WHITEPAPER

PERIMETRIX® SAFEUSE™

ЗАЩИТА ДАННЫХ ВО ВРЕМЯ ИСПОЛЬЗОВАНИЯ

KEEPING SECRETS SAFE

PERIMETRIX®

PERIMETRIX®

1. ВВОДНЫЕ

Топ-менеджмент ждет, пока на горизонте появится не только эффективное, но и по-настоящему комплексное решение.

В настоящее время не вызывает сомнений, что защита корпоративных секретов (конфиденциальной информации, интеллектуальной собственности, персональных данных служащих и клиентов) является необходимым условием для существования организации. Причем защищать перечисленные классы информации приходится не столько от внешних злоумышленников, сколько от внутренних нарушителей.

Руководители отчетливо понимают, что утечка корпоративных секретов подрывает конкурентоспособность организации, осложняет отношения с клиентами, партнерами и инвесторами, а также с государством и регулирующими органами, которые принимают соответствующие законы, стандарты, директивы и кодексы. Однако до сих пор далеко не все коммерческие и государственные организации используют системы защиты от утечек. Виной тому низкая эффективность представленных на рынке решений, которые либо способны предотвратить только случайные утечки, либо настолько сложны и бюрократичны, что парализуют работу служащих и снижают эффективность бизнеса.

Кроме того, предлагаемые продукты не позволяют решать проблему утечек в комплексе. Вместо этого они концентрируются на отдельных направлениях. Например, блокируют порты рабочей станции или фильтруют исходящий сетевой трафик. Все остальное поставщики оставляют на откуп самой организации, специалисты которой должны решить самостоятельно, как защититься от кражи и потери ноутбуков и мобильных носителей с конфиденциальной информацией или предотвратить утечку через принтеры.

В результате компании считают неэффективным инвестировать средства в современные DLP-решения. Во-первых, им не понятно, за что платить, ведь потребность в обеспечении комплексной безопасности по сути остается неудовлетворенной. А во-вторых, приобритенная система может чрезвычайно быстро устареть, поскольку на рынке все время появляются новые и более интересные технологии. Такова неминуемая судьба любого неэффективного решения.

Руководители потенциальных клиентов понимают, что все перечисленные проблемы обусловлены незрелостью технологий защиты от утечек. Топ-менеджмент ждет, пока на горизонте появится не только эффективное, но и по-настоящему комплексное решение.

Именно таким продуктом является система Perimetrix® SafeSpace™ и одна из его составляющих – Perimetrix® SafeUse™.

PERIMETRIX®

2. ЭВОЛЮЦИЯ ПОДХОДОВ К ЗАЩИТЕ ДАННЫХ

Gartner указывает, что доступные на рынке продукты не позволяют создать надежной защиты. Их эффективность в лучшем случае достигает лишь 80%, так что о полном решении проблемы даже не приходится говорить.

Почему все предлагавшиеся до сегодняшнего дня решения так и не нашли своего покупателя? Ответ на этот вопрос дает научно-исследовательская компания Gartner. В своем последнем исследовании «Hype Cycle for Information Security, 2007» аналитики четко дают понять, что технологии предотвращения утечек еще не достигли своей зрелости. По мнению Gartner, это произойдет в течение последующих 2-5 лет, а сейчас внедрение предлагаемых решений сулит лишь «умеренные» преимущества для бизнеса.

Хотя технологию защиты от утечек обычно рассматривают в качестве эффективного средства защиты интеллектуальной собственности, эксперты Gartner указывают, что на практике применяемые технологии эффективны лишь при выявлении некачественных бизнес-процессов и только случайных утечек. Это означает, что предлагаемые технологии не в состоянии остановить мотивированного внутреннего нарушителя.

Таким образом, Gartner указывает, что доступные на рынке продукты не позволяют создать надежной защиты. Более того, их эффективность в лучшем случае достигает лишь 80%, так что о полном решении проблемы даже не приходится говорить.

2.1. ПРИЧИНЫ НЕУДАЧ

Ключевой недостаток существующих решений заключается в самой постановке задачи. Хотя разработчики совершенно справедливо считают, что утечка происходит только тогда, когда конфиденциальные данные покидают корпоративный периметр, они совершенно необоснованно сужают область защиты теми каналами, по которым данные могут попасть наружу. Это электронная почта, Интернет, мобильные носители и принтеры.

В результате многие аспекты проблемы остаются нерешенными. Например, ничто не мешает служащему скопировать данные на ноутбук, а потом симулировать его кражу. Взаимодействие между партнерами, связанными договором о неразглашении, целиком и полностью полагается на их порядочность, честное слово и отсутствие случайностей. Кроме того, защита от утечек на рабочих станциях работает обычно по принципу «разрешить/запретить», никак не учитывая уровень конфиденциальности того контента, который копируется, скажем, на

USB-носитель. Таким образом, сотрудник, имеющий легальный доступ к секретным данным, выпадает из сферы контроля и может злоупотребить своими правами в корыстных целях.

Между тем все эти проблемы выглядят лишь легким недомоганием на фоне той раковой опухоли, которую представляет собой крайне низкая эффективность предлагаемых продуктов.

2.2. ВЧЕРАШНИЙ ДЕНЬ НЕЗРЕЛЫХ ТЕХНОЛОГИЙ

Второе поколение технологий позволяет со 100% эффективностью защитить все классифицированные файлы.

Низкая эффективность используемых технологий обусловлена, прежде всего, их незрелостью. Хотя методы распознавания конфиденциальной информации прошли уже две ступени эволюции, они по-прежнему ограничены в своей эффективности и удобстве использования.

Первое поколение технологий – различные виды вероятностного анализа. В том числе, лингвистический и сигнатурный анализ, технология цифровых отпечатков (Digital Fingerprints). Те 80%, на которые указывает в своем исследовании Gartner, это самое лучшее, что могут предложить перечисленные методы, использующиеся для фильтрации исходящего трафика, чтобы отличить конфиденциальный документ от публичного. Даже с учетом контекста найденных ключевых слов, даже при использовании базы контентной фильтрации, учитывающей специфику конкретного заказчика, эффективность вероятностного анализа падает ниже 80%.

Отметим, что если вместо лингвистического анализа для выявления конфиденциального контента используются цифровые отпечатки, это никак не меняет ситуацию. Например, цифровые отпечатки легко обмануть – злоумышленнику ничто не мешает воспользоваться стеганографией или применить простейшее кодирование своего послания (используя различные кодировки, заменяя буквы цифрами и т.д.).

Второе поколение технологий – детерминистские методы или специальная разметка всех конфиденциальных документов – позволяет со 100% эффективностью защитить все секретные файлы, которые были признаны таковыми на этапе классификации данных. Однако здесь возникает целый ряд дополнительных препятствий: непонятно, что делать с новыми документами, которые пользователи создают после того, как система внедрена. Проблема в том, что продукт не справляется с задачей поддержания актуальности классификации документов.

PERIMETRIX®

Более того, такие решения обычно очень сложно внедрять, а на выходе получается система, лишенная всякой гибкости. Ее использование приводит к разрастанию бюрократии в организации, что в конечном итоге провоцирует конфликты между службой информационной безопасности (ИБ) и другими департаментами.

