WHITEPAPER

PERIMETRIX® SAFESTORE™

ЗАЩИТА ДАННЫХ ВО ВРЕМЯ ХРАНЕНИЯ

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® SafeStore™.

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.

PERIMETRIX®

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® SAFESTORE™

3.1. SAFESTORE В СТРУКТУРЕ SAFESPACE

SafeStore представляет собой централизованное хранилище зашифрованных документов с регламентированным доступом.

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.

3.2. СХЕМА PERIMETRIX® SAFESTORE™

Заказчик получает максимальный функционал локальной части только при одновременном внедрении SafeStore и SafeUse.

Perimetrix® SafeStore™ можно разделить на серверную и локальные части. Серверная часть продукта представляет собой централизованную базу конфиденциальных документов, которые хранятся в зашифрованном виде. Локальная часть отвечает за процессы, связанные с шифрованием на локальных носителях данных – десктопах и ноутбуках, мобильных накопителях, портативных или оптических дисках.

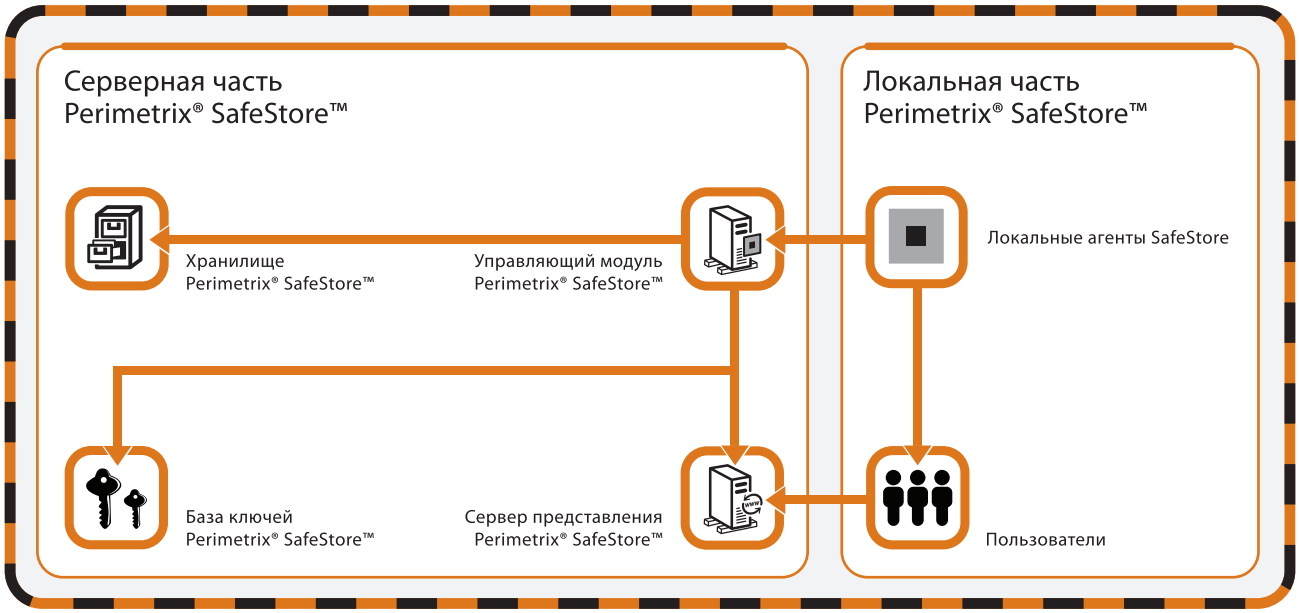

Рисунок 1. Схема Perimetrix® SafeStore™

PERIMETRIX®

Отметим, что локальная часть SafeStore реализована в виде специального приложения, которое интегрируется с агентом Perimetrix® SafeUse™. Таким образом, заказчик получает максимальный функционал локальной части только при одновременном внедрении SafeStore и SafeUse.

Основная задача серверной части Perimetrix® SafeStore™ – это поддержка защищенной базы классифицированных[1] документов и обеспечение работы пользователей с ними. По сути, SafeStore является защищенной средой для работы с конфиденциальными сведениями. Показательным аналогом SafeStore можно считать специально оборудованные помещения для работы государственной тайной, которые создавались в режимных предприятиях советских времен.

Однако хранить все конфиденциальные документы в защищенной базе данных на практике слишком неудобно, особенно в условиях мобильного бизнеса. Во-первых, это негативно сказывается на производительности: скорость работы с документами в базе через шлюз всегда ниже локальной скорости работы. И, во-вторых, такой подход снижает доступность данных. Часто у сотрудников возникает необходимость удаленного доступа к конфиденциальным документам в отсутствии доступа к хранилищу. Например, работа с документами дома или на презентации у клиентов.

