



SECRET DOCUMENTS LIFECYCLE™

НОВОЕ ПОКОЛЕНИЕ ТЕХНОЛОГИЙ
ДЛЯ ЗАЩИТЫ КОРПОРАТИВНЫХ
СЕКРЕТОВ

KEEPING SECRETS SAFE



PERIMATRIX



1. ВВОДНЫЕ

2. ЭВОЛЮЦИЯ ПОДХОДОВ К ЗАЩИТЕ ОТ УТЕЧКИ

- 2.1. ПЕРВОЕ ПОКОЛЕНИЕ: ВЕРОЯТНОСТНЫЕ МЕТОДЫ ФИЛЬТРАЦИИ
- 2.2. ВТОРОЕ ПОКОЛЕНИЕ: ДЕТЕРМИНИСТСКИЕ МЕТОДЫ ЗАЩИТЫ
- 2.3. ВЫВОДЫ

3. КОНЦЕПЦИЯ SECRET DOCUMENTS LIFECYCLE™

- 3.1. ЖИЗНЕННЫЙ ЦИКЛ СЕКРЕТНОГО ДОКУМЕНТА
- 3.2. ЗАЩИТА НА ВСЕХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА
- 3.3. ЗАЩИТА СЕКРЕТОВ ПРИ МОБИЛЬНОЙ РАБОТЕ
- 3.4. АУДИТ НА ВСЕХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА
- 3.5. АУДИТ ЦЕЛОСТНОСТИ СЕКРЕТНЫХ ДОКУМЕНТОВ
- 3.6. ВЫВОДЫ

4. О КОМПАНИИ PERIMETRIX



1. ВВОДНЫЕ

По оценкам Ponemon Institute, средний ущерб всего от одной утечки составляет 4,7 млн. долларов.

Корпоративные секреты это любая информация, которая принадлежит фирме и которую необходимо сохранить в тайне. Персональные данные служащих и клиентов, конфиденциальные сведения партнеров, интеллектуальная собственность компании, стратегии и планы развития бизнеса – все это представляет огромную ценность для фирмы и не должно покинуть ее пределов. Если корпоративные секреты попадут в руки конкурентов, мошенников, журналистов или будут преданы всеобщей огласке, это нанесет ущерб акционерам, менеджменту, служащим и/или партнерам компании.

Между тем, такие утечки случаются буквально ежедневно. Многие всемирно известные компании уже отметились в заголовках газет. Среди них самые престижные консалтинговые фирмы, крупные промышленные производители, авторитетные банки и др. Все это приводит к потере имиджа, снижению конкурентоспособности и инвестиционной привлекательности, преследованию со стороны государства и регулирующих органов за нарушение законов, директив и стандартов.

Очевидно, что ни одна организация не хочет стать следующим героем в скандале об утечке. К тому же предотвратить утечку намного проще и дешевле, чем потом тратить время и ресурсы, чтобы нейтрализовать ее последствия.

По мнению компании Gartner, утечки обходятся намного дороже, чем внедрение средств по их предотвращению¹. Эта экономия в среднем достигает 500%. Между тем по оценкам Ponemon Institute, средний ущерб всего от одной утечки составляет 4,7 млн. долларов².

Существует целый ряд технологий, которые так или иначе позволяют предотвратить утечку и защитить корпоративные секреты. Данный документ ставит своей целью рассмотреть и проанализировать применяющиеся сегодня подходы со всеми их преимуществами и недостатками, а затем представить концепцию Secret Documents Lifecycle™ (далее SDL) – новое поколение технологий защиты корпоративных секретов, разработанное компанией Perimetrix.

¹ Источник: Авива Литан (Avivah Litan), вице-президент и известный аналитик Gartner

² Источник: 2006 Ponemon Data Breach Study

2. ЭВОЛЮЦИЯ ПОДХОДОВ К ЗАЩИТЕ ОТ УТЕЧКИ

К настоящему моменту технологии выявления корпоративных секретов прошли две стадии эволюции.

С концептуальной точки зрения, утечка происходит тогда, когда корпоративные секреты покидают периметр информационной системы компании. Например, служащий распечатывает конфиденциальный отчет и выносит его из офиса в портфеле. При этом вместо принтера внутренний нарушитель может воспользоваться любым другим каналом передачи данных. Поэтому все разработчики систем защиты от утечки первоначально сфокусировались на контроле над каналами, по которым конфиденциальная информация может покинуть корпоративный периметр.

В общем виде все эти коммуникационные каналы можно разделить на четыре основных группы: электронная почта, Интернет, средства печати, а также съемные носители и мобильные устройства. Идея большинства технологий защиты корпоративных секретов состоит как раз в том, чтобы проверять все исходящие документы на выходе. То есть в тот момент, когда данные пытаются покинуть сеть организации по одному из четырех каналов.

Таким образом, вся задача свелась к тому, чтобы научиться отличать секретные файлы от публичных документов. Причем делать это автоматически, с минимальным привлечением человека.

