Трошин Сергей Владимирович. Мониторинг работы пользователей корпоративных сетей : диссертация ... кандидата физико-математических наук : 05.13.11 / Трошин Сергей Владимирович; [Место защиты: Моск. гос. ун-т им. М.В. Ломоносова].- Москва, 2010.- 170 с.: ил. РГБ ОД, 61 10-1/559

**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. Ломоносова**

**ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ**

На правах рукописи

**04.2.01 0 5598 1 \***

Трошин Сергей Владимирович

**МОНИТОРИНГ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ
КОРПОРАТИВНЫХ СЕТЕЙ**

Специальность 05.13.11 - математическое и программное обеспечение
вычислительных машин, комплексов и компьютерных сетей

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико-математических наук

Научные руководители: д.ф-м.н., проф. И. В. Машечкин к.ф-м.н., доц. М. И. Петровский

МОСКВА

2010

**Содержание**

[**СОДЕРЖАНИЕ 2**](#bookmark0)

**ВВЕДЕНИЕ 4**

; ‘ 1 »

**, к**

[**ГЛАВА 1. МЕТОДЫ. ПОДХОДЫ И СИСТЕМЫ МОНИТОРИНГА 16**](#bookmark2)

1. [Существующие классы решений **16**](#bookmark3)
2. Критические параметры **18**
3. Критерии сравнения **24**
4. **Выбор решений для сравнения 25**
5. [Сравнение решений **29**](#bookmark5)
6. [**Системы управления информацией и событиями безопасности 29**](#bookmark6)
7. [**Системы мониторинга работы персонала 44**](#bookmark9)
8. **Выводы** II РЕЗУЛЬТАТЫ **46**

[**ГЛАВА 2. МОДЕЛЬ МОНИТОРИНГА РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ 51**](#bookmark12)

1. ИСХОДНЫЕ ДАННЫЕ ДЛЯ МОНИ IОРИНГА **51**
2. [**СОЗДАІІИЕ ФАКТОВ АКТИВІЮСТИ 56**](#bookmark13)
3. **Объединение фактов 60**
4. **Выборка и проекция 61**
5. Предлагаемый подход к мониторингу **62**
6. Шаблоны поведения пользователей и поиск аномалий **64**
7. [**Формальное описание шаблонов поведения 66**](#bookmark18)
8. **Поиск аномалий 71**
9. **Решение практических задач 76**
10. Профили использования ресурсов и поиск изменений в работе **78**
11. [**Формальное описание профилей работы 79**](#bookmark19)
12. [**Визуализация профилей работы 81**](#bookmark21)
13. [**Поиск изменений в работе 83**](#bookmark22)
14. **Выводы** и результаты **85**

[**ГЛАВА 3. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ 88**](#bookmark24)

1. **Архитектура системы мониторинга 88**
2. **Подсистема сбора данных 91**
3. **Сбор журналируемых событий 95**
4. [**Организация журналирования работы пользователей 102**](#bookmark25)
5. [**Фильтрация журналируемых событий 114**](#bookmark27)
6. [**Организация буферизации и отправки данных на сервер 116**](#bookmark28)
7. **Консолидация и централизованное хранение данных 118**
8. [**Форматы представления данных и организация хранилища 119**](#bookmark29)
9. **Устойчивость к сбоям в работе сервера консолидации 126**
10. **Организация приема данных и очереди импорта на сервере консолидации 129**
11. [**Настройка и контроль параметров сбора 132**](#bookmark31)
12. [**Обновление исполняемых файлов установленных агентов 134**](#bookmark32)
13. **подсистема анализа данных 134**
14. [**Запрос данных для анализа 134**](#bookmark33)
15. [**Построение моделей поведения 139**](#bookmark34)
16. [**Планирование выполнения анализа данных 143**](#bookmark35)
	1. **Практические эксперименты 144**

з

* + 1. [**Оценка производительности сервера консолидации 145**](#bookmark36)
		2. [**Производительность методов анализа данных 146**](#bookmark37)
		3. [**Оценка качества обнаружения аномалий 147**](#bookmark38)

**3.6. Выводы** И РЕЗУЛЬТАТЫ **152**

**ЗАКЛЮЧЕНИЕ 154**

[**ЛИТЕРАТУРА 156**](#bookmark39)

[**ПРИЛОЖЕНИЯ К ПРОГРАММНОЙ РЕАЛИЗАЦИИ 164**](#bookmark41)

