http://www.lanmag.ru ФЕВРАЛЬ 2010

ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ LAN

ЗАЩИТА

ОТ УТЕЧКИ ДАННЫХ

> СГБП для небольшого ЦОД

> Виртуализация на всех уровнях

> Как защитить базу данных

ISSN 1027086-8
10002
9 771027 086001

Недремлющее око

Системы защиты от утечек конфиденциальных данных – это глаза и уши администраторов, ответственных за обеспечение информационной безопасности. Разработчикам решений для быстро развивающегося рынка DLP предстоит сделать немало, однако им уже сейчас есть что предложить своим заказчикам.

Сергей Орлов

Для российского рынка информационной безопасности минувший год выдался непростым, но, как отмечают специалисты компании Aladdin, никто из серьезных игроков «с дистанции не сошел». Напротив, они сумели не только адаптироваться к трудным финансовым условиям, но и открыть для себя новые перспективные сегменты. Однако рынок ИБ в целом в прошлом году не вырос, поскольку даже закон «О персональных данных» немногие озаботились соблюсти в полной мере, тогда как большинство предприятий только начало присматриваться к этому нормативному акту. «Небольшое количество проектов, реализованных в этой области, позволило лишь компенсировать спад продаж продуктов и услуг по другим направлениям рынка ИБ», — констатирует Алексей Лукацкий, бизнес-консультант по безопасности Cisco Systems.

По наблюдениям сотрудников компании Aladdin, в прошлом году основной интерес был прикован к развитию ситуации вокруг закона «О персональных данных» (№152-ФЗ). Обсуждение реальных сроков выполнения его требований вышло за рамки специализированных мероприятий. Волна дискуссий, которую подняли операторы персональных данных, разработчики систем защиты информации, системные интеграторы, докатилась до Госдумы. Регулирующие органы прислушались к опасениям участников рынка, и срок приведения информационных систем в соответствие с законом №152-ФЗ был перенесен с 2010 на 2011 год.

Как показывают результаты опросов, руководители компаний осознают, что утечка данных (сведений о сделках, финансовых отчетов и бизнес-планов, объектов интеллектуальной собственности) и безответственность служащих остаются главными информационными угрозами. Количество краж растет: в прошлом году они стали причиной более половины инцидентов (см. Рисунок 1). Бороться с такими правонарушениями гораздо сложнее, чем с непреднамеренными утечками.

В этом контексте может получить развитие относительно новый сегмент систем защиты от утечек конфиденциальной информации/предотвращения потерь данных (Data Leakage Prevention/Data Loss Prevention, DLP). Однако в настоящее время в «обязательный защитный комплект» оператора персональных данных эти системы не входят. Компания или организация для выполнения требований закона вправе применять любые решения, в том числе DLP, хотя регулирующие органы, выполняя плановую проверку, как правило, положительно оценивают факт наличия такой системы.

На мировом рынке основным фактором роста сегмента DLP являются именно законодательные требования. За рубежом работа с персональными данными в различных отраслях регламентируется нормами HIPAA, GLBA и PCI-DSS. В использовании систем DLP лидируют финансовая отрасль, розничная торговля и здравоохранение.

Несмотря на то что в требованиях регулятора (ФСТЭК) нет такого класса систем, как DLP, представители заказчиков понимают их ценность для защиты персональных данных, полагает Николай Зенин, руководитель направления защиты коммерческих тайн LETA IT-company. Именно поэтому в рамках реализации программ по защите персональных данных было инициировано несколько проектов DLP. По экспертной оценке, около 30% крупных и средних российских предприятий уже используют у себя ту или иную функциональность DLP. Сегодня DLP — узнаваемый тип решений для конкретных задач борьбы с утечками.

По мнению участников рынка, закон №152-ФЗ стимулирует внедрение DLP в России. Рамиль Яфизов, ведущий специалист компании McAfee убежден, что шаги государства пойдут на пользу рынку ИБ в целом и DLP в частности. Аналитики Gartner относят законодательные и отраслевые требования, регламентирующие работу с важной информацией, к ключевым факторам, стимулирующим развитие рынка.

Однако закон «О персональных данных» может нарушить нормальное развитие рынка. Компаниям необходимо «созреть» для внедрения DLP. Кирилл Керценбаум, руководитель группы технических консультантов по безопасности Symantec, предостерегает: «Системы DLP должны помогать бизнесу, их нельзя устанавливать "для галочки", иначе заказчики придут к выводу, что это плохая технология».

В условиях рецессии идея защиты от инсайдеров техническими средствами стала еще более актуальной, ведь по данным зарубежных исследований, почти 60% уволенных сотрудников уносят с собой важные корпоративные данные, а около 70% используют конфиденциальную информацию покинутой ими компании. Как рассказывает Николай Зенин, из-за повышенной ротации кадров сотрудники стали «прикапывать» корпоративную информацию для повышения собственной значимости в глазах потенциального работодателя, поэтому у организаций появились дополнительные мотивы к внедрению решений, препятствующих такому хищению, — систем предотвращения утечек и шифрования хранилищ данных.

Решения DLP, именуемые «системами защиты конфиденциальных данных от внутренних угроз», могли бы помочь в борьбе с такими утечками. С другой стороны, сокращение бюджетов ИТ и высокая стоимость предлагаемых решений DLP (см. врезку «Проблема стоимости») могут воспрепятствовать росту данного сегмента. Как отмечают системные интеграторы, за время экономического спада несколько крупных проектов внедрения DLP было отложено в связи с «заморозкой», однако появилось еще больше новых заказчиков, в планах которых подобных проектов раньше не было.

Российские клиенты часто покупают комплексные решения DLP для защиты максимального числа каналов. DLP — неотъемлемая часть системы ИБ, неэффективная без других мер защиты, таких как межсетевые экраны, антивирусы и пр. Данный элемент защиты информации и минимизации рисков отнюдь не устраняет необходимости в защите периметра и контроле доступа (FW, IDS/IPS, NAC). Причем DLP — это не только продукты, но и административные меры, а также консалтинг.

В последние годы лишь немногие технологии безопасности пользуются столь пристальным вниманием. Технические семинары, круглые столы и конференции, посвященные DLP, собирают полные залы. Большой интерес российского бизнеса к проблеме защиты конфиденциальных данных продемонстрировала II Всероссийская конференция DLP-Russia 2009, прошедшая в октябре в Подмосковье. В ней приняли участие около 200 представителей отечественных и зарубежных компаний.