К настоящему моменту технологии выявления корпоративных секретов в потоке трафика прошли две стадии эволюции. Во-первых, разработчики систем предотвращения утечек обратили свое внимание на вероятностные методы, суть которых состоит в использовании лингвистического анализа или «цифровых отпечатков пальцев» (Digital Fingerprints). Во-вторых, поставщики реализовали детерминистские методы, основанные на том, что каждый секретный документ должен быть специальным образом помечен.

Подробнее каждый из этих подходов будет рассмотрен далее в этой главе. Однако уже сейчас можно сказать, что эффективность вероятностных и детерминистских подходов оставляет желать много лучшего. По мнению компании Gartner¹, это крайне ненадежные технологии: смысленный внутренний нарушитель сможет их легко обмануть, а эффективность защиты достигает лишь 80%. Другими словами, эти подходы позволяют предотвратить только случайные и невежественные утечки, да и то не всегда.

¹ Источник: Hype Cycle for Information Security, 2007

Эффективность лингвистической фильтрации в самом лучшем случае достигает лишь 80%.

2.1. ПЕРВОЕ ПОКОЛЕНИЕ: ВЕРОЯТНОСТНЫЕ МЕТОДЫ ФИЛЬТРАЦИИ

Вероятностные методы фильтрации исходящего трафика предполагают использование лингвистических технологий или цифровых отпечатков (Digital Fingerprints), снятых с секретных документов.

Применение лингвистического анализа подразумевает поиск в исходящих документах ключевых фраз, заданных заранее, а потом их анализ с учетом контекста. Для этого требуется предварительное обучение фильтра на тех документах, для которых уже известно, что они являются секретными.

Внедрение системы защиты на основе лингвистического анализа требует предварительного создания базы контентной фильтрации. В нее входят своего рода сигнатуры конфиденциальных документов данной конкретной организации. Каждая сигнатура представляет собой шаблон или цифровой отпечаток секретного документа с учетом ключевых слов и контекста.

Анализ исходящего трафика осуществляется именно с использованием этой базы: движок сканирует поступивший документ, находит ключевые слова, а потом анализирует текст, используя базу лингвистических сигнатур или цифровых отпечатков.

Результатом анализа является определенная оценка, например, от 1 до 10. Чем выше полученное значение, тем более уверен лингвистический фильтр в секретности проверенного документа. Другими словами, тем выше вероятность, что исходящий файл имеет конфиденциальный характер. Именно поэтому первое поколение технологий предотвращения утечек получило название вероятностных.

У рассмотренного подхода существует три основных недостатка, собранных в таблице 1. Во-первых, основная проблема данной технологии состоит в крайне низкой эффективности. Специалистов по информационной безопасности или управлению рисками ждет глубокое разочарование, так как ни о каких «четыре девятках», т.е. эффективности на уровне 99,99%, здесь говорить не приходится.

Даже при создании базы данных контентной фильтрации эффективность фильтрации с применением лингвистических технологий достигает лишь 80%. Это означает, что 20% корпоративных секретов беспрепятственно покидают сеть компании. Между тем, практика показывает, что утечка всего 20% корпоративных секретов в 60% случаев приводит фирму к банкротству. Наконец, даже самый передовой лингвистический анализ легко обойти с помощью простейших элементов стеганографии и кодирования сообщения.

Таблица 1. Ключевые недостатки лингвистической фильтрации

Проблема	Описание
Низкая эффективность даже в самом лучшем случае	Самый лучший случай – когда перед внедрением создается база контентной фильтрации, учитывающая специфику данной конкретной организации. Однако даже при таком раскладе эффективность фильтрации достигает лишь 80%. Другими словами, 20% корпоративных секретов беспрепятственно покинут информационную сеть, а 20% ложных срабатываний превратят работу офицеров безопасности в ад.
Отсутствие защиты от утечек на уровне рабочей станции	Лингвистическая фильтрация легко реализуется для проверки сетевого трафика на уровне шлюза. Однако утечки могут произойти и через рабочую станцию: порты, съемные носители, мобильные устройства, беспроводные сети. Между тем, реализовать анализ копируемых, например, через USB-порт файлов через удаленный сервер контентной фильтрации технически очень сложно. Поэтому разработчики предпочитают вообще не защищать рабочие станции, рекомендуя закрыть все открытые порты административно или аппаратно.
Внутренний нарушитель может легко обхитрить систему	Концепция контроля только четырех коммуникационных каналов имеет существенные ограничения. Например, ничто не мешает сотруднику потерять свой ноутбук с корпоративными секретами, что столь часто бывает на практике. Таким образом, системы защиты на основе лингвистических технологий решают лишь часть проблемы, оставляя своих клиентов с неудовлетворенной потребностью в полноценной защите от утечек.

Отметим, что точно такой же высокий процент ложных срабатываний (20%) при интенсивном трафике способен превратить работу специалистов по информационной безопасности в ад. Например, если ежедневно через почтовый шлюз организации проходят 100 000 писем, то 20 000 ложных срабатываний офицерам безопасности придется обрабатывать вручную. Между тем, указанный объем почтового трафика является довольно щадящим для крупных компаний, где реальное количество отсылаемых сообщений может измеряться миллионами.