Для устранения этих недостатков была создана локальная часть Perimetrix® SafeStore™. Она позволяет не только шифровать данные по запросу от пользователей, но и гарантировать локальное хранение документов заданного уровня секретности только в зашифрованном виде в соответствии с корпоративной политикой информационной безопасности. Таким образом, риски утечки конфиденциальной информации вследствие кражи (потери) тех или иных носителей данных практически полностью исчезают.

1 Подробнее про классификацию документов читайте в WhitePaper по системе Perimetrix® SafeUse™

PERIMETRIX®

3.3. ПОНЯТИЕ КРИПТЕКСА. ИСПОЛЬЗОВАНИЕ КРИПТЕКСОВ В PERIMETRIX® SAFESTORE™

С точки зрения пользователя, криптексы ничем не отличаются от обычных незашифрованных архивов.

Ключевым понятием, определяющим механизмы локального хранения данных в Perimetrix® SafeStore™, является «криптоконтейнер» или «криптекс». Криптекс представляет собой зашифрованный файл, который содержит один или несколько классифицированных документов. Простейшим аналогом криптекса является классический файловый архив, использующий шифрование заархивированных данных.

Главное отличие криптексов от таких архивов заключается в специальном механизме расшифровки. Для извлечения зашифрованных файлов из архива, пользователю требуется вручную ввести ключ (или пароль), что автоматически означает ряд проблем. В частности, при достаточно большом количестве архивов пользователю приходится либо запоминать внушительное количество ключей, либо использовать один и тот же ключ, тем самым снижая безопасность информации.

В случае с криптексами расшифровка документов происходит с помощью ключей, которые хранятся в централизованной базе. Таким образом, обеспечивается защита документов в случае кражи или потери носителя, поскольку их новые владельцы не смогут получить доступ к ключам для расшифровки. При этом сам пользователь не испытывает затруднений при работе с зашифрованными документами, поскольку ключи извлекаются в автоматическом режиме и без его непосредственного участия. С точки зрения пользователя, криптексы ничем не отличаются от обычных незашифрованных архивов. Подобная прозрачность бизнес-логики продукта позволяет достичь с одной стороны исключительно высокого комфорта работы, а с другой – максимального уровня защиты.

Важно отметить, что криптекс также является файлом, а значит – он может обладать каким-то набором категорий конфиденциальности (уровнем) в рамках продукта Perimetrix® SafeUse™. Все перемещения криптекса в корпоративной среде регулируются этими категориями в стандартном режиме. Однако для открытия (расшифровки) криптекса система использует другой набор категорий, который задается уже в рамках Perimetrix® SafeStore™ и определяется конфиденциальностью файлов, хранящихся внутри криптекса. Чтобы открыть криптекс, уровень пользователя должен быть как минимум не ниже уровней всех внутренних файлов.

PERIMETRIX®

Другими словами, каждый криптекс обладает сразу двумя уровнями конфиденциальности, которые могут отличаться друг от друга. **Уровень криптекса в SafeUse** контролирует операции с криптексом, как с защищенным файлом, а его **уровень в SafeStore** контролирует процессы открытия и расшифровки криптекса. Такой подход позволяет хранить криптекс в незащищенных местах и в то же время контролировать доступ к нему на основе общих прав пользователей в соответствии с корпоративной политикой информационной безопасности.

В продукте Perimetrix® SafeStore™ криптексы выполняют две основные задачи. Прежде всего, они являются безопасными контейнерами для хранения конфиденциальных документов на незащищенных носителях – таких как ноутбуки или мобильные накопители. Тем самым, обеспечивается защита информации от утечки в случае кражи или потери того или иного носителя.

Во-вторых, криптексы являются основой централизованного хранилища Perimetrix® SafeStore™. Все документы защищенной базы хранятся и передаются исключительно в виде криптексов. Таким образом, обеспечивается безопасность самого хранилища, а также коммуникационных каналов между хранилищем и пользователем.

3.4. ЦЕНТРАЛИЗОВАННОЕ ХРАНИЛИЩЕ PERIMETRIX® SAFESTORE™

Главной особенностью хранилища SafeStore является возможность построения защищенной среды работы с конфиденциальными данными.

Централизованное хранилище Perimetrix® SafeStore™ состоит из четырех компонентов:

- База данных (хранилище) классифицированных документов. Документы хранятся в зашифрованном виде (в виде криптексов).
- База ключей для расшифровки документов из хранилища. Ключи также хранятся в зашифрованном виде;
- Управляющий модуль SafeStore, который обеспечивает взаимодействие между всеми компонентами системы;
- Сервер представления, предназначенный для организации взаимодействия пользователей с хранилищем.

Таким образом, Perimetrix® SafeStore™ предполагает раздельное хранение зашифрованных документов и ключей к ним. Это означает, что доступ к отдельной базе данных окажется практически бесполезным для злоумышленника. Получив доступ к базе документов, он не сможет их расшифровать, а получив доступ к базе ключей – использовать их для расшифровки документов.

