Защита информации на всех этапах жизненного цикла

text: Владимир Ульянов

Как обеспечить должный уровень безопасности информации? Проблема в том, что безопасность приложений совсем не обязательно означает безопасность информации. Так, даже самая неуязвимая система окажется бессильной перед инсайдерами — пользователями, которые имеют к ней вполне легальный доступ.

Но с точки зрения заказчиков именно безопасность информации играет ключевую роль. Конечно, если «упадет» корпоративное приложение, компания понесет определенные потери, равные стоимости времени простоя. Однако в случае утечки критически важных данных потери будут измеряться значительно более серьезными суммами.

Таким образом, защищенный жизненный цикл разработки логичным образом перерастает в защищенный жизненный цикл информации. Это означает, что к каждому документу должны применяться инструменты защиты на всех этапах его жизненного цикла — начиная от создания и заканчивая уничтожением (схема 1). В нашей статье мы рассмотрим методы защиты информации на примере методологии Secret Documents Lifecycle компании Perimetrix.

Несмотря на очевидность последнего тезиса, сегодня нет четкого понимания данной концепции. Причем не только со стороны заказчиков, но и со стороны производителей ПО. О целостной инфраструктуре защиты информации лишь изредка говорят в теории, а увидеть ее реализацию на практике почти невозможно.

1. Создание документа

Существует два инструмента защиты документа на начальной стадии его жизненного цикла. Первый — админис-

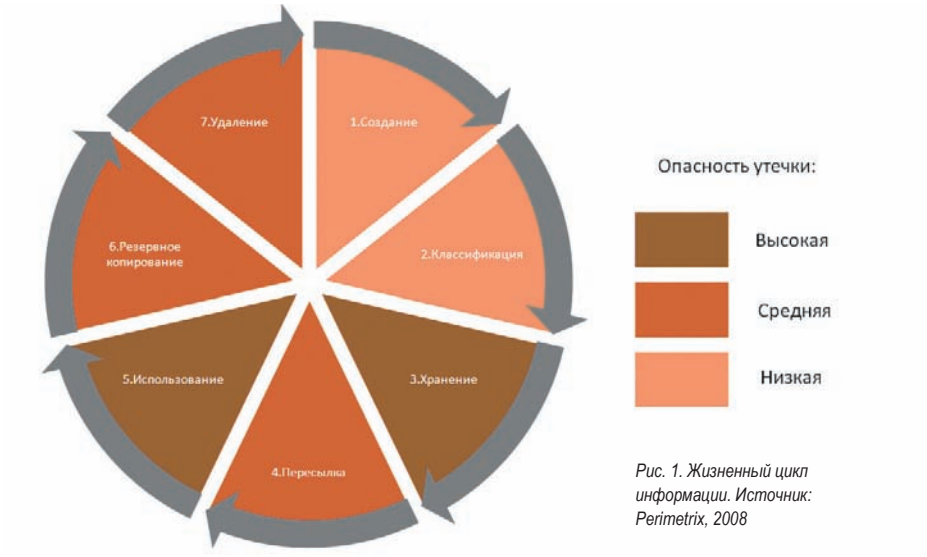


Рис. 1. Жизненный цикл информации. Источник: Perimetrix, 2008

Защита документа во время хранения должна обеспечиваться комплексом систем безопасности — системами контроля доступа, обнаружения вторжений, криптографическими комплексами, решениями по защите от утечек ◑●●

тративный инструмент декларирует создание только той информации, которая требуется для бизнес-процессов организации. Избыточное хранение конфиденциальных данных не только создает лишнюю нагрузку на ИТ-инфраструктуру, но и приводит к росту вероятности утечки. Таким образом, каждый сотрудник компании должен создавать только действительно необходимые ему документы. Второй — технический инструмент защиты предполагает инкапсуляцию специальных меток или грифов конфиденциальности в новые документы. В том случае, если новый документ создается из старого файла или некоего шаблона, этот процесс может произойти уже на этапе создания. В качестве примера можно привести механизм трансляции меток, реализованный в системе Perimetrix SafeSpace. Если же документ создается «с чистого листа», то расстановка меток производится уже на этапе классификации. Впрочем, в реальной жизни таких документов абсолютное меньшинство (менее 5%).