Кроме того, что эффективность в 80% удается достичь только при создании базы контентной фильтрации, учитывающей специфику данной конкретной организации. Однако для этого требуется провести классификацию всей корпоративной информации. Поставщики систем защиты от утечек часто не идут на это, предоставляя клиенту стандартную или типовую контентную базу. В этом случае продукт очень просто внедряется – буквально за считанные дни, но страдает и без того невысокая эффективность, которая опускается до 60%.

Во-вторых, еще одна проблема, связанная с лингвистической фильтрацией, состоит в том, что ее очень сложно реализовать для несетевых видов трафика. Одно дело анализировать почтовый трафик, а совсем другое – те файлы, которые копируются на внешние устройства. Попытки создать систему предотвращения утечек, которые бы смогли проводить лингвистический анализ файлов, копируемых на съемные носители, не увенчались успехом. Для этого требуется отсылать все исходящие файлы на удаленный сервер, а потом осуществлять контроль на уровне рабочей станции с учетом полученного вердикта.

Вряд ли такой подход можно считать целесообразным, так как это приводит к повышенной нагрузке на рабочую станцию, вычислительную сеть и все равно приводит к низкой эффективности. Именно поэтому разработчики, использующие лингвистический анализ, зачастую вообще не предоставляют защиту от утечек на уровне рабочей станции, либо рекомендуют административно или аппаратно перекрыть все открытые порты.

В-третьих, последний ключевой недостаток рассматриваемой технологии состоит в том, что у внутреннего нарушителя всегда есть множество обходных путей, чтобы обмануть систему защиты корпоративных секретов. Например, сегодня очень популярны утечки через ноутбуки.

Сотрудник легко может потерять свой мобильный компьютер, а преступник специально может выкрасть нужный ему ноутбук с секретными документами. Это не укладывается в рамки обычной концепции о четырех каналах утечки, поэтому поставщики систем защиты на основе лингвистической фильтрации на самом деле решают лишь часть проблемы, не удовлетворяя потребности своих клиентов в полноценной защите от утечек.

Таким образом, лингвистические технологии не позволяют в полной мере сохранить корпоративные секреты. Применение этого подхода на практике – уже вчерашний день.

Детерминистские методы защиты славятся отсутствием гибкости.

2.2. ВТОРОЕ ПОКОЛЕНИЕ: ДЕТЕРМИНИСТСКИЕ МЕТОДЫ ЗАЩИТЫ

Детерминистские технологии предполагают, что все конфиденциальные файлы должны быть специальным образом помечены. В некоторых продуктах эта метка может быть вшита прямо в имя файла. В этом случае каждый файл должен начинаться, например, с класса конфиденциальности или уровня секретности, что приводит к созданию корпоративных политик именования файлов. Естественно, на практике это очень не удобно и не прозрачно, так как мешает служащим эффективно работать.

Между тем, есть более изощренные методы работы с документами, которые не предполагают такое грубое встраивание меток. Например, метка может быть встроена внутрь файла, скажем, в один из его служебных заголовков.

В этом случае, когда документ покидает корпоративную сеть через сетевые каналы, например, по электронной почте, фильтру не нужно анализировать контент. Достаточно лишь считать метку и применить положения политики безопасности. Другими словами, зная метку, система защиты может безошибочно определить, является файл секретным или публичным. Отсюда пошло название второго поколения систем защиты от утечек – детерминистское.

Очевидно, что для внедрения такой системы требуется провести полную классификацию всех электронных документов в компании и пометить все секретные файлы соответствующим образом. Также понятно, что эффективность защиты помеченных файлов равна 100%.

Однако возникает целый ряд других проблем. В частности, непонятно, что делать с новыми документами, которые каждый день создаются в организации. Например, что мешает внутреннему нарушителю скопировать в буфер обмена часть секретного текста, создать новый документ, вставить в него уже скопированный текст, а потом попытаться украсть этот файл.

Все это приводит к тому, что система защиты, работающая на уровне рабочей станции, просто запрещает работать с буфером обмена, если документ является секретным. Даже если служащий пытается скопировать ничего не значащую фразу для нового публичного документа, система все равно наложит вето.

Таким образом, у детерминистского подхода тоже есть свои недостатки, из которых следует отметить два ключевых (см. таб. 2). Во-первых, очень существенная проблема данной технологии – отсутствие гибкости, которая словно цепная реакция приводит к снижению доступности документов, ухудшению производительности труда, усилению бюрократии. Если в организации с 50-100 служащими все эти проблемы можно урегулировать, то в крупной компании с разветвленной сетью филиалов или просто числом сотрудников более 500 отсутствие гибкости похоронит все плюсы системы защиты от утечек.

Таблица 2. Ключевые недостатки детерминистских методов

Проблема	Описание
Отсутствие гибкости	Отсутствие гибкости заложено в самом названии и в самой концепции технологии. Система принимает только те решения, которые predeterminedены заранее. В результате существенно снижается доступность документов в корпоративной сети, ухудшается производительность труда служащих, разрастается бюрократия и нарастает социальная напряженность между безопасностью и бизнесом.
Невозможность решить проблему в комплексе	По-прежнему, ничто не мешает сотруднику потерять свой ноутбук с корпоративными секретами. Хотя агент системы защиты может проследить за выполнением политики безопасности при работе сотрудника вне офиса, это никак не спасет от физической кражи мобильного компьютера и дальнейшего несанкционированного доступа. Резюмируя, детерминистские методы не решают проблему в комплексе, адресуют лишь одну ее небольшую часть.

