WHITEPAPER

PERIMETRIX:

ПРОДУКТЫ И ТЕХНОЛОГИИ

KEEPING SECRETS SAFE

PERIMETRIX®

PERIMETRIX®

1. ВВОДНЫЕ

Топ-менеджмент ждет, пока на горизонте появится не только эффективное решение, но еще и такое, которое адресует всю проблему в комплексе, а не точечно.

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 осложняет взаимоотношения 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. В качестве примера подобных систем можно привести DLP-решения, базирующиеся на принципах контентной фильтрации. Обратимся к отчету Gartner «Hype Cycle for Information Security, 2007». В документе показано, что эффективность подобных систем составляет в лучшем случае не более 80%. И только при кропотливой предварительной работе по внедрению. В дополнение к этой цифре необходимо сказать о 20% пропущенных инцидентов и еще 20% ложных срабатываний. Последние чрезвычайно затруднят работу офицеров безопасности по расследованию инцидентов и внесут разногласия в отношения бизнес-пользователей и специалистов по информационной безопасности (ИБ).

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.

PERIMETRIX®

В результате компании считают неэффективным инвестировать средства в систему защиты от утечек. Во-первых, не понятно, за что платить, ведь потребность в обеспечении комплексной безопасности остаётся неудовлетворённой. Во-вторых, даже то, за что заплачено, завтра, с развитием технологий, появлением новых операционных систем, портативных устройств, средств хранения и коммуникации, может легко устареть. Такова неминуемая судьба любого неэффективного решения.

Для руководителей компаний является очевидным, что все перечисленные проблемы обусловлены незрелостью технологий защиты от утечек. Топ-менеджмент ждет, пока на горизонте появится не только эффективное решение, но еще и такое, которое адресует всю проблему в комплексе, а не точечно.

Именно таким продуктом является решение Perimetrix® SafeSpace™.

PERIMETRIX®

2. КОНЦЕПТУАЛЬНЫЙ ПОДХОД PERIMETRIX

В основе решения Perimetrix лежит несколько базовых концепций. Во-первых, это многомерная модель категорий. Во-вторых, это унифицированная модель принятия решений. И, в-третьих, это механизм наследования категорий при работе с классифицированными документами.

В основе решения Perimetrix лежит несколько базовых концепций, которые отличают коренным образом систему от конкурентов. Во-первых, это многомерная модель категорий, позволяющая исключительно точно классифицировать информацию. Во-вторых, это унифицированная модель принятия решений, единая для перемещения информации в пределах рабочей станции и по сети. И, наконец, в-третьих, это механизм наследования категорий при работе с классифицированными документами. Ниже мы кратко рассмотрим все эти концепции.

2.1. МНОГОМЕРНАЯ МОДЕЛЬ КАТЕГОРИЙ

В основе работы SafeUse лежит корпоративная политика безопасности. В системе защиты от утечек политика реализована как комплекс правил и настроек, которые определяют возможности доступа к данным. Сами данные разделены на онтологические категории, отражающие их содержание. Пользователи системы наделяются полномочиями – разрешениями работать с информацией определенных категорий. Помимо этого, доступ (разрешения хранить и/или обрабатывать информацию) к категориям настраивается для конкретных устройств и программ на компьютерах пользователей.

Деление на категории производится в соответствии с настроенной в системе моделью. В отличие от продуктов конкурентов, многомерная модель, которую использует Perimetrix, является настраиваемой, а потому может быть максимально приближена к реальности. Любые данные характеризуются множеством категорий, разнесенных по разнородным измерениям. Так, финансовый отчет фирмы «Пример» из города «Н» может быть описан категориями, принадлежащими следующим измерениям: «Функциональность», «Секретность», «География».

Представим, что измерение «Функциональность» имеет набор равнозначных категорий, например, «IT», «Финансы», «Развитие», «Кадры». Очевидно, рассматриваемый отчет относится к финансовым документам.

Измерение «секретность» может быть иерархическим, т.е. «Публичные документы» – «Для внутреннего использования» – «Строго конфиденциально». Пусть финансовый отчет имеет категорию «для внутреннего использования».

PERIMETRIX®

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

В результате финансовый отчет описывается трехмерной моделью категорий, состоящей из измерений «Финансы», «Для внутреннего использования», «Уфа». 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. На рис. 1 представлен некий документ и его возможная классификация в модели категорий Perimetrix. Совокупный набор категорий различных измерений называется уровнем, и является одним из ключевых понятий в системе принятия решений Perimetrix.

