http://www.lanmag.ru
ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ LAN

DLP в России

Согласно определению экспертов, защита от утечки данных (Data Leakage Prevention, Data Loss Prevention, DLP) — это автоматизированное средство для распознавания и/или блокирования перемещения большого объема конфиденциальных данных за пределы защищаемой информационной системы по любым используемым в повседневной работе каналам. В нашей стране системы DLP стали узнаваемым типом решений для борьбы с утечками. Реализации проектов по внедрению подобных систем, препятствующих хищению конфиденциальной информации, способствует изменение законодательных требований (в частности, закон о защите персональных данных) и растущее понимание важности защиты ценных информационных ресурсов, хранящихся в государственных и коммерческих организациях. Российским заказчикам доступны продукты DLP зарубежных вендоров (Symantec, WebSense, RSA, McAfee, Trend Micro, Verdasys), а также российские разработки, из которых наиболее известными являются решения InfoWatch.

Чем сегодня определяется интерес к системам DLP в России? Насколько они востребованы? Как считает Вениамин Левцов, глава представительства Trend Micro в России и СНГ, спрос на проекты DLP есть, и это подтверждают данные продаж. По его оценке, в 2010 году объем российского рынка решений DLP составит не менее 10 млн долларов, однако данный сегмент пока только формируется. На протяжении нескольких лет это был рынок одного игрока, компании InfoWatch, причем заказы поступали в основном от крупных компаний, да и тех было немного. В 2007–2008 годах на российский рынок были выведены сразу несколько решений DLP западных производителей. В результате активной работы системных интеграторов началась реализация целого ряда проектов. Появился выбор, сложилась практика использования, но системы DLP все еще воспринимаются как некоторое «излишество», их применение не предусматривается большинством общих политик безопасности, многие специалисты знают о них лишь понаслышке. Тем не менее, можно ожидать, что на рубеже 2011 года рынок перейдет на следующий уровень, когда внедрение таких систем станет общей практикой и для компаний среднего размера.

Как утверждает Рустэм Хайретдинов, заместитель генерального директора InfoWatch, системы DLP в классическом понимании слабо востребованы даже на американском рынке, где и возникло это понятие. В отличие от решений по защите инфраструктуры (антивирусов, межсетевых экранов, средств защиты от спама и т. п.), внедрение систем DLP — достаточно трудоемкая процедура, для успеха которой требуется обращение к консалтинговым услугам. Кроме того, отдачу от внедрения сложно измерить, поэтому мировой рынок «чистых» продуктов DLP стагнирует, а в России, по сути, он и не начал развиваться. Например, продукты DLP компании InfoWatch большинство клиентов используют не для предотвращения утечек, а для мониторинга обращений к конфиденциальной информации. Однако задачу защиты никто не отменял, как бы соответствующий класс продуктов ни назывался и какими бы разнообразными ни были сценарии их использования. Поэтому спрос есть, хотя и не такой большой, как прогнозировали аналитики.

Дмитрий Михеев, эксперт центра информационной безопасности компании «Инфосистемы Джет», указывает на следующую специфику данного сегмента рынка. Во-первых, в России сильны традиции тотального контроля в сочетании с игнорированием вопросов конфиденциальности и доступа к личной информации. Во-вторых, утечки действительно существуют, и вред от них значителен как в плане финансовых потерь, так и угрозы репутации. В-третьих, целый ряд регулирующих органов выдвигает требования к контролю утечек — от PCI/DSS для компаний, работающих с кредитными картами, до законодательных актов о защите персональных данных. Указанные обстоятельства приводят к проблемам, решить которые невозможно без систем DLP. На этом фоне все более заметной становится тенденция к «взаимопроникновению» систем DLP, решений для защиты рабочих станций (Endpoint Security) и контроля доступа (Network Access Control/Protection, NAC/NAP).