Кроме того, внедрение такого решения может спровоцировать обострение внутрикорпоративного конфликта, когда требования бизнеса расходятся с требованиями безопасности. В результате интересы менеджеров могут столкнуться с интересами офицеров безопасности, что, конечно же, идет далеко не на пользу обеим сторонам и самой организации в целом.

Во-вторых, детерминистские методы предотвращения утечек точно так же беззащитны перед кражей мобильных устройств, носителей и компьютеров. Даже если служащий установит на ноутбук агент системы защиты, все это ничем не поможет от физической кражи или потери ноутбука. Другим словами, рассматриваемая технология адресует лишь часть комплексной проблемы, оставляя все остальное на усмотрение самой организации.

Таким образом, можно смело утверждать, что использование детерминистских систем – это такой же вчерашний день, как и применение лингвистической фильтрации.

Ответом на потребность в полноценной защите корпоративных секретов является новое, третье поколение технологий – Secret Documents Lifecycle™ – разработанное компанией Perimetrix.

2.3. ВЫВОДЫ

Оба поколения технологий предотвращения утечек сегодня устарели. Они не позволяют достичь приемлемого уровня эффективности, прозрачности и доступности. Кроме того, ни один подход не позволяет решить проблему в комплексе. Между тем, потребность любой организации состоит в том, чтобы защитить свои корпоративные секреты от утечки вне зависимости от того, как эта утечка может произойти. Таким образом, инвестирование в рассмотренные выше методы защиты приводит лишь к частичному решению проблемы, да и то с серьезными ограничениями.

Ответом на потребность в полноценной защите корпоративных секретов является новое, третье поколение технологий – Secret Documents Lifecycle™ – разработанное компанией Perimetrix. Его ключевыми преимуществами являются, во-первых, 100% эффективность защиты классифицированных конфиденциальных документов, во-вторых, высокий уровень прозрачности и доступности, а в-третьих, решение проблемы целиком, а не какой-то ее отдельной части.

3. КОНЦЕПЦИЯ SECRET DOCUMENTS LIFECYCLE™

Пять китов концепции: классификация, контроль, мониторинг, нотификация, аудит.

Технология Secret Document Lifecycle™ (далее SDL) решает задачу защиты целостности и конфиденциальности данных «от и до». То есть, с момента создания документа и до момента его официального уничтожения. В основе концепции лежат пять базовых процессов информационной безопасности: классификация, контроль, мониторинг, нотификация, аудит.

1. Классификация. На первом этапе построения системы защиты от утечки необходимо провести классификацию и категоризацию информации. Другими словами, следует отделить зёрна от плевел и понять, что именно требуется защищать. К классифицированной информации сразу же прописываются соответствующие уровни допуска, а для вновь создаваемых и «входящих» документов описывается и настраивается процедура их учета.

2. Контроль. Вторая ступень предполагает защиту секретных документов в местах хранения и распределение прав доступа к этой информации на основе классов и уровней допуска, полученных на первом этапе. При этом используется многомерная модель конфиденциальности. Кроме того, защита в местах хранения предполагает использование шифрования. В результате, корпоративные секреты защищены от несанкционированного доступа и утечки при краже или потере вычислительной техники, мобильных компьютеров и устройств. Кроме того, на данном шаге обеспечивается необходимый документооборот, соответствующий политике доступа пользователей к классифицированным данным.

3. Мониторинг. Третий этап подразумевает защиту секретных документов в использовании, в процессе работы служащих с конфиденциальными файлами на своих компьютерах. На данном этапе осуществляется мониторинг действий с секретными документами с использованием комбинации, как вероятностных, так и детерминистских методов. При этом система защиты всегда знает, кто, когда и что сделал с данным конфиденциальным файлом.

4. Нотификация. Четвертым шагом является предотвращение нарушений в масштабе реального времени и оповещение обо всех инцидентах офицера безопасности. Так что служба безопасности всегда сможет быстро отреагировать на утечку.

5. Аудит. Пятым и обязательным этапом построения системы защиты является архив всех данных, циркулирующих в корпоративной сети и покидающей ее пределы, и действий, которые пользователи совершают с этими данными. При помощи данного архива организации легко могут пройти аудит, провести ретроспективный анализ или расследование инцидента. Кроме того, такой архив поможет достичь соответствия нормативным актам вроде закона SOX (Sarbanes-Oxley Act) и Basel II.

Чтобы глубже понять, что представляет собой технология SDL, следует рассмотреть цикл жизни любого конфиденциального документа.

Разработчики Perimetrix не изобретали колеса, а воспользовались передовым опытом режимных организаций.

