Г. Милославская, А.Т. Махмудова

АКТУАЛЬНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ БОЛЬШИХ ДАННЫХ В МОНИТОРИНГЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ

Введение

За последние годыколичество различных сетевых атак на информационные системы (ИС) организаций, начиная от компрометации конфиденциальных данных и заканчивая отказами в работе физических устройств, во всем мире возросло. Атаки обычно направлены на чрезвычайно важные сферы деятельности, включая системы электронной коммерции, корпоративные сети, средства обслуживания центров обработки данных, промышленные системы и т.п. Например, в августе 2012 г. национальная нефтяная компания Саудовской Аравии Aramco стала объектом масштабной атаки, затронувшей 3000 рабочих станций корпорации [1]. В апреле того же года крупный поставщик платежных услуг GlobalPayments подтвердил массовое нарушение ИБ, которое позволило раскрыть данные держателей около 1,5 млн пластиковых карт [2]. В январе 2013 г. министерство энергетики США подверглось атаке, распространившейся на 14 серверов государственного органа, а также многие рабочие станции, находившиеся в главном управлении министерства [3]. В мае 2014 г. от правоохранительных органов США поступила информация о совершении атаки на сетевые ресурсы Университета Батлера [4], в результате чего были похищены персональные данные и финансовая информация около 163 тыс. студентов. А в начале февраля 2015 г. стало известно о крупной утечке данных 80 млн клиентов компании Anthem, второго по величине гиганта на рынке медицинского страхования США [5].

В таких условиях организации все острее осознают, что на используемые ими сетевые инфраструктуры могут быть направленыразличные по своему характеру атаки, и поэтому необходимо своевременно идентифицировать угрозы ИБ и устранять уязвимости, способствующие их реализации.

На протяжении долгого времени мониторинг ИБ в сетях является неотъемлемой частью функционирования вычислительных сетей и обеспечивет контроль выполнения операций в сети и их производительность, защищенную передачу данных, устранение возникающих угроз ИБ и отказов, поддержание соответствия требованиям по обеспечению ИБ и т.д. [6]. Учитывая, что существует большое количество решений по обра-

ботке и анализу сетевых данных, рассчитанных на различные варианты конфигурации сети и ее платформы, возникает обоснованный вопрос о применимости новых системобработки данных или включения этих данных в общую систему больших данных организации (англ. *bigdata*). Такой подход имеет как свои преимущества, так и недостатки, оказывающие существенное влияние на процесс интеграции технологии больших данных и мониторинга ИБ в вычислительной сети. Поэтому целью данной статьи и является анализ преимуществ и выявление проблем применения технологии больших данных для целей мониторинга ИБ в сетях и методов решения выявленных проблем. В разделе 1 рассматриваются особенности мониторинга ИБ в сетях на основе анализа больших данных, приводятся характеристики использования технологии, обосновывается необходимость интеграции систем обработки больших данных и систем мониторинга ИБ. В разделе 2 сформулированы главные проблемы обработки больших данных при мониторинге ИБ в сетях. Рекомендации по их решению предложены в разделе 3 и кратко обобщены в заключении.

Использование анализа больших данных в процессе мониторинга ИБ в сетях

Анализ больших данных активно используется во многих областях и за последнее время привлек внимание целого ряда сообществ из мира ИБ благодаря возможности эффективно анализировать и коррелировать данные, относящиеся к ИБ. Наибольшее применение технология получила в системах обнаружения и предотвращения вторжений (IDPS). Такие процедуры, как анализ журналов событий и сетевых потоков с их содержимым, многие десятилетия указывали на сложность обеспечения ИБ в сети и не всегда позволяли в полной мере поддерживать долгосрочный, масштабируемый анализ этих данных. Причин несколько.

Во-первых, до недавнего времени хранение больших объемов данных не было возможным с экономической точки зрения. В результате в классических инфраструктурах большая часть журналов системных событий и других действий в ИС удалялась по истечении определенного периода времени, например, через месяц.

Во-вторых, выполнение анализа и сложных запросов к большим, неструктурированным множествам данных с неполными характеристиками было неэффективным. Например, несколько популярных систем управления событиями и информацией об ИБ (SIEM) были спроектированы таким образом, что не позволяли анализировать и управлять неструктурированными данными, и работали по строго определенным схемам[7]. Однако новые технологии, использующие большие данные, становятся частью систем управления ИБ, позволяя эффективно обрабатывать данные, собранные от различных по своей природе источников в неоднородных средах.