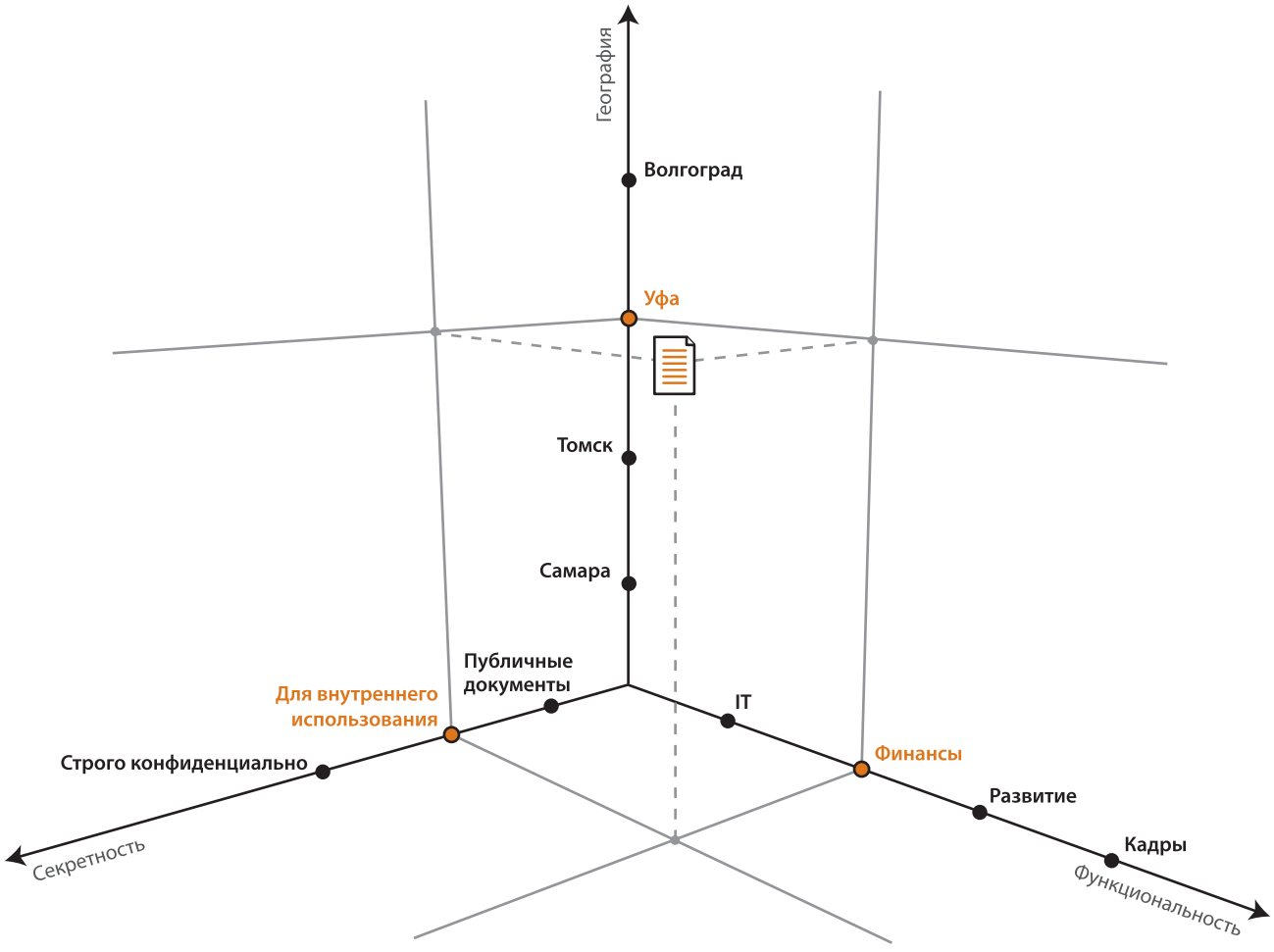

Рисунок 1. Графическое представление классификации конфиденциального документа в многомерной модели категорий

PERIMETRIX®

2.2. УНИВЕРСАЛЬНАЯ МОДЕЛЬ ПРИНЯТИЯ РЕШЕНИЙ

Часто вендоры используют различные подходы к мониторингу и защите информации на рабочих станциях и на шлюзе сети. Такой композитный метод легче реализовать на практике, однако он недостаточно эффективен. Поэтому Perimetrix разработал универсальную модель перемещения информации и систему принятия решений на ее основе.