Набор собираемых фактов активности в **ОС** Windows **164**

Пример описания структуры текстового журнала **167**

Алгоритмы работы со справочниками **168**

Пример файла конфигурации агента **169**

**Введение**

Одной из важных особенностей современных корпоративных сетей является их размер, который зачастую исчисляется тысячами, а и иногда и десятками тысяч компьютеров. При этом деятельность пользователей может быть распределена среди различных компьютеров, а одна и та же проблема часто решается группами пользователей [1]. Важной задачей является контроль работы, как отдельных пользователей, так и групп пользователей. Основными целями контроля являются: обеспечение информационной безопасности, выявление случаев некорректного, непрофессионального или нецелевого использования ресурсов, оценка характеристик функционирования корпоративной сети и параметров использования ресурсов.

Основной задачей **обеспечения информационной безопасности** является **«раннее обнаружение»** внутренних[[1]](#footnote-1) вторжений, т.е. выявление действий пользователей, которые могут предшествовать внутренним вторжениям. Чем крупнее организация, тем актуальней является для нее проблема предотвращения внутренних вторжений, в частности кражи информации, так как именно кража является конечной целью большинства внутренних вторжений. Связано это с тем, что в больших организациях затрудняется контроль над обращением информации и существенно возрастает цена ее утечки. Более 90% компаний и организаций сталкивались и получали ущерб от внутренних вторжений, а 60% сталкиваются с этим регулярно [2,3]. Указанные обстоятельства определяют высокий уровень озабоченности данной проблемой со стороны крупного бизнеса и правительственных организаций [4,5].

Так как не все внутренние вторжения удается предотвратить, актуальна задача **поиска и анализа попыток и результатов** уже произошедших внутренних вторжений. Поиск таких прецедентов позволяет определить виновных, оценить убытки и, главное, обнаружить уязвимость. Более 30% времени работы отделов IT безопасности уходит на обнаружение следов уже случившихся внутренних вторжений [2,3].

Очевидно, желательно обнаружить внутреннее вторжение именно на подготовительном этапе. Практика показывает, что в большинстве случаев внутреннему вторжению предшествует активность пользователя, которая является легитимной, но в то же время нехарактерной с точки зрения его предыдущей активности или активности его пользовательской группы. В большинстве случаев такая активность является следствием поиска уязвимостей и может продолжаться довольно длительное время. Особенностью обнаружения такой активности является тот факт, что всевозможные подготовительные к внутреннему вторжению действия пользователей невозможно описать заранее и тем более невозможно формализовать.

**Некорректное использование вычислительных и информационных ресурсов** часто является следствием отсутствия навыков или желания у сотрудников использовать специализированные программные продукты, применяемые в организации. Например, похожая ситуация была замечена на практике и заключалась в том, что после внедрения специализированной системы документооборота, сотрудники компании не использовали предоставляемые системой сервисы хранения и передачи данных, обеспечивающие надежность и защищенность, а передавали корпоративную информацию как делали это ранее, в незащищенных файлах посредством электронной почты. Причиной этому было «непонимание» и неумение пользоваться системой, о чем сотрудники не сообщали руководству. Непрофессиональное использование ресурсов может приводить к потере производительности, снижению качества результата работы, повышению нагрузки на вычислительные ресурсы, а так же к снижению уровня надежности и безопасности сети и данных. В 71 % случаев причиной утечки корпоративных данных были не спланированные вторжения, а беспечность пользователей и пренебрежение правилами [7].

**Обнаружение фактов нецелевого использования вычислительных ресурсов.** К нецелевой активности относят действия сотрудников, связанные с использованием корпоративных ресурсов в нерабочих целях. В частности это может быть использование доступа к сети Интернет в личных целях, просмотр видеофильмов, компьютерные игры, музыка, электронные книги и другое [8]. Перечисленная активность может приводить как к снижению эффективности труда, так и косвенно к снижению надежности и увеличению рисков утечки конфиденциальных данных. Например, за счет создания уязвимостей вследствие распространения вирусов и другого вредоносного ПО, распространение которого сопряжено с посещением «зараженных» интернет сайтов или установкой «зараженных» программ.

**Анализ характеристик функционирования корпоративной сети и параметров использования ресурсов** заключается в определении состава используемых информационных и вычислительных ресурсов, а так же параметров их использования. Контроль указанных параметров позволяет заблаговременно определить «узкие» места функционирования вычислительных ресурсов и уязвимости систем доступа к информационным ресурсам. Построить профили работы пользователей с ресурсами, в частности определить, кто из пользователей, для решения каких задач какие ресурсы использует.