ТЕХНОЛОГИИ DLP

Программное обеспечение DLP осуществляет мониторинг передаваемых по сети и хранимых данных с целью предотвращения их несанкционированного использования или передачи. По мнению Николая Зенина, термин «предотвращение потери/утечки данных» звучит слишком многообещающе. В действительности системы DLP могут лишь контролировать перемещение и выявлять места хранения конфиденциальной информации, а предотвратить утечку удается только при выполнении нескольких условий: DLP была предварительно «обучена» на опознавание конкретных конфиденциальных данных, нарушитель передал достаточный для реагирования системы объем данных через тот канал, на который она настроена, и включен режим блокирования подозрительных действий.

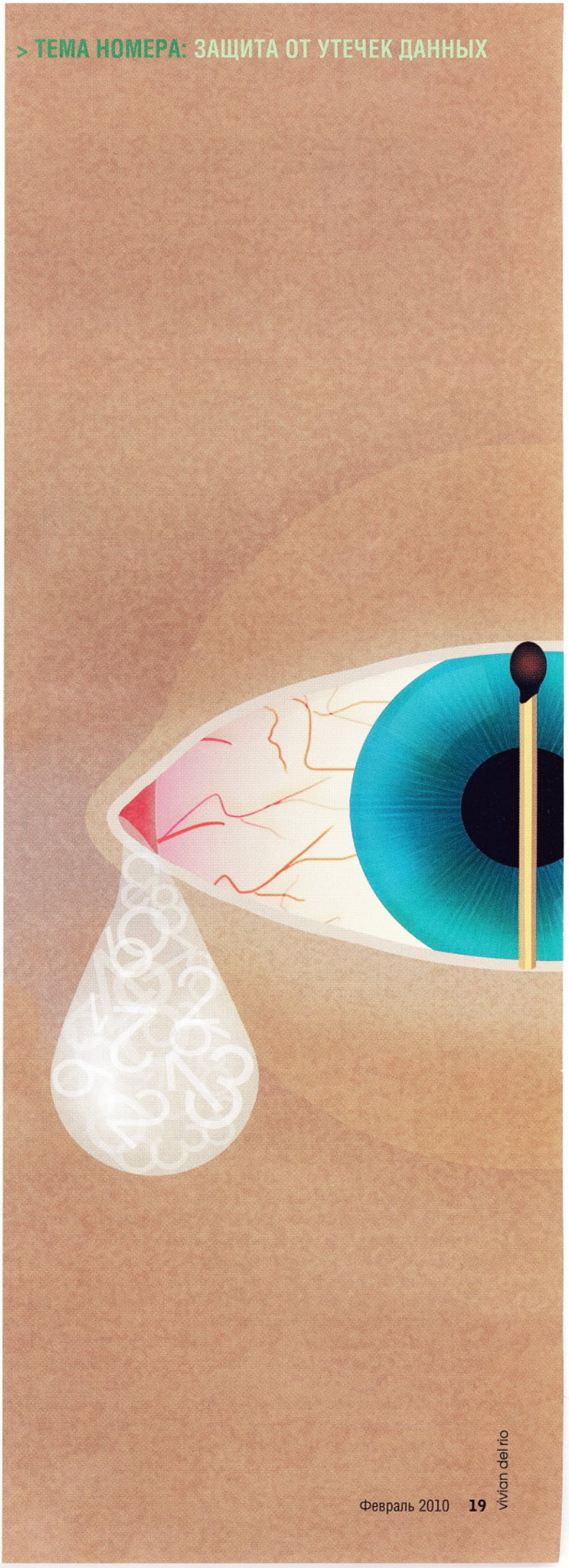
Специалисты LETA IT-company определяют DLP как автоматизированное средство, позволяющее распознавать и/или блокировать перемещение конфиденциальных данных в существенном объеме за пределы защищаемой информационной системы по всем каналам, используемым в повседневной работе. Валерий Боронин, руководитель лаборатории защиты информации от внутренних угроз «Лаборатории Касперского», считает более правильным говорить о контроле над преобразованием и перемещением данных, хотя термин DLP уже устоялся. По словам Алексея Лукацкого, DLP предполагает защиту конфиденциальных и персональных данных на уровне содержимого при их использовании, передаче и хранении, включая защиту от случайных или намеренных утечек (см. Рисунок 2), причем данные интересны для злоумышленников только в контексте, то есть когда становятся информацией. Такого же мнения придерживается Николай Зенин.

Система DLP должна обладать функциональными возможностями в трех сферах:

- Data-in-Motion (контроль передачи информации по каналам электронной почты и Web);
- Data-in-Use (контроль над операциями с конфиденциальной информацией на уровне рабочей станции);
- Data-at-Rest (сканирование сетевых ресурсов для обнаружения мест ее хранения).

Функции управления системой (задание правил реагирования, политик, логики классификации информации) должны выполняться с единой консоли и предусматривать гибкое распределение прав доступа. По крайней мере, часть названных функций реализована в самых разных продуктах: их поставляют производители средств шифрования, защиты клиентских систем, межсетевых экранов.

С точки зрения технологии система DLP должна реализовывать сравнение шаблонов ключевых слов, точное сравнение данных, карантин для файлов при нарушении



vivian del rio

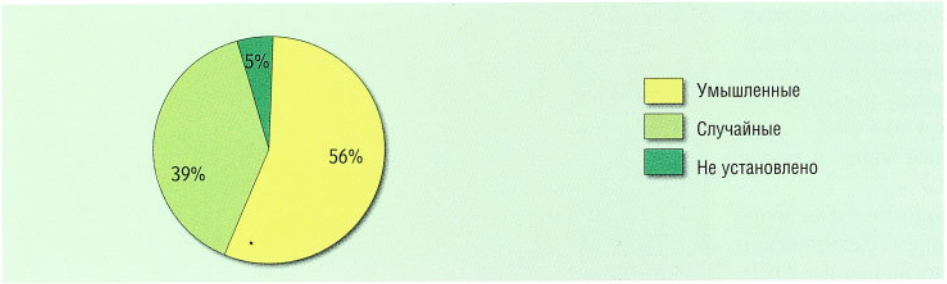


Рисунок 1. Доли умышленных и случайных утечек в I полугодии 2009 года (по данным InfoWatch).

Проблема стоимости

По данным опроса Forrester, в числе основных проблем внедрения решений DLP — высокая стоимость (на это указывают 49% опрошенных), архитектурная сложность и трудоемкость использования (36%), наличие собственных внутренних стандартов и политик (35%), сложность и незрелость технологий (27%), сложность классификации данных (16%). Треть респондентов, опрошенных аналитиками GTB Technologies, отмечают, что стоимость реализации системы DLP оказалась выше планируемой, а четверть говорят о высокой — по сравнению с ожидаемой — стоимости управления.