2. Классификация документов

Классификацию данных нужно рассматривать как комплексную деятельность, направленную не только на защиту конфиденциальных данных, но и на подготовку к следующему этапу их жизненного цикла —эффективному хранению. В рамках классификации каждый конфиденциальный документ получает набор атрибутов:

- метка конфиденциальности (степень секретности документа);
- тип информации (проприетарные коммерческие данные, интеллектуальная собственность, персональные данные);
- создатель информации (пользователь, подразделение);
- текущий владелец информации (пользователь, подразделение)
- права доступа к информации.

Некоторые из этих атрибутов автоматически экспортируются из стандартных метаданных документа, некоторые — требуется прописывать вручную (или с использованием специальных систем). После классификации становится ясно, что необходимо делать с документом на следующих этапах жизненного цикла. Если же классификация документов не проводилась — в организации наступает информационный хаос. Администратор не понимает, где хранятся секретные документы, а также не может проконтролировать их передачу, использование и уничтожение. Опасность в том, что этот хаос далеко не всегда приводит к видимым последствиям, поскольку происходящие утечки не заметны. Классификация данных полезна и с точки зрения эффективности бизнес-процессов. В условиях

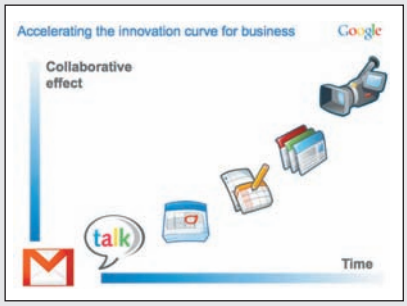
Новые электронные ключи Guardant

●●◐ Компания «Актив» анонсировала три модели электронных ключей Guardant: Guardant Stealth III Sign и Stealth III Time, а также Guardant Code.
Электронный ключ Guardant Stealth III Sign предлагает ряд новых возможностей, призванных повысить стойкость защиты: аппаратная реализация алгоритма электронной цифровой подписи на основе эллиптических кривых и симметричного шифрования AES; возможность работать в ОС Windows без установки драйверов Guardant; поддержка Linux и Windows CE; аппаратная защита от нескольких запусков защищенной программы в разных терминальных сессиях; защита от анализа на уровне протокола обмена.

Электронный ключ Guardant Code отличается возможностью исполнения кода внутри своего микропроцессора. Устройство будет выпускаться в двух вариантах: с часами реального времени и без. По сути, Guardant Code — это логическое продолжение технологии заказных ключей, в которые загружались программные модули клиента, только теперь все этапы построения защиты клиент может пройти самостоятельно, и нет ограничения на размер минимальной партии ключей.

Корпоративная версия Google Video

●●◐ Компания Google объявила о запуске корпоративной версии видеосервиса Google Video — Google Video for Business. Новая версия сервиса обладает функционалом, аналогичным обычной версии, и предназначена для обмена различным видеоконтентом, который так или иначе связан с бизнесом и может оказаться полезным сотрудникам компаний.



Google Video for Business будет включен в пакет приложений Google Apps Premier Edition бесплатно (цена пакета составляет $50 на одного пользователя в год). Каждому пользователю предоставляется 3 Гбайт свободного дискового пространства.

Серия надежных USB-накопителей Imation (TDK TRANS-IT USB 2.0)

●●◐ Компания Imation объявила о выпуске серии флэш-накопителей TDK TRANS-IT USB 2.0. Благодаря функции Flash Lock флэш-накопители обеспечивают надежную защиту данных.

Пользователь может задать свой собственный пароль, который оградит USB-устройство от несанкционированного доступа, автоматически блокируя его при введении неправильного пароля при определенном числе попыток. Если владелец забыл пароль, восстановить доступ поможет система подсказок. Накопители TDK TRANS-IT выпускаются в нескольких модификациях объемом от 2 до 16 Гбайт.

Таблица 1. Основные угрозы утечки на стадии хранения документа. Источник: Perimetrix, 2008

Угроза	Описание	Реальный кейс утечки	Системы защиты
Внешнее вторжение (хакерская атака).	Внешние злоумышленники каким-то образом взламывают защиту корпоративной сети и получают доступ к конфиденциальным данным.	В конце 2006 года группа злоумышленников взломала беспроводную сеть одного из офисов американского ритейлера TJX и похитила приватную базу с записями о 95 млн транзакций по банковским картам. Данная утечка остается крупнейшим инцидентом такого рода за всю историю.	Системы периметральной защиты от внешних вторжений, системы контроля доступа, криптографические системы и т. д.
Неавторизованный доступ внутренними сотрудниками.	Доступ к конфиденциальным данным получают сотрудники, которые не обладают соответствующими правами.	Младший трейдер Societe Generale Жером Кервьель сумел получить доступ к активам банка и совершил ряд сделок, которые привели к убыткам в €5 млрд.	Системы контроля доступа и идентификации пользователей.