Наконец, управление большими хранилищами данных обычно обходилось дорого, а их развертывание требовало строгого технико-экономического обоснования. Сейчас технология больших данных позволяет минимизировать расходы на проектирование широкомасштабных, надежных кластеров и потому предоставляет новые возможности для обработки и анализа данных.

По своей природе большие данные расширяют возможности вычислительных сетей организаций. Объем данных, требуемый для различных проектов, является неприемлемым для использования в традиционных сетевых архитектурах.Именно поэтому широко применяются виртуальные хранилища и облачные архитектуры. Для того чтобы поддерживать производительность и защищенность активоворганизации, необходимы средства и процедуры, позволяющие сохранять, защищать, корректно классифи-

цировать и в дальнейшем исследовать потокиисходных данных и полученных на их основе промежуточных и окончательных результатов обработки данных.

Одним из компонентов архитектуры больших данных являются распределенные базы данных (БД). Причем большие объемы данных обрабатываются и динамически распределяются в ИС, что обеспечивает высокую доступность и масштабируемость.

Использование технологии больших данных для мониторинга ИБ в сетях может решать следующие задачи [8]:балансировка нагрузки, управление сетевыми потоками в режиме реального времени; фильтрация данных (выявление подозрительной активности, исключение ненужных потоков данных для оптимизации полосы пропускания, приоритезация трафика); анализ данных в режиме реального времени (автоматизация ответных действий при обнаружении сетевых аномалий на основе анализа больших данных);управление виртуальными ресурсами. Таким образом, использование технологии больших данных для мониторинга ИБ в сетях позволяет обеспечивать более высокий уровень производительности сети и защиты данных, несмотря на то, что основные характеристики больших данных (модель 3V: большой объем, скорость и неструктурированность данных) усложняют сам процесс мониторинга потока данных.

Проблемы обработки больших данных при мониторинге ИБ в сетях

Данные мониторинга ИБ в сетях позволяют получить ценную информацию для анализа состояния динамически меняющейся в течение времени вычислительной сети организации и своевременного выявления возникающих угроз ИБ. Однако вопросы обработки больших объемов данных, собираемых в сети, и получения информации в режиме реального времени остаются главными проблемами. Использование технологии больших данных предусматривает применение новых подходов для сбора, хранения, измерения и анализа большого объема данных.

SIEM-системы используются в основном для регулирования соответствия требованиям по обеспечению ИБ, сформулированным в политиках ИБ организации или в каких-либо ведомственных, национальных и международных нормативных и правовых актах, позволяя собирать большой объем данных. Различные средства отслеживания потоков данных служат целямкомпьютерной форензики (англ. *computerforensics*): они полезны только в том случае, если известно, что необходимо искать, отслеживать и фиксировать во время управления ИБ после состоявшегося инцидента ИБ. Информационные панели (англ. *dashboards*) могут выполнять сбор статистических данных, но они не позволяют идентифицировать конкретные угрозыИБ. Большинство коммерческих средств мониторинга трафика используют сигнатурный анализ полезной нагрузки и поэтому являются неэффективными для обнаружения атак и уязвимостей «нулевого дня». Частота обновления сигнатур данных продуктов не достаточно высока. Разработчики вредоносного ПО могут быстро адаптироваться к изменяющимся условиям, поскольку они имеют такой же уровень доступа к сигнатурным файлам коммерческих продуктов, как и любой другой пользователь.

Специалисты в области ИБ видят решение проблем противодействия сетевым атакам в составлении профилей поведения (проведении поведенческого профилирования). Независимо от того, выполняются ли атаки с помощью вредоносного ПО или людьми, они в основном содержат в себе поведенческие характеристики, которые являются отклонением от статистических норм [6]. Если существует возможность смоделировать данные нормы, то можно будет выделить категории потенциальных угроз ИБ, ценных для дальнейшего исследования. Так называемая система обнаружения анома-

лий (разновидность IDPS) дополняет традиционные методы сигнатурного анализа данных. В этой системе профилируется и является объектом мониторинга каждый элемент вычислительной сети. Здесь очевидно применение больших данных. Но, к сожалению, при этом возникают три проблемы.