Как отмечает Наталья Касперская, в настоящее время основные заказчики систем DLP — достаточно крупные компании (1—5 тыс. пользователей), однако к ним проявляют интерес и в сегменте SMB. По данным InfoWatch, более 60% небольших компаний (100—200 рабочих мест) планируют внедрение DLP, и в этом сегменте высок уровень понимания проблемы.

Что касается зарубежных вендоров, то их системы DLP рассчитаны не только на средний и крупный бизнес. Они вполне по карману небольшим компаниям: начальная стоимость составляет 100 долларов за рабочее место (для сети из 100 рабочих станций), а в августе 2009 года компания Sophos представила решение Endpoint Security and Data Protection 9, где в расчете на одного пользователя придется заплатить 35 долларов (для сети из 500 рабочих станций). Однако в среднем цены пока высоки. По данным Forrester Research, внедрение системы DLP для пары тысяч рабочих мест обойдется от 250 до 500 тыс. долларов, хотя с ростом конкуренции потенциальные расходы будут снижаться.

Системы DLP могут вполне успешно справляться со своими обязанностям, но заказчикам следует быть готовыми к тому, что их внедрение связано со скрытыми затратами и потребует значительных усилий в плане управления. Как показывают опросы зарубежных компаний, около половины организаций, внедривших DLP, планируют заменить его на иное решение. В ближайшую пару лет сложный и дорогостоящий процесс внедрения DLP должен значительно упроститься.

ими политики безопасности, предусматривать возможность задавать комбинации данных для сравнения и выявления при хранении и при перемещении, а также включать в себя средства вывода отчетов.

В системах DLP применяются сложные механизмы анализа: сравнение по шаблонам с использованием словарей и регулярных выражений, лингвистический и контекстный анализ, цифровые отпечатки. Словари и шаблоны удобно применять в конкретных областях, например, для контроля номеров кредитных карт и других персональных данных. В лингвистическом и контекстном анализе используются морфология и статистические модели, учитывается контекст, характер отправителя и получателя информации. Этот метод хорош для динамических данных. Цифровые отпечатки (аналогичные сигнатурам в антивирусных продуктах) подходят для контроля статических данных, например, для защиты интеллектуальной собственности.

Между тем внедрение системы DLP ничего не даст, если в организации отсутствует четкое представление о том, каким образом данные распространяются внутри компании и выводятся за ее пределы. Для определения типов данных нужно классифицировать информацию согласно ее характеру и местонахождению. Например, интеллектуальную собственность могут представлять электронные чертежи и документы, персональные данные используются в различных приложениях (системах онлайновых продаж, обработки заказов и пр.).

Полноценная защита от утечек данных требует организационных и технических мер. Внедрение DLP необходимо начинать с реализации корпоративной политики по работе с данными. Кроме того, для этого нужен определенный уровень зрелости компании.

Несмотря на достаточно ощутимое продвижение DLP и связанную с этим информационную активность со стороны вендоров и системных интеграторов, многие заказчики переоценивают возможности подобных решений. Нередко сначала выбирается решение, а затем его пытаются «наложить» на бизнес-процессы и инфраструктуру в организации, хотя последние следует анализировать в первую очередь. Только в этом случае, как считает Николай Романов, технический консультант Trend Micro в России и СНГ, удается сформировать четкую схему построения защиты.

Forrester рекомендует начать внедрение DLP с решения конкретной задачи, например, с защиты информации о кредитных картах, вовлечь в этот процесс максимальное число сотрудников разного уровня и совершенствовать процессы DLP на основе полученных результатов. Для успеха реализации необходимы классификация данных, локальные правила их использования и выявление инцидентов. Нужно проанализировать, как работают пользователи, чтобы автоматический контроль был действенным.

Для защиты персональных данных требуется поиск и изучение обрабатываемой и хранимой информации, оценка рисков и угроз, выработка эффективных методов противодействия утечкам, построение информационной системы и процессов работы с данными, мониторинг и отчетность. Начальный этап предполагает контроль всех передаваемых по сети данных и выявление мест их хранения. Он должен дать руководителям предприятия четкое понимание того, что происходит с конфиденциальной информацией.

Список возможных действий с данными Gartner рекомендует ограничить 10–15 ситуациями, включая передачу данных за периметр сети, их хранение в неразрешенных местах, перемещение, копирование, использование в бизнес-процессах. Реакция на инциденты должна соответствовать степени опасности. Как минимум, это уведомление администратора, отвечающего за безопасность, и запись в журнал для последующего анализа. В более серьезных случаях — автоматическое шифрование данных, их перемещение из зоны риска, получение подтверждения операции у пользователя или автоматическая отмена (блокирование) операции.

К системам DLP с функциями анализа контента эксперты Gartner относят технологии классификации содержимого объектов (файлов, сообщений или передаваемых по сети данных), к которым можно динамически применять политики — ставить метки, шифровать или использовать средства Enterprise Digital Rights Management (EDRM). При классификации контента применяются цифровые отпечатки, статистические методы (байесовские или обучение), ключевые слова и сравнение по словарю,

а также распознавание «водяных знаков». В Forrester считают, что к определенной категории данных нужно применять соответствующую категорию DLP (контроль хранимых данных, фильтрацию трафика и др.) и средства шифрования — в зависимости от их стоимости.

При выборе DLP нужно ответить на ряд вопросов: какие данные и объемы данных покидают сеть, во что обходятся инциденты, сколько стоит контроль безопасности, как повлияет на уровень риска изменение этого контроля. Перед внедрением системы DLP полезно развернуть другие решения ИБ, классифицировать данные, разграничить права пользователей. Обычно это сопровождается совершенствованием корпоративной политики передачи и хранения важных данных. Положительный побочный эффект — наведение порядка в данных. Кроме того, DLP может стать эффективным средством для сбора доказательной базы при расследовании инцидентов. Однако в процессе внедрения DLP трудно определить, данные какого типа следует контролировать и что делать с отмечаемыми системой сообщениями.

Возможно, как подчеркивает Валерий Боронин, полноценная система DLP в каких-то ситуациях просто не нужна. Иногда есть смысл использовать узкоспециализированные продукты, снимающие риски более точечно. Это системы класса Rights Management Services/Digital Rights Management (RMS/DRM), контроль устройств, шифрование, мониторинг и архивирование почты и т. д. Системы управления правами (RMS) — наиболее мощный конкурент DLP, с его помощью удается избежать многих известных сценариев утечки информации и ограничить перечень разрешенных операций: печать документа, копирование фрагментов, отправка по каналам электронной почты и т. д. Однако на мировом рынке нет однозначного лидера, и даже понимание того, как следует развивать это направление, отсутствует. Технологии ведущих компаний мало похожи, и их применение в проектах, различающихся по масштабам (количество узлов) и типам защищаемых данных, может привести к противоположным результатам.