PERIMETRIX®

Но даже если злоумышленник получит доступ к обоим хранилищам, это вовсе не повлечет утечки данных. Ключи для документов также хранятся в зашифрованном виде, и для их расшифровки требуется программный или аппаратный токен, который используется администратором системы в момент запуска хранилища SafeStore. Другими словами, Perimetrix® SafeStore™ обеспечивает максимальную защиту зашифрованных документов от несанкционированного доступа извне, а также позволяет избежать проблем в случае физической кражи хранилища или его резервной копии.

Доступ пользователей к хранилищу SafeStore осуществляется только с помощью веб-интерфейса и только по защищенным каналам связи. Такой подход избавляет организацию от проблем, связанных с установкой дополнительных локальных приложений, и позволяет пользователям безопасно работать с хранилищем из любой точки земного шара.

Являясь составной частью Perimetrix® SafeSpace™, хранилище SafeStore поддерживает все механизмы контроля доступа, заложенные общей концепцией продуктов Perimetrix. Поскольку все документы хранилища классифицированы, SafeStore способен контролировать доступ пользователей к ним. Заходя на веб-интерфейс, пользователь увидит только те документы, уровень конфиденциальности которых не превышает допустимый уровень самого пользователя.

Однако главной особенностью хранилища SafeStore является возможность построения защищенной среды работы с конфиденциальными данными. Хранилище предоставляет пользователю все необходимые инструменты для решения этой задачи. Такими инструментами, в частности, являются:

- Создание новых документов с определенным набором категорий;
- Отправка заявок на просмотр файлов, к которым в данный момент у пользователя нет доступа;
- Отправка заявок на изменение категорий тех или иных классифицированных документов, а также допустимых категорий пользователя;
- Использование персональных папок внутри хранилища;
- Поиск по формальным атрибутам документов: их типу, названию, размеру и присвоенным категориям;
- Контентный поиск по содержимому документов – все документы хранилища индексируются;
- И другие функции защиты конфиденциальных данных.

PERIMETRIX®

Другими словами, работа с хранилищем Perimetrix® SafeStore™ во многом аналогична процессу работы с бумажными документами в режимных предприятиях классического типа. Благодаря такому подходу, система обеспечивает непревзойденный уровень безопасности классифицированных документов в хранилище, который сочетается с высоким уровнем доступности.

Добавим, что все действия пользователей с защищенным хранилищем фиксируются в базе данных Perimetrix® ShadowCore™. Таким образом, служба безопасности может провести ретроспективный анализ истории действий с защищенным документом, начиная с момента его создания.

В качестве основы для создания защищенного хранилища может использоваться практически любая промышленная СУБД. Все криптопровайдеры, используемые в Perimetrix® SafeStore™, разрабатываются сторонними компаниями и имеют все необходимые лицензии и сертификаты.

3.5. ЛОКАЛЬНАЯ РАБОТА С КРИПТЕКСАМИ. ПРОЗРАЧНОЕ ШИФРОВАНИЕ ДАННЫХ НА РАБОЧЕЙ СТАНЦИИ

С точки зрения пользователя, разделы прозрачного шифрования ничем не отличаются от дополнительного локального диска.

Рассмотрим криптекс, который располагается на локальной рабочей станции. Какие действия может выполнить пользователь с этим криптексом?

Бизнес-логика системы подразумевает три базовых действия: пользователь может открыть криптекс, извлечь из него файлы и записать новые файлы. Отметим, что открытие криптекса является необходимым условием для остальных действий. Оно легитимно в тех и только тех случаях, когда уровни криптекса в системах SafeUse и SafeStore не превышают допустимый уровень пользователя.

Чтобы просмотреть или изменить файл, этот файл должен быть извлечен из криптекса и записан в файловой системе. Это означает, что для локальной работы с секретными документами на диске должна быть создана безопасная среда, в которую будут записываться конфиденциальные документы из криптексов. В Perimetrix® SafeStore™ такой средой являются разделы прозрачного шифрования.

PERIMETRIX®

С точки зрения пользователя, разделы прозрачного шифрования ничем не отличаются от дополнительного локального диска. Работа с документами в разделах прозрачного шифрования аналогична работе с обычными документами – для их расшифровки, система извлекает ключи из удаленной базы в незаметном для пользователя режиме. В случае кражи носителя связь с этой базой теряется, и, тем самым, гарантируется безопасность документов.

Система Perimetrix® SafeUse™ воспринимает раздел прозрачного шифрования, как контейнер с определенным набором категорий. Работа пользователя с этим разделом контролируется на базе стандартных политик SafeUse и ничем не отличается от работы с другими контейнерами.

Добавим, что все действия пользователей с защищенным хранилищем фиксируются в базе данных Perimetrix® ShadowCore™. Таким образом, служба безопасности может провести ретроспективный анализ истории действий с защищенным документом, начиная с момента его создания:

1. Пользователь заходит на сервер представления хранилища и находит нужный документ;
2. Пользователь загружает документ на рабочую станцию в виде криптекса;
3. Пользователь открывает криптекс;
4. Пользователь извлекает документ из криптекса в раздел прозрачного шифрования;
5. Пользователь открывает документ в авторизованном приложении.

