



PERIMETRIX® SAFEEDGE™

ЗАЩИТА ДАННЫХ В ДВИЖЕНИИ

KEEPING SECRETS SAFE





1. ВВОДНЫЕ

2. ЭВОЛЮЦИЯ ПОДХОДОВ К ЗАЩИТЕ ДАННЫХ

- 2.1. ПРИЧИНЫ НЕУДАЧ
- 2.2. ВЧЕРАШНИЙ ДЕНЬ НЕЗРЕЛЫХ ТЕХНОЛОГИЙ
- 2.3. РЕВОЛЮЦИОННАЯ КОНЦЕПЦИЯ SECRET DOCUMENTS LIFECYCLE™

3. ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ PERIMETRIX® SAFEEDGE™

- 3.1. SAFEEDGE В СТРУКТУРЕ SAFESPACE
- 3.2. СХЕМА PERIMETRIX® SAFEEDGE™
- 3.3. ТЕХНОЛОГИИ ФИЛЬТРАЦИИ ТРАФИКА В PERIMETRIX® SAFEEDGE™
- 3.4. ИНТЕГРАЦИЯ SAFEEDGE И SAFEUSE.
АВТОМАТИЧЕСКАЯ КЛАССИФИКАЦИЯ (ИНВЕНТАРИЗАЦИЯ) ДАННЫХ
- 3.5. ПОДДЕРЖКА ПРОТОКОЛОВ, ФАЙЛОВЫХ ФОРМАТОВ И ЯЗЫКОВ
- 3.6. ТИПОВЫЕ СЦЕНАРИИ РАБОТЫ PERIMETRIX® SAFEEDGE™
- 3.7. ФУНДАМЕНТАЛЬНЫЕ ПРЕИМУЩЕСТВА PERIMETRIX® SAFEEDGE™

4. ТЕХНОЛОГИЧЕСКИЕ ПРЕИМУЩЕСТВА SAFEEDGE

5. ВЫВОДЫ

6. СИСТЕМНЫЕ ТРЕБОВАНИЯ

7. О КОМПАНИИ 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, приобретенная 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® SafeEdge™.



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.



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™.

3. ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ PERIMETRIX® SAFEEDGE™

3.1. SAFEEDGE В СТРУКТУРЕ SAFESPACE

SafeEdge перехватывает, фильтрует, а также проводит автоматическую классификацию исходящего трафика.

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.

Если классифицированная порция данных (например, сообщение, отправленное через ICQ) не соответствует корпоративной политике ИТ-безопасности, то действие будет заблокировано, а офицер ИТ-безопасности извещен об инциденте. SafeEdge использует сразу несколько методик классификации и анализа, чтобы обеспечить максимально высокую точность фильтрации.



Рисунок 1. Платформа решений 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.

3.2. СХЕМА PERIMETRIX® SAFEEDGE™

Perimetrix® SafeEdge™ анализирует исходящий сетевой трафик и автоматически принимает решение о его блокировке в том случае, если он нарушает политику безопасности компании.

Изолированная система Perimetrix® SafeEdge™ является классическим решением класса DLP первого поколения. Она позволяет производить вероятностный анализ (контентную фильтрацию) данных, передаваемых по основным сетевым каналам – веб-протоколам (HTTP, FTP, IM) и электронной почте (SMTP). В том случае, если исходящий трафик противоречит корпоративной политике безопасности (например, выполняется попытка передачи конфиденциальных данных), его пересылка блокируется.

Perimetrix SafeEdge состоит из следующих компонентов (сервисов):

- **Перехватчики трафика** (HTTP, SMTP, ICQ) отправляют потоки исходящего трафика на сервис экстракции текста.
- **Сервис экстракции текста** извлекает файлы из общего потока информации, определяет их язык и кодировку и выделяет из них «чистый» текст (plain text). Этот текст отправляется на сервис контентной фильтрации.
- **Сервисы контентной фильтрации** анализируют полученный текст, используя преднастроенную лингвистическую базу, а также базу цифровых отпечатков. Результаты анализа (оценка уровня конфиденциальности текста) отправляются на сервис принятия решений.
- **Сервис принятия решений** выносит вердикт о блокировке исходящего трафика или его дальнейшем прохождении. Вердикт выносится на основе политик безопасности, формальных атрибутов трафика (размер, формат файла, время и т.п.) и результатов контентного анализа.
- В **централизованный архив** Perimetrix® SafeEdge™ могут попадать теневые копии всех исходящих документов или только тех документов, которые нарушают политику безопасности (в зависимости от настроек).
- Наконец, **web-консоль управления** SafeEdge служит для определения всех настроек, формализации требований политики безопасности, контроля работы системы и мониторинга событий. Библиотеки лингвистической фильтрации, а также настройки снятия цифровых отпечатков также задаются с помощью данной консоли.