Аналитики прогнозируют успех системам DLP, интегрированным со средствами защиты авторских прав (DRM), управления учетными данными пользователей (Identity Management, IDM) и доступом. DRM обеспечивает доступ к информации только уполномоченных лиц, но не предотвращает утечки данных и не заменяет DLP. Разработчики продолжают совершенствовать технологии DLP, растет осведомленность о них потенциальных заказчиков.

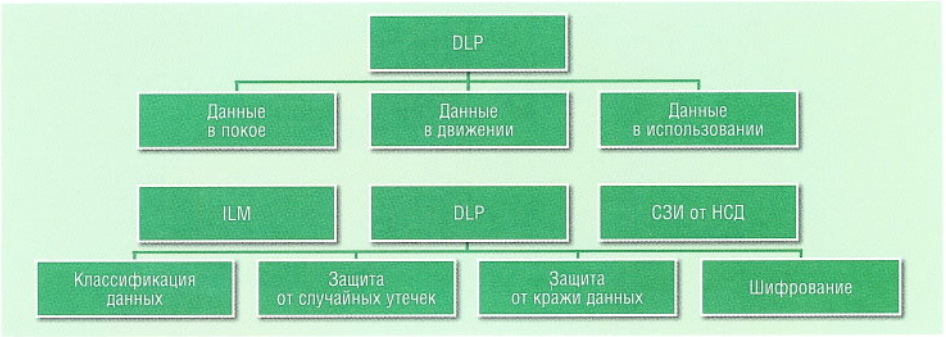


Рисунок 2. Классификация DLP (по данным Cisco). Система DLP должна, как минимум, идентифицировать, отслеживать и защищать данные «в движении», «в покое» и во время их использования с помощью глубокого анализа контента. Смежными областями являются управление жизненным циклом хранения информации (ILM) и защита от несанкционированного доступа (НСД).

КОНСОЛИДАЦИЯ РЫНКА И ПРОДУКТЫ DLP

За последние несколько лет на мировом рынке произошли заметные изменения: начинающие разработчики DLP — Reconnex, Orchestria, Vontu, Provilla и Tablus — были поглощены более крупными производителями решений безопасности. RSA Security (подразделение EMC) приобрела компанию Tablus, разработки которой стали частью пакета RSA Data Loss Prevention Suite, Symantec купила Vontu, McAfee — Reconnex, Websense стала владельцем PortAuthority Technologies, а Orchestria вошла в состав компании CA. В числе немногих оставшихся независимых поставщиков DLP — Code Green Networks, Fidelis Security Systems и разработчики ПО с открытым исходным кодом.

Symantec использовала разработки Vontu в девятой версии Symantec DLP, выпущенной в марте 2009 года. В настоящее время этот продукт состоит из трех технологических и одного управляющего модуля. Два отвечают за контроль сетевого трафика (Network Monitor и Network Prevent) и рабочих станций (агент Endpoint Discover и Endpoint Prevent), а третий предназначен для контроля систем хранения — он проверяет по заданному графику, соответствует ли хранение конфиденциальных данных корпоративной политике.

Кроме того, Symantec интегрировала DLP в свой шлюз электронной почты BrightMail и продукт управления Altiris. При помощи ПО Altiris 7 можно осуществлять развертывание агентов Prevent и Discover, контролирующих рабочие станции. Например, если пользователь пытается переписать важные данные на накопитель USB, то в клиентской системе фиксируется инцидент, действие отменяется, а сведения о нем регистрируются в системе DLP. Соответствующее сообщение отправляется в Altiris, и порт USB блокируется, пока инцидент не будет разрешен.

Как считает Кирилл Керценбаум, защита должна быть многоуровневой и эшелонированной (см. Рисунок 3). ПО информационной безопасности для пользовательских ПК должно включать в себя не только антивирус, межсетевой экран, системы защиты от различных атак, но и функции контроля использования съемных устройств, запуска приложений и доступа к сети. Это первый эшелон обороны для предотвращения утечек конфиденциальной информации. В арсенале Symantec таковым является продукт Symantec Endpoint Protection (SEP) 11.0. Защита серверов баз данных и систем ERP составляет второй уровень. Для него Symantec предлагает IPS/IDS под названием Symantec Critical System Protection 5.2, который оберегает критически важные системы и сервисы ОС UNIX/Linux/Windows. Третий уровень — защита периметра информационной системы от утечек данных. Ее обеспечивает Symantec DLP.

В ноябре 2009 года Symantec выпустила продукт Symantec Data Loss Prevention 10. Компания позиционирует его как первую открытую платформу DLP для защиты данных в корпоративной среде и предотвращения их утечки, при этом подчеркивается многоуровневый и контентно-ориентированный характер защиты. Он поддерживает управление правами (Enterprise Rights Management, ERM) на основе контента, позволяет шифровать информацию, задавать политики, управлять инцидентами и будет интегрирован с другими решениями Symantec.

Symantec сочетает технологии DLP с услугами консалтинга: заказчики получают детальный анализ пробелов в защите, количественную оценку потерь данных в сетях, приложениях Web и клиентских системах. Компания планирует теснее интегрировать DLP с приложе-