Во-первых, конечные сетевые устройства каждый деньгенерируют большие объемы данных (например, в каждойорганизации в среднем ежедневновырабатывается один терабайт данных). Такой большой объем информации практически не позволяет коммерческим средствам обеспечения ИБ выполнять долгосрочный анализ данных. Это препятствует быстрому анализу, модельным экспериментам и пониманию полученных результатов исследователями в области ИБ [9].

Во-вторых, в любойорганизации используется множество устройств и источников данных, которые генерируют разнородные данные в различных форматах. Для каждого устройства настроены разные уровни журналирования и параметры обновлений. Обеспечение ИБ в сети требует гибкости в отношении анализа данных из журналов событий, поступающих от новых устройств ИС, и быстрой оценки и использования полученной информации. В настоящий момент вендоры разрабатывают средства мониторинга ИБ, фокусируясь в основном на сборе данных и меньше всего на их превентивном анализе. Кроме того, такие решения не обладают способностью быстрой обработки журналов событий, поступающих от новых устройств, поскольку они настроены на работу с уже известными источниками данных [9].

В-третьих, большинство специалистов в области ИБ не имеют достаточного математического базиса для проведения исследований в области статистического и корреляционого анализа, используемого при обнаружении сетевых аномалий. Статистических метрик среднего и стандартного отклонения часто не достаточно. Здесь возникают вопросы, связанные с тем, какие поведенческие индикаторы следует вводить и как оценивать и объединять их определенным образом. В распоряжении организаций обычно нет таких возможностей. С другой стороны, для приобретения знаний и накопления статистики в области мониторинга ИБ в сетях на основе больших данных требуются годы исследований. Поэтому для эффективного анализа данных мониторинга ИБ необходимо, чтобы эти два аспекта рассматривались совместно [10].

В статье Г. Одина «Большие данные: средство, а не ответ» описываются пять факторов, которые ставят сложные задачи перед каждым, кто занимается обработкой больших данных и генерацией полезных, своевременных результатов их анализа [11]:

1)*количество* – объем данных, производимых большим разнообразием сетевых источников, постоянно увеличивается, при этом данные поступают как в структурированной, так и в неструктурированной форме в зависимости от поставщиков ресурсов. Объем является одной из важнейших характеристик сетевых данных, создающей серьезную проблему для существующих средств их обработки, имеющихся в средствах мониторинга ИБ в сетях. Количество информации, обрабатываемой на сегодняшний день в ИС, растет с огромной скоростью. Согласно данным InternationalDataCorporation (IDC), вычислительные сети производят более 3.5 эксабайт данных каждый месяц. Также ожидается, что данное число возрастет в 300 раз за последующие 5 лет [12];

2) *скорость доставки* –скорость доставки данных не должна препятствовать их быстройобработке. Изменения трафика и конфигурации ресурсов внутри вычислительной сети может происходить за миллисекунды. Если не выполнить своевременный анализ этих данных, то их значимость может существенно снизиться. Тогда эти данные не могут быть использованы для обработки и прогнозирования ситуаций в режиме реального времени;

3) *видоизменяемость* – создание данных происходит не по заранее известному графику. Большие данные могут появиться как в результате непредсказуемых событий (например, резкое увеличение объема трафика, сбои в работе ресурсов, атаки), так и в результате регулярных событий;

4) *множество форматов* – все данные различаются по своему формату. Вендоры добавляют к данным специальные расширения, обеспечивая больший объем собираемой информации и делая свои продукты наиболее привлекательными. Разнообразие форматов и расширений данных, таким образом, усложняет проведение анализа данных;

5) *множество источников* – сбор, сравнение и преобразование больших данных, полученных от различных источников, является весьма сложной задачей. В случае невозможности составления правил единой корреляции для обработки информации данные могут разбиваться на несколько частей и, если данные об одном событии попадут в разные части, конечный результат анализа не будет достаточно полезным и действенным.

Кроме названных проблем укажем на то, что и природа сетевых данных постоянно меняется. Все больше сетевых данных используется в виртуальных средах. Стоимость генерации трафика в виртуальных инфраструктурах стремится к нулю, а стоимость управления и обеспечения ИБ сетей, в которых обрабатываются потоки данных, возрастает. Сложность сетевых данных повышается по мере того, как повышается число сетевых сервисов, существенно изменяющихсодержание трафика. В соответствии с этим инструменты анализа становятся более специализированными.Таким образом, растет число средств, необходимых для более полного и детального мониторинга сетевого трафика. Кроме того, организации переходят к высокоскоростным сетям передачи данных (от 40 до 100 Гбит/с), что требует использования методов анализа данных, изначально идущих в ногу со временем, или средств предварительной обработки трафика до управляемых потоков [12].