Таким образом, Perimetrix® SafeEdge™ анализирует исходящий сетевой трафик и автоматически принимает решение о его блокировке в том случае, если он нарушает политику безопасности компании.

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

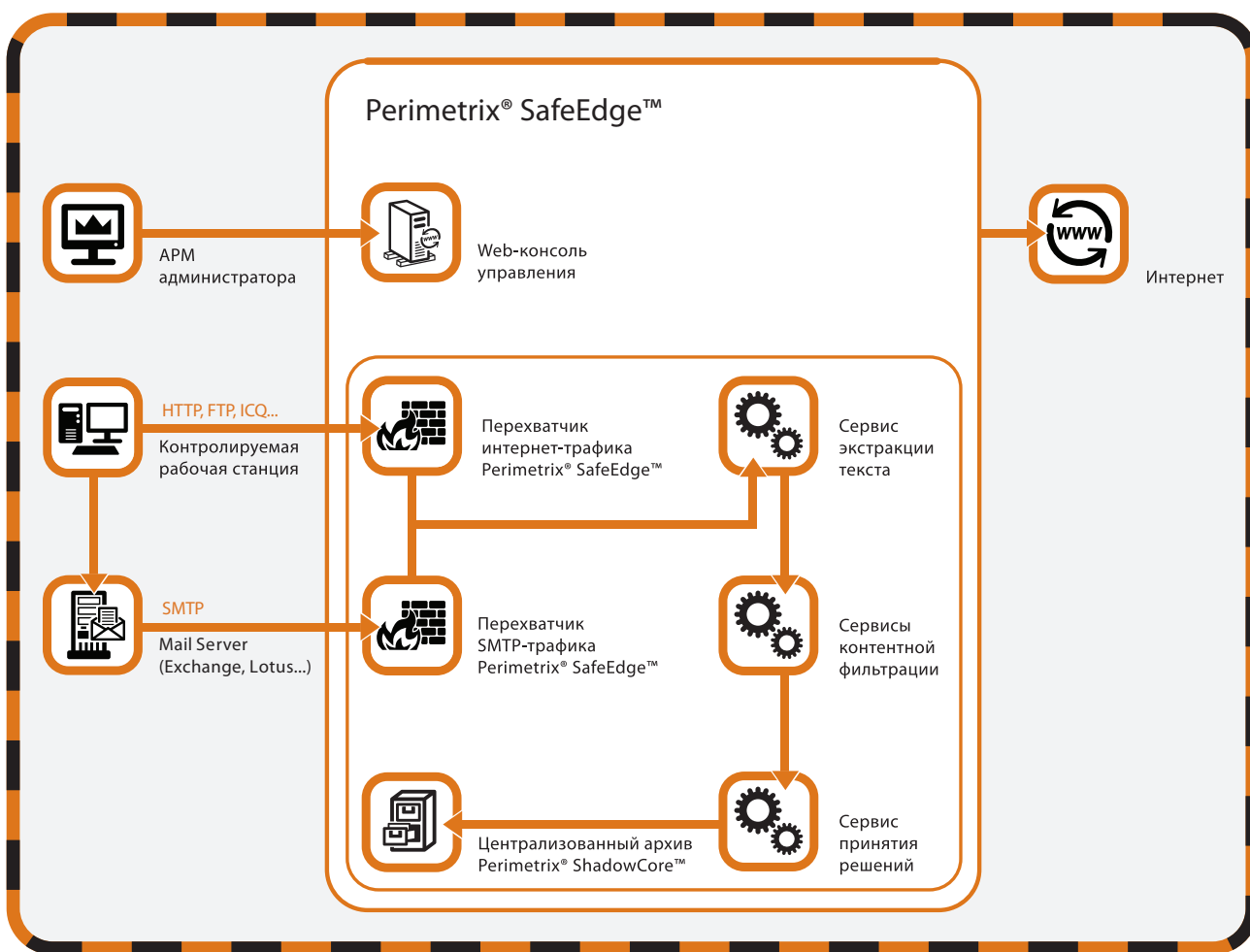


Рисунок 2. Схема Perimetrix® SafeEdge™

3.3. ТЕХНОЛОГИИ ФИЛЬТРАЦИИ ТРАФИКА В SAFEEDGE

В Perimetrix® SafeEdge™ применяются два механизма контентной фильтрации: лингвистический анализ и цифровые отпечатки.