3.6. ТИПОВЫЕ СЦЕНАРИИ РАБОТЫ PERIMETRIX® SAFESTORE™

Чтобы проиллюстрировать основные функции и сценарии работы Perimetrix® SafeStore™, рассмотрим несколько типичных примеров. Во всех примерах предполагается, что в организации была проведена классификация документов и внедрено не только решение Perimetrix® SafeStore™, но и система Perimetrix® SafeUse™.

Все представленные примеры рассматриваются в рамках общей концепции перемещений информации Perimetrix[2].

2 Подробнее об этой концепции читайте в WhitePaper по системе Perimetrix® SafeUse™ и в документе «Perimetrix: продукты и технологии»

PERIMETRIX®

Пример 1. Некий пользователь Алексей Иванов запрашивает конфиденциальный файл в хранилище Perimetrix® SafeStore™ и скачивает его на свой ноутбук в виде криптекса.

Представим, что пользователь Алексей Иванов заходит на сервер представления хранилища, осуществляет поиск и находит нужный ему файл Ufa_Technology.doc с уровнем конфиденциальности «ДСП/Уфа/Технология». Алексей Иванов сумеет увидеть этот документ в хранилище, поскольку уровень конфиденциальности документа ниже допустимого уровня пользователя («Секретно/Россия/Технология»). Для того чтобы прочитать документ, ему необходимо скачать его на свою рабочую станцию в виде криптекса (рис. 2).

Таким образом, продукт формирует криптекс из одного документа и отправляет его на локальный жесткий диск. Уровень криптекса в Perimetrix® SafeStore™ совпадает с уровнем внутреннего файла