Решение указанных задач может быть построено на основе мониторинга2 за параметрами и характеристиками работы пользователей с ресурсами. Целью мониторинга при этом является выявление соответствующих фактов или нарушений в работе. На сегодняшний день для обнаружения интересующих фактов работы (активности) успешно применяется сигнатурный поиск, основанный на сравнении текущей активности с набором правил [9]. Правила задаются экспертом априори, и описывают интересующие шаблоны активности или характеристики функционирования. Параметры текущей активности фиксируются и сравниваются с правилами, в случае

*'У .* **.**

**~ Под мониторингом понимается систематический сбор и анализ информации**

удовлетворения хотя бы одному из правил, система генерирует оповещение соответствующего типа. Стоит заметить, что методы сигнатурного поиска работают с ограниченным набором исходных данных, для которых существуют правила, это является недостатком, так как некоторые значимые действия пользователей могут попросту не оставлять следов в используемых источниках. Методы сигнатурного поиска не являются автономными, т.е. зависят от внешних баз знаний, что, во-первых, недопустимо в некоторых организациях, а, во-вторых, делает качество обнаружения существенно зависящим от качества базы знаний. Основной же проблемой использования сигнатурного подхода является невосприимчивость к еще неописанным экспертом шаблонам, или к модифицированным старым шаблонам. Таким образом, метод не работает, пока эксперт не обновит базу сигнатур. И, что более важно, метод просто неприменим, когда невозможно заранее формализовать объект поиска, как, например, в задаче раннего обнаружения внутренних вторжений.

Развитием сигнатурного поиска являются интеллектуальные методы поиска злоупотреблений, работающие по принципу построения моделей активности, которую требуется обнаружить, и сравнения текущей активности с построенной моделью [9]. Данный подход позволяет обнаруживать модифицированные известные сценарии работы, однако, так же практически неприменим для обнаружения активности, которую невозможно априори формализовать.

Выявление неформализуемой или плохо формализуемой деятельности пользователей, такой как подготовка внутренних вторжений или некоторые виды нецелевого или непрофессионального использования ресурсов, как правило, возможно, только с помощью подхода на основе обнаружения аномалий [9]. Обнаружение аномалий предполагает, что любые действия, отличающиеся от «обычной» активности, интерпретируются системой как аномалия. Для этого строится модель нормального поведения, а текущая активность сравнивается с моделью. Так, например, одним из сценариев использования подхода может быть определение отклонений в работе пользователя по сравнению с моделью работы его пользовательской группы. Найденные отклонения (аномалии) свидетельствуют об отличии активности пользователя от активности его группы. Учитывая тот факт, что группа в целом обычно работает корректно, найденные аномалии могут свидетельствовать о поиске уязвимостей, нецелевом использовании ресурсов или об иных нарушениях со стороны пользователя. Однако, учитывая особенности современных корпоративный сетей, а именно тот факт, что пользователи могут работать в группах и на различных компьютерах, вторжения или иные нарушения могут так же носить групповой характер, а следы таких действий могут быть распределены по сети. Требуется совокупный анализ различных данных, описывающих параметры работы различных пользователей. Спецификой такой задачи является необходимость поиска неявных закономерностей в больших объемах данных. Поэтому для построения моделей поведения и поиска аномалий требуются методы на основе современных алгоритмов машинного обучения и методов интеллектуального анализа данных, позволяющие выявлять скрытые закономерности, и факты [10].

Минусом подхода, основанного на поиске аномалий, является то, что система не может самостоятельно безошибочно без вмешательства аналитика отличить типы и корректность найденных аномалий. Как следствие, затруднена возможность автоматического проведения мероприятий по реагированию.

Часто для принятия решения помимо аномального события или набора аномальных параметров требуется уточнение различных характеристик работы. Задачу наглядного представления требуемых данных в работе предложено решать с помощью проведения статистического анализа. Результатом статистического анализа в общем случае является набор агрегационных показателей и зависимостей, отражающих характер работы пользователей и функционирования компонентов. Основным требованием к методам статистического анализа является возможность гибкого построения и уточнения отчетов с целью детализации результатов по произвольным параметрам, вплоть до конкретных фактов и отображение результатов в «понятном» аналитику виде. Учитывая то, что такие отчеты будут использоваться с целью поиска информации, формирование статистических отчетов должно происходить достаточно оперативно, в идеале — в режиме реального времени. Детализированный статистический анализ, удовлетворяющий поставленным требованиям, позволяет полностью решить задачу определения характеристик функционирования корпоративной сети.