3.1. ЖИЗНЕННЫЙ ЦИКЛ СЕКРЕТНОГО ДОКУМЕНТА

Компания Perimetrix, реализовавшая технологию SDL, не изобретала колеса. Вместо этого разработчики обратили внимание на то, как с секретными документами работали режимные организации еще до того, как практически все документы стали электронными (см. рис. 1).



Рисунок 1. Жизненный цикл секретного документа

Создание документа. Цикл жизни секретного документа начинается с его создания. Служащий, который хочет создать новый документ, подает заявку по установленной форме и проходит процесс одобрения и утверждения этой заявки. Результатом этой процедуры является создание бланка документа с присвоением ему уровня секретности и инвентарного номера. Другими словами, еще до того, как в документе появится какая-либо информация, он уже имеет уровень секретности (регулирующие права доступа к документу) и инвентарный номер (указывающий на местоположение документа). Лишь после этого происходит наполнение документа контентом и передача в рабочее использование или на хранение.

Использование документа. Само место использования документа, а также сам процесс жестко регламентированы. В каждой режимной организации есть секретная часть (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 при помощи инвентарного номера и выдает его на руки. Отметим, что варианты доступа к документу могут быть самыми разными. Это своего рода политики: доступ для обычных операций, разовый доступ, доступ в зависимости от уровня документа, временный доступ и т.д.

Получив документ на руки, служащий никуда не уходит. Он может работать с секретными бумагами только в специально отведенном для этого месте. То есть в распоряжении сотрудника есть читальный зал при секретной части, где можно сесть и почитать документ. В то же время вся работа с документом полностью контролируется. 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 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.

Уничтожение документа. Любой секретный документ в конце своего жизненного цикла подлежит либо уничтожению, либо архивированию, либо передаче в другое место хранения. В этом случае точно так же, как и на самом первом этапе создания документа, необходимо составить заявку на уничтожение, архивирование или передачу документа (это же относится к операциям с «исходящими» документами). В последнем случае передается не только секретный документ, но и ответственность за его целостность и конфиденциальность. Лишь после утверждения заявки происходит сам процесс безопасного уничтожения документа или его защищенной передачи в другое хранилище. Либо документ направляется в архив. Не следует забывать и о стандартном документообороте: все действия должны быть отражены в соответствующих журналах. Например, кто, когда и какой документ уничтожил по отведенной для этого процедуре. Таким образом, всегда можно провести аудит всех совершенных действий, проследить историю документа, вычислить виновного.

Отметим, что жизненный цикл документа может закончиться также понижением или повышением его уровня секретности. В этом случае появляется уже новый документ с менее или более жесткими правами доступа и использования.

Рассмотренный только что жизненный цикл секретного документа в режимных организациях связан с большим количеством формальных процедур и высоким уровнем бюрократии. Отсюда проистекает медлительность всего процесса, а о доступности и прозрачности вообще говорить не приходится. Между тем, перенос описанного формального цикла работы с секретными документами в электронную среду позволяет избавиться от всех негативных моментов. Например, все журналы событий ведутся автоматически, а заявки путешествуют со скоростью сетевых пакетов.

Secret Documents Lifecycle™ – защита документов при хранении, использовании и в движении.

3.2. ЗАЩИТА НА ВСЕХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА

Смысл технологии SDL состоит в том, чтобы обеспечить защиту секретного документа на всех этапах его жизненного цикла. Очевидно, что на момент построения системы предотвращения утечек в организации уже существует огромное количество документов. Поэтому первым этапом, как уже говорилось ранее, является классификация и категоризация всей информации.

Когда стало понятно, насколько конфиденциален тот или иной документ, происходит следующее: каждый документ помечается в соответствии со своим классом конфиденциальности или уровнем доступа. Для этого используется специально разработанная технология, позволяющая инкапсулировать метку в документ таким образом, чтобы она была никак не видна пользователю, и он не смог ее изменить. При этом метка помимо служебной информации содержит сведения, как о классе документа и правах доступа к нему, так и о владельце документа. Здесь используется уже упомянутая ранее многомерная модель конфиденциальности.

Защита в местах хранения. На следующем этапе все классифицированные документы складываются в специальное хранилище Perimetrix SafeHouse™, где они хранятся только в зашифрованном виде. С точки зрения реализации, это хранилище может быть, как централизованным, так и распределенным. В последнем случае документы по-прежнему находятся на рабочих станциях пользователей, но уже в зашифрованном виде и с инкапсулированными метками. Таким образом, реализуется то самое защищенное хранилище, которое даже при краже вычислительной техники, потери ноутбука и любой другой атаке несанкционированного доступа надежно защитит секретные документы от утечки и разглашения. Отметим, что для защищенного хранилища все равно, в каком виде и формате хранятся данные. Это могут быть текстовые документы, таблицы, рисунки, мультимедиа и даже базы данных. Например, в случае базы данных, сама база не помещается в хранилище, но пользователи работают только с безопасным хранилищем, а данные из базы перед тем, как попасть к пользователю, проходят хранилище.