Анализ конкурентных решений выявил, что компании используют различные подходы к мониторингу и защите информации на рабочих станциях и на шлюзе сети. Такой композитный метод легче реализовать на практике, однако он имеет ряд недостатков, связанных с эффективностью выявления конфиденциальных данных. Поэтому Perimetrix разработал универсальную модель перемещения информации и систему принятия решений на ее основе (см. рис. 2). Модель пригодна для защиты информации вне зависимости от того, где данные находятся.

В рамках рассматриваемой модели следует говорить о мониторинге перемещения информации. Именно на этом этапе может произойти утечка. Перемещение – во многом виртуальная конструкция. Однако именно такими типовыми перемещениями можно описать практически любой процесс, пересылку письма по электронной почте, копирование файлов на съемный носитель, открытие документа с помощью программы и др.

Рисунок 2. Универсальная модель перемещения информации Perimetrix

PERIMETRIX®

Задача системы Perimetrix – это мониторинг и блокировка нежелательных перемещений информации. Система получает информацию от различных компонентов и т.н. сенсоров. Все эти сенсоры (или датчики) являются поставщиками весьма разнородных данных. И первая цель – это привести все разнородные данные к понятиям единой модели.

В универсальной модели перемещения информации выделяют следующие составляющие. Контейнер-источник, физический носитель информации, находящейся в начальной точке. Владельцем контейнера-источника является некоторый пользователь. Когда этот или другой пользователь (инициатор перемещения) перемещает информацию по какому-то каналу, она попадает в контейнер-получатель, владельцем которого является третий пользователь (владелец контейнера-получателя). При перемещении информации в рамках рабочей станции, все три роли (владелец контейнера-источника, владелец контейнера-получателя и инициатор перемещения) обычно выполняет один пользователь. Все элементы универсальной модели обладают допустимыми уровнями – наборами категорий, к которым они имеют доступ. В свою очередь информация обладает фактическими уровнями – наборами действительных в данный момент категорий. При каждом перемещении информации система Perimetrix осуществляет проверку, входят ли фактические уровни в набор допустимых уровней контейнера-источника, контейнера-получателя и канала передачи. Кроме того, владельцы контейнеров и инициатор перемещения должны обладать правами на доступ к данным фактических уровней. И только если все условия выполняются, перемещение будет разрешено.

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 др.

Приведем несколько реальных примеров, как система принимает решения о предоставлении пользователю доступа к классифицированным данным.

PERIMETRIX®

Пример 1.
Пользователь открывает файл типа *.doc в MS Word (см. рис. 3).

Поскольку операция осуществляется в рамках одной рабочей станции, владельцем контейнера-источника, контейнера-получателя и инициатором перемещения выступает сам пользователь Сергей Иванов с допустимыми (максимальными разрешенными) уровнями по многомерной модели (Секретно/Россия/Технология). Сергей Иванов может получить доступ к файлу doc1.doc, поскольку степень секретности ДСП ниже, чем Секретно, а регион Красноярск входит в регион Россия. Категория Технология и у пользователя, и у контейнера-источника совпадает. Итак, пользователь перемещает информацию с актуальным уровнем (ДСП/Красноярск/Технология) по некоторому каналу в память процесса winword.exe. Последний также имеет допустимый уровень (ДСП/Красноярск/Технология), а потому перемещение легитимно и не блокируется.