Предлагаемые методы устранения существующих недостатков мониторинга ИБ в сетях с использованием технологии больших данных

Сетевые данные обладают очень выраженными свойствами модели 3V больших данных. Для того чтобы понять, почему существующие решения по мониторингу ИБ в сетях отстают в управлении сетевыми данными, необходимо детальное исследование текущихзадач, процессов и данных мониторинга ИБ. Очевидно, что для ИС необходимо эффективно масштабировать обработку и хранение сетевых данных для организации взаимодействия со средствами повышения производительности, системами обеспечения ИБи доступности данных для других приложений, таких, как средства контроля соответствия различным требованиям по обеспечению ИБ. В то же время они должны поддерживать гибкий контроль данных и всей архитектуры, осуществляющей их передачу. В устранения недостатков мониторинга ИБ, связанных с характеристиками больших сетевых данных, наиболее эффективными могут быть следующие методы.

1. *Разделение функций работы сбольшими данными.* Одним из решений для масштабирования мониторинга ИБ и управления сетевыми данными (особенно в случае развертывания систем контроля соответствия и поддержки компьютерной форензики) является разбиение основных функций вертикально интегрированных сетевых средств. Это означает, что работа с сетевыми данными разделяется на несколько этапов, таких как хранение, передача, обработка и анализ данных, выполняемых независимо друг от друга. Процесс разделения проводится на стороне организаций при проектировании

архитектуры мониторинга ИБ в сети. Особо важно, что происходит отделение хранения и обработки данных от их анализа. Обеспечение независимости процесса хранения данных высокоуровневых приложений предусматривает также использование аппаратного обеспечения для поддержки хранения данных на физическом уровне, где данные доступны для использования сразу несколькими приложениями.

Развертывание средств анализа, независимых от структуры обработки, приводит к однородности в управлении сетевыми данными и позволяет предотвратить недоступность данных за пределами одного набора средств. Кроме того, учитывая большой объем данных, очевидно, что собирать и обрабатывать данные на одном ресурсе достаточно сложно, поскольку это оказывает существенное влияние на производительность обработки. Подобное разделение подразумевает распределение данных между различными информационными платформами, а затем эти данные могут быть объединены (при необходимости с предварительной обработкой) для масштабируемого хранения. Такая оптимизация внутренних процессов приводит к увеличению скорости обработки и анализа данных и, следовательно, к увеличению производительности и эффективности.

2. *Использование потоковой обработки данных* (англ. *stream processing*). Она спроектирована таким образом, что позволяет обрабатывать и анализировать данные в режиме «жесткого» реального времени (англ. *hard real time*) с помощью технологии так называемых постоянных запросов при взаимодействии с внешними источниками и базами данных. Обработке подвергаются данные, находящиеся в оперативной памяти, без сохранения на энергонезависимых носителях. Вероятностно-временные характеристики процесса преобразования данных в основном определяются темпом поступления исходных данных, так как появление очередей на обрабатывающих узлах приводит к их безвозвратной утрате.

Потоковая обработка данных в разрезе технологии больших данных позволяет решить следующие важные вопросы: обработка больших объемов информации в режиме реального времени; увеличение производительности и масштабируемости при работе с данными по мере увеличения их объема и сложности; постоянная доступность данных на стороне конечных пользователей (администраторов ИБ); объединение данных, полученных от различных информационных платформ (например, в ходе разбиения, описанного в п.1); повышение эффективности анализа данных. Отсюда видно, что потоковая обработка информации является наиболее подходящей для работы с большими сетевыми данными, поскольку она позволяет решить проблемы обработки больших объемов данных в режиме реального времени, обеспечивая быстрый анализ сетевых данных, выявление инцидентов ИБ в сети и оперативное оповещение о них.