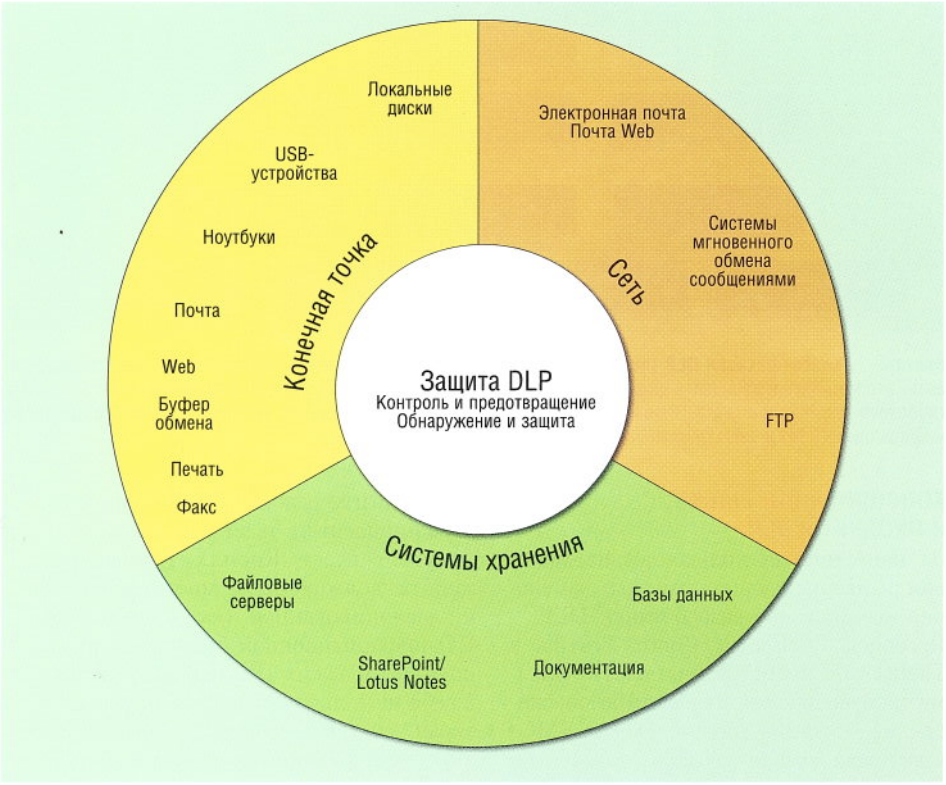


Рисунок 3. Решения Symantec для защиты персональных данных. DLP представляет собой один из элементов общей системы информационной безопасности.

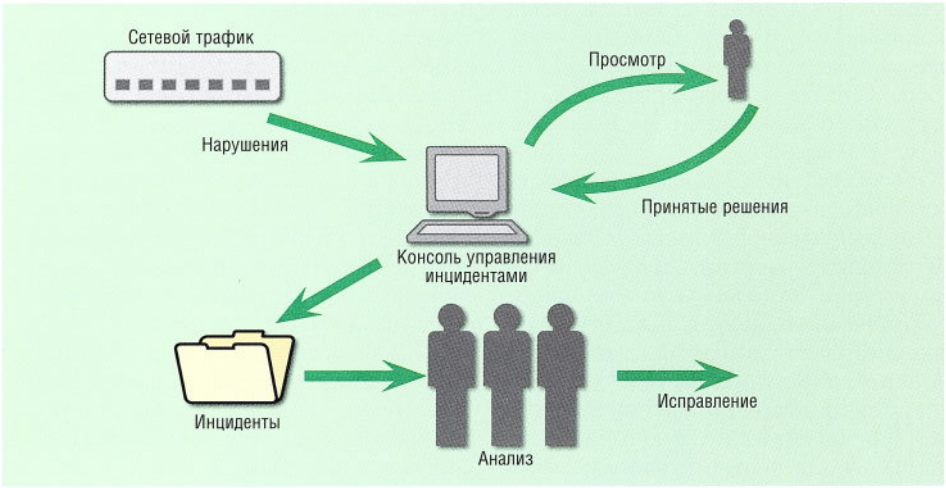


Рисунок 4. Управление инцидентами в системе DLP от McAfee. Консоль работы с инцидентами дает представление о событии, она позволяет быстро обрабатывать инциденты и при необходимости настраивать политики. Администраторы получают возможность работы с архивными данными инцидентов для выявления причин и угроз.

ниями хранения данных. Например, ПО Symantec DLP Discover уже интегрировано с Backup Exec System Recovery.

Стратегическим партнером Symantec по DLP является HP: EDS, приобретенная этой компанией, поддерживает Symantec DLP на основе аутсорсинговых соглашений с корпоративными клиентами и даже предоставляет Symantec услуги по управлению системой DLP. Как ожидается, некоторые функции Symantec DLP будут интегрированы с коммутаторами HP ProCurve и развернуты в ЦОД HP.

Такие гиганты, как Microsoft и Cisco, еще не приобрели разработчиков DLP, но зато они сотрудничают в этой области с RSA. Например, Cisco объявила об интеграции функций DLP от RSA в решение Cisco IronPort. Microsoft намерена использовать технологию RSA в своих будущих продуктах, однако сейчас эти разработки находятся на ранней стадии.

В апреле 2009 года RSA обновила свой пакет DLP, добавив более десятка шаблонов политик для распознавания персональной информации. Продукт RSA Data-Loss Prevention (DLP) 7.0 осуществляет мониторинг несанкционированного использования или передачи важной информации и включает в себя сетевые, клиентские компоненты и средства управления. Он интегрирован с платформой управления событиями безопасности RSA EnVision. Сведения об инцидентах собираются в централизованную базу данных и могут использоваться для расследования. Начальная стоимость DLP 7.0 составляет 50 тыс. долларов.

RSA является частью EMC, владеющей также VMware, поэтому дополнение продуктов виртуализации VMware функциями DLP — вопрос времени. Специалисты RSA считают, что средства DLP вполне можно встроить и в системы резервного копирования; кроме того, они должны играть важную роль в сборе информации для расследования инцидентов (eDiscovery) и управлении жизненным циклом данных (ILM).

В конце 2008 года с приобретением начинающего разработчика Reconnex на рынок DLP вышла компания McAfee. Компоненты ее системы DLP, которой уже пользуются более 500 корпоративных клиентов, устанавливаются на рабочих станциях (хост-системах) и сетевых шлюзах.

McAfee Host DLP можно использовать как автономное ПО или как часть пакета McAfee Total Protection for Data Endpoint. Продукт интегрирован и с McAfee SafeBoot, предназначенным для шифрования данных. Host DLP устанавливается через консоль ePolicy Orchestrator. С помощью функции контроля устройств (Device Control) можно задавать правила работы с устройствами разных типов или с конкретными устройствами (по серийному номеру), оснащенными функциями блокировки операции, оповещения пользователя и ограничения доступа (например, «только чтение»).

Как подчеркивает Рамиль Яфизов, нельзя полагаться только на сетевые компоненты DLP. McAfee Host DLP следит за соблюдением корпоративных политик на пользовательских ПК под управлением Windows и Linux, предусматривает интеграцию с Microsoft AD, централизованную систему мониторинга и сбор событий в журналах безопасности.

Решение DLP включают в себя также шлюзы Prevent (защита от угроз по каналам электронной почты и Web), Discover (выявление и индексация всех данных в организации), Monitor (защита данных

при их перемещении в сети) и Manage (централизованное управление защитой персональных данных и разбор инцидентов). Разные серверы-шлюзы отвечают за разные части технологии DLP. McAfee Host DLP, Network DLP Prevent и Monitor работают с консолью управления McAfee ePolicy. В 2010 году McAfee собирается добавить движок DLP в интегрированную систему, объединяющую шлюз Web, шлюз электронной почты, межсетевой экран и IPS (см. врезку «На волне интеграции»).