Защита при использовании. После того, как все документы классифицированы и помещены в хранилище, начинается рабочий процесс. При этом все операции с секретными документами контролируются Perimetrix SafeUse™. Однако в процессе работы служащие используют не только уже классифицированные документы, а также создают новые документы. Казалось бы, здесь должны проявиться все недостатки детерминистских методов, рассмотренные ранее. Однако разработчики нашли элегантное решение: при создании новых документов с использованием информации из уже существующих файлов происходит «заражение» нового документа метками конфиденциальности тех документов, которые использовались для его наполнения. Таким образом, все новые документы классифицируются автоматически (за исключением тех, которые создаются с нуля, без использования каких-либо существующих документов).

Исследование компании Perimetrix показало, что служащие очень редко создают и наполняют новые документы без использования каких-либо уже существующих. В зависимости от специфики работы сотрудника число таких создаваемых с нуля документов (и без использования предопределенных шаблонов) обычно не превышает 0,5% от общей массы создаваемых документов. Лишь в некоторых исключительных случаях (например, работа художников, дизайнеров и т.д.) это значение достигает в среднем 3%. Другими словами, автоматической классификации не подвергается лишь малая часть вновь создаваемых в компании документов.

Попытка украсть классифицированный и помеченный документ наталкивается на 100% эффективность защиты, характерную для детерминистских методов. Система прекрасно знает, что документ является секретным, поэтому не выпустит его наружу, если у сотрудника нет соответствующих прав.

В то же самое время попытка выкрасть неклассифицированный документ (то есть недавно созданный и наполненный информацией из головы служащего) наталкивается на Perimetrix SafeEdge™, в основе которого лежат сразу три вероятностных метода защиты: цифровые отпечатки, лингвистический (эвристический) и сигнатурный анализ. В этом случае эффективность защиты существенно выше классического подхода, описанного выше, так как число неклассифицированных файлов в любой момент времени не превышает 0,5% от общего числа документов. Таким образом, доля ложных срабатываний или пропущенных секретных документов по теории вероятности составляет $0,005 \times 0,8 = 0,004$. Другими словами, эффективность технологии равна 99,6%, что вполне подходит для оценки рисков и моделирования угроз. Говорить о ложных срабатываниях здесь вообще не приходится.



PERIMETRIX

При этом обеспечивается защита неклассифицированных документов, даже если они покидают сеть не через сетевой шлюз (почта, Интернет, принтер), а через порты рабочей станции. Например, если файлы копируются на USB-носитель. В этом случае файл все равно отправляется на сервер фильтрации для классификации в режиме реального времени. Это не создает дополнительной нагрузки на рабочую станцию и сеть организации, так как число таких неклассифицированных документов крайне низко.

Конечно, неклассифицированные документы могут храниться и накапливаться на рабочих станциях пользователей, если те не высылают их за пределы сети, что приводит к автоматической классификации документов. Однако в этом случае концепция SDL предполагает, что по определенному расписанию (ночью раз в сутки или на выходных еженедельно – в зависимости от размера организации) система сама будет производить инвентаризацию документов. Все новые документы будут автоматически классифицированы и помещены в хранилище.