3. Стандартизация. Стандартизация процессов обработки и представления больших данных позволяет обеспечивать совместимость данных на различных этапах процесса мониторинга ИБ в сети. Значимость стандартизации определяется разнородностью данных как по отношению к форматам их представления, так и на уровне источников, из которых поступают данные, и приложений, которые используются для их обработки. Такая мера также позволила бы решить проблему взаимодействия различных организаций при обмене информацией об атаках и уязвимостях, используемой при мониторинге ИБ в сетях, обеспечивая прозрачность источников данных, а также методов их объединения и анализа. Это особо важно для исследовательских лабораторий и центров, занимающихся изучением инцидентов ИБ в сетях, поскольку при этом сокращаются расходы и время на проведение исследований. Пока не будут предприняты шаги к стандартизации данных, конечные результаты анализа больших данных, выработанных в результате мониторинга ИБ в сетях, будут не столь эффективны, а возможно и убыточны, для организации.

Заключение

Анализ данных играет ключевую роль в контроле событий, происходящих в ИС, и обнаружении в них аномалий. На сегодняшний день существует множество инструментов мониторингаИБ в сетях, таких как журналы событий, IDPS, SIEM-системы и т.п. Однако успешная реализация последних атак показала, что используемые механизмы защиты не столь действенны. Размеры сетей различных организаций, ассоциируемая с ними генерация растущего числа данных (по информации исследователей VSSMonitoring объем таких данных возрастет примерно в 300 раз к 2020 г.) и все большая необходимость объединения хранилищ информации и ее визуализации доказывают своевременность перехода к применению технологии больших данных для мониторинга ИБв сетях [12].

Проблема обработкой больших данных типична для многих организаций и состоит в следующем. Огромные объемы данных, накапливаемых в режиме реального времени и за длительный период, имеют различные форматы и источники. Конечные пользователи работают с таким разнообразием данных, используя специальные приложения, управление которыми требует знаний в этой области и определенных экспертных навыков. Наиболее важные данные извлекаются из источников информации с помощью заранее определенных запросов, встроенных в приложения. Более того, такие запросы обычно направлены только на конкретные источники с идентичной структурой.

Именно поэтому использование технологии больших данных при мониторинге ИБ в сетях ставит множество важных вопросов, требующих эффективных методов обработки информации. Они необходимы для углубленного понимания и оперативного принятия обоснованных решений по изменению стратегии обеспечения ИБ для ИС в соответствии с результатами анализа собранных данных. Кроме того, учитывая, что анализу подвергаются сетевые данные, становятся очевидными причины замедления интеграции мониторинга ИБ в сетях и технологии больших данных. Сетевые данные имеют различную структуру, что усложняет процесс их идентификации и эффективного анализа, поскольку используемые для данной цели приложения не позволяют с легкостью распознавать формат данных.

Краткое исследование, представленное в статье, позволило наметить основные меры устранения существующих недостатков мониторинга ИБ в сетях. Наиболее значимым является обеспечение масштабирования обработки, анализа и хранения сетевых данных, обеспечение гибкого контроля данных и лежащей в их основе архитектуры. Для этого предусматриваются следующие процедуры:разбиение основных функций, реализуемых сетевыми средствами обработки больших данных, а также обеспечение независимости процесса хранения данных на аппаратном и программном уровне; применение технологии потоковой обработки больших данных; стандартизация процессов представления и обработки больших данных. Поэтому для повышения эффективности процесса мониторинга ИБ в сетях, необходим целостный подход к анализу больших данных, собранных в результате мониторинга, объединение различных методов обработки полученных данных, а также расширение возможностей средств анализа и визуализации информации, чему и посвящены дальнейшие исследования авторов статьи.

СПИСОК ЛИТЕРАТУРЫ:

1. Zors Z. Help Net Security.Hackers allegedly breached Saudi Aramco again [**Электронныйресурс**]. URL: http://www.net-security.org/secworld.php?id=13493 (**дата обращения** 15.02.2015).
2. Zors Z. Help Net Security.1.5 million cards compromised in Global Payments breach [**Электронныйресурс**]. URL: http://www.net-security.org/secworld.php?id=12680 (**дата обращения** 15.02.2015).
3. Zors Z. Help Net Security.Hackers breach U.S. Energy Department networks [**Электронныйресурс**]. URL: http://www.net-security.org/secworld.php?id=14353 (**дата обращения** 15.02.2015).
4. Zors Z. Help Net Security. 163k individuals affected in Butler Uni data breach[**Электронныйресурс**]. URL: http://www.net-security.org/secworld.php?id=17069 (**дата обращения** 16.02.2015).
5. Zors Z. Help Net Security. US health insurer Anthem suffers massive data breach[**Электронныйресурс**]. URL: http://www.net-security.org/secworld.php?id=17917 (**дата обращения** 16.02.2015).
6. **Милославская Н.Г., Толстой А.И., Бирюков А.И. Визуализация информации при управлении информационной безопасностью информационной инфраструктуры организации** // **Научная визуализация**. 2014. **Том** 6, **№**2. **Стр**. 74 – 91.
7. Lin D. Big Data Analytics for Network Security Monitoring [**Электронныйресурс**]. URL: http://blog.pivotal.io/pivotal/products/big-data-analytics-for-network-security-monitoring(**дата обращения** 17.02.2015).
8. Green C. Big Security: Big Data and the End of SIEM [**Электронныйресурс**]. URL: http://www.information-age.com/technology/security/123458055/big-security-big-data-and-end-siem(**дата обращения** 17.02.2015).
9. Miloslavskaya N.G., Senatorov M.Y., Tolstoj A.I., Zapechnikov S.V. Information Security Maintenance Issues for Big Security-Related Data. In Proceedings of 2014 2nd International Conference on Future Internet of Things and Cloud (FiCloud). 2014. P. 361 – 366.
10. Big Data Blog. 4 Benefits of Big Data Network Monitoring [**Электронныйресурс**]. URL: http://www.ingrammicroadvisor.com/big-data/4-benefits-of-big-data-network-monitoring(**дата обращения** 20.02.2015).
11. Audin G. Big Data: A Tool, Not an Answer [**Электронныйресурс**]. URL: http://www.nojitter.com/post/240166379/big-data-a-tool-not-an-answer(**дата обращения** 22.02.2015).
12. VSS Monitoring. Leveraging a Big Data Model in the Network Monitoring Domain [**Электронныйресурс**]. URL: http://www.vssmonitoring.com/resources/whitepapers/Leveraging-a-BD-Model-Whitepaper.pdf(**дата обращения** 22.02.2015).

REFERENCES:

1. Zors Z. Help Net Security. Hackers allegedly breached Saudi Aramco again. URL: http://www.net-security.org/secworld.php?id=13493 (17.01.2015).
2. Zors Z. Help Net Security. 1.5 million cards compromised in Global Payments breach. URL: http://www.net-security.org/secworld.php?id=12680 (18.01.2015).
3. Zors Z. Help Net Security. Hackers breach U.S. Energy Department networks. URL: http://www.net-security.org/secworld.php?id=14353 (18.01.2015).
4. Zors Z. Help Net Security. 163k individuals affected in Butler Uni data breach. URL: http://www.net-security.org/secworld.php?id=17069 (28.01.2015).
5. Zors Z. Help Net Security. US health insurer Anthem suffers massive data breach. URL: http://www.net-security.org/secworld.php?id=17917 (14.02.2015).
6. Miloslavskaya N.G., Tolstoj A.I., Birjukov A.I. Information Visualization in Information Security Management for Enterprises Information Infrastructure // Scientific Visualization. 2014. Volume 6, **№**2. P. 74 – 91.
7. Lin D. Big Data Analytics for Network Security Monitoring. URL: http://blog.pivotal.io/pivotal/products/big-data-analytics-for-network-security-monitoring(24.01.2015).
8. Green C. Big Security: Big Data and the End of SIEM. URL: http://www.information-age.com/technology/security/123458055/big-security-big-data-and-end-siem (24.01.2015).
9. Miloslavskaya N.G., Senatorov M.Y., Tolstoj A.I., Zapechnikov S.V. Information Security Maintenance Issues for Big Security-Related Data. In Proceedings of 2014 2nd International Conference on Future Internet of Things and Cloud (FiCloud). 2014. P. 361 – 366.
10. Big Data Blog. 4 Benefits of Big Data Network Monitoring. URL: http://www.ingrammicroadvisor.com/big-data/4-benefits-of-big-data-network-monitoring (02.02.2015).
11. Audin G. Big Data: A Tool, Not an Answer. URL: http://www.nojitter.com/post/240166379/big-data-a-tool-not-an-answer (03.02.2015).
12. VSS Monitoring. Leveraging a Big Data Model in the Network Monitoring Domain. URL: http://www.vssmonitoring.com/resources/whitepapers/Leveraging-a-BD-Model-Whitepaper.pdf (03.02.2015).