разветвленной ИТ-инфраструктуры сотрудникам приходится тратить время на поиск нужных документов, а с помощью классификации его можно существенно сократить. Кроме того, классификация позволяет исправить ошибки, сделанные на этапе создания документов, и снизить утилизацию ресурсов за счет удаления избыточных данных.

3. Хранение документа

На этапе хранения документа впервые возникают масштабные риски его утечки. Риски делятся на две части — внутренние (инсайдерские) инциденты и внешние вторжения. Проводя дальнейшую декомпозицию, можно выявить сразу несколько более конкретных рисков внутри каждой из обозначенных групп.

Именно поэтому защита документа во время хранения должна обеспечиваться комплексом систем безопасности. К нему относятся системы контроля доступа, обнаружения вторжений, криптографические комплексы, а также решения по защите от утечек и даже антивирусы. Практически любая система безопасности так или иначе защищает информацию именно на этапе ее хранения.

В этом свете становится очевидной важность процесса классификации — без него нельзя понять, как именно следует защищать документ. На каком физическом сервере он должен быть размещен, кто должен иметь к нему доступ и требуется ли его шифровать. Другими словами, эффективное и безопасное хранение нельзя построить без классификации данных.

4. Пересылка документа

Современные компании почему-то уделяют этой стадии жизни документа повышенное внимание, хотя реальные риски утечки здесь не очень высоки.

Темы защищенных соединений, шифрованных туннелей и прочих технологий безопасной пересылки широко освещаются в современных СМИ. Однако на практике указанные технологии оказываются почти бесполезными — реальных случаев перехвата пересылаемых сведений критически мало. Данный факт косвенно объясняется спецификой процесса пересылки и тем объемом знаний, которым должен обладать злоумышленник, пытающийся перехватить документ. Чтобы поймать информацию в этот момент, он должен как минимум знать о факте пересылки, иметь информацию о времени пересылки и используемых инструментах защиты. Слишком много для одного мошенника, не правда ли? При этом за гранью внимания остается другая сто-

Таблица 2. Основные угрозы утечки на стадии пересылки документа. Источник: Perimetrix, 2008

Угроза	Описание	Реальный кейс утечки	Системы защиты
Взлом сетевых каналов пересылки.	Внешние злоумышленники каким-то образом перехватывают данные во время пересылки по незащищенным сетевым каналам.	Весной 2008 года американская розничная сеть Hannaford пострадала от действий хакеров, которые перехватили сведения о 4,2 млн транзакций в процессе передачи данных для авторизации банковских карт.	Создание защищенных (шифрованных) каналов передачи данных.
Кража/потеря физического носителя (ленты, диска и т. д.).	Как правило, услуги пересылки носителей оказывают третьи логистические компании. Очень часто они теряют подотчетные носители.	В начале нынешнего года банк New York Mellon объявил о пропаже резервной ленты с приватной информацией 4,5 млн клиентов.	Шифрование. Остальные методы защиты неэффективны.
Кража ноутбука.	Концептуально не отличается от угрозы кражи физического носителя. Выделена в специальный пункт из-за чрезвычайной актуальности.	В мае 2006 года один из сотрудников Министерства по делам ветеранов США потерял корпоративный ноутбук с приватной информацией 26,5 млн человек.	Шифрование. Остальные методы защиты неэффективны.

рона — отправка сведений на физических носителях. Здесь проблем хоть отбавляй: и риски высоки, и кейсов много, и защищенность компаний весьма слаба. Единственным способом обеспечить безопасность «физической» транспортировки является шифрование, однако применяется оно весьма неохотно.

Между прочим, известная проблема «украденного ноутбука» также относится к этой стадии жизненного цикла. Согласно последнему исследованию Dell и Ponemon Institute, только в американских аэропортах за год теряется 637 тыс. (!) мобильных компьютеров, многие из которых содержат конфиденциальную информацию. Практика показывает, что в подавляющем большинстве случаев на пропадающих ноутбуках не используется ПО для шифрования данных.