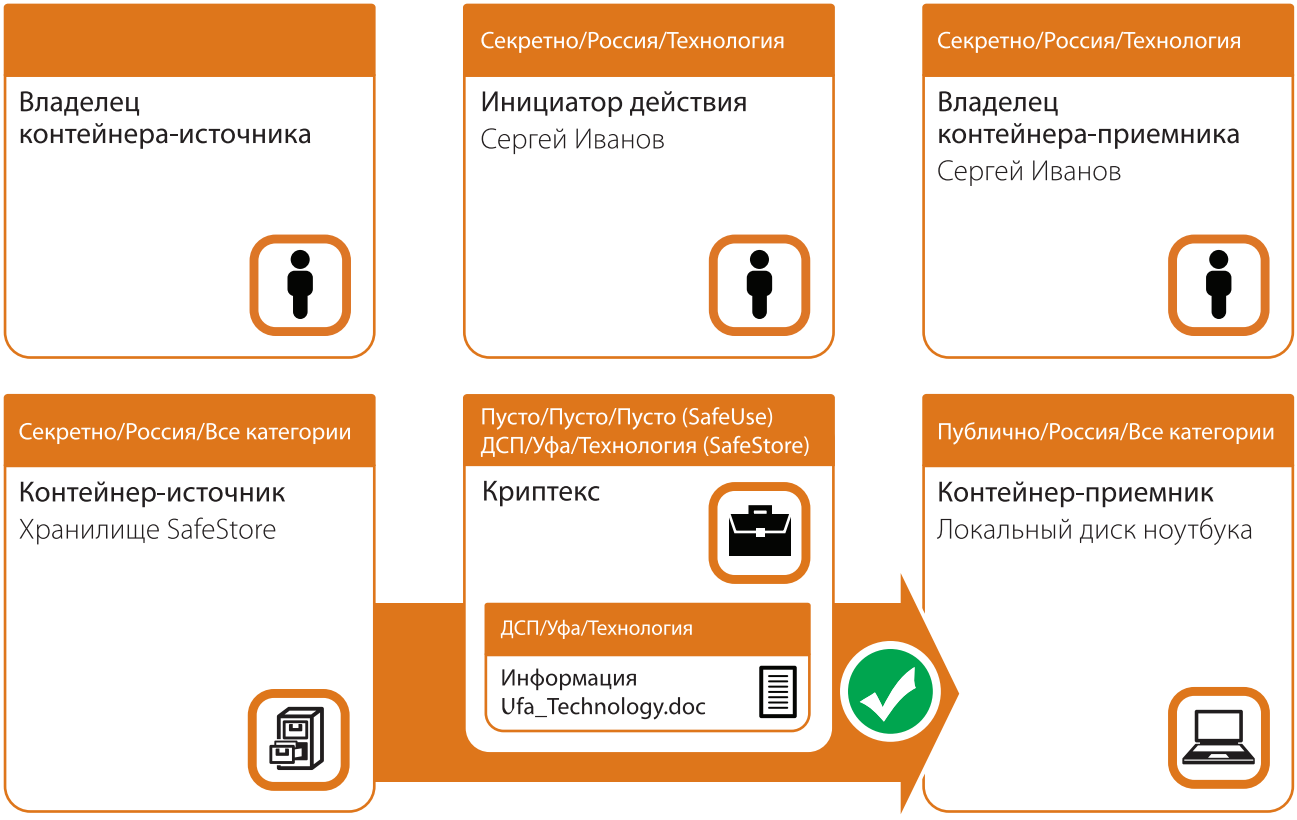

Рисунок 2. Доставка криптекса из хранилища

PERIMETRIX®

(«ДСП/Уфа/Технология»), а его уровень в системе SafeUse по умолчанию не определен. Как следствие, локальный агент SafeUse разрешает сохранить криптекс на жестком диске, даже несмотря на то, что уровень диска предусматривает хранение только публичных документов, а в криптексе лежит файл категории «ДСП».

Пример 2. Пользователь пытается извлечь документ из криптекса.

Сохранив криптекс на диске, пользователь Алексей Иванов решил просмотреть содержимое документа. Чтобы сделать это, он должен выполнить три микрооперации: открыть криптекс, сохранить файл из него в файловой системе и непосредственно открыть этот файл с помощью приложения. Последняя микрооперация не связана с SafeStore и контролируется стандартными средствами Perimetrix® SafeUse™.

Первое действие – открытие криптекса (рис. 3) – в данном случае легитимно, поскольку допустимый уровень пользователя превышает уровни криптекса как в SafeUse, так и в SafeStore. Таким образом, пользователь получает ключ для расшифровки криптекса и доступ к файлу Ufa_Technology.doc

Чтобы выполнить второе действие – сохранение файла на диске – пользователь должен выбрать раздел с достаточно высоким допустимым уровнем. В данном случае корпоративная политика информационной безопасности разрешает хранить в шифрованном разделе файлы с категорией «ДСП» (рис. 4), а в незашифрованном разделе – только публичные файлы (рис. 5). Таким образом, Алексею Иванову приходится извлекать файл только в раздел прозрачного шифрования. В противном случае операция будет заблокирована.

Рисунок 3. Открытие криптекса

PERIMETRIX®

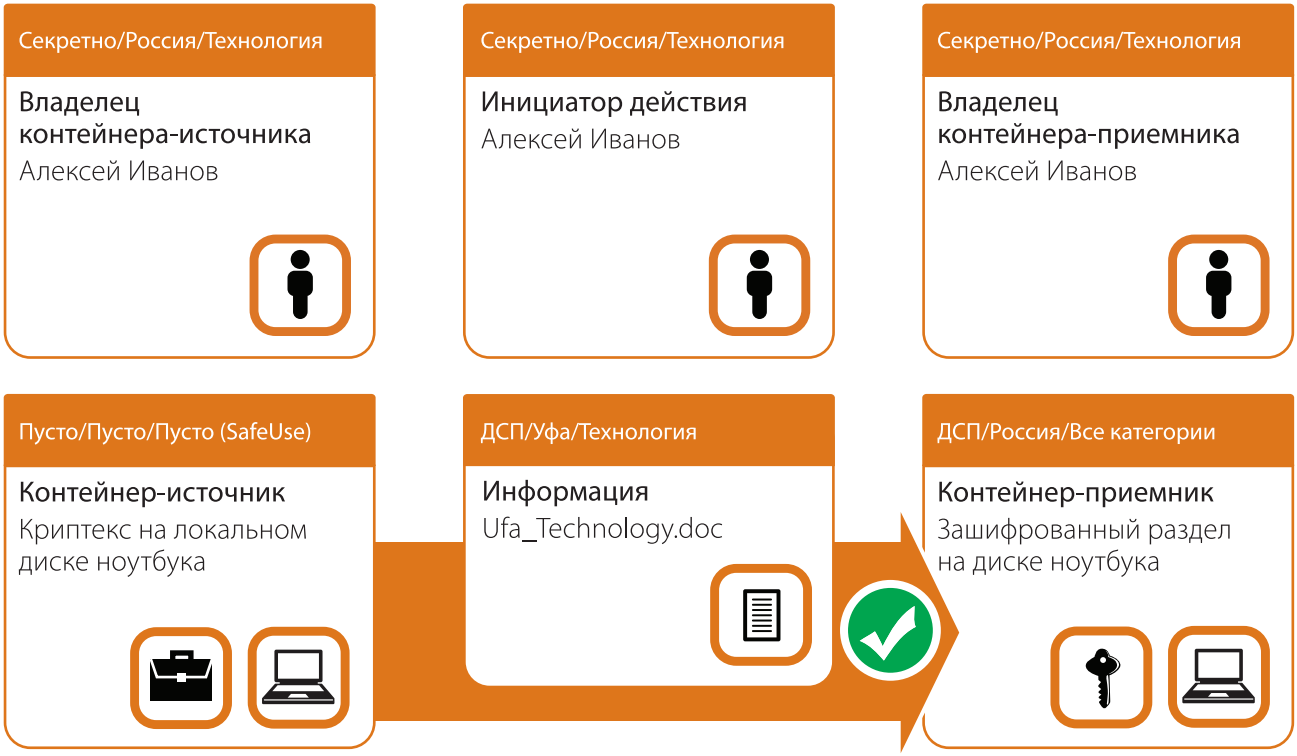

Рисунок 4. Запись файла в зашифрованный раздел

Рисунок 5. Запись файла в незашифрованный раздел

PERIMETRIX®

Пример 3. Пользователь добавляет новый конфиденциальный документ в криптекс.