Основой работы Perimetrix® SafeEdge™ являются технологии фильтрации трафика. Для решения этой задачи система использует сразу несколько вероятностных алгоритмов, которые позволяют добиться максимальной точности определения.

На вход каждого вероятностного алгоритма поступает «чистый текст» (plain text)¹, на выходе – возвращается определенный набор категорий конфиденциальности, которые содержатся в анализируемом файле. Так, результатом контентного анализа может являться вердикт о том, что данный файл содержит конфиденциальные маркетинговые данные, а также публичные технические сведения. Решение о пропуске или блокировке трафика принимается с помощью полученного вердикта и настроенных политик безопасности. Отметим, что результаты анализа являются не единственным аргументом политик. Кроме них, могут быть также использованы формальные атрибуты файлов: их тип, размер, время передачи, пользователь и т.п.

В зависимости от форматов анализируемых файлов определение «чистого текста» может меняться. Например, в случае анализа html-страниц в анализируемый текст могут быть включены служебные теги. А в случае пересылки сложных электронных писем, состоящих из html- и plain text частей, анализируемый текст содержит в себе информацию из всех компонентов пересылаемого письма.

В Perimetrix® SafeEdge™ применяются два механизма контентной фильтрации: лингвистический анализ и цифровые отпечатки. Отметим, что технология лингвистического анализа является семейством из трех алгоритмов: фильтрации по ключевым словам, ключевым фразам и регулярным выражениям.

Лингвистическая фильтрация

Методы лингвистической фильтрации позволяют анализировать содержимое документов и определять их уровни конфиденциальности. В общем случае, лингвистические методы недостаточно точны – их применение сопровождается сравнительно высоким количеством ошибок как первого (пропуск конфиденциальных документов), так и второго типа (ложное срабатывание). Однако благодаря использованию комбинации из сразу нескольких лингвистических алгоритмов, Perimetrix SafeEdge обеспечивает хорошее качество фильтрации.

¹ Метод цифровых отпечатков позволяет также анализировать бинарные файлы без текста (картинки, видео и т.п.)



В продукте Perimetrix® SafeEdge™ реализованы следующие алгоритмы лингвистической фильтрации:

- **Фильтрация по ключевым словам.** Данный алгоритм предполагает настройку списка из ключевых слов, которые относятся к какой-то категории конфиденциальности. Каждому слову и категории может быть приписан определенный вес. Анализируя поступивший документ, система оценивает встречаемость ключевых слов из различных категорий и делает вывод об общем содержании документа. Поскольку фильтрация по ключевым словам является самым неточным методом, обычно ей присваивается максимально низкий приоритет.
- **Фильтрация по ключевым фразам** аналогична фильтрации по ключевым словам. Однако использование фраз вместо слов позволяет добиться более высокой точности распознавания (при условии подготовленной базы эталонных фраз).
- **Фильтрация по регулярным выражением** (маскам) позволяет определить в документе информацию с устойчивым форматом. Примерами такой информации могут являться номера банковских счетов, кредитных карт или каких-либо договоров.

В рамках внедрения системы для каждого из лингвистического алгоритмов формируется исходная база, состоящая из ключевых слов, фраз и шаблонов регулярных выражений вместе с соответствующими категориями конфиденциальности. Кроме того, каждому из лингвистических алгоритмов может быть присвоен определенный приоритет.

Цифровые отпечатки

Вторым механизмом контентной фильтрации Perimetrix® SafeEdge™, является технология цифровых отпечатков, которая широко применяется во многих современных DLP-системах. В общем виде она состоит из двух этапов: на первом этапе с исходных документов снимаются отпечатки, а на этапе фильтрации – отпечатки исходящего документа сравниваются с эталонными.