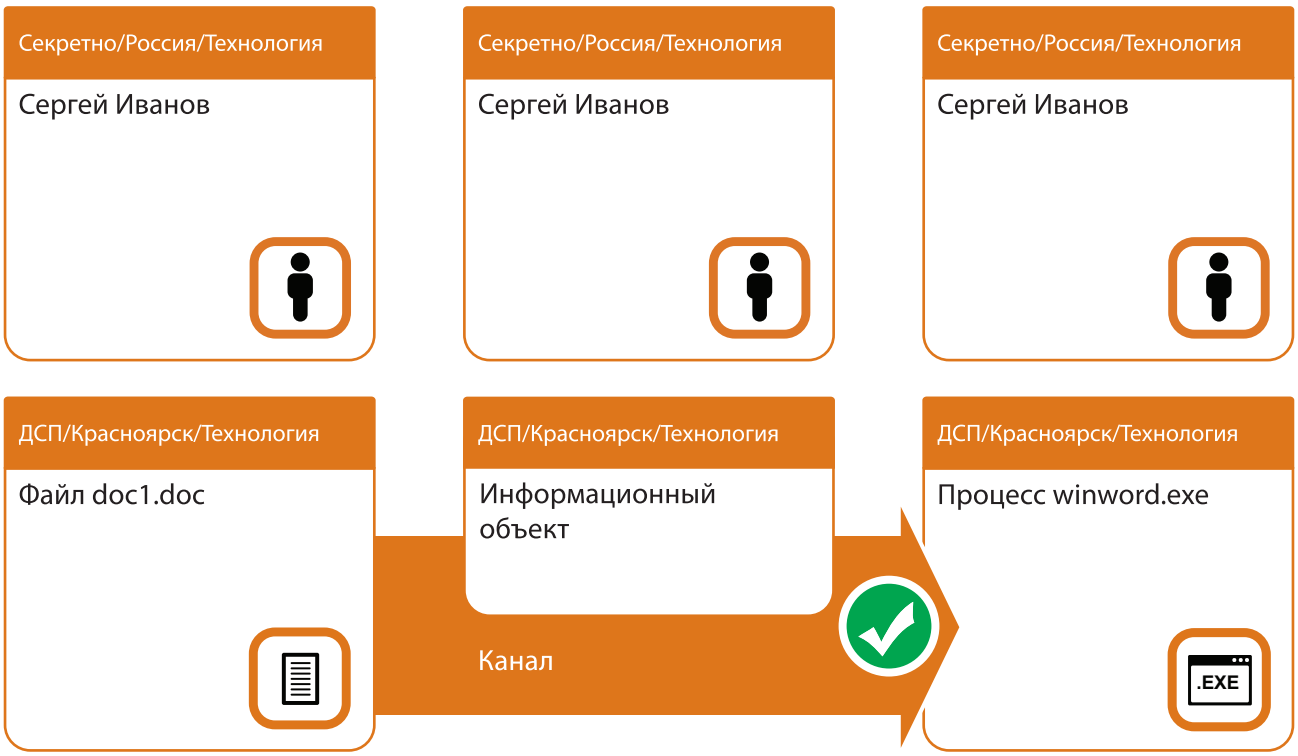

Рисунок 3. Пользователь открывает doc-файл с помощью MS Word

PERIMETRIX®

Пример 2.
Пользователь открывает файл типа *.doc в блокноте Windows (см. рис. 4).

Владельцем контейнера-источника, контейнера-получателя и инициатором перемещения выступает уже знакомый нам пользователь Сергей Иванов с допустимыми уровнями по многомерной модели (Секретно/Россия/Технология). Сергей Иванов может получить доступ к файлу doc1.doc, поскольку степень секретности ДСП ниже, чем Секретно, а регион Красноярск входит в регион Россия. Категория Технология и у пользователя, и у контейнера-источника совпадает. Итак, пользователь перемещает информацию с актуальным уровнем (ДСП/Красноярск/Технология) по некоторому каналу в память процесса notepad.exe. Однако последний не имеет заданных допустимых уровней, то есть не предназначен для хранения классифицированной информации, поэтому операция блокируется.