2.3. РЕВОЛЮЦИОННАЯ КОНЦЕПЦИЯ SECRET DOCUMENTS LIFECYCLE™

Пространство, в котором используется и хранится секретный документ, находится под полным контролем, а потому абсолютно безопасно.

Вместо того, чтобы концентрироваться на каналах утечки и попадать в ловушку предыдущих поколений, компания Perimetrix реализовала работу с данными в том виде, в котором она десятилетиями используется на режимных объектах для защиты государственной тайны. В результате появилось новое поколение технологий, защищающих секретные документы на всех этапах жизненного цикла – Secret Documents Lifecycle™ (далее SDL).

Ключевая идея концепции SDL состоит в том, чтобы создать безопасное аудируемое пространство, в котором пользователи могут работать с секретными документами под контролем системы защиты. Действительно, в каждой режимной организации есть специальный отдел, куда приходит человек, желающий получить доступ к секретному документу.

Прежде всего, он расписывается в журнале, где указывается, кто, когда, с какой целью и какой документ получил на руки. Далее другой служащий – хранитель архива секретных документов и своего рода библиотекарь – отыскивает нужный документ и выдает его на руки.

Получив документ на руки, служащий никуда не уходит. Он может работать с секретными бумагами только в специально отведенном для этого месте – в том самом безопасном пространстве. То есть в распоряжении сотрудника есть читальный зал при секретной части, где можно сесть и ознакомиться с документом.

В то же время вся работа с документом протоколируется. Служащий не может исказить полученные секретные сведения, т.е. внести изменения в оригинал, уничтожить документ или каким-то образом скопировать.

Конечно, если у сотрудника есть определенный уровень допуска, то он может модифицировать секретный документ, но в этом случае в отдельном журнале остаются записи о том, кто, когда, какие изменения и в какой документ внес. Так что в случае разбирательства всегда можно вычислить внутреннего нарушителя.

Отметим, что при таком подходе к работе с документом обеспечивается как аудит целостности секретного документа, так и защита его конфиденциальности от самых различных инцидентов, связанных с несанкционированным доступом. Например, сотрудник не может свободно выйти из отведенного помещения с секретным документом, а потом его потерять или стать жертвой преступников, которые документ выкрадут.

Все дело в том, что пространство, в котором используется и хранится секретный документ, находится под полным контролем, а потому абсолютно безопасно.

Конечно, только что описанный порядок работы с документом связан с большим количеством формальных процедур и высоким уровнем бюрократии. Однако все эти недостатки легко устранить, перенеся все операции и журналы событий в электронную среду: система защиты сама будет вести файл-отчет, отслеживать все изменения в документе, сохранять различные копии в архиве.

Однако концепция SDL позволяет контролировать не только использование секретных документов. Она покрывает и все остальные этапы жизненного цикла документа: создание, хранение, архивирование, удаление, а также такие специфические вещи, как понижение уровня конфиденциальности документа и перенос его в другое хранилище.

Таким образом, SDL позволяет создать безопасное пространство, в котором документы хранятся, используются, передвигаются, в конечном счете, официально уничтожаются. Реализация этого безопасного пространства нашла свое место в комплексном решении Perimetrix® SafeSpace™.

PERIMETRIX®

3. ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ PERIMETRIX® SAFEUSE™

3.1. SAFEUSE В СТРУКТУРЕ SAFESPACE

SafeUse создает аудируемую среду распределенного хранения и обработки конфиденциальной информации в соответствии с политиками безопасности компании.

Perimetrix® SafeSpace™ представляет собой комплексное решение для защиты корпоративных секретов от утечек. SafeSpace на практике реализует концепцию Secret Document Lifecycle™, и обеспечивает сохранность конфиденциальной информации на всех этапах жизненного цикла документа.

В состав SafeSpace входят три основных продукта, Perimetrix® SafeStore™, Perimetrix® SafeUse™, Perimetrix® SafeEdge™, а также ядро системы Perimetrix® ShadowCore™, с помощью которого осуществляется администрирование режима секретности, в соответствии с политиками компании. Кроме того, ShadowCore включает архив действий пользователей при работе с конфиденциальными документами для последующего анализа и аудита.

Защиту данных на этапе хранения обеспечивает продукт Perimetrix® SafeStore™. SafeStore представляет собой централизованное хранилище зашифрованных документов с регламентированным доступом. Шифрование позволяет предотвратить компрометацию данных при физической краже носителя или резервной копии. В свою очередь, контроль прав пользователей исключает неавторизованный доступ к информации. Еще одна функция SafeStore – шифрование данных на компьютерах и ноутбуках пользователей. Это исключает угрозу нарушения конфиденциальности данных даже в случае утери или кражи мобильного компьютера.

Защиту информации во время использования реализует Perimetrix® SafeUse™. SafeUse создает аудируемую среду распределенного хранения и обработки конфиденциальной информации в соответствии с политиками безопасности компании. Агенты SafeUse предотвратят утечку данных через съемные носители, принтеры и локальные порты компьютеров. SafeUse также не допустит копирование секретных сведений в новые документы или передачу данных нежелательным приложениям.

Третий продукт, предназначенный для защиты данных в движении – Perimetrix® SafeEdge™. SafeEdge перехватывает, фильтрует, а также проводит автоматическую классификацию исходящего трафика.

PERIMETRIX®

Если классифицированная порция данных (например, сообщение, отправленное через ICQ) не соответствует корпоративной политике ИТ-безопасности, то действие будет блокировано, а офицер ИТ-безопасности извещен об инциденте. SafeEdge использует сразу несколько методик классификации и анализа, чтобы обеспечить точность определения категории данных на уровне 99,6%.

Несмотря на то, что SafeStore, SafeUse и SafeEdge могут успешно применяться и по отдельности, целесообразно объединить все функции продуктов в рамках комплексного решения SafeSpace. Это позволит создать всеобъемлющую систему защиты от утечек, и повысить эффективность вложений в безопасность.

Изолированная система Perimetrix® SafeUse™ относится ко второму поколению DLP-решений (рис. 1) и предполагает установку меток на все классифицированные документы. В ее основе лежат несколько базовых концепций, которые коренным образом отличают систему от конкурентов. Во-первых, многомерная модель категорий позволяет исключительно точно классифицировать информацию. Во-вторых, механизм наследования категорий при работе с классифицированными документами поддерживает их классификацию в актуальном состоянии. И в-третьих, в продукте реализована унифицированная методология принятия решений, единая для перемещения информации в пределах рабочей станции и по сети.

Рисунок 1. Платформа решений Perimetrix

3.2. СХЕМА РАБОТЫ PERIMETRIX® SAFEUSE™

Локальные агенты Perimetrix® SafeUse™ обеспечивают контроль над любыми перемещениями информации и непосредственно предотвращают утечки.

Perimetrix® SafeUse™ можно разделить на серверную и локальные части, причем основной функционал системы реализован именно в агентских приложениях. Серверная часть системы имеет вспомогательный характер и служит для управления пулом агентов, ведения централизованной базы аудита, а также поддержки актуальной разметки документов с течением времени.