В общем случае, цифровой отпечаток – это хеш-функция от текстового массива (слова, строки, предложения или абзаца). Другими словами, в системе предусмотрен специальный алгоритм, который сопоставляет каждому массиву определенное число - отпечаток - и помещает его в специальную базу данных. Алгоритм снятия отпечатков построен таким образом, что совпадение отпечатков почти всегда эквивалентно совпадению исходных строк.



Для успешного применения технологии цифровых отпечатков, Perimetrix® SafeEdge™ создает базы отпечатков с заданными категориями конфиденциальности. Для решения этой задачи анализируется файловое хранилище (файл-сервер, папка, диск и т.п.) с документами определенной категорий (например, с техническими документами). Модуль снятия отпечатков открывает каждый файл, разбивает его текст на части и считывает значение отпечатков для каждой из полученных частей. В дальнейшем, эти значения помещаются в базу отпечатков и используются для анализа исходящих документов.

Отметим, что ключевым преимуществом метода цифровых отпечатков по сравнению с лингвистической фильтрацией является практически полное отсутствие ложных срабатываний. Совпадение отпечатка практически со 100% вероятностью говорит о совпадении исходных строк. Поэтому данная технология позволяет исключить случайные утечки информации из тех документов, с которых когда-то снимались отпечатки.

Недостатком цифровых отпечатков является слабая устойчивость к изменениям частей документа, с которых снимаются отпечатки. Если заменить в каждой из таких частей несколько символов – общий набор цифровых отпечатков документа может практически полностью измениться. Это означает, что существует вероятность утечки посредством внесения каких-то изменений в исходный документ. Однако на практике она невелика, поскольку для правильного внесения таких изменений необходимо знать особенности алгоритма, а также политики безопасности системы. Понятно, что большинство обычных пользователей такими знаниями не обладают.

Добавим, что метод цифровых отпечатков можно применить не только к текстовой, но и к любой бинарной информации. В этом случае с файла считывается единственный эталонный отпечаток, который сравнивается с отпечатками исходящих документов. Данный функционал может применяться для контроля утечек графических или видео-файлов, а также любых документов, текстовый разбор которых не поддерживается в системе SafeEdge.

Изолированные методы цифровых отпечатков и лингвистической фильтрации имеют ряд принципиальных недостатков и не могут обеспечить приемлемого качества распознавания. Однако совместное использование данных технологий, реализованное в Perimetrix® SafeEdge™, позволяет подчеркнуть их достоинства и избежать основ-



ных проблем. При условии качественной настройки исходных баз и правил принятия решений, SafeEdge совмещает в себе универсальность лингвистической фильтрации и безошибочность цифровых отпечатков. Тем самым, обеспечивается фильтрация всех без исключения документов и точное выявление конфиденциальных сведений в общем потоке трафика.

3.4. ИНТЕГРАЦИЯ SAFEEDGE И SAFEUSE. АВТОМАТИЧЕСКАЯ КЛАССИФИКАЦИЯ (ИНВЕНТАРИЗАЦИЯ) ДАННЫХ

Возможность инвентаризации позволяет легко проставлять метки конфиденциальности в SafeUse на основе алгоритмов контентной фильтрации, заложенных в функционале SafeEdge.

Важнейшая особенность Perimetrix® SafeEdge™ связана с автоматической классификацией или инвентаризацией данных для продукта Perimetrix® SafeUse™². Возможность инвентаризации позволяет легко проставлять метки конфиденциальности в SafeUse на основе алгоритмов контентной фильтрации, заложенных в функционале SafeEdge. С помощью данного механизма происходит поддержка актуальности классификации документов в системе SafeUse с течением времени – новым и входящим документам присваиваются определенные категории, а категории старых документов обновляются в соответствии со случившимися изменениями.

Для инвентаризации документов может использоваться один или несколько механизмов контентной фильтрации. Администратор системы задает объект инвентаризации (файл-сервер, диск, папку или документ), а также время и периодичность инвентаризации.

В заданное время Perimetrix® SafeEdge™ автоматически анализирует документы внутри объекта и присваивает им определенные категории. В дальнейшем, эти категории могут быть подтверждены или отклонены в ручном режиме.