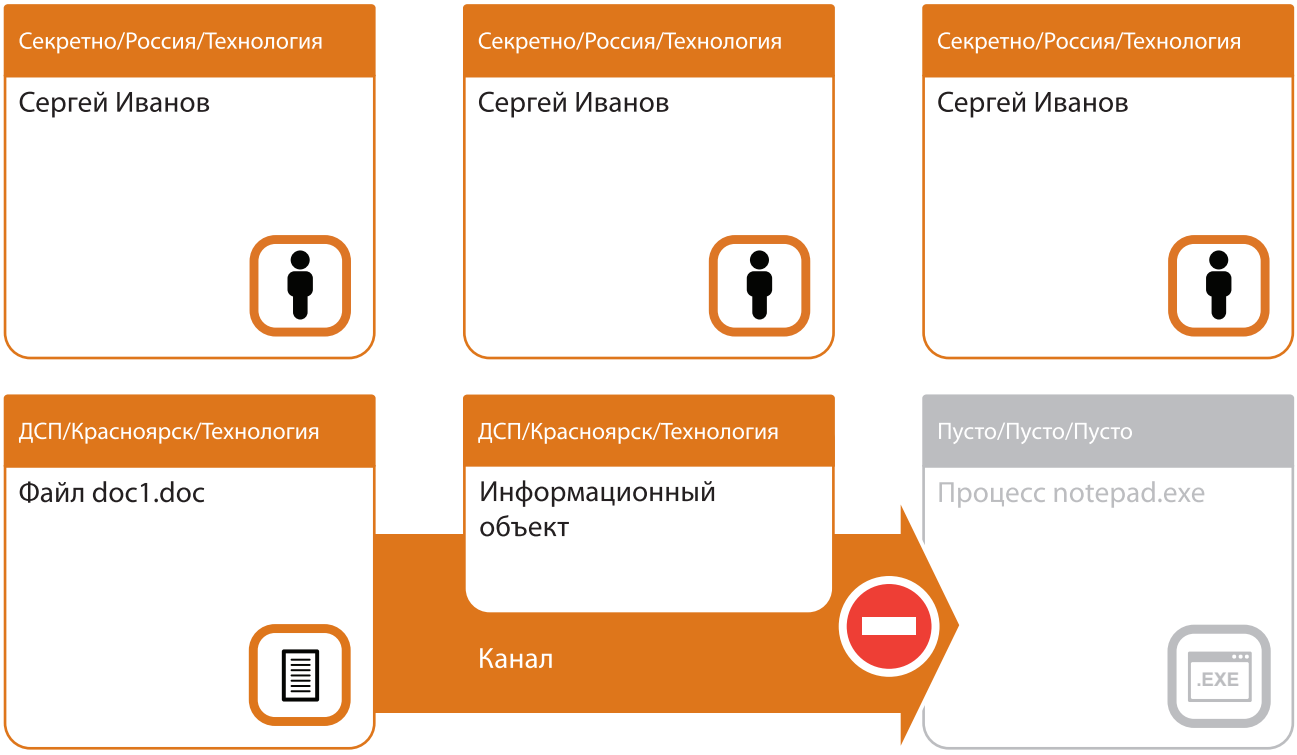

Рисунок 4. Пользователь не может открыть doc-файл с помощью блокнота Windows

PERIMETRIX®

Пример 3.
Пользователь копирует информацию из файла типа *.doc на флэшку (см. рис. 5).

Владельцем контейнера-источника, контейнера-получателя и инициатором перемещения выступает Сергей Иванов с допустимыми уровнями по многомерной модели (Секретно/Россия/Технология). Сергей Иванов может уже получил доступ к файлу doc1.doc и открыл его с помощью MS Word (см. Пример 1). Далее пользователь пытается переместить информацию с актуальным уровнем (ДСП/Красноярск/Технология) на флэш-носитель. Однако данный контейнер не достаточно хорош для хранения конфиденциальной информации и имеет максимально допустимые уровни (Не секретно/Красноярск/Технология). И если категории информации и контейнера Красноярск и Технология совпадают, то данные категории ДСП не могут быть помещены в контейнер с допустимой категорией Не секретно. Поэтому операция блокируется.

Рисунок 5. Пользователь не может скопировать информацию из doc-файла на флэшку

PERIMETRIX®

Пример 4.
Пользователь направляет письмо по электронной почте (см. рис. 6).

В данном примере владельцем контейнера-источника и инициатором перемещения выступает Сергей Иванов с допустимыми уровнями по многомерной модели (Секретно/Россия/Технология). Владелец контейнера-получателя уже другой – пользователь Сергей Петров. Актуальный уровень информации в письме (ДСП/Красноярск/Технология) соответствует правам Сергея Иванова, однако не входит в допустимые уровни контейнера-получателя и владельца контейнера-получателя. Так, корпоративная почта и Сергей Петров имеют допустимые уровни (Секретно/Москва/Технология). Но регион Москва не входит в регион Красноярск, поэтому операция блокируется.