Таким образом, Perimetrix® SafeUse™ состоит из следующих компонентов (рис. 2):

- **Локальные агенты** Perimetrix® SafeUse™ обеспечивают контроль над любыми перемещениями информации и непосредственно предотвращают утечки.
- **Управляющий модуль** SafeUse служит для управления массивом агентов, изменения настроек и правил обработки событий, а также доставку этих изменений агентам. Кроме того, управляющий модуль обеспечивает работу централизованной базы аудита и классификатора документов SafeUse.
- С помощью **Web-консоли** SafeUse обеспечивается управление системой, настройка правил и политик доступа, а также автоматической классификации;

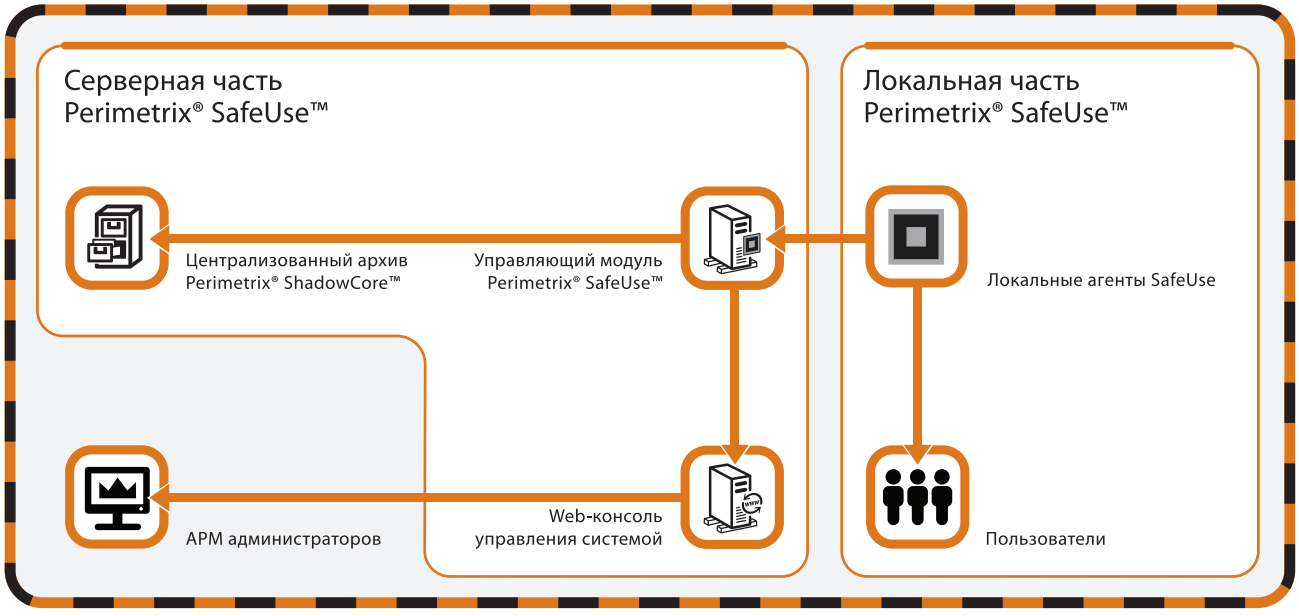

Рисунок 2. Схема работы Perimetrix® SafeUse™

PERIMETRIX®

- В **централизованный архив** Perimetrix® SafeUse™ попадает информация о зафиксированных событиях, перемещениях информации и инцидентах

Важно отметить, что перечисленные сетевые сервисы могут располагаться как на одном физическом компьютере, на выделенных серверах, или быть распределенными в кластере Perimetrix® Expansion™, который обеспечивает балансировку не только нагрузки, но и функциональности между доступными вычислительными мощностями.

3.3. МНОГОМЕРНАЯ МОДЕЛЬ КАТЕГОРИЙ

В основе работы Perimetrix® SafeUse™ лежит корпоративная политика безопасности, реализованная как комплекс правил и настроек доступа к конфиденциальным данным.

В основе работы Perimetrix® SafeUse™ лежит корпоративная политика безопасности, реализованная как комплекс правил и настроек доступа к конфиденциальным данным. Сами данные разделены на **онтологические категории**, отражающие их содержание и степень важности для организации. Пользователи системы наделяются полномочиями – разрешениями работать с информацией определенных категорий. Кроме того, доступ (разрешения хранить и/или обрабатывать информацию) к категориям настраивается для конкретных устройств и программ на компьютерах пользователей.

Деление на категории – одно из главных ноу-хау системы. В отличие от продуктов конкурентов, модель категорий Perimetrix является многоуровневой, а потому может быть максимально приближена к реальности. Любые данные характеризуются множеством категорий, разнесенных по разнородным измерениям. Например, финансовый отчет фирмы «Пример» из города «Н» может быть описан категориями «Сущность», «Секретность» и «География».

Так, измерение «Сущность» имеет плоский набор категорий, например, «IT», «Финансы», «Развитие», «Кадры». Очевидно, рассматриваемый отчет относится к финансовым документам.

Измерение «Секретность» может иметь иерархический набор категорий: «Публичные документы» – «Для внутреннего использования» – «Строго конфиденциально». Предположим, что финансовый отчет имеет категорию «Для внутреннего использования».

Измерение «География» – древовидное, т.е. родительский уровень «Россия» имеет несколько ветвей-регионов, в том числе и «Самара»,

PERIMETRIX®

«Томск», «Уфа», «Волгоград». Предположим, что рассматриваемый отчет относится к уфимскому отделению фирмы.

Таким образом, финансовый отчет описывается трехмерной моделью категорий, состоящей из измерений «Финансы», «Для внутреннего использования», «Уфа» (рис. 3). Подобным образом, любой документ в системе, в соответствии со своим содержанием, может быть описан исключительно точно. Так же как это сделал бы обычный человек, а не машина. Совокупный набор категорий различных измерений называется **уровнем**, и является одним из ключевых понятий в системе принятия решений Perimetrix.