Однако, несмотря на предусмотренные механизмы классификации, в корпоративной сети могут все равно остаться незамеченные документы, содержащие конфиденциальные данные. Проверка таких документов на конфиденциальность не может проводиться в SafeUse и всегда осуществляется с помощью SafeEdge. Таким образом, Perimetrix® SafeEdge™ дополняет функционал SafeUse и ликвидирует основную проблему последней системы, связанную с появлением

² Подробнее про классификацию документов читайте в WhitePaper по системе Perimetrix® SafeUse™



неклассифицированных документов. Именно эта задача определяет позиционирование SafeEdge как важного дополнения к SafeUse, а не только как изолированной системы безопасности.

3.5. ПОДДЕРЖКА ПРОТОКОЛОВ, ФАЙЛОВЫХ ФОРМАТОВ И ЯЗЫКОВ

В зависимости от потребностей заказчика компания Perimetrix обеспечит разработку дополнительных модулей для специфических протоколов, форматов или иностранных языков.

Являясь типичной DLP-системой, основанной на механизмах контентной фильтрации, решение Perimetrix® SafeEdge™ завязано на поддержке протоколов передачи трафика, форматов файлов и языка. В стандартной версии система поддерживает:

- Протоколы SMTP, HTTP и ICQ;
- Разбор файлов форматов Plain Text (*.txt), HTML (*.htm, *.html), Microsoft Office Word (*.doc, *.docx), Excel (*.xls, *.xlsx), PowerPoint (*.ppt, *.pptx), Open Office (*.odf), Adobe Acrobat (*.pdf), а также Zip- и производных архивов (*.zip, *.tar.gz...). Отметим, что файлы могут иметь произвольную кодировку, а формат файла определяется системой и не обязательно совпадает с его расширением;
- Русский, английский и немецкий языки.

В зависимости от потребностей заказчика компания Perimetrix обеспечит разработку дополнительных модулей для специфических протоколов, форматов или иностранных языков, используемых в сети организации.

3.6. ТИПОВЫЕ СЦЕНАРИИ РАБОТЫ PERIMETRIX® SAFEEDGE™

В отличие от Perimetrix® SafeUse™ и SafeStore сценарии работы Perimetrix® SafeEdge™ предельно просты. С точки зрения рядового пользователя существует всего лишь один сценарий – блокировка передачи документа по электронной почте, протоколу HTTP или ICQ.

Пример. Пользователь Алексей Иванов посылает конфиденциальный файл на внешнюю электронную почту.

Представим, что пользователь Алексей Иванов решил отправить своему коллеге из другой компании конфиденциальный файл. Для этого он прикрепил свой файл к электронному письму и отправил это письмо на внешний почтовый ящик.



Файл Ufa_Technology.doc, который отправил Алексей Иванов, был обработан перехватчиком SMTP-трафика, попал на сервис экстракции текста и затем – на сервис контентной фильтрации. В процессе анализа выяснилось, что данный файл содержит конфиденциальную техническую информацию. Однако поскольку политика безопасности запрещает передачу таких файлов на внешние адреса, эта передача блокируется, а информация об этом событии попадает в архив SafeEdge. Пользователю и системному администратору по почте отправляются соответствующие оповещения.

Точно так же Алексей Иванов мог загрузить файл по стандартному протоколу HTTP на сервис веб-почты либо отправить его коллеге с помощью системы мгновенных сообщений ICQ. В обоих случаях, SafeEdge действует аналогичным образом и выносит вердикт о легитимности действий на базе политик безопасности.

Добавим, что SafeEdge использует скриптовый язык Jess для описания политик безопасности. С помощью данного языка администратор может реализовывать политики любого уровня сложности, вплоть до контроля отдельных электронных адресов, форматов файлов, языков, кодировок или пользователей.