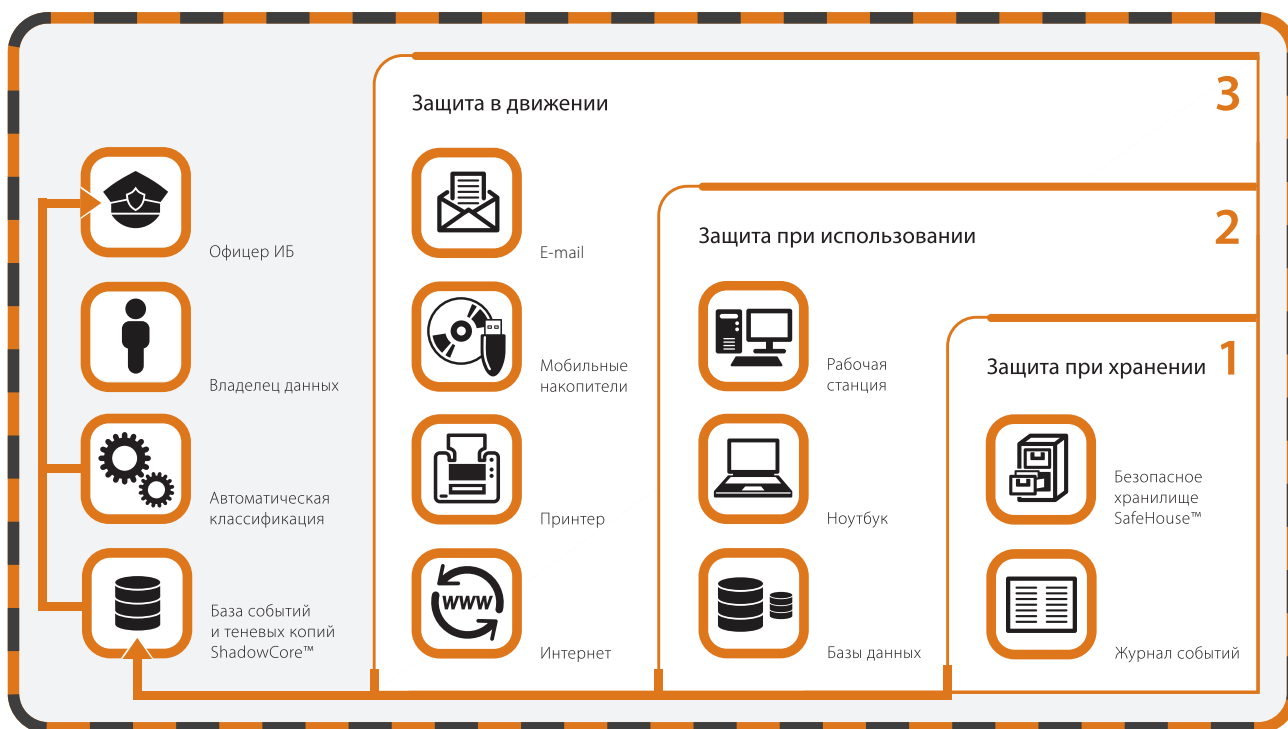


Рисунок 2. Три уровня защиты технологии Secret Documents Lifecycle™

Защита в движении. Следует также отметить, что все секретные документы являются зашифрованными. Поэтому при их передаче передается документ, защищенный криптографией, что означает защиту данных в движении в дополнение к той защите, которая была обеспечена при хранении и использовании (см. рис. 2). Кроме того, если секретный документ покидает корпоративную сеть и направляется, например, к партнеру, то шифрование исходящего трафика может производиться автоматически и абсолютно прозрачно.

В заключение заметим, что технология SDL предполагает и такую процедуру, как понижение уровня конфиденциальности документа. Очевидно, что, копируя данные из секретного документа, служащий может создать публичный файл, предназначенный для дальнейшего использования или пересылки за пределы организации. В этом случае сотрудник может инициировать процедуру понижения уровня секретности, что потребует участия еще одного или двух других сотрудников, в зависимости от действующей политики безопасности. Например, офицера безопасности, непосредственного руководителя или уполномоченного лица. Для пользователей, которые часто создают публичные документы, предусмотрены определенные шаблоны документов, которые позволяют сразу же создавать несекретные файлы. Однако во время этого процесса служащие не смогут работать с конфиденциальной информацией в других документах, что вполне логично.

Технология Secret Documents Lifecycle™ значительно упрощает работу пользователей вне пределов корпоративной сети.

3.3. ЗАЩИТА СЕКРЕТОВ ПРИ МОБИЛЬНОЙ РАБОТЕ

Как уже говорилось выше, защита в местах хранения предполагает использование шифрования, а потому секретные документы точно так же защищены от несанкционированного доступа на ноутбуках, как и в корпоративной сети. Однако при мобильной работе с конфиденциальными документами, например, во время командировки, возникает проблема безопасной аутентификации пользователей и эффективной защиты при использовании этих документов. Технология SDL значительно упрощает работу пользователей вне пределов корпоративной сети. Для этой цели вводятся несколько политик безопасности, определяющих условия доступа к классифицированным документам.

Основные уровни доступа:

- **Для служебного пользования (ДСП).** В этом случае командировочный сотрудник может получить доступ к документам с использованием личного ключа, например, воспользовавшись сильной аутентификацией или авторизовавшись с помощью пароля. При данном уровне доступа контроль над тем, как служащий использует документ, не осуществляется.
- **Секретно.** Этот уровень доступа предполагает аутентификацию и последующий контроль использования секретных документов, который осуществляется точно так же, как и контроль внутри корпоративной сети. При этом, естественно, реализуется полный документооборот, посредством которого можно провести аудит целостности. При последующем подключении мобильного компьютера к корпоративной сети, все журналы событий и базы аудита передаются в центральный архив¹.
- **Совершенно секретно.** В этом случае для получения доступа к документу необходимо пройти аутентификацию и установить VPN-соединение с корпоративной сетью. После этого можно работать с совершенно секретным документом. Естественно, все действия контролируются и записываются для последующего аудита. Кроме того, обеспечивается нотификация о любых нарушениях в режиме реального времени. В результате в случае необходимости офицер безопасности может удаленно лишить мобильного сотрудника прав доступа к совершенно секретному документу.

Таким образом, технология SDL адресует в полной мере проблему защиты и аудита целостности секретных документов за пределами корпоративной сети. В то же самое время, вся работа мобильных сотрудников ведется абсолютно прозрачно.

Аудит целостности – ключевой приоритет технологии Secret Documents Lifecycle™.

3.4. АУДИТ НА ВСЕХ ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА

Аудит конфиденциальности и целостности конфиденциальных документов на всех этапах жизненного цикла – столь же важная составляющая часть технологии SDL, сколь и сам по себе защита от утечки. Концепция SDL предполагает ведение центральной базы данных Perimetrix ShadowCore™, в которую складываются, как все события (кто, когда, какую операцию произвел и с каким документом), так и сами документы (циркулирующие внутри сети, покидающие ее пределы). Таким образом, создается мощная основа для аудита целостности, ретроспективного анализа и расследования инцидентов.