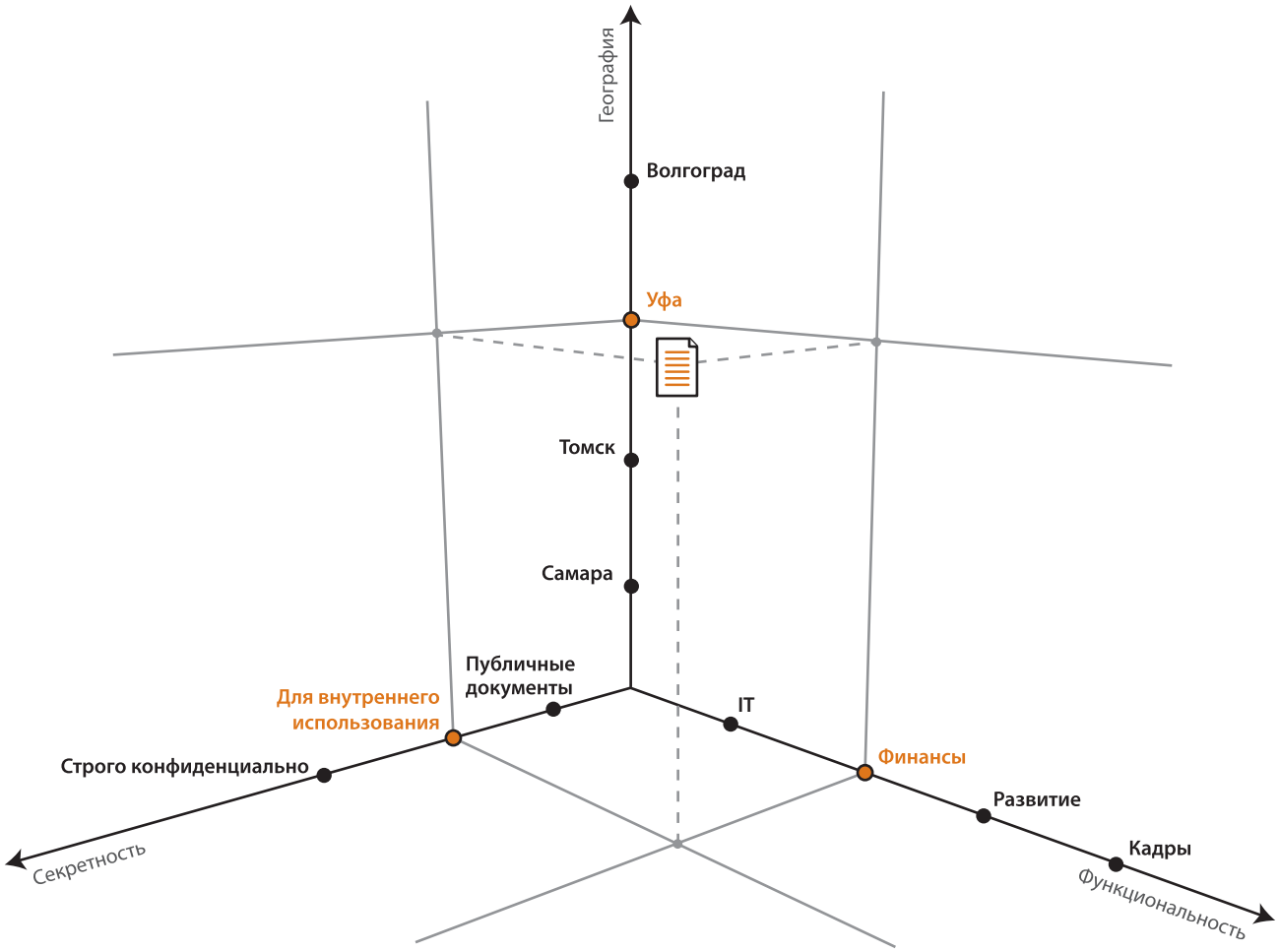

Рисунок 3. Графическое представление классификации конфиденциального документа в многомерной модели категорий.

PERIMETRIX®

3.4. МЕХАНИЗМ НАСЛЕДОВАНИЯ КАТЕГОРИЙ КОНФИДЕНЦИАЛЬНОСТИ И АВТОМАТИЧЕСКАЯ КЛАССИФИКАЦИЯ ДАННЫХ

В Perimetrix® SafeUse™ предусмотрен механизм наследования категорий конфиденциальности. Суть этого механизма состоит в том, что при копировании данные из классифицированных документов (или других источников) не теряют своих категорий, а переносят их в новый документ.

С точки зрения теории информационной безопасности, обозначенные выше категории являются усовершенствованием классической модели мандатного распределения доступа к информации (модели Белла-Лападула). Напомним, что в рамках данной модели всем субъектам (пользователям) и объектам (документам) присваиваются определенные метки безопасности. Для определения, разрешен ли субъекту доступ к объекту, его уровень безопасности (метка) сравнивается с меткой интересующего объекта, и на основе этого сравнения принимается какое-либо решение.

Основная проблема мандатного доступа давно известна – организациям крайне трудно поддерживать актуальную разметку документов. Для решения этой проблемы в системе Perimetrix® SafeUse™ предусмотрен механизм наследования категорий конфиденциальности. Суть этого механизма состоит в том, что при копировании данные из классифицированных документов (или других источников) не теряют своих категорий, а переносят их в новый документ.

Приведем в качестве примера самый распространенный кейс – копирование и вставка классифицированной информации в новый документ. На первом этапе (копирование) уровни документа будут присвоены буферу обмена, а затем – они будут перенесены в только что созданный новый документ. Подобным образом происходит передача уровней конфиденциальности между любыми контейнерами информации в рамках универсальной модели событий Perimetrix (см. 3.5). Потери уровней при перемещении классифицированной информации не происходит, и, таким образом, устраняется возможность деклассификации данных.

Решения класса ИАС РСКД (информационно-аналитические системы режима секретности конфиденциальных данных) предполагают не только технические средства защиты информации, но и ряд организационных мер, способствующих повышению уровню безопасности. Основные усилия в данном контексте должны быть направлены на повышение уровня культуры работы с конфиденциальными сведениями. Именно поэтому локальные агенты Perimetrix предлагают три режима работы, красный, желтый и зеленый.

PERIMETRIX®

Зеленый режим ориентирован на работу с неконфиденциальной информацией. В этом режиме пользователь не имеет права работать с классифицированной информацией вне зависимости от прав доступа и настроек системы.

Желтый и красный режимы, в свою очередь, предназначены для работы с классифицированными данными. Переключаясь на работу в одном из этих режимов, сотрудник должен отдавать себе отчет в том, что он работает с ценной информацией, и на него накладываются определенные ограничения по перемещению этой информации. Разница между красным и желтым режимом заключается в том, что в красном режиме происходит объединение уровней конфиденциальности при переносе информации между контейнерами. В желтом режиме объединения уровней не происходит, поскольку пользователю не разрешено перемещать информацию между контейнерами с отличными уровнями.

Однако даже несмотря на механизмы наследования, в системе все равно могут накапливаться входящие документы и документы, созданные «с чистого листа». Понятно, что такие файлы не будут размечены. Для решения этой проблемы (а также для первоначальной классификации документов) в системе SafeUse предусмотрен механизм автоматической классификации или **инвентаризации** данных. В заданное по расписанию время Perimetrix® SafeUse™ автоматически анализирует документы внутри указанного объекта (носителя, диска, файл-сервера) и присваивает им категории конфиденциальности. В дальнейшем, эти категории могут быть подтверждены или отклонены в ручном режиме.

В рамках процесса инвентаризации могут быть использованы формальные признаки документов (их тип, размер, размещение и др.) или применены один или несколько механизмов контентной фильтрации. Отметим, что функционирование данных механизмов обеспечивается системой Perimetrix® SafeEdge™ [1].Таким образом, полный функционал автоматической классификации будет доступен лишь в случае одновременного внедрения SafeUse и SafeEdge.

1 Подробнее см. в White Paper, посвященном Perimetrix® SafeEdge™

PERIMETRIX®

3.5. УНИВЕРСАЛЬНАЯ МОДЕЛЬ ПРИНЯТИЯ РЕШЕНИЙ

Отличительной особенностью Perimetrix® SafeUse™ является универсальная модель перемещения информации и система принятия решений на ее основе.