5. Использование документа

На данном этапе жизненного цикла возникают лишь внутренние риски, которые являются достаточно опасными. К этой стадии мы относим только угрозы легитимного доступа к конфиденциальным сведениям. Работая с документом, сотрудник может исказить его содержимое, скопировать его в ненадлежащее место, опубликовать на общедоступном веб-ресурсе или переслать конкуренту. Совсем не обязательно он поступает так специально, однако компании от этого легче не становится. Контроль данных во время использования — основная проблема информационной безопасности. С помощью специальных систем защиты класса DLP, перехватывающих трафик по различным каналам, компаниям приходится следить за собственными сотрудниками. Причем одни продукты контролируют только сетевые каналы (e-mail, HTTP, FTP, IM, P2P), другие — только локальные (USB, CD/DVD), а третьи предоставляют комплексную защиту. Существует два основных способа контроля трафика, идущего по различным каналам. Первый способ — контентная фильтрация (решения InfoWatch Traffic Monitor, Symantec Vontu DLP 8, RSA Data Loss Prevention). Он предполагает угадывание конфиденциальных документов на основе их контента или метаданных (контекста). Понятно, что подобное «гадание» по определению является не точным — по оценкам компании Gartner, контентная фильтрация блокирует не более 80% конфиденциальных документов.

ПК Dell под защитой «Касперского»

●●◐ «Лаборатория Касперского» и компания Dell сообщили о начале продаж на российском рынке ПК Dell с предустановленным защитным комплексом Kaspersky Internet Security 2009. Данным решением будут комплектоваться настольные компьютеры и ноутбуки Dell серий XPS, Inspiron и Vostro.

Комментирует Дмитрий Лисовицкий, менеджер по развитию сервисной поддержки Dell: «Модельный ряд компьютеров Dell ориентирован на разные целевые группы — от домашних пользователей до офисных сотрудников, большая часть которых пользуется Интернетом. К сожалению, многие задумываются о приобретении защитного решения только после того, как вредоносное ПО причинит ущерб. Теперь покупатели компьютеров Dell с первого дня эксплуатации устройства находятся под защитой Kaspersky Internet Security 2009». Решение Kaspersky Internet Security 2009 будет поставляться в виде пробной версии сроком на 30 дней. Продление лицензии осуществляется на общих основаниях.

Новая версия сервера баз данных от Microsoft

●●◐ Компания Microsoft выпустила очередной релиз сервера баз данных — SQL Server 2008. Новая версия поддерживает управление по схеме политик; функции аудита; также в ней расширен функционал служб анализа и предоставления отчетов.

Доступны следующие версии: SQL Server 2008 Enterprise ($24 тыс. за один серверный процессор или $9 тыс. за сервер и $160 за каждую клиентскую лицензию) позволяет консолидировать серверы и обеспечивать широкомасштабную обработку транзакций; SQL Server 2008 Standard ($6 тыс. за один серверный процессор или $1 тыс. за сервер и $160 за каждую клиентскую лицензию) предполагает организацию баз данных для работы на уровне одного подразделения крупной компании.

Второй подход — расстановка меток — используется в продуктах Perimetrix SafeSpace и McAfee Total Protection for Data. В отличие от контентной фильтрации, этот метод гарантирует 100%-ную точность, но только для классифицированных документов.

6. Резервное копирование документа

На этой стадии не исчезают риски, характерные для этапов хранения и транспортировки документов. Теоретически доступ к архивам могут получить и хакеры, и внутренние сотрудники, а диски с резервными копиями теряются во время транспортировки не реже остальных носителей. Однако при тех же механизмах защиты риски утечки на указанной стадии снижаются, поскольку ценность информации падает, а к резервным копиям обычно относятся достаточно бережно. Вот почему на этапе резервного копирования лучше бороться с другими проблемами, а именно с избыточным хранением документов. Зачастую компании допускают утечки устаревших персональных данных, однако из-за таких происшествий репутация фирм все равно страдает. Поэтому при построении систем резервного копирования важно хранить минимально возможное количество информации.