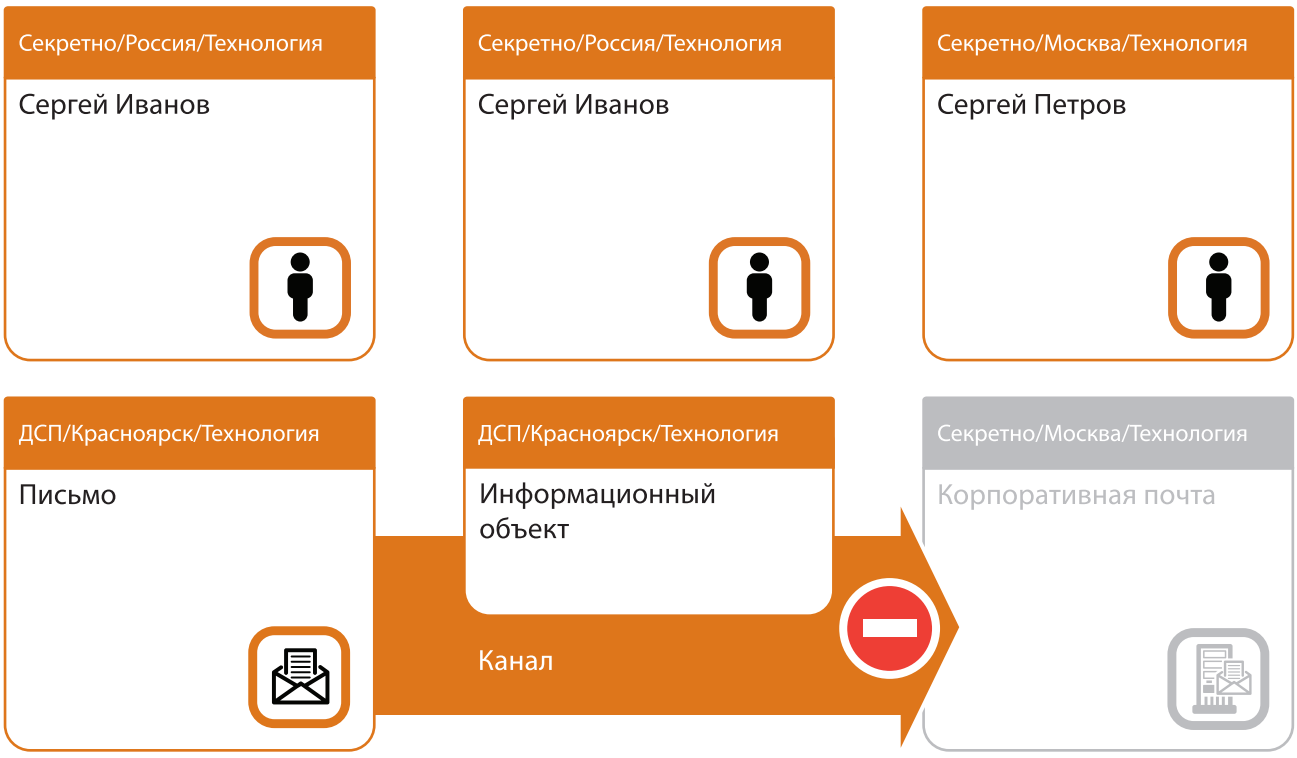

Рисунок 6. Пользователь не может переслать письмо коллеге по корпоративной почте

PERIMETRIX®

2.3. МЕХАНИЗМ НАСЛЕДОВАНИЯ УРОВНЕЙ КОНФИДЕНЦИАЛЬНОСТИ

При копировании данные из классифицированных документов не теряют своего уровня конфиденциальности, а переносят его в новый документ.

Работа с документами в корпоративной среде немыслима без использования разнородных данных из множества источников, как общедоступных, так и классифицированных. Возникает вопрос, каким образом можно защитить содержимое секретных контейнеров (например, документа, области памяти и т.д.), не отключая легитимным бизнес-пользователям доступа к ним? Для этого Perimetrix предлагает механизм наследования уровней конфиденциальности. При копировании данные из классифицированных документов (или других источников) не теряют своего уровня, а переносят его в новый документ (или другой тип контейнера). То есть копирование информации из классифицированного источника в буфер обмена сначала наделит буфер уровнями конфиденциальности этой информации. А затем перенесет те же уровни из буфера в конечный контейнер, например, какой-либо документ. Подобным образом происходит передача уровней конфиденциальности между любыми контейнерами информации в рамках универсальной модели событий. 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. **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.

PERIMETRIX®

3. ПРОДУКТОВАЯ ЛИНЕЙКА PERIMETRIX

Несмотря на то, что SafeStore, SafeUse и SafeEdge могут успешно применяться и по отдельности, целесообразно объединить все функции продуктов в рамках комплексного решения SafeSpace.

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 (см. рис. 7) входят три основных продукта, Perimetrix® SafeStore™, Perimetrix® SafeUse™, Perimetrix® SafeEdge™, а также ядро системы Perimetrix® ShadowCore™. Дополнительно система оснащается модулями (Network Exposal) NetEx и Enterprise Integration Server (EIS).