Особенностью такого подхода является проведение анализа в отложенном режиме, т.е. по требованию аналитика на основе заданных им параметров.

Следует отметить, что существует множество систем, с разной степенью полноты решающих некоторые перечисленные задачи, однако, совокупное решение всех задач, очевидно, будет обладать существенным преимуществом, так как результаты анализа дополняют друг друга. С одной стороны, фиксация фактов нецелевого использования может стать сигналом к более глубокому контролю активности с целью обнаружения попыток внутренних вторжений, с другой стороны, похожие на атаку или аномальные действия со стороны пользователя могут являться причиной для проведения детального анализа использования ресурсов.

ч

Особенностью мониторинга пользователей современных корпоративных сетей является необходимость сбора и совокупного анализа широкого спектра параметров работы. Для анализа требуется объединение информации, собранной из различных источников. Указанная задача может решаться различными методами, однако с ростом корпоративных сетей становится все более необходимой консолидация и централизованное хранение всех собранных параметров и характеристик функционирования. Консолидация позволяет получать полную информацию об активности объекта, производить сравнение поведения объектов, а так же проводить агрегацию и корреляцию данных из различных источников. Решения, построенные с использованием общего хранилища, предоставляют ряд дополнительных сервисов, таких как возможность проведения отложенного анализа, поддержание доказательной базы для расследования уже случившихся нарушений. Так же наличие исторических данных позволяет отслеживать изменение поведения. Централизованный анализ не нагружает наблюдаемые системы, более того они могут быть выключены.

Одним из основных вопросов построения систем мониторинга является выбор исходных данных. Можно выделить следующие основные источники: контентная информация - содержательные данные, с которыми работают пользователи и журналируемая информация — данные из системных журналов, журналов прикладных программ и других источников журналируемой информации.

На основе контроля перемещения контентной информации с большой вероятностью могут обнаруживаться утечки корпоративных данных, так как копирование данных является конечной целью большинства внутренних вторжений. По такой схеме работают, например, решения компании InfoWatch [6]. Однако использование контентной информации имеет и ряд недостатков. Во-первых, контентная информация не формализована, требуется разработка методов извлечения требуемых данных из контента различных форматов. При этом содержание контентной информации не подходит для решения некоторых задач, в частности затруднен статистический анализ, так как контент не содержит параметров функционирования. Во-вторых, контентная информация занимает больший объем, поэтому задачи ее консолидации, хранения и анализа обычно более ресурсоемкие. И главное, анализ контентной информации потенциально снижает уровень защищенности корпоративных данных и сети. Это происходит по следующим причинам:

• За счет предоставления экспертам, разрабатывающим наборы правил и настраивающих систему, ключевых слов или иных признаков документов фактически происходит их ознакомление с конфиденциальной информацией, которую следует охранять от несанкционированного доступа.

• Системам безопасности предоставляется доступ ко всей информации, тем самым снижается уровень безопасности, т.к. образуется программный продукт, через который проходит вся конфиденциальная информация.

Использование событий журналируемой информации позволяет избежать обозначенных проблем. Журналируемая информация легко формализуется, содержит явные параметры и характеристики работы пользователей, функционирования устройств и программ. Журналируемая информация не компрометирует безопасность организации, так как не содержит конфиденциальных данных. Данная работа посвящена разработке средств мониторинга, основанных на использовании журналируемой информации.

Для решения каждого конкретного типа задач часто требуется специализированный набор данных [11]. Так для контроля характеристик функционирования вычислительных ресурсов могут применяться параметры их использования каждым пользователем. Для обнаружения нецелевого использования, параметры, описывающие работу пользователя с файлами, сетью и программами. О подготовке внутреннего вторжения же может свидетельствовать, практически, любой из параметров работы. В то же время состав программных и аппаратных средств, используемых в организациях, и соответственно журналов может сильно варьироваться. Следует отметить тот факт, что для проведения некоторых типов анализа могут требоваться дополнительных данные, не представленные ни в контентном, ни в журналируемом виде. Решить проблему получения необходимых данных можно только с помощью установки дополнительного программного обеспечения, в задачу которого входит определение требуемых параметров. В связи с этим, актуальным является разработка унифицированных моделей и методов, позволяющих производить сбор, консолидацию и анализ журналированных событий из различных источников и наблюдаемых систем, с учетом особенностей и ограничений использования сети передачи данных и других компонентов корпоративной сети.

