Обзор DLP-систем

Сегодня рынок DLP-систем является одним из самых быстрорастущих среди всех средств обеспечения информационной безопасности. Впрочем, Беларусь пока не совсем успевает за мировыми тенденциями, в связи с чем у рынка DLP-систем в нашей стране есть свои особенности.

Что такое DLP и как они работают?

Прежде чем говорить о рынке DLP-систем, необходимо определиться с тем, что, собственно говоря, подразумевается, когда речь идёт о подобных решениях. Под DLP-системами принято понимать программные продукты, защищающие организации от утечек конфиденциальной информации. Сама аббревиатура DLP расшифровывается как Data Leak Prevention, то есть, предотвращение утечек данных.

Подобного рода системы создают защищенный цифровой «периметр» вокруг организации, анализируя всю исходящую, а в ряде случаев и входящую информацию. Контролируемой информацией должен быть не только интернет-трафик, но и ряд других информационных потоков: документы, которые выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываемые на принтере, отправляемые на мобильные носители через Bluetooth и т.д.

Поскольку DLP-система должна препятствовать утечкам конфиденциальной информации, то она в обязательном порядке имеет встроенные механизмы определения степени конфиденциальности документа, обнаруженного в перехваченном трафике. Как правило, наиболее распространены два способа: путём анализа специальных маркеров документа и путём анализа содержимого документа. В настоящее время более распространен второй вариант, поскольку он устойчив перед модификациями, вносимыми в документ перед его отправкой, а также позволяет легко расширять число конфиденциальных документов, с которыми может работать система.

«Побочные» задачи DLP

Помимо своей основной задачи, связанной с предотвращением утечек информации, DLP-системы также хорошо подходят для решения ряда других задач, связанных с контролем действий персонала. Наиболее часто DLP-системы применяются для решения следующих неосновных для себя задач:

- Контроль использования рабочего времени и рабочих ресурсов сотрудниками;
- Мониторинг общения сотрудников с целью выявления «подковерной» борьбы, которая может навредить организации;
- Контроль правомерности действий сотрудников (предотвращение печати поддельных документов и пр.);
- Выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность;

За счет того, что многие организации полагают ряд этих задач (особенно контроль использования рабочего времени) более приоритетными, чем защита от утечек информации, возник целый ряд программ, предназначенных именно для этого, однако способных в ряде случаев работать и как средство защиты организации от утечек. От полноценных DLP-систем такие программы отличает отсутствие развитых средств анализа перехваченных данных, который должен производиться специалистом по информационной безопасности вручную, что удобно только для совсем небольших организаций (до десяти контролируемых сотрудников). Тем не менее, поскольку данные решения востребованы в Беларуси, они также включены в сравнительную таблицу, сопровождающую эту статью.

Справка ТБ

Станкевич Вадим Юрьевич. Образование: высшее (физфак БГУ), редактор Web-издания «Компьютерные вести». Профессионально занимается ИТ-журналистикой с 2005-го года. Автор множества публикаций на тему защиты информации, в том числе и от утечек, а также на тему DLP-систем, читал лекции по защите от утечек данных в институте «Кадры индустрии».

Классификация DLP-систем

Все DLP-системы можно разделить по ряду признаков на несколько основных классов. По способности блокирования информации, опознанной как конфиденциальная, выделяют системы с активным и пассивным контролем действий пользователя. Первые умеют блокировать передаваемую информацию, вторые, соответственно, такой способностью не обладают. Первые системы гораздо лучше борются со случайными утечками данных, но при этом способны допустить случайную остановку бизнес-процессов организации, вторые же безопасны для бизнес-процессов, но подходят только для борьбы с систематическими утечками. Ещё одна классификация DLP-систем проводится по их сетевой архитектуре. Шлюзовые DLP работают на промежуточных серверах, в то время как хостовые используют агенты, работающие непосредственно на рабочих станциях сотрудников. Сегодня наиболее распространенным вариантом является совместное использование шлюзовых и хостовых компонентов.