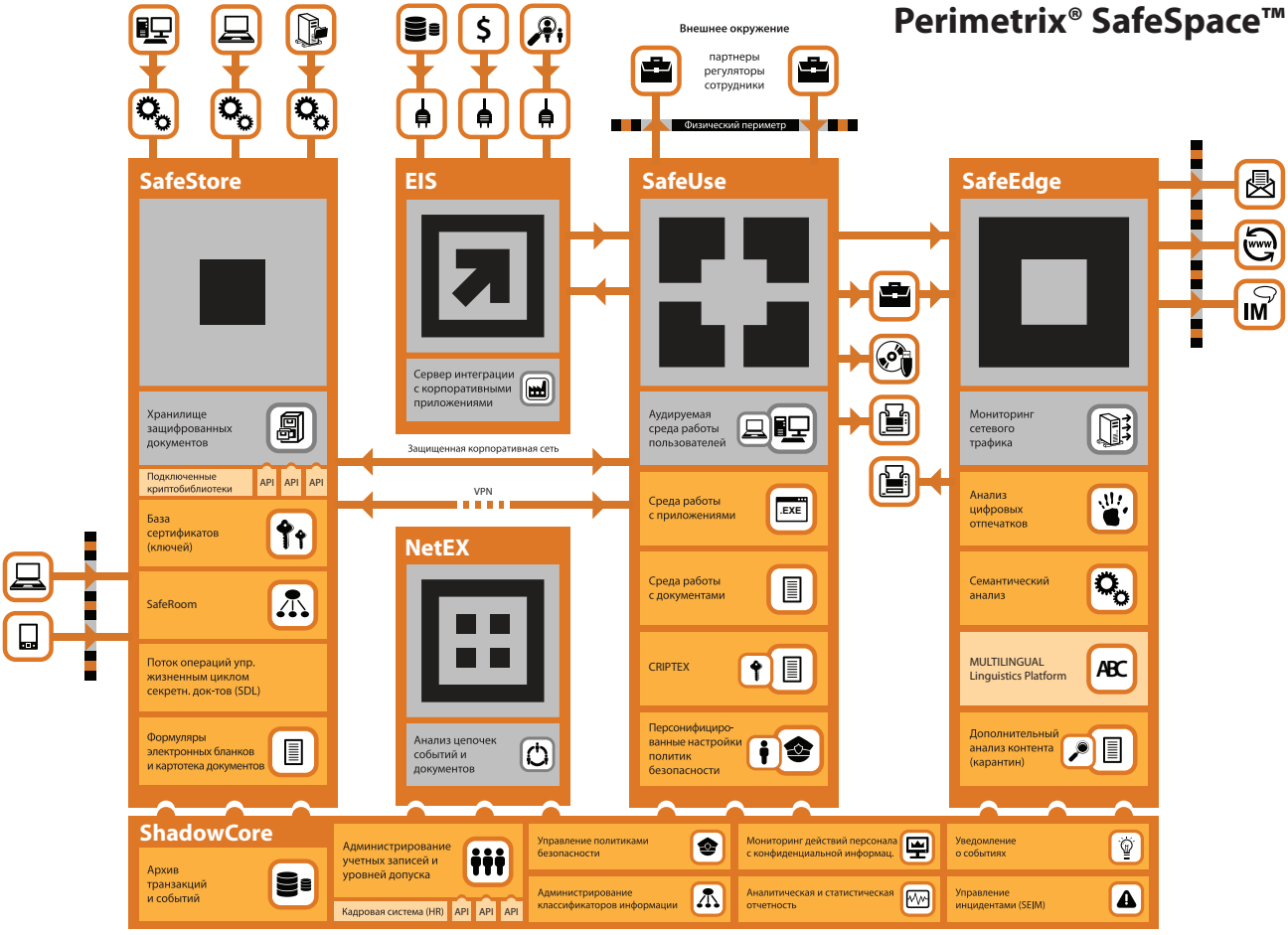

Рисунок 7. Функциональная схема Perimetrix® SafeSpace™

PERIMETRIX®

- С помощью Perimetrix® ShadowCore™ осуществляется администрирование режима секретности, в соответствии с политиками компании. Кроме того, ShadowCore включает архив действий пользователей при работе с конфиденциальной информацией 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 перенос секретных сведений в неклассифицированные 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. 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 категорий информации на уровне 99,6%.
- Network Exposal (NetEX) – модуль выявления и анализа скрытых зависимостей между конфиденциальными данными, связанными с ними событиями и сотрудниками компании. По сути – это уникальная система проактивного предотвращения утечек.
- Enterprise Integration Server (EIS) – сервер взаимодействия Perimetrix с гетерогенными корпоративными средами хранения и обработки данных (RDBMS, системами класса ERP, CRM, HRMS, PLM и проч.). Данный модуль позволяет системе защиты от инсайдеров пронизывать всю технологическую инфраструктуру организации и лучше защищать от утечек.