Отличительной особенностью Perimetrix® SafeUse™ является универсальная модель перемещения информации и система принятия решений на ее основе (см. рис. 4). Данная модель пригодна для защиты информации вне зависимости от того, где эта информация находится – на шлюзе сети, локальной станции или сетевом принтере. Главная цель системы – недопущение попадания информации к неавторизованным лицам, мониторинг и аудит действий авторизованных лиц.

Ключевым термином Perimetrix® SafeUse™ является понятие **перемещения информации**. Перемещение информации – это любое действие, которое приводит к возникновению информационных потоков в каналах передачи данных. Очевидно, что для каждого перемещения определен его **контейнер-источник** и **контейнер-приемник** информации.

Рисунок 4. Универсальная модель перемещения информации Perimetrix

PERIMETRIX®

Продемонстрируем данный понятийный аппарат на примерах (таб.1):

Таблица 1. Примеры перемещения информации

Сценарий перемещения	Контейнер-источник	Контейнер-приемник
Пользователь открывает текстовый документ в редакторе Microsoft Office Word	Локальный диск	Процесс winword.exe
Пользователь сохраняет документ Microsoft Word на флеш-накопителе	Процесс winword.exe	Флеш-накопитель
Пользователь копирует информацию из файла Microsoft Office Word в буфер обмена	Процесс winword.exe	Буфер обмена
Пользователь вставляет информацию из буфера обмена в блокнот	Буфер обмена	Процесс notepad.exe
Пользователь отправляет документ с локального диска по электронной почте	Почтовый ящик 1	Почтовый ящик 2

Основная задача Perimetrix® SafeUse™ реализуется на основе контроля над перемещениями информации, поскольку концептуальной причиной утечки всегда является абстрактное перемещение. Например, если утечка случилась из-за кражи ноутбука, то ее истинной причиной является копирование конфиденциальных данных в незашифрованный контейнер на жестком диске мобильного компьютера. Если же утечка произошла по электронной почте – ее причиной было перемещение информации в рамках отправки электронного письма.

Контроль перемещений информации реализован на основе сравнения уровней документов (см. раздел 3.3) и уровней атрибутов перемещения. Два атрибута перемещения (контейнер-источник и контейнер-приемник) уже были описаны выше. Кроме них можно выделить еще четыре атрибута:

- **Владелец контейнера-источника** – пользователь системы, который управляет контейнером-источником.
- **Инициатор действия** – пользователь системы, который непосредственно выполняет перемещение.
- **Владелец контейнера-приемника** – пользователь системы, который управляет контейнером-приемником.
- **Канал передачи данных**.

PERIMETRIX®

В рамках внедрения Perimetrix® SafeUse™ определяются все атрибуты перемещения и задаются допустимые уровни (наборы категорий) для них (аналогично уровням документов). Например, заказчик может присвоить контейнеру «флеш-накопитель» уровень «Публичный/Россия/Маркетинг». Такая настройка будет означать, что в данный контейнер могут перемещаться только публичные маркетинговые документы российских офисов компании.

Строго говоря, контроль над перемещением информации включает в себя несколько основных шагов:

1. **Перехват перемещения.** Система получает информацию о перемещении от сенсоров-перехватчиков.
2. **Определение атрибутов.** Система определяет атрибуты перемещения и считывает их уровни. Отметим, что в некоторых случаях могут быть заданы не все атрибуты. Так, в случае открытия файла в определенной программе формально не задан канал передачи, а в случае пересылки электронного письма в другую фирму – не задан владелец контейнера-получателя.
3. **Принятие и реализация решения.** Система сравнивает допустимые уровни каждого атрибута и фактические уровни перемещаемой информации. Если допустимые уровни всех атрибутов не ниже фактических уровней информации - перемещение разрешается. Если уровень хотя бы одного атрибута ниже – перемещение блокируется.
4. **Аудит перемещения.** Запись о перемещении появляется в специальной базе данных Perimetrix® ShadowCore™.

Еще один элемент универсальной модели – намерения. Определив намерения человека, перемещающего информацию, система сможет проактивно предотвращать утечки. Ведь пользователь может по долгу службы иметь доступ к конфиденциальным данным. Но отклонения от его нормального поведения подскажут, что действие может привести к инциденту. В качестве примера подобных событий можно привести пересылку конфиденциальных данных в нерабочее время, повышенный трафик на определенные адреса и т.д.

PERIMETRIX®

3.6. ТИПОВЫЕ СЦЕНАРИИ РАБОТЫ PERIMETRIX® SAFEUSE™

Чтобы проиллюстрировать основные функции и сценарии работы Perimetrix® SafeUse™, рассмотрим несколько примеров. Все представленные примеры рассматриваются в контексте общей концепции перемещений информации Perimetrix.

Пример 1. Пользователь Алексей Иванов, который занимается технологическими вопросами компании по всей территории России, открывает локальный файл Microsoft Word с описанием производства компании в городе Уфа (рис. 5).

Поскольку операция осуществляется в рамках одной рабочей станции, владельцем контейнера-источника, контейнера-приемника и инициатором действия выступает сам пользователь Алексей Иванов с допустимым уровнем по многомерной модели «Секретно/Россия/Технология». Алексей Иванов может получить доступ к файлу Ufa_Technology.doc, поскольку категория секретности файла «ДСП» (для служебного пользования) ниже, чем «Секретно» (категория секретности пользователя), а регион «Уфа» входит в регион «Россия».