Пользователь Алексей Иванов создал на основе исходного документа новый документ Ufa_Technology_New.doc, который автоматически унаследовал категории конфиденциальности исходного файла («ДСП/Уфа/Технология»). После завершения редактирования, Алексей Иванов решил добавить новый файл в криптекс, который был создан при скачивании исходного файла (рис. 6).

Как и в случае примера 2, данное действие разбивается на две микрооперации – сначала открывается криптекс (уровень Алексея Иванова позволяет это сделать), а потом в него дописывается новый файл. Отметим, что в конфиденциальность добавляемых файлов не имеет значения – пользователь может дописать любой файл, при условии наличия доступа к этому файлу и самому криптексу. После добавления новых файлов, уровень криптекса в SafeStore может автоматически повыситься.

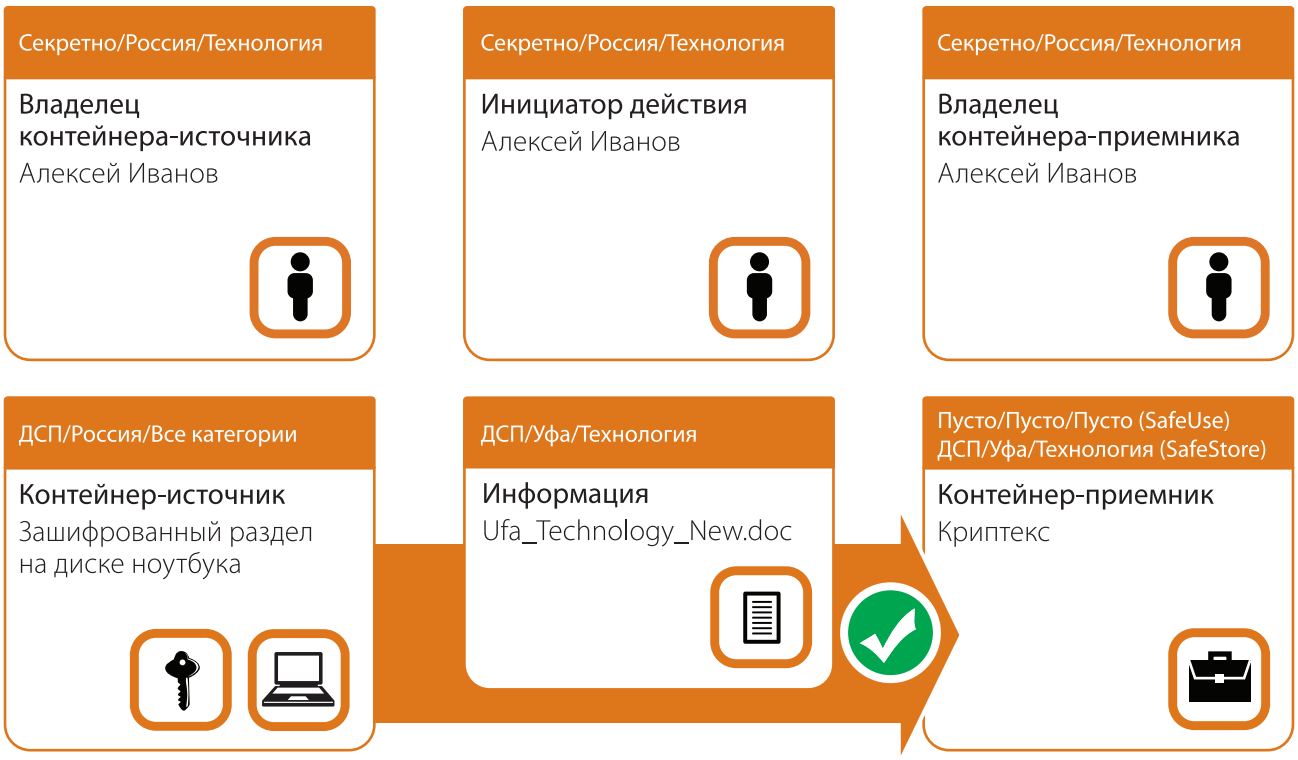

Рисунок 6. Пользователь добавляет новый конфиденциальный документ в криптекс

PERIMETRIX®

3.7. ФУНДАМЕНТАЛЬНЫЕ ПРЕИМУЩЕСТВА PERIMETRIX® SAFESTORE™

Perimetrix® SafeStore™ (в комплексе с SafeUse) обеспечивает форсированное шифрование классифицированных документов независимо от воли и желания пользователей.