¹ См. подробнее главу «Аудит на всех этапах жизненного цикла»



PERIMETRIX

Используя эту базу данных, офицеры безопасности могут собирать и анализировать статистику, строить графики и отчеты. На основании этих сведений можно определить, насколько эффективно используются информационные ресурсы организации, сбалансировать и оптимизировать потоки данных и внутренние коммуникационные процессы.

Важно, что технология SDL содержит встроенную единую систему идентификации пользователей. Это означает, что при помощи центральной базы всегда можно точно выяснить личность служащего, совершившего те или иные действия. Тем самым удается обойти ключевое ограничение лоскутных системы защиты от утечек, которые состоят из нескольких не интегрированных компонентов. Такие лоскутные системы позволяют отслеживать действия с каналом Интернета, идентифицируя пользователей только в виде обезличенных IP-адресов (которые могут быть динамическими), с email – по почтовым адресам (которые легко фальсифицируются), со съемными носителями – по именам учетных записей.

Наконец заметим, что, анализируя центральную базу и расследуя уже случившийся инцидент, можно выявить цепочку событий, которая предшествовала попытке утечки или другим нарушениям. При накоплении такой информации становится возможной проактивная защита от внутренних угроз информационной безопасности, когда защитные меры принимаются еще до того, как нарушитель успеет подготовиться к реальным действиям.

Аудит целостности предполагает, что каждый чувствительный документ должен быть защищен от искажения.

3.5. АУДИТ ЦЕЛОСТНОСТИ СЕКРЕТНЫХ ДОКУМЕНТОВ

Аудит целостности специально выделен в отдельную главу, так как является ключевым требованием целого ряда нормативных актов, стандартов и директив. В частности аудиту целостности финансовых документов особое внимание уделяет закон SOX, ставший стандартом де-факто в сфере корпоративного управления. Кроме того, аудит целостности секретных документов является краеугольным камнем любого стандарта по информационной безопасности, управлению рисками и т.д.

Аудит целостности предполагает, что каждый чувствительный документ должен быть защищен от искажения (вплоть до полного уничтожения). Для этого создаются средства внутреннего контроля, которые в общем виде не могут помешать модификации важных документов теми служащими, у которых есть на это соответствующие права. Однако средства внутреннего контроля позволяют всегда выявить кто, какие изменения и в какой документ внес, а также восстановить важные файлы в оригинальном виде (даже после уничтожения).

Технология SDL в полной мере адресует задачу аудита целостности и защиты от искажения и уничтожения документов. Центральный архив, описанный в предыдущей главе, содержит в себе все необходимые для аудита сведения: различные версии документов, а также указания, кто, когда, как и что изменил. В случае необходимости легко поднять историю любого документа и проследить весь его жизненный цикл. Найти тот момент, когда внутренний нарушитель исказил отчет. Узнать, когда и как он это сделал, а потом откатить изменения, просто восстановив оригинальную версию документа.

Эффективность технологии Perimetrix достигает 99,6%.

3.6. ВЫВОДЫ

В отличие от стандартных и уже устаревших подходов с использованием детерминистских и вероятностных методов, технология SDL позволяет обеспечить крайне высокий уровень безопасности (с эффективностью более 99%), защитить данные при хранении и использовании, а также в движении. Ключевым преимуществом концепции SDL является то, что данный подход решает проблему комплексно и целиком. Вне зависимости от того, потеряют служащие организации ноутбук с секретными документами или попытаются скопировать конфиденциальную информацию на USB-носитель, утечки не произойдет. Таким образом, реализация концепции SDL в организации позволяет раз и навсегда, а также полностью решить проблему утечек.

Аналогично рассмотренному ранее бумажному документообороту, концепция SDL позволяет создать безопасное пространство, в котором документы хранятся, используются, передвигаются, в конечном счете, живут и умирают. Реализация этого безопасного пространства нашла свое место в комплексном решении Perimetrix SafeSpace™².

² Подробнее см. документ «Perimetrix SafeSpace™ – комплексная защита конфиденциальности и целостности данных».



4. О КОМПАНИИ PERIMETRIX

Компания Perimetrix разрабатывает системы защиты корпоративных секретов третьего поколения. Благодаря реализации революционной концепции Secret Documents Lifecycle™ наши решения обеспечивают гарантированную 100% защиту секретных документов, полный контроль над каналами коммуникаций и полноценный аудит электронных операций.

В отличие от конкурентов Perimetrix концентрирует весь свой потенциал, инновационный подход и уникальный опыт на решении важнейшей задачи заказчиков – сохранении корпоративных секретов для повышения конкурентоспособности, установления плодотворных отношений с инвесторами и партнерами, соответствия государственным требованиям.

Компания основана в 2007 году инновационной командой профессионалов, стоявших у истоков создания современных систем защиты от внутренних IT-угроз. Perimetrix входит в группу компаний «КомпьюЛинк» – лидирующий альянс на российском рынке информационных технологий. Устойчивое финансовое положение группы, ее уникальный опыт и знания, внушительная база заказчиков служат надежным фундаментом развития Perimetrix. Благодаря мощной поддержке «КомпьюЛинка» компания имеет возможность выполнять комплексные проекты по внутренней IT-безопасности, выйти в лидеры российского рынка и создать основу для международной экспансии.



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