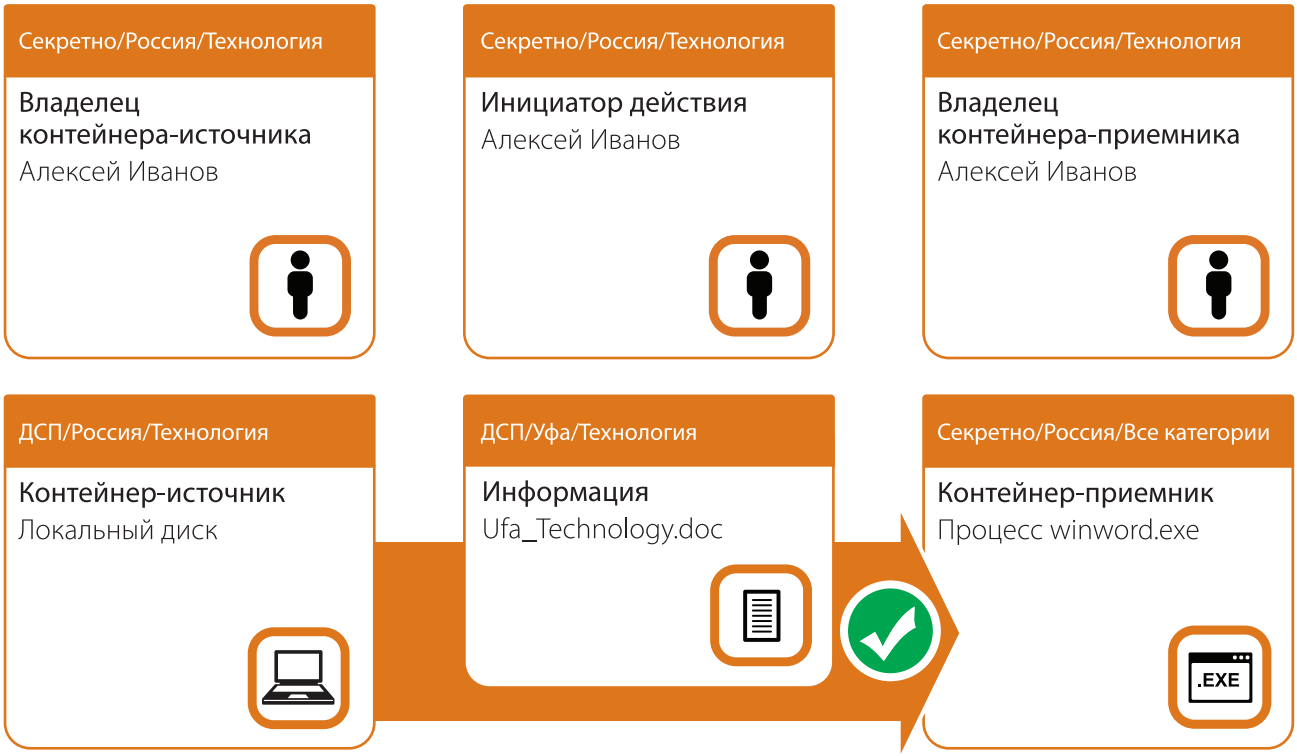

Рисунок 5. Открытие документа в приложении

PERIMETRIX®

Категория «Технология» и у пользователя, и у контейнера-источника совпадает. Таким образом, пользователь перемещает информацию с фактическим уровнем «ДСП/Уфа/Технология» по некоторому каналу в память процесса winword.exe. Последний имеет достаточно высокий допустимый уровень «Секретно/Россия/Все Категории», а потому перемещение легитимно и не блокируется.

Пример 2. Тот же самый пользователь Алексей Иванов открывает файл Ufa_Technology.doc в блокноте Windows (рис. 6).

Владельцем контейнера-источника, контейнера-приемника и инициатором действия выступает уже знакомый нам пользователь Алексей Иванов с допустимым уровнем «Секретно/Россия/Технология». Как и в предыдущем случае, Алексей Иванов может получить доступ к файлу Ufa_Technology.doc, однако не может открыть файл в блокноте, поскольку процесс notepad.exe не имеет заданных допустимых уровней. Другими словами, данный процесс не предназначен для обработки классифицированной информации, поэтому операция блокируется.

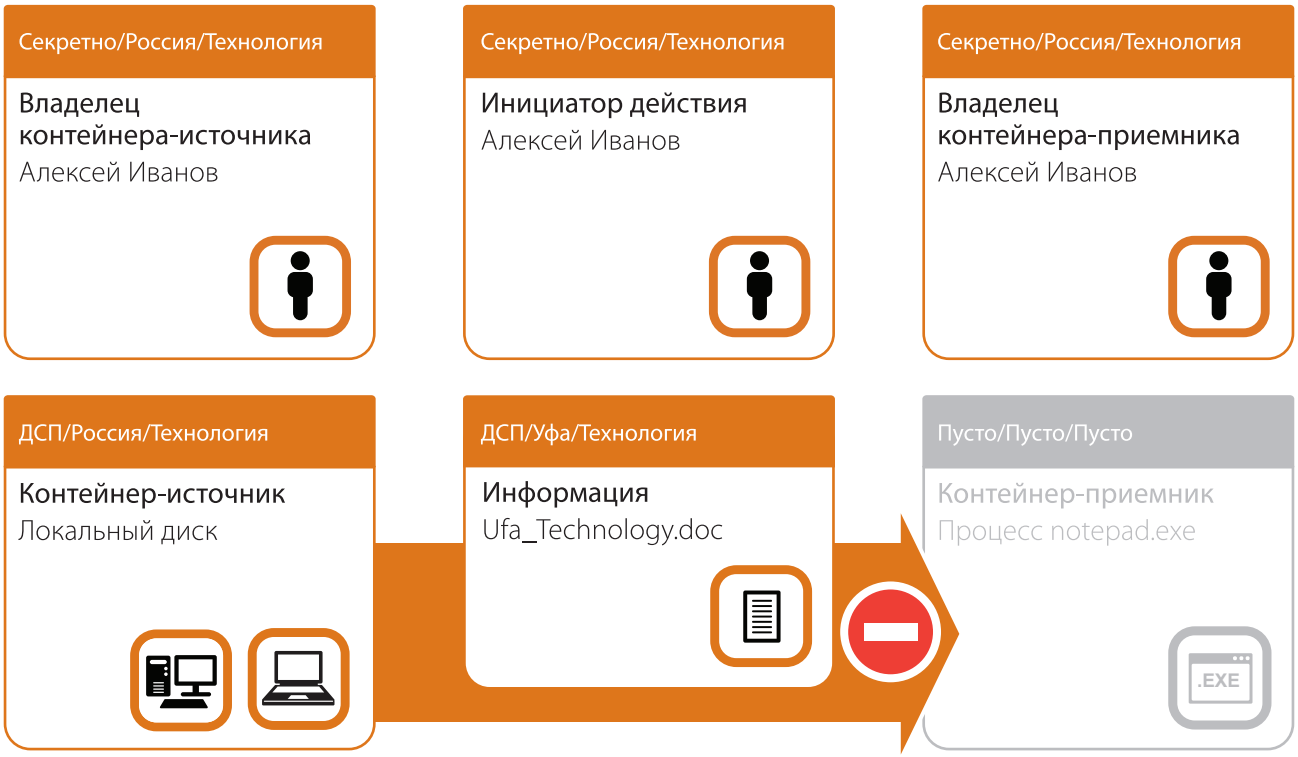

Рисунок 6. Блокировка открытия документа

PERIMETRIX®

Очевидно, что аналогичным образом блокируется перемещение файла в любой другой контейнер с более низким уровнем. Таким контейнером может быть незашифрованное дисковое пространство мобильного носителя или ноутбука, сетевой принтер и т.д.

Пример 3. Пользователь Алексей Иванов отправляет электронное письмо с файлом Ufa_Technology.doc другому пользователю Ивану Сидорову (рис. 7).

В данном примере владельцем контейнера-источника и инициатором действия по-прежнему выступает пользователь Алексей Иванов с допустимыми уровнями «Секретно/Россия/Технология». Владелец контейнера-приемника уже другой – пользователь Иван Сидоров. Фактический уровень информации в письме «ДСП/Уфа/Технология» соответствует правам Алексея Иванова, однако не входит в допустимые уровни контейнера-приемника и владельца контейнера-приемника, поскольку Иван Сидоров имеет доступ только к технологическим документам по московскому региону (а не по всей России). Таким образом, операция блокируется.

Рисунок 7. Отправка секретного документа по электронной почте

PERIMETRIX®

Пример 4. Пользователь Алексей Иванов пытается сохранить секретный файл Ufa_Tech_Plans.doc на локальном диске (рис. 8).

В последнем типовом примере все тот же пользователь Алексей Иванов пытается сохранить на локальном диске секретный файл Ufa_Tech_Plans.doc, который хранится на некотором файловом сервере. Данная операция разбивается на два этапа: на первом этапе он открывает документ в процессе winword.exe, а затем – пытается сохранить файл на локальном диске[2].