Разработчики McAfee автоматизировали подготовительный этап развертывания DLP: обычно на него отводится 6–12 месяцев — автоматизация позволяет сделать работу за считанные дни. Система McAfee «слушает» и индексирует весь корпоративный трафик, чтобы получить полную картину перемещения данных, которые реконструируются из сетевых пакетов и индексируются. Как утверждают в McAfee, такой подход позволяет достаточно быстро построить законченное решение для защиты персональных данных (см. Рисунок 4). Готовые компоненты остается лишь установить и запустить в эксплуатацию. Типичная стоимость проекта составляет 50—100 тыс. долларов.

Решение DLP компании McAfee поддерживает присваивание данным грифа секретности с помощью меток — по контенту (с анализом регулярных выражений), приложениям, местонахождению (в соответствии с классификатором). Гриф хранится вместе с файлом, и удалить эту метку невозможно — операции контролируются процессами DLP. Сами процессы DLP на рабочей станции тоже «неубиваемы»: таких процессов два, и каждый из них проверяет правильность действий другого. Гриф можно использовать для контроля соблюдения политики безопасности, причем система сохраняет его при последующих преобразованиях файла.

Trend Micro, купившая продукт LeakProof компании Provilla, которую в Gartner считают нишевым игроком на рынке DLP, сейчас фокусирует внимание на рабочих станциях («конечных точках»), однако, уже в середине 2010 года должен появиться шлюз с функциями DLP, который компания собирается интегрировать с почтовыми и интернет-шлюзами. Кроме того, в 2010 году функциональность DLP появится и в продукте ScanMail for Exchange для защиты серверов Microsoft Exchange. В текущей версии LeakProof работает как автономный агент DLP. Его можно скрыть в списке системных процессов, что при корректных политиках в организации дает возможность отслеживать и блокировать несанкционированные действия незаметно для сотрудников. Решение обеспечивает как контроль записи на периферийные устройства (USB, Bluetooth, оптические приводы, вывод на печать и пр.), так и передачу через информационные каналы (почтовая переписка, включая почту Web, общение в Skype и программах обмена мгновенными сообщениями; пересылка файлов по сети внутри организации и др.).

В августе 2009 года Trend Micro анонсировала две редакции системы DLP для клиентских систем под управлением Windows. LeakProof 5.0 Standard служит для мониторинга пользователей и данных, а Advanced — для защиты интеллектуальной собственности и исходного кода программ. Стандартная редакция нацелена в основном на мониторинг важных данных, а расширенная добавляет контроль документов по цифровым отпечаткам. Управление обеими осуществляется с помощью специализированного устройства LeakProof Server или виртуального сервера на базе VMware ESX 3.5. Кроме того, работа с защищаемыми документами облегчается за счет автоматизированного сбора данных из различных источников (сейчас это файловые хранилища и серверы SharePoint, а в 2010 году к ним добавятся базы данных и другие хранилища). ПО LeakProof 5.0 поставляется с шаблонами для защиты данных от утечек, разработанными согласно законодательным требованиям, например, для стандарта PCI DSS. Продукты LeakProof 5.0 Standard и Advanced стоят, соответственно, 48 и 68 долларов за место.

Год назад CA приобрела недавно созданную компанию Orchestria. Продукты последней для шлюзов и мониторинга ПК теперь называются CA DLP. Они интегрированы со средствами шифрования Voltage, PGP и BitArmor, поэтому разрешенные для отправки важные данные можно автоматически шифровать. Кроме того, CA является сильным игроком на рынке IDM и управления доступом. Для задания политики работы с данными ее система DLP может взаимодействовать с продуктом CA IDM или с решениями, поддерживающими LDAP (например, Microsoft Active Directory).

На волне интеграции

Как и другие решения безопасности, системы DLP подхватила волна интеграции. Этому способствовала покупка разработчиков систем DLP крупными игроками рынка ИБ. Создатели систем информационной безопасности ищут новые способы использования функций DLP, интегрируя их с системами хранения, антивирусными пакетами и т. д. Применение в системе DLP нескольких интегрированных технологий позволяет достичь синергетического эффекта и получить ряд преимуществ.

Кроме того, функции DLP расширяются за рамки отдельных продуктов и встраиваются в другое оборудование и ПО. Например, вендоры встраивают движки DLP в шлюзы Web, электронной почты, межсетевые экраны и IPS, а компоненты для защиты хост-систем объединяются с антивирусами. В конечном счете функции DLP станут стандартной частью решений безопасности.

Как указывает Николай Зенин, уже сейчас разработчики активно интегрируют свои решения DLP с технологиями управления цифровыми правами на документы, криптографической защитой рабочих станций, средствами мониторинга и корреляции событий безопасности, почтовыми архивами. На смену им придут технологии, способные не только отслеживать, классифицировать, блокировать отправку информации, но и осуществлять интеллектуальное применение правил шифрования конфиденциальных документов. Несмотря на это, в ближайшие годы продукты DLP останутся отдельным классом решений, что предполагает особый подход в продвижении и реализации проектов.

Смысл интеграции — уменьшение стоимости владения и риска конфликтов между различными решениями, подчеркивает Валерий Боронин. В идеальном варианте должна быть единая консоль управления. Вместе с тем, объединять защиту от внутренних угроз с защитой от внешних (например, антивирусами) не всегда целесообразно по ряду причин, в первую очередь не технических. Системы DLP используют разные политики, логику работы и администрирование, поэтому в ближайшие годы они будут достаточно автономны.

Тем временем вендоры интегрируют функции DLP в существующие средства защиты рабочих станций и шлюзы. По мнению аналитиков Forrester, шлюз — наиболее простой и дешевый способ. В настоящее время технологии защиты рабочих станций рассматриваются как дополнение к DLP, однако, по прогнозам Gartner, к 2011 году наряду с быстрым ростом рынка следует ожидать широкого распространения средств защиты для клиентских платформ с функциями анализа контента и снижения на 50% стоимости программных агентов DLP для рабочих станций.

Многие крупные игроки на рынке ИБ приобретают вендоров, специализирующихся на разработке средств DLP. Однако на практике часто оказывается, что внедрение таких решений малоэффективно: новые функции плохо интегрируются с существующими средствами ИБ. Компании, которые пошли по пути самостоятельной разработки решений DLP, могут предложить своим заказчикам более сбалансированное, управляемое и масштабируемое решение, убежден Алексей Андрияшин, консультант по безопасности Check Point Software Technologies. Важнейший показатель эффективности системы ИБ — централизованное управление.