Мировой рынок DLP

В настоящее время основными игроками мирового рынка DLP-систем являются компании, которые широко известны другими своими продуктами для обеспечения информационной безопасности в организациях. Это, прежде всего, Symantec, McAffee, TrendMicro, WebSense. Общий объём мирового рынка DLP-решений оценивается в 400 млн. долларов, что совсем не-

много по сравнению с тем же рынком антивирусов. Тем не менее, рынок DLP демонстрирует бурный рост: ещё в 2009 году он оценивался немногим более 200 млн.

На рынок Беларуси огромное влияние имеет рынок её восточного соседа, России, уже достаточно большой и сформировавшийся. Основными игроками на нём сегодня являются российские компании: InfoWatch, «Инфосистемы Джет», SecurIT, SearchInform, Perimetrix и ряд других. Общий объём российского рынка DLP оценивается в 12 15 млн. долларов. Растет он при этом теми же темпами, что и мировой.

Белорусский рынок DLP

Серьезных исследований рынка DLP-систем в Беларуси пока никто, к сожалению, не проводил — причина этого кроется, прежде всего, в малых размерах самого рынка, не представляющего большого интереса для крупных игроков: эксперты оценивают его докризисный объём в 2-3 миллиона долларов, соответственно, его теперешние размеры в 2 2,5 раза меньше. Причина невысокого интереса белорусских компаний к DLP-системам заключается, прежде всего, в их высокой стоимости, а также в непонимании руководства организаций механизмов экономического ущерба в результате утечек конфиденциальной информации.

На белорусском рынке, отличающемся от российского значительно большей фрагментарностью, представлены сегодня как мировые гранды, так и перечисленные выше российские компании. Собственные разработчики DLP-систем пока о себе предпочитают не заявлять, но центры разработки нескольких российских DLP-вендоров сегодня базируются в Минске. Назвать доли конкретных производителей на белорусском рынке сложно из-за недостаточного количества данных.

Применение DLP в Беларуси пока ограничивается, зачастую, контролем внешних USB-носителей и принтеров. Только сравнительно немногие организации строят полноценный «защитный контур», перекрывающий все потенциальные каналы утечки конфиденциальной информации. Кроме того, одним из основных пожеланий белорусских заказчиков является архивирование с помощью DLP перехваченных данных для последующего анализа и широкий перечень контролируемых каналов.

Перспективы и тенденции

В связи с тем, что из-за сложной экономической обстановки достаточно сложно прогнозировать ситуацию на белорусском рынке DLP-систем, поговорим о прогнозах развития DLP-систем как класса программного обеспечения.

Главной из таких тенденций, как полагают эксперты, является переход от «заплаточных» систем, состоящих из компонентов от различных производителей, решающих каждый свою задачу, к единым интегрированным программным комплексам. Причина подобного перехода очевидна: комплексные интегрированные системы избавляют специалистов по информационной безопасности от необходимости решать проблемы совместимости различных компонентов «заплаточной» системы между собой, позволяют легко изменять настройки сразу для больших массивов клиентских рабочих станций в организациях, а также позволяют не испытывать сложностей при переносе данных из одного компонента единой интегрированной системы в другой. Также движение разработчиков к интегрированным системам идёт в силу специфики задач обеспечения информационной безопасности: ведь если оставить без контроля хотя бы один канал, по которому может произойти утечка информации, нельзя говорить о защищенности организации от подобного рода угроз.

Западные производители DLP-систем, пришедшие на рынок стран СНГ, столкнулись с рядом проблем, связанных с поддержкой национальных языков (в случае Беларуси, впрочем, уместно говорить о поддержке русского, а не белорусского языка). Поскольку рынок СНГ весьма интересен западным вендорам, сегодня они ведут активную работу над поддержкой русского языка, которая является основным препятствием для их успешного освоения рынка.

Ещё одной важной тенденцией в сфере DLP является постепенный переход к модульной структуре, когда заказчик может самостоятельно выбрать те компоненты системы, которые ему необходимы (например, если на уровне операционной системы отключена поддержка внешних устройств, то нет необходимости доплачивать за функциональность по их контролю). Важную роль на развитие DLP-систем будет оказывать и отраслевая специфика — вполне можно ожидать появление специальных версий известных систем, адаптированных специально для банковской сферы, для госучреждений и т.д., соответствующих запросам самих организаций.