Чтобы подвести черту к описанию основного функционала системы, приведем краткое концептуальное сравнение SafeStore с некоторыми классами продуктов, имеющих похожий функционал. В данном случае мы сознательно избегаем слова «конкурентов», поскольку прямых аналогов SafeStore на рынке просто не существует.

Аналог первый: системы электронного документооборота (СЭД)

Краткое описание функционала: система, обеспечивающая процессы создания, обеспечения доступа и распространения электронных документов в корпоративных сетях, контроль потоков документов и совместную работу пользователей.

Преимущества Perimetrix® SafeStore™: хранилище SafeStore не является системой документооборота, а всего лишь предоставляет защищенную среду для работы с классифицированными данными. Основная задача SafeStore лежит в области защиты, а не в области эффективной совместной работы или достижения максимального уровня доступности документов. С точки зрения безопасности SafeStore контролирует не только доступ к файлам (как большинство СЭД), но и дальнейшую работу пользователей с ними. Тем самым, система минимизирует риски утечки классифицированных данных вследствие действий авторизованных пользователей.

Аналог второй: классические системы шифрования

Краткое описание функционала: система, обеспечивающая шифрование и расшифровку документов на основе неких криптографических алгоритмов.

Преимущества Perimetrix® SafeStore™: в классических криптографических системах «богом» является пользователь, которые самостоятельно шифрует данные и расшифровывает их. Такие продукты способны обеспечить безопасность только тогда, когда все пользователи кристально честны и никогда не допускают ошибок. В отличие от них Perimetrix® SafeStore™ (в комплексе с SafeUse) обеспечивает форсированное шифрование классифицированных документов независимо от воли и желания пользователей. При этом используются стандартные криптографические алгоритмы, которые реализованы производителями тех же систем классического шифрования.

PERIMETRIX®

Аналог третий: системы прозрачного шифрования

Краткое описание функционала: система, обеспечивающая работу пользователей с зашифрованными документами в прозрачном (незаметном) режиме.

Преимущества Perimetrix® SafeStore™: при грамотном внедрении, системы прозрачного шифрования защищают компании от угрозы «потерянного ноутбука». Например, с помощью технологии Microsoft EFS можно зашифровать жесткие диски всех носителей внутри компании. Однако все подобные системы не могут определить конфиденциальность документов и проконтролировать работу пользователей с ними. Пользователь компьютера с EFS легко расшифрует документ и скопирует его на мобильный носитель, спровоцировав, тем самым, утечку.

В этом смысле, системы прозрачного шифрования мало чем отличаются от классических криптосистем – они также основаны на парадигме честного и безошибочного пользователя. Perimetrix® SafeStore™ использует обратный посыл и защищает компанию от халатности собственных сотрудников.

PERIMETRIX®

4. ТЕХНОЛОГИЧЕСКИЕ ПРЕИМУЩЕСТВА SAFESTORE

Все действия пользователей в централизованном хранилище и с криптексами протоколируются в централизованной базе транзакций и событий Perimetrix® ShadowCore™.

Perimetrix® SafeStore™ предоставляет заказчикам два основных преимущества. Во-первых, централизованное хранилище классифицированных документов позволяет создать **по-настоящему защищенную рабочую среду**. Во-вторых, локальный модуль SafeStore – защищает от утечек информации **в результате кражи** ноутбуков, мобильных носителей и других устройств.

Централизованное хранилище Perimetrix® SafeStore™ **консолидирует хранение** конфиденциальных документов. Таким образом, существенно упрощается управление этими документами, а также процесс обеспечения их физической безопасности.

Все классифицированные документы в базе Perimetrix® SafeStore™ **хранятся в зашифрованном виде** с использованием стойких алгоритмов шифрования сторонних производителей. Расшифровка этих документов без ключей и за приемлемое время технически невозможна.

Зашифрованные документы **хранятся отдельно** от зашифрованных же ключей к ним. Такой подход позволяет избежать проблем в случае физической кражи хранилища, базы ключей к нему или обоих серверов одновременно.

Работа с каждым документом централизованного хранилища происходит в рамках **глобальных политик Perimetrix® SafeSpace™**. В результате обеспечивается максимальная защита от несанкционированного доступа на основе уровней конфиденциальности.

В случае санкционированного доступа, работа пользователя с **централизованным хранилищем также контролируется системой** на основе стандартных политик. В веб-интерфейсе хранилища, пользователь увидит только те документы, уровень конфиденциальности которых не превышает допустимый уровень самого пользователя.

Шифрование данных на локальных носителях (ноутбуках, десктопах, мобильных накопителях и др.) производится **в прозрачном для пользователя режиме**. Для расшифровки локальных зашифрованных документов система использует ключи из единой централизованной базы. С точки зрения пользователя, работа с разделом прозрачного шифрования ничем не отличается от работы с обычными файлами.