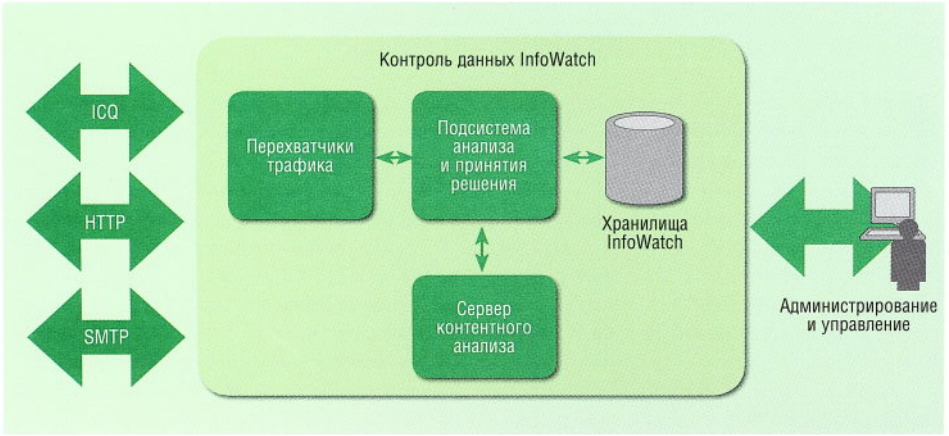


Рисунок 5. InfoWatch Data Control включает в себя сервер, обеспечивающий перехват, анализ и фильтрацию данных, хранилище для перехваченных данных и ретроспективного анализа, консоль администрирования и управления.

В сентябре 2009 года американская компания Trustwave приобрела Vericept. Trustwave разрабатывает ПО и предлагает услуги в сфере соблюдения стандарта PCI DSS для клиентов, осуществляющих операции с кредитными картами. Как ожидается, технологии Vericept DLP смогут сыграть важную роль в развитии этого направления. У Vericept около 400 заказчиков, и компания планирует продолжить продажу автономных продуктов DLP для рабочих станций и шлюзов, а также использовать эти разработки для предоставления услуг DLP по модели SaaS и сервисов удаленного управления шлюзами Vericept DLP на площадках своих клиентов. Функции DLP будут встроены и в программный агент Trustwave для защиты рабочих станций.

В октябре 2009 года Sophos объявила о покупке технологии DLP с анализом контента и добавила функции DLP к своему ПО для рабочих станций. Продукт Sophos Endpoint Security and Data Protection (ESDP) 9 содержит клиентские агенты как для DLP, так и для защиты от вредоносных программ. Система осуществляет мониторинг контента, передаваемого пользователем по электронной почте, через Web, носители USB или DVD, и при необходимости блокирует его. Программный агент проверяет наличие в содержимом вредоносного кода и конфиденциальной информации.

Новая версия Sophos ESDP имеет улучшенные функции контроля работы с внешними устройствами, включая накопители USB, внешние жесткие диски и беспроводные устройства (Wi-Fi, Bluetooth, IrDA). С помощью панели управления Enterprise Console администратор может централизованно задавать групповые политики и выводить различные отчеты. Разработчики Sophos подчеркивают, что использовали целостный подход с единым управлением — это позволило сделать продукт относительно недорогим и простым. В планах Sophos — выпуск шлюзового решения DLP.

Решения DLP российской компании InfoWatch (продукты InfoWatch Traffic Monitor Enterprise, InfoWatch Device Monitor и InfoWatch CryptoStorage Enterprise) успешно внедрены и используются крупнейшими российскими и зарубежными компаниями государственного сектора, финансовыми учреждениями, предприятиями телекоммуникационной отрасли, энергетики и др. InfoWatch накопила большую базу контентной фильтрации по опыту работы с крупными компаниями из разных отраслей.

По словам генерального директора InfoWatch Натальи Касперской, InfoWatch Traffic Monitor 3.3 эффективен как для статической, так и для динамической информации. Разработчики постарались сделать его простым в установке и эксплуатации. В нем применяется эвристический и контекстный анализ, все инциденты записываются, с файлов и трафика снимаются копии. Полученную информацию можно использовать в качестве доказательной базы при расследовании.

На конференции Cisco Expo 2009 было объявлено об интеграции InfoWatch Traffic Monitor с программно-аппаратным решением Cisco IronPort для защиты корпоративных сетей от внешних и внутренних угроз при передаче данных по протоколам HTTP, FTP и HTTPS. Интеграция двух продуктов осуществляется по протоколу Internet Content Adaptation Protocol (ICAP). Настройка политик позволяет определять правила работы для групп и отдельных пользователей.

В прошлом году компания выпустила решение InfoWatch Data Control для SMB (см. Рисунок 5). Как и Traffic Monitor оно представляет собой шлюзовую систему, устанавливается на сервере и осуществляет перехват и фильтрацию трафика HTTP, IM, SMTP, однако программных агентов для защиты рабочих станций не предусматривает. Инструменты InfoWatch защищают в основном от случайных утечек. Разработчики понимают необходимость защиты «конечных точек», но считают, что добавление этой функции сделает систему более сложной и дорогой.

В системе используется детектор объектов на основе регулярных выражений (паспортные данные, номера кредитных карт и пр.), цифровых отпечатков (защита статических данных) и защита на базе эвристики и контекстного анализа. Как утверждает Наталья Касперская, такой комбинации дополняющих друг друга технологий (особенно эвристики и контекстного анализа) у конкурентов нет. В основном система защищает три категории данных: интеллектуальную собственность, клиентские данные и информацию, обработка которой контролируется регуляторами (данные пластиковых карт, персональные данные и др.).

Разработчики постарались уложиться в приемлемую для заказчиков цену и предоставить требуемую функциональность. С помощью InfoWatch Data Control реализуется система аудита, позволяющая получить полную картину о потоках информации. Продукт поставляется в виде программно-аппаратного комплекса. Все компоненты интегрированы на одном сервере, простом в установке и администрировании.

InfoWatch намерена удешевить свой продукт (сейчас за него надо заплатить примерно 10 тыс. долларов). Однако разработчики подчеркивают, что в DLP применяются сложные технологии, и цена системы никогда не опустится до стоимости антивируса. Кроме того, внедрение такой системы предполагает предпроектный консалтинг и составление списка рекомендаций для клиента, поскольку затрагивается уровень бизнес-процессов. Одна лишь инсталляция программно-аппаратного решения эффекта не даст.

Стоимость, высокая сложность решений DLP и оправданность их применения для бизнеса являются для заказчиков важными факторами выбора. Поэтому рынок пока к ним только присматривается.

ЗАКЛЮЧЕНИЕ

По мнению аналитиков Gartner, стратегия DLP должна начинаться с определения типов данных, создания списка возможных операций с ними и составления корпоративной политики. Лишь после этого можно приступать к пере-

говорам с вендорами, которые обычно акцентируют внимание на отдельных аспектах DLP, но эффективной эта технология будет только при комплексной стратегии. По словам Николая Зенина, перед выбором решения DLP, организация должна сформировать собственные требования и иметь представление о параметрах защиты конфиденциальной информации: типах защищаемых информационных ресурсов и форматах хранения, ответственных владельцах этих ресурсов, способах обработки и каналах передачи информации, которые следует защищать в первую очередь.