PERIMETRIX®

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.

Тем не менее, при внедрении системы необходимо понимать цели, которые стоят перед подразделениями ИБ. Внедрение и обслуживание различных модулей сильно отличается по трудоемкости. Если SafeEdge можно назвать шлюзовым решением, которое может быть интегрировано в корпоративную информационную систему относительно просто и безболезненно, то установка агентов SafeUse вряд ли обойдет стороной бизнес-процессы организации. В этом случае потребуется выполнить и значительную подготовительную работу. А именно:

- разработать матрицу классификации. Т.е. определить измерения и категории для каждого измерения в рамках многомерной модели;
- дать описания контейнеров (файлов, процессов, сетевых ресурсов и т.д.). Кроме того, необходимо будет задать допустимые уровни для приложений, определить стационарные метки для сетевых ресурсов (например, БД), а также классифицировать файлы;
- дать описания полномочий пользователей. В том числе необходимо задать допустимые уровни информации, к которым у пользователей есть доступ.

PERIMETRIX®

4. ЧТО ДЕЛАЕТ PERIMETRIX УНИКАЛЬНЫМ

- Perimetrix® SafeSpace™ предлагает единый унифицированный подход к мониторингу рабочих станций и сетевого периметра.
- Perimetrix® SafeSpace™ использует вероятностные (морфологический анализ, анализ цифровых отпечатков) и детерминистские (электронная разметка) методы для выявления классифицированной информации.
- Perimetrix® SafeSpace™ блокирует доступ к портам и устройствам только при попытке совершения неправомочной операции. Система не мешает пользователям выполнять основные служебные обязанности.
- Серверная часть Perimetrix® SafeSpace™ является платформонезависимой, работает с большим количеством операционных систем (поскольку модули написаны на java) и с множеством баз данных (благодаря применению методов Hibernate).
- Серверная часть Perimetrix® SafeSpace™ состоит из набора балансируемых сервисов, работающих на узлах кластера. Для системы не принципиально, на каких именно узлах размещены сервисы. Кроме того, сама система может запускать сервисы на различных узлах, в зависимости от их загрузки. В результате система отличается высокой надежностью и легко масштабируется в широких пределах.

PERIMETRIX®

5. ЗАКЛЮЧЕНИЕ

Важной особенностью SafeSpace является и то, что использование комплекса не нарушает существующие бизнес-процессы организации и не препятствует выполнению сотрудниками основных обязанностей.

Perimetrix® SafeSpace™ обладает множеством уникальных возможностей. Прежде всего, это 100% эффективность при работе с классифицированными данными, что достигается за счет использования электронных меток. Отсюда – и высокая скорость распознавания классифицированной информации. Однако SafeSpace работает и с неклассифицированными данными. Поэтому в арсенале решения имеются технологии морфологического анализа, анализа по цифровым отпечаткам, а также методика контекстного анализа. В сочетании эти методы позволяют добиться исключительно высокой точности распознавания – свыше 99%.

Важной особенностью SafeSpace является и то, что использование комплекса не нарушает существующие бизнес-процессы организации и не препятствует выполнению сотрудниками основных обязанностей. В то же время система чутко следит за соблюдением политик безопасности.

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

Кроме того, кластерная архитектура сервисов SafeSpace обеспечивает исключительную масштабируемость решения. Система будет расти с развитием компании. Если возрастает нагрузка, и текущая конфигурация не успевает обслуживать запросы от локальных агентов или сетевых сервисов, достаточно будет добавить в кластер свободный компьютер. Благодаря технологии Perimetrix® Expansion™ система обеспечивает динамическое распределение не только нагрузки, но и функциональности. Даже в случае выхода из строя одного или нескольких компьютеров кластера их функции будут оперативно распределены между другими. В результате достигается высочайший уровень бесперебойности работы для обслуживания активных бизнес-процессов организации без ущерба для защиты конфиденциальности данных.

PERIMETRIX®

4. 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®