Масштабы современных сетей, интенсивность функционирования компонентов, а так же комплексный состав используемых прикладных программ приводят к потокам в сотни, а зачастую и тысячи журналируемых событий в секунду, при этом большинство событий не представляет практической ценности для решения необходимых задач. Однако, очевидно, для решения различных задач, требуются различные журналируемые события. Требуется наличие настраиваемых механизмов фильтрации и агрегации собираемых данных, а так же планирования нагрузки на сеть, необходимы эффективные средства консолидации и централизованного хранения журналируемых данных. Принимая во внимание тот, факт, что любой мониторинг не имеет смысла, если существует возможность повлиять на достоверность исходных данных или результатов анализа, системы мониторинга должны обеспечивать защищенность данных от аварийных ситуаций и противодействий со стороны пользователя, как на этапе сбора и консолидации, так и на этапе хранения и анализа. Все модули системы должны быть защищены от «обхода» пользователем и от возможного отключения злоумышленником.

Обобщая вышеуказанное, можно утверждать, что актуальным является разработка технологии, позволяющей создавать системы мониторинга работы корпоративных пользователей, основанные на сборе, консолидации, централизованном хранении и анализе журналируемой информации, которые удовлетворяют следующим требованиям:

1. Подготовка исходных данных на основе использования различных источников журналируемой информации.
2. Эффективная консолидация и долговременное централизованное хранение данных.
3. Оперативная аналитическая обработка накопленной информации с целью вычисления явных зависимостей, статистических оценок параметров работы пользователей с ресурсами и поиска отклонений в работе.
4. Применение методов интеллектуального анализа данных с целью обнаружения неявных (скрытых) зависимостей в работе пользователей и аномалий в работе.
5. Минимизация дополнительной нагрузки на наблюдаемые системы и сеть передачи данных.
6. Обеспечение надежности и защищенности собранных данных и компонентов системы мониторинга.

**Целью диссертации** является исследование методов, алгоритмов и подходов проведения мониторинга и разработка, на основе результатов исследования, новой технологии построения специализированных систем мониторинга работы пользователей с ресурсами корпоративной сети. Технология должна основываться на использовании журналируемой информации и реализовывать моделирование поведения и поиск аномалий в работе пользователей. Построенные на-основе технологии системы должны позволять накапливать информацию, описывающую параметры работы пользователей, и проводить отложенный анализ с целью решения ряда специфических задач, таких как раннее обнаружение внутренних вторжений, выявление нецелевого и непрофессионального использования ресурсов корпоративной сети.

**Постановка задачи.** Исследование и разработка технологий построения систем мониторинга работы пользователей в рамках современных корпоративных сетей:

1. Исследование и разработка модели мониторинга, основанной на

формализации сбора и обработки данных, описывающих работу

пользователей с ресурсами корпоративной сети. Модель должна реализовывать концепцию раннего обнаружения за счет поиска аномалий в работе пользователей.

1. Исследование и разработка алгоритмических и программных решений, реализующих сбор, консолидацию, долговременное хранение и анализ журналируемых данных, позволяющих учитывать особенности конкретных корпоративных сетей, обладающих необходимой производительностью, обеспечивающих надежность работы и защищенность данных.

Результаты диссертационной работы докладывались на следующих конференциях и научных семинарах:

1. XIII Международная конференция студентов, аспирантов и молодых учёных «ЛОМОНОСОВ-2006», МГУ, Москва, 2006 г.
2. Конференция «Ломоносовские чтения 2006», МГУ, Москва, 2006 г.
3. Конференция «Тихоновские чтения», МГУ, Москва, 2006 г.
4. First Spring Young Researches’ Colloquium on Software Engineering (SYRCoSE’2007), Moscow, Russia, 2007.
5. Вторая международная конференция «Системный анализ и информационные технологии» САИТ-2007, Обнинск, Россия, 2007 г.
6. 13-я Всероссийская конференция «Математические методы распознавания образов», Зеленогорск, Россия, 2007 г.
7. 6-я международная конференция по программированию «УкрПРОГ’2008», Киев, Украина, 2008 г.

Основные результаты работы изложены в девяти научных публикациях [11, 12,61,63,74, 77, 80, 85, 86].

Диссертационная работа состоит из введения, трех глав, заключения, библиографии и приложений. Далее излагается краткое содержание работы.

В первой главе формируется набор критических параметров для сравнения систем мониторинга, формируются критерии оценки систем, проводится сравнительный анализ существующих систем.