Первое действие аналогично первому примеру и потому легитимно. Алексей Иванов не может выполнить второго действия – сохранения файла на локальном диске – поскольку допустимый уровень данного контейнера «ДСП/Россия/Технология» не предусматривает хранения секретных файлов.

2 Прямое копирование файла в рамках универсальной модели принятия решений Perimetrix также разбивается на два перемещения. Первое перемещение – считывание информации в пямять некоторого копирующего процесса – аналогично открытию файла в редакторе Microsoft Word; второе перемещение – сохранение информации на диске – аналогично сохранению файла из Microsoft Word.

Рисунок 8. Запись секретного документа на небезопасный носитель

PERIMETRIX®

3.7. ИНТЕГРАЦИЯ SAFEUSE С ДРУГИМИ КОМПОНЕНТАМИ ПЛАТФОРМЫ PERIMETRIX® SAFESPACE™

Для того, чтобы обеспечить максимальную защиту от внутренних угроз необходима интеграция SafeUse с системами Perimetrix® SafeEdge™ и SafeStore.

Perimetrix® SafeUse™ в отрыве от остальных компонентов платформы Perimetrix относится к классу DLP-систем второго поколения. Для того, чтобы обеспечить максимальную защиту от внутренних угроз необходима интеграция SafeUse с системами Perimetrix® SafeEdge™[3] и SafeStore[4]. Такая интеграция реализована в комплексном решении Perimetrix® SafeSpace™ (см. рис. 1).

Взаимодействие с Perimetrix® SafeEdge™

В предыдущих разделах отмечалось, что основной проблемой DLP-систем второго поколения является сложность классификации (разметки) данных и поддержка этой разметки в актуальном состоянии. В рамках системы SafeUse эта проблема решается с помощью взаимодействия с SafeEdge.

Во-первых, при одновременном внедрении SafeUse и SafeEdge заказчику предоставляется функционал автоматической классификации данных в корпоративной сети. Тем самым, существенно упрощается процесс первичной классификации, а также поддержка классификации документов в актуальном состоянии, разметка новых и входящих документов.

Во-вторых, интеграция SafeEdge и SafeUse позволяет избежать утечек даже в том случае, если какой-то документ не успел пройти классификацию. Такая ситуация может возникнуть для входящих документов или файлов, создававшихся с «чистого листа». Контроль перемещений неразмеченных документов не может осуществлять в системе SafeUse и входит в сферу компетенции SafeEdge.

Другими словами, интеграция SafeUse и SafeEdge фактически обеспечивает двойной контроль над перемещениями информации. В некоторых случаях, механизмы контентной фильтрации SafeEdge позволяют найти ошибки классификации, повысив, тем самым, качество работы SafeUse.

3 Подробнее про Perimetrix® SafeEdge™ читайте в WhitePaper по Perimetrix® SafeEdge™
4 Подробнее про Perimetrix® SafeStore™ читайте в WhitePaper по Perimetrix® SafeStore™

PERIMETRIX®

Взаимодействие с Perimetrix® SafeStore™

Perimetrix® SafeStore™ обеспечивает шифрование документов на рабочих станциях, а также поддерживает зашифрованное хранилище классифицированных данных. Интеграция продуктов SafeUse и SafeStore позволяет привести процессы шифрования в соответствие с корпоративной политикой информационной безопасности.

Изолированная система SafeStore по сути является специальной средой для работы с хранилищем документов и шифрования данных на рабочих станциях. Однако SafeStore не определяет конфиденциальность документов и потому не может проконтролировать работу пользователей с ними. Именно поэтому интеграция SafeStore и SafeUse чрезвычайно важна – она предоставляет не только возможности шифрования пользовательских данных, но и средства контроля этих возможностей. В частности, взаимодействие SafeUse и SafeStore позволяет гарантировать хранение секретных данных только в зашифрованном виде, а также использование только зашифрованных носителей. Таким образом, обеспечивается непревзойденный уровень безопасности, соответствие национальным и международным нормативным актам, а также индустриальным стандартам.

3.8. ФУНДАМЕНТАЛЬНЫЕ ПРЕИМУЩЕСТВА PERIMETRIX® SAFEUSE™

Чтобы подвести черту к описанию основного функционала системы, приведем краткое концептуальное сравнение SafeUse с некоторыми классами продуктов, имеющих похожий функционал.

Аналог первый: DLP-системы первого поколения

Краткое описание функционала: система, фильтрующая трафик, идущий по сетевым каналам (SMTP, HTTP, IM), на предмет конфиденциальности.

Преимущество Perimetrix® SafeUse™: в отличие от DLP-систем первого поколения, которые по определению не могут давать точных результатов распознавания, SafeUse использует механизм меток и обеспечивает 100% защиту от утечек классифицированных документов. При этом, благодаря механизму наследования категорий SafeUse поддерживает разметку документов в актуальном состоянии.

Аналог второй: DLP-системы второго поколения

Краткое описание функционала: система, фильтрующая трафик с помощью заранее установленных меток.

Преимущество Perimetrix® SafeUse™: в отрыве от остальных компонентов платформы Perimetrix, SafeUse действительно является DLP-системой второго поколения. Однако в отличие от большинства аналогов, данная система способна проводить автоматическую классификацию новых и входящих документов (при условии одновременного внедрения с SafeEdge), а также поддерживать актуальность разметки, используя механизм наследования категорий. Кроме того, интеграционные возможности SafeUse позволяют строить на основе данной системы комплексные решения внутренней безопасности, которые обеспечивают защиту от всех видов утечек.

Аналог третий: системы контроля мандатного доступа

Краткое описание функционала: система, контролирующая доступ к ресурсам на базе сравнения метки ресурса и прав активного пользователя.

Преимущество Perimetrix® SafeUse™: система SafeUse обеспечивает более широкий функционал мандатного доступа, чем большинство доступных на рынке аналогов. Принцип работы большинства конкурирующих решений похож на железнодорожный шлагбаум – если доступ к ресурсу предоставлен, пользователь волен делать с ним все что угодно. Однако в Perimetrix® SafeUse™ работает полностью другая логика – система не только контролирует доступ, но и отслеживает все дальнейшие перемещения классифицированной информации. В дополнение SafeUse обеспечивает архивирование событий и пользовательской активности.

PERIMETRIX®

4. ТЕХНОЛОГИЧЕСКИЕ ПРЕИМУЩЕСТВА SAFEUSE

Главная особенность Perimetrix® SafeUse™ – 100% эффективность при работе с классифицированными данными – достигается за счет использования электронных меток.

Perimetrix® SafeUse™ обладает множеством уникальных возможностей, отличающих это решение от продуктов конкурентов. Главная особенность продукта – **100% эффективность при работе с классифицированными данными** – достигается за счет использования электронных меток. Отсюда же возникает и высокая скорость распознавания конфиденциальной информации.

Однако полагаться на одни лишь метки нельзя, поскольку в корпоративной среде присутствует и неклассифицированная информация. Благодаря интеграции SafeUse и SafeEdge заказчик получает дополнительные инструменты для работы с входящими или вновь созданными документами, классификация которых еще не проводилась. **Контентный анализ** подобных документов включает еще три метода – простейшую проверку совпадений по ключевым словам и фразам, анализ регулярных выражений, а также технологию цифровых отпечатков. Вместе с метками, эти методы позволяют добиться исключительно высокой точности распознавания – свыше 99%.