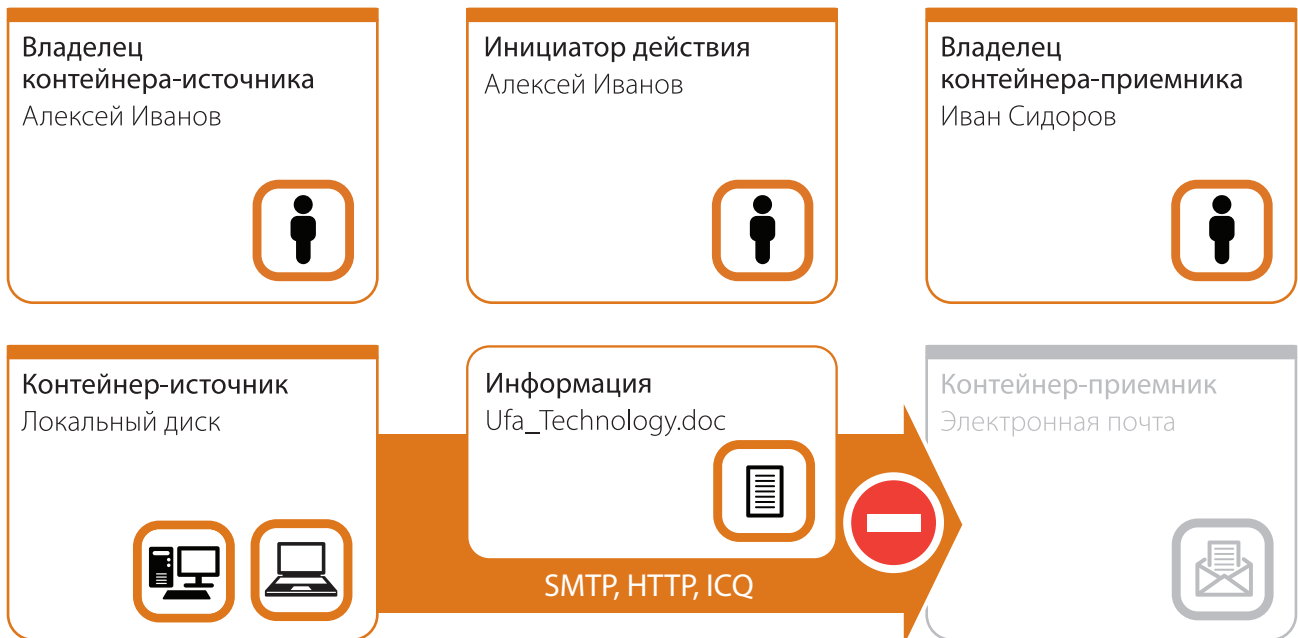


Рисунок 3. Основной сценарий работы Perimetrix® SafeEdge™

3.7. ФУНДАМЕНТАЛЬНЫЕ ПРЕИМУЩЕСТВА SAFEEDGE

Связка SafeUse + SafeEdge практически полностью покрывает риски утечек, в то время как большинство классических DLP-систем не могут решить эту проблему в комплексе.

Чтобы подвести черту к описанию основного функционала системы, приведем краткое концептуальное сравнение SafeEdge 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® SafeEdge™: с концептуальной точки зрения, изолированная система Perimetrix® SafeEdge™ не отличается от других DLP-продуктов первого поколения, построенных на базе контентной фильтрации. Главным отличием SafeEdge является уникальное позиционирование – в первую очередь, SafeEdge является дополнением к аудируемой среде Perimetrix® SafeUse™ и только потом – отдельным решением. Связка SafeUse + SafeEdge практически полностью покрывает риски утечек, в то время как большинство классических DLP-систем не могут решить эту проблему в комплексе.

Аналог второй: системы архивирования почтовой корреспонденции

Краткое описание функционала: система, обеспечивающая архивирование почтовой корреспонденции в базе данных с целью ретроспективного расследования инцидентов.

Преимущество Perimetrix® SafeEdge™: в Perimetrix® SafeEdge™ предусмотрен пассивный режим, в рамках которого происходит лишь фиксация всех событий без каких-либо блокировок. Это означает, что SafeEdge полностью покрывает функционал систем архивирования почтовой корреспонденции. Однако SafeEdge способен на большее – система не только фиксирует действия, но и блокирует их, причем не только по почтовым, но и по интернет-каналам.

4. ТЕХНОЛОГИЧЕСКИЕ ПРЕИМУЩЕСТВА SAFEEDGE

Все действия пользователей протоколируются в централизованной базе транзакций и событий Perimetrix® ShadowCore™. Таким образом, служба безопасности может проводить ретроспективный анализ и ретроспективное расследование инцидентов.

Perimetrix® SafeEdge™ имеет двойное позиционирование. С одной стороны, SafeEdge решает главную проблему системы SafeUse, **контролируя передачу неклассифицированных в SafeUse документов**. В то же время, SafeEdge можно рассматривать как **полноценную DLP-систему**, которая использует сразу несколько современных механизмов контентной фильтрации.