Во второй главе описывается предложенная концепция мониторинга, основанная на моделировании поведения пользователей. Построенные модели поведения используются для поиска аномалий в действиях пользователей и изменений состава используемых ресурсов и параметров их использования. Найденные аномалии являются сигналом эксперту. Для описания законченных действий пользователей введено понятие факта активности, предложен метод построения фактов активности на основе журналируемой информации. Для решения задач построения моделей и поиска единичных аномалий используются алгоритмы интеллектуального анализа данных (data mining). Для построения профилей использования ресурсов применяется технология оперативной аналитической обработки OLAP. Так же в главе ставится ряд задач исследования и разработки методов, реализующих предложенную модель.

В третьей главе приводится архитектура предлагаемого решения и методы построения систем мониторинга, реализующих предложенную модель. Описываются методы сбора журналируемой информации, унифицирующие представление, чтение, фильтрацию и агрегацию журналируемых данных. Описываются предложенные методы построения централизованного хранилища, методы защиты хранилища от аварийных ситуаций и противодействий. Описывается экспериментальная апробация и оценка производительности построенного хранилища, сервера консолидации и подсистемы анализа данных. Представлены оценки качества работы методов обнаружения аномалий на тестовых данных, а так же практические примеры работы экспериментальной системы мониторинга.

В заключении приводится описание полученных результатов, данные об опытной эксплуатации и внедрениях систем мониторинга, построенных на основе предложенной технологии.

**Заключение**

Основными результатами диссертации являются:

1. Предложена модель мониторинга, формализующая сбор и анализ данных, описывающих работу пользователей с информационными и вычислительными ресурсами корпоративной сети. Модель реализует концепцию раннего обнаружения внутренних вторжений и нецелевого использования ресурсов корпоративной сети за счет поиска отдельных аномалий в работе пользователей и изменений статистики работы.
2. Разработана технология построения специализированных систем мониторинга работы пользователей корпоративных сетей, реализующая предложенную модель. Предложенные в рамках технологии алгоритмические и программные решения позволяют учитывать особенности конкретных корпоративных сетей, обладают необходимой производительностью, обеспечивают надежность работы и защищенность данных.

Разработанная технология апробирована в виде экспериментальной системы мониторинга. Построенная система мониторинга официально внедрена в эксплуатацию в один из органов государственной власти Российской Федерации, насчитывающий более 1250 рабочих мест пользователей, и успешно эксплуатируется с 2009 года.

Результаты опытной эксплуатации системы мониторинга показали, что:

1. Средний объем информации, передаваемый с одного компьютера на сервер консолидации агентом сбора, составил приблизительно 400 Кбайт в сутки;
2. Система при своем функционировании не нарушала эксплуатационных характеристик локальной вычислительной сети — не выявлены факты нарушения работоспособности компьютеров, на которые были установлены агенты сбора, не выявлены факты нарушения работоспособности сети за счет чрезмерного увеличения трафика, связанного с передачей собираемой агентами информации, не выявлены факты нарушения работы основных информационных сервисов;
3. Технология предоставляет возможности по выявлению фактов в работе пользователей, которые могут представлять интерес подразделению, ответственному за информационную безопасность (обращения к определенным категориям электронных документов, использование РпР устройств и обращение к документам на удаленных компьютерах, работа с определенными сетевыми ресурсами, использование игр, установка программного обеспечения, изменение аппаратной конфигурации и пр.);
4. Технология позволяет выявлять вирусы, пропущенные антивирусными средствами.

Построенные на основе технологии системы обладают следующими характеристиками:

1. Автономность. Не использует в своей работе данные внешних баз знаний. Для оценки аномальности фактов активности используются модели, построенные на собранных данных.
2. Адаптивность и самообучаемость. Система способна обнаруживать новые виды внутренних вторжений и аномалии в работе пользователей наблюдаемой компьютерной системы.
3. Масштабируемость. Система позволяет подключать к мониторингу дополнительные рабочие места пользователей за счет распространения агентов сбора данных.
4. Расширяемость. Система позволяет расширять набор исходных журналируемых данных и методов анализа данных за счет унификации сбора и представления собранных данных.
5. Безопасность. Система не понижает существующий уровень безопасности организации, в частности не использует контентную информацию. Передаваемые по сети данные шифруются с помощью SSL. Собранные данные хранятся во внутреннем представлении и защищены средствами разграничения прав доступа ОС.
1. Под внутренним вторжением понимаются действия легального пользователя, направленные на нарушение целостности, конфиденциальности или доступности данных корпоративной сети. [↑](#footnote-ref-1)