Благодаря технологиям прозрачного шифрования и криптексов, Perimetrix® SafeStore™ может гарантировать локальное хранение се-

PERIMETRIX®

кретных документов **только в зашифрованном виде**. Это означает, что организация полностью покрывает риски безопасности, связанные с кражей носителей, содержащих конфиденциальные данные.

Все действия пользователей в централизованном хранилище и с криптексами **протоколируются** в централизованной базе транзакций и событий Perimetrix® ShadowCore™. Это означает, что служба безопасности может провести рестроспективный анализ истории действий с защищенным документом, начиная с момента его создания.

Управление и настройка SafeStore и других продуктов линейки Perimetrix **централизованно осуществляется через веб-консоль**. С помощью механизма разделения ролей администраторов и коллегиального принятия решений, в продукте SafeStore 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.

Серверная часть SafeStore **реализована на платформе Java** и, таким образом, может работать под управлением любой совместимой операционной системы, в том числе Windows, Unix и Linux. В качестве технологической базы для создания хранилища SafeStore могут использоваться все распространенные промышленные СУБД, в том числе Miscrosoft SQL Server, Oracle Database, IBM DB2, PostgreSQL и др. Вся информация сохраняются в удобной для пользователя базе данных и не налагает дополнительных ограничений.

Кластерная архитектура сервисов SafeStore обеспечивает исключительную **масштабируемость решения**. Система будет расти с развитием компании. В случае роста нагрузки, достаточно добавить в кластер свободный компьютер любой конфигурации. Кроме того, уникальная технология Perimetrix® Expansion™ обеспечивает динамическое распределение не только вычислительных мощностей, но и функциональности системы. В результате достигается высочайший уровень бесперебойности работы для обслуживания активных бизнес-процессов организации без ущерба для защиты конфиденциальности данных.

PERIMETRIX®

5. ВЫВОДЫ

В отличие от конкурирующих продуктов, SafeStore способен обеспечить гарантированное шифрование классифицированных данных на всех локальных носителях.

Perimetrix® SafeStore™ является важнейшим элементом платформы SafeSpace и позволяет максимально покрыть риски утечки данных вследствие кражи мобильных и стационарных носителей. Эта проблема является достаточно серьезной – по данным исследования Ponemon Institute «Airport Insecurity: The Case of Lost Laptops» только в крупнейших аэропортах США ежегодно теряется 637 тыс. ноутбуков, свыше половины из которых (53%) содержат корпоративную конфиденциальную информацию.

Такие мероприятия, как, например, пароль на вход в операционную систему, не могут серьезно рассматриваться в качестве средств безопасности, потому что легко обходятся даже неискушенными пользователями. Только стойкое шифрование чувствительных данных может исключить утечку в случае потери или кражи ноутбука или другого компьютерного устройства. В отличие от конкурирующих продуктов, SafeStore способен обеспечить гарантированное шифрование классифицированных данных на всех локальных носителях.

Вторым важнейшим преимуществом SafeStore является защищенное хранилище – первая по-настоящему защищенная среда работы с секретными документами. Благодаря хранилищу SafeStore, организация консолидирует расходы на защиту конфиденциальных документов, а также достигает совместимости с отраслевыми, национальными и международными нормативными актами.

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

PERIMETRIX®

6. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Локальная часть

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

- Криптопровайдер с поддержкой Microsoft CryptoAPI. Тестировались КриптоПро CSP 3.0 (отвечает требованиям законодательства РФ, имеет все необходимые лицензии и сертификаты ФСБ и ФСТЭК), а также Microsoft Enhanced Cryptographic Provider (входит в комплект поставки Microsoft Windows XP/Vista).

Серверная часть

- Любой сервер стандартной архитектуры. Тестировалось на сервере с процессором Intel 3,6 ГГц и оперативной памятью 1 Гб.

- Любая операционная система с поддержкой JAVA. Тестировалось на ОС OpenSuse 11.0.

- Java JRE 6.0 update 7 и выше

- Криптопровайдер с поддержкой Java Cryptography Architecture (JCA). Тестировались криптопровайдеры КриптоПро JCP 1.0 (отвечает требованиям законодательства РФ, имеет все необходимые лицензии и сертификаты ФСБ и ФСТЭК), Bouncy Castle (бесплатный криптопровайдер с открытым исходным кодом, поддержку оказывает компания Lock Box Labs) и встроенные в JRE криптопровайдеры Sun (поддержка в рамках поддержки JRE).

- Любая СУБД с поддержкой Hibernate (Oracle, DB2, Sybase, MS SQL Server, PostgreSQL, MySQL и т.д.). Тестировалось на Oracle Database 11g.

Сервисы Perimetrix® SafeStore™ могут функционировать на различных физических серверах. Выбор аппаратной части серверов и установка СУБД производятся по рекомендациям фирмы разработчика СУБД, а также на базе прогнозируемых размеров хранилища.

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®