На основе сформированных требований следует выбрать правильную платформу, подходящую именно конкретному предприятию. Различные системы DLP имеют разный уровень охвата каналов передачи информации, различаются архитектурной реализацией, применяют разные способы обнаружения и методики обработки инцидентов. Проект DLP предполагает определенную организационную подготовку. В компании должны быть налажены процессы классификации информации и обращения с ней. Он затрагивает уровень бизнес-процессов, однако для успешной реализации проект не должен предполагать серьезной перестройки процессов.

По словам Алексея Андрияшина, нередко приходится слышать негативные отзывы от компаний, решившихся на внедрение DLP. Причина тому — завышенные ожидания в отношении возможностей системы и ошибки на этапе планирования. Перед внедрением системы DLP в первую очередь нужно понять, от чего требуется защищаться — от умышленных или неумышленных действий сотрудников. Как показывает практика, наиболее эффективны системы DLP против неумышленных, ошибочных, халатных действий. Безусловно, они должны обладать функционалом, который позволяет выявить злоумышленника, но не менее важно суметь вовремя предостеречь сотрудника от совершения неверного действия при работе с корпоративной информацией. В большинстве случаев предупреждения будет вполне достаточно, чтобы предотвратить утечку информации.

Не все организации нуждаются в сложных и полнофункциональных инструментах DLP. Некоторым достаточно простых инструментов сканирования, не требующих значительных вычислительных ресурсов. Каждый проект по-своему уникален, но в любом случае сначала необходимо осуществить пилотное развертывание системы. Оно позволит оценить существующий уровень угроз и выбрать наиболее критичные для первого этапа эксплуатации способы

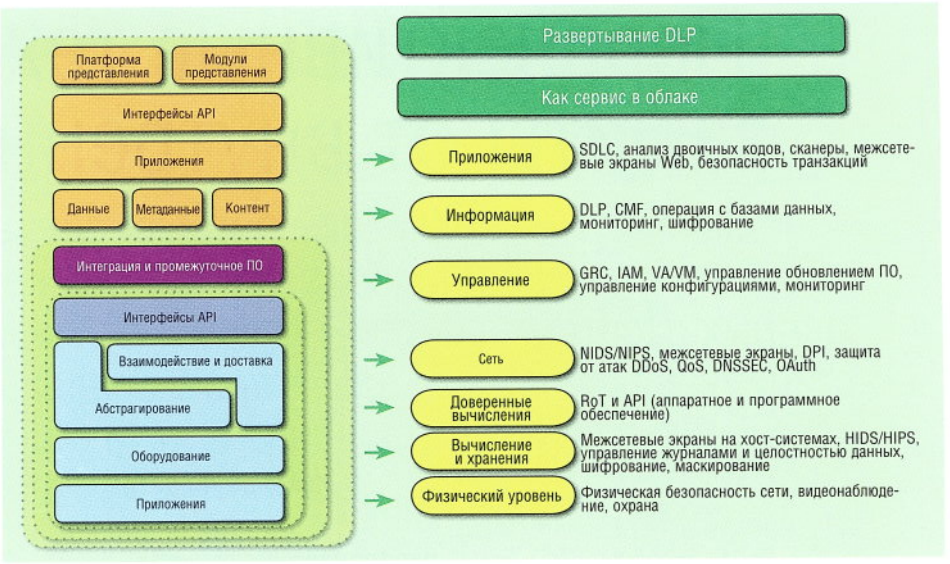


Рисунок 6. Развертывание DLP как «облачного» сервиса (по данным Cloud Security Services Alliance, CSA).

обработки информации. Иногда внедрение DLP требует длительной пилотной фазы (до трех лет).

По оценкам IDC, к 2012 году около 20% мирового рынка ИБ будут составлять услуги «безопасность как сервис». Новым подходом к внедрению DLP, особенно привлекательным в условиях кризиса, является модель «DLP как сервис» (см. Рисунок 6), когда заказчик платит лишь за услугу — ему не требуется покупать ПО, платформы, лицензии. Провайдер предоставляет полную поддержку, поэтому при возникновении какой-либо проблемы заказчик не остается с ней «один на один». Однако для подобного аутсорсинга DLP нужен надежный провайдер и четко сформулированные условия SLA. Дополнительно возникает проблема контроля утечек на стороне провайдера и традиционная для аутсорсинга проблема доверия к поставщику услуг.

Модель «DLP как услуга» в нашей стране не приживется, уверен Николай Зенин. В таком случае пришлось бы передавать «на сторону» обработку инцидентов, связанных именно с той информацией, которая не должна выходить за пределы организации. Вместе с тем системы DLP предусматривают гибкое разграничение прав при обработке инцидентов, и, например, внешней сервисной организации можно передать функции обработки потока инцидентов без ознакомления с содержимым, однако и эта модель вряд ли будет востребована.

Подчас системы DLP оснащаются дополнительными возможностями. Например, с их помощью можно выявлять сотрудников, недовольных компанией, или пресекать не предусмотренное политикой использование каналов доступа в Интернет. Такие функции могут оказаться полезными для заказчиков.

Внедрение решения DLP рассматривается в качестве важного элемента подготовки инфраструктуры ИТ к аудиту. В процессе реализации проекта приходится выяснять, где именно находятся конфиденциальные данные, как хранятся и используются, кто имеет к ним доступ. DLP позволяет пользователям эффективно взаимодействовать с конфиденциальными данными и автоматически обеспечивает выполнение заданных правил.

Однако очень малое число организаций обладает достаточной экспертизой в данной области, необходимой для оказания помощи в выборе, развертывании и правильной настройке даже самых лучших на сегодняшний день систем DLP, считает Валерий Боронин. Успех проекта DLP зависит от того, насколько руководители компании способны осознать его основные аспекты и обеспечить достаточное финансирование. Инициатива должна исходить от бизнес-подразделений. Подбирать решение, планировать пилотный проект и поэтапно решать все задачи необходимо при участии экспертов.

Оценить результат внедрения DLP довольно сложно. Нередко его считают успешным, если удалось приучить пользователей избегать рискованных действий, ведь чаще всего утечки случаются непреднамеренно. По прогнозам Gartner, в ближайшие шесть лет системы DLP получат в Европе широкое распространение. Многие компании уже подумывают об их развертывании. LAN

Сергей Орлов — ведущий редактор «Журнала сетевых решений/LAN». С ним можно связаться по адресу: sorlov@lanmag.ru.