В рамках интеграции с системой SafeUse, Perimetrix® SafeEdge™ проводит **автоматическую инвентаризацию** документов, поддерживая актуальность классификации данных с течением времени. Кроме того, SafeEdge позволяет ставить метки на неклассифицированные (новые и входящие) документы.

Благодаря одновременному применению методов лингвистической фильтрации и цифровых отпечатков, система Perimetrix® SafeEdge™ обеспечивает максимально **точное распознавание** конфиденциальных документов.

Perimetrix® SafeEdge™ **поддерживает основные сетевые протоколы, распространенные форматы файлов и языки**. В отличие от большинства зарубежных DLP-систем, требующих адаптации к русскому языку, в Perimetrix® SafeEdge™ русская лингвистика поддерживается изначально. В случае необходимости модульная архитектура SafeEdge позволяет добавлять функционал для поддержки новых протоколов, файловых форматов, языков.

Принятие решения о легитимности действий пользователей происходит в рамках **глобальных политик Perimetrix® SafeSpace™**. Эти политики используют не только результаты контентной фильтрации, но и формальные атрибуты объекта – размер и формат файла, время передачи, тип адресата и т. п. В рамках настройки системы политики могут быть заданы сколь угодно подробно – вплоть до контроля отдельных электронных адресов, форматов файлов, языков, кодировок или пользователей.

Все действия пользователей **протоколируются** в централизованной базе транзакций и событий Perimetrix® ShadowCore™. Таким образом, означает, что служба безопасности может проводить ретроспективный анализ и ретроспективное расследование инцидентов.



Управление и настройка SafeEdge и других продуктов линейки Perimetrix **осуществляется через центральную веб-консоль**. С помощью механизмов разделения ролей администраторов и коллегиального принятия решений, в SafeEdge 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 SafeEdge (за исключением сервисов-перехватчиков) 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 SafeEdge могут использоваться все распространенные промышленные СУБД, в том числе Microsoft SQL Server, Oracle Database, IBM DB2, PostgreSQL и др.

Кластерная архитектура сервисов SafeEdge 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.

5. ВЫВОДЫ

В Perimetrix® SafeEdge™ используются сразу несколько механизмов контентной фильтрации, совокупность которых способствует высокой точности распознавания конфиденциальных документов.

Perimetrix® SafeEdge™ является ключевым элементом платформы Perimetrix® SafeSpace™. Система SafeEdge решает три основные задачи – она самостоятельно фильтрует трафик по сетевым каналам, проводит инвентаризацию данных и контролирует утечки неклассифицированных документов.

В Perimetrix® SafeEdge™ используются сразу несколько механизмов контентной фильтрации, совокупность которых способствует высокой точности распознавания конфиденциальных документов. SafeEdge поддерживает установку максимально гибких политик и настроек, которые могут использовать атрибуты вплоть до отдельного пользователя или формата файлов.

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

6. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Все перечисленные 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.

Web-интерфейс консоли управления

- Сервер с процессором Intel Pentium IV с частотой 3 GHz, оперативная память не менее 1 Gb
- Любая операционная система, поддерживающая JAVA. Тестировалось на Open SUSE 10.3 и 11.0 (32 и 64 bit), Windows XP
- Java JRE 6.0 update 7 и выше
- Apache Tomcat 6.0.14 и выше

Сервис контентной фильтрации и сервис экстракции текста

- Сервер с процессором Intel Pentium IV с частотой 3 GHz, оперативная память не менее 1 Gb
- Любая операционная система, поддерживающая JAVA. Тестировалось на Open SUSE 10.3 и 11.0 (32 и 64 bit).
- Java JRE 6.0 update 7 и выше

Сервисы перехвата сетевых пакетов

- Сервер с процессором Intel Pentium IV с частотой 3 GHz, оперативная память не менее 1 Gb
- Любая операционная система семейства Linux, версия ядра > 2.6.
- Java JRE 6.0 update 7 и выше
- Apache Tomcat 6.0.14 и выше
- iptables-1.4
- itclib-1.1.3
- log4cpp-1.0
- Сетевой интерфейс должен выполнять функции шлюза, т.е. иметь как минимум две сетевые карты.

Сервер СУБД

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

Остальные сервисы

- 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



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 клиентов 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.



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