7. Удаление документа

Удаление документа важно провести. Большинство документов хранятся в архивах, пока не кончится место, повышая тем самым вероятность возможной утечки данных. Зачастую архивные носители продаются третьим лицам или компаниям, вместе с содержащейся на них информацией. Однако и удаление документа должно быть организовано правильно. Простое нажатие кнопки Delete и даже удаление файла из корзины совсем не означает очистку соответствующих областей диска. Фактически исчезает лишь заголовок файла в файловой системе, но его содержание остается на месте. Информацию, удаленную столь примитивным образом, легко восстановить с помощью специальных программных комплексов. Некоторые компании предпочитают не связываться с «мягким» (программным) удалением и «жестко» уничтожают физические носители с особенно секретными сведениями. Понятно, что такой подход обеспечивает максимальную надежность, однако требует определенных инвестиций в новое оборудование.

Кроме удаления цифровых сведений, нельзя забывать и об уничтожении (шреддинге) бумажных документов. Бумаги со строго секретными сведениями до сих пор появляются во многих мусорных контейнерах, и вряд ли эта ситуация радикально изменится.

Таблица 3. Основные угрозы утечки на стадии использования документа. Источник: Perimetrix, 2008

Угроза	Описание	Реальный кейс утечки	Системы защиты
Инсайдерская утечка.	Кража конфиденциальной информации сотрудником компании, который имеет к ней легальный доступ.	В августе нынешнего года был арестован сотрудник крупнейшей ипотечной компании Countrywide. Предполагается, что он украл и продал более 2 млн. приватных записей соискателей ипотечных кредитов.	Системы защиты от утечек (DLP), системы блокировки доступа к локальным портам.
Веб-утечка.	Публикация конфиденциальной информации на интернет/интранет-серверах. Одна из наиболее популярных угроз утечки.	В конце августа нынешнего года на сайте американского агентства Bloomberg случайно был опубликован некролог на живого главу компании Apple Стива Джобса. По-видимому, издание не верит в выздоровление Джобса, который уже достаточно давно борется с раковой опухолью.	Системы защиты от утечек (DLP), административные методы (обучение).
Саботаж или искажение сведений.	Сознательное изменение или удаление информации сотрудниками компании.	Администратор муниципальной сети Сан-Франциско Терри Чайлдс заблокировал доступ к управлению сетью после того, как его уволили с работы. После длительных переговоров Чайлдс раскрыл пароль администратора мэру города, однако часть сетевых сервисов так и не удалось восстановить.	Системы резервного копирования.

Единая система или разрозненные комплексы?

Итак, риски утечки возникают практически на всех стадиях существования документа. Популярные DLP-системы защищают от утечки только на одной жизненной стадии и потому не могут предоставить никаких гарантий. В идеале любая компания хочет получить комплексное решение, способное предоставить защиту информации на всех этапах жизненного цикла. Проблема только в том, что полностью универсальных решений не бывает и вряд ли они появятся когда-либо. Вендор, который ориентируется на борьбу с вирусами, не сможет обеспечить хорошую защиту от внутренних утечек и наоборот. Другими словами, совмещать все инструменты защиты в одном решении бесполезно; гораздо важнее добиться синергии за счет интеграции отдельного функционала. Например, если решение умеет проводить классификацию документов — ему значительно проще защитить компанию от внутренних утечек. А также использовать шифрование для защиты только конфиденциальных сведений. К сожалению, подавляющее большинство современных продуктов такой синергией не обладает. Изначально эти системы разрабатывались для защиты от конкретных угроз на конкретных этапах жизненного цикла и потому не обеспечивали целостной защиты. В дальнейшем продукты эволюционировали, в них появлялись новые функции, но новые концепции — практически никогда. В итоге в компании возникает «зоопарк» разрозненных и не интегрированных друг с другом решений. Каждое решение несет ответственность за свой уникальный участок, но ни одна система не отвечает за утечки информации в целом. Для построения целостной концепции защиты необходимы продукты, которые поддерживают эту концепцию и обеспечивают синергию защитных инструментов на разных этапах жизненного цикла. Отличным примером такого решения является продукт Perimetrix SafeSpace, который изначально проектировался под методологию защиты информации на всех этапах жизни документа Если же отсутствие целостной защиты для вашей компании не является критичным — то выбор может лежать в другой плоскости, в частности в применении разрозненных систем.

Контроль данных во время использования — основная проблема информационной безопасности. Приходится следить за сотрудниками с помощью систем защиты класса DLP, которые перехватывают трафик по различным каналам