Еще одно конкурентное преимущество SafeUse заключается в полном **контроле над всеми операциями с конфиденциальными данными в рамках локальной рабочей станции**. Вне зависимости от того, куда (документ, программа, веб-форма и т.д.) и каким образом попадают эти данные, SafeUse будет знать, что это действительно секретные сведения. Соответственно, получатель тоже станет носителем конфиденциальной информации определенного класса, и на работу с ним будут наложены ограничения, предусмотренные политиками безопасности.

SafeUse контролирует любые устройства, подключенные к локальному компьютеру как через внешние, так и через внутренние порты. Система допускает детальное конфигурирование всех подключаемых устройств, различая их по множеству параметров, в том числе по заводскому идентификатору. Последнее обстоятельство позволяет индивидуально настраивать каждое устройство, каждый USB-накопитель в соответствии с политиками безопасности. Разумеется, можно ограничиться и групповыми политиками для быстрой настройки системы.

В отличие от конкурирующих продуктов, SafeUse осуществляет **динамический контроль портов и подключенных к ним устройств**. Вместо двух опций (блокировка включена/отключена) продукт обеспечивает доступ к устройствам в зависимости категории используемых данных. Например, при отсутствии открытых конфиденциальных документов или в зеленом режиме пользователь имеет возможность работать с любыми USB-накопителями. В случае переключения режима или

открытия конфиденциального документа SafeUse автоматически перекрывает доступ к неразрешенным носителям. Порт при этом функционирует в обычном порядке и пользователь может применять его для любого разрешенного устройства. Такой подход не накладывает ограничений на актуальные бизнес-процессы организации, обеспечивает надежную защиту, совместим с любыми устройствами, а также не обременяет офицера безопасности избыточными функциями регулирования доступа к портам в зависимости от производственной необходимости сотрудников.

Управление и настройка SafeUse и других продуктов линейки Perimetrix **централизованно осуществляется через веб-консоль**. С помощью механизмов разделения ролей администраторов и коллегиального принятия решений в продукте SafeUse реализована система защиты от сговора. Каждый пользователь имеет строго определенный круг обязанностей и полномочий с четко разграниченным доступом.

Все коммуникации в системе защищаются **при помощи стойкого крипто-алгоритма**, чем достигается защита от перехвата. **Агенты SafeUse не имеют ограничений по количеству защищаемых объектов** и отслеживают все операции, связанные с перемещением секретных данных.

Серверная часть SafeUse **реализована на платформе Java** и, таким образом, может работать под управлением любой совместимой операционной системы, в том числе Windows и Linux. SafeUse интегрируется со всеми распространенными базами данных, в том числе Miscrosoft SQL Server, Oracle Database, IBM DB2, PostgreSQL, Informix, Firebird и др. История действий пользователей, журналы обработки конфиденциальных данных сохраняются в удобной для пользователя базе данных и не налагают дополнительных ограничений.

Кроме того, кластерная архитектура сервисов SafeUse обеспечивает исключительную **масштабируемость решения**. Система будет расти с развитием компании. Если возрастает нагрузка, и текущая конфигурация не успевает обслуживать запросы от локальных агентов SafeUse, достаточно будет добавить в кластер свободный компьютер любой конфигурации. Благодаря технологии Perimetrix® Expansion™ система обеспечивает динамическое распределение не только нагрузки, но и функциональности. В результате достигается высочайший уровень бесперебойности работы для обслуживания активных бизнес-процессов организации без ущерба для защиты конфиденциальности данных.

PERIMETRIX®

5. ВЫВОДЫ

Продукт Perimetrix® SafeUse™ работает как с категоризированной, так и с некатегоризированной информацией, обеспечивая исключительно высокую точность фильтрации классифицированных данных.

Продукт Perimetrix® SafeUse™ работает как с категоризированной, так и с некатегоризированной информацией, обеспечивая исключительно высокую точность фильтрации классифицированных данных. Кроме того, SafeUse отличает полный контроль над процессами по перемещению конфиденциальной информации на рабочих станциях.

SafeUse вписывается в бизнес-ориентированную концепцию, заложенную для всех продуктов, входящих в состав Perimetrix® SafeSpace™. SafeUse не препятствует выполнению работниками своих основных обязанностей, но предотвращает утечки конфиденциальных данных.

Таким образом, Perimetrix® SafeUse™ может с успехом использоваться в качестве самостоятельного решения для защиты конфиденциальных данных от утечек. Однако синергия совместного применения компонентов SafeSpace существенно увеличивает эффективность как SafeUse, так и других продуктов линейки.

PERIMETRIX®

6. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Клиентская часть

- Любая рабочая станция под управлением ОС Microsoft Windows XP или VIsta. Требования к аппаратной части определяются операционной системой

Серверная часть

- Сервер с процессором Intel Pentium IV с частотой 3 GHz, оперативная память не менее 1 Gb
- Любая операционная система, поддерживающая JAVA.
- Java JRE 6.0 update 7 и выше

Сервер СУБД

- Любая СУБД с поддержкой Hibernate (Oracle, DB2, Sybase, MS SQL Server, PostgreSQL, MySQL и т.д.)

Различные сетевые сервисы могут быть развернуты как на одном физическом сервере, так и на нескольких. Выбор аппаратной части серверов и установка СУБД должны производиться по рекомендациям фирмы разработчика СУБД.

PERIMETRIX®

7. О КОМПАНИИ PERIMETRIX

Компания Perimetrix разрабатывает уникальные решения для реализации режима секретности конфиденциальности данных. В отличие от конкурентов Perimetrix концентрирует свой потенциал, инновационный подход и уникальный опыт на создании корпоративной платформы внутренней информационной безопасности и интеграции с актуальными бизнес-процессами, организационной и технологической инфраструктурой заказчика. Наша цель – повышение стоимости бизнеса заказчиков за счёт поддержания непрерывности бизнес-процессов, минимизации риска утечки, повышения конкурентоспособности, а также установления плодотворных отношений с инвесторами и партнерами, соответствия государственным требованиям.

Благодаря реализации революционной концепции Secret Documents Lifecycle™ Perimetrix обеспечивает защиту секретных документов на всех этапах жизненного цикла, мониторинг каналов коммуникаций и аудит электронных операций. Технологическая основа системы – знание объекта защиты, контроль доступа и действий пользователей с целью предотвращения нарушения корпоративной политики.

Компания основана в 2007 году командой профессионалов, стоявших у истоков создания современных систем защиты от внутренних угроз информационной безопасности, и входит в Группу компаний «КомпьюЛинк» – лидирующий альянс на российском рынке информационных технологий.

PERIMETRIX®

Штаб-квартира Perimetrix

Российская Федерация,
119607, Москва,
Мичуринский проспект, д. 45

Телефон: +7 495 737 99 91
Факс: +7 495 737 99 92

info@perimetrix.com
www.perimetrix.com

KEEPING SECRETS SAFE

PERIMETRIX®