В последнее время решения для защиты рабочих станций стали включать в себя базовые функции DLP — выявление в передаваемых или копируемых файлах конфиденциальной информации по стандартным алгоритмам: атрибутам, ключевым словам и т. д. Поэтому можно говорить о взаимопроникновении технологий, что и подтверждает Рустэм

Хайретдинов. «Но клиенты, мне кажется, пока не готовы платить за эти функции, — предостерегает Вениамин Левцов. — Покупая продукт Endpoint Security, они приобретают в первую очередь антивирус, радуясь, что получают дополнительные инструменты. Увы, невозможно построить сколько-нибудь серьезную систему для борьбы с перемещением конфиденциальной информации, используя доступные в продукте Endpoint Security фрагменты DLP». Что касается NAC/NAP, то, по его мнению, со временем такие системы будут отнесены к классу систем, обеспечивающих соответствие политикам и контролю ИТ (Compliance). Когда это случится, внедрение NAC будет осуществляться как отдельный проект в рамках глобальной программы внедрения проекта по обеспечению соответствия законодательным требованиям.

По словам Рустэма Хайретдинова, большинство решений Endpoint Security выпускается на базе известных антивирусных движков. Как показывает опыт InfoWatch, заказчики прежде всего выбирают производителя антивируса, а затем оценивают остальные средства защиты. К примеру, если поставщик Endpoint Security не выпускает антивирусов, то продукты этого вендора зачастую приобретаются в качестве дополняющих другие инфраструктурные решения данного производителя.

Рассматривая такое решение, прежде всего надо убедиться, что оно совместимо с бизнес-процессами, от которых зависит доход компании. Если средство безопасности препятствует основной деятельности, его просто не станут использовать в наиболее критичных точках инфраструктуры, а, как правило, именно они и являются основными источниками утечек. Далее следует проанализировать стоимость приобретения и владения, поскольку системы «на основе агентов» зачастую вызывают немало хлопот при внедрении и эксплуатации. Кроме того, даже самые развитые решения DLP и продукты для защиты конечных точек не способны в полной мере обеспечить безопасность внутрикорпоративных данных и решить проблему несанкционированной утечки информации. То или иное решение выбирается в зависимости от «набора рисков» и бюджета. «Система DLP — хороший инструмент для работы со случайными утечками либо с утечками по стандартным каналам, — считает Дмитрий Михеев. — На такие утечки, по нашей оценке, приходится более 85% подобных инцидентов, поэтому типовые проблемы логично решать с помощью готовых инструментов».

Системы DLP рассчитаны, прежде всего, на защиту от действий безалаберных сотрудников. Со злонамеренными инсайдерами дело обстоит сложнее — здесь нужен комплекс организационных и технических мер противодействия, тогда и пробелов в защите будет значительно меньше. Уже сегодня большинство продуктов DLP интегрируются с другими средствами защиты, системами проведения расследований, а также со средствами мониторинга инфраструктуры, системами электронного документооборота, решениями по защите контента (DRM и шифрование). Некоторые поставщики СЭД и UTM встроили в свои решения модули DLP, лицензируя их у известных производителей. «Полагаю, что данная тенденция сохранится в ближайшем будущем. Именно по этой причине “Лаборатория Касперского” и InfoWatch планируют расширение взаимовыгодного сотрудничества», — отмечает Рустэм Хайретдинов.

По словам Вениамина Левцова, продукты DLP являются важнейшими поставщиками информации для систем корреляции событий ИБ (SIEM), и зачастую их внедрение ведется в рамках смежных проектов. «Но в интеграцию с RMS/IRM-системами я не верю, как и в будущее развитие систем разделения прав на документы с использованием “контейнерного” шифрования. Основная причина — резкий рост нагрузки на корпоративные службы поддержки и невозможность содержать рубрикаторы конфиденциальной информации, которые были бы адекватны реальным потокам данных в крупных средах. Насколько я понимаю, таких проектов единицы, несмотря на целый ряд продуктовых предложений от крупнейших игроков».

«Даже если технология DLP будет интегрирована с другими продуктами, она не исчезнет, — считает Дмитрий Михеев. — Ведь это не только технические средства, но и определенная методика их использования. Организовать предотвращение утечек можно и без приобретения выделенной системы DLP. Вопрос в том, сколько сил и средств потребует такая работа. Проблема безопасности — это проблема контроля деятельности людей. Пока в организации есть хотя бы два человека, которые занимаются коммерческой деятельностью, риск утечек существует. Какие именно технологии будут применяться для контроля, не очень-то и важно в конечном счете».

Сергей Орлов — ведущий редактор «Журнала сетевых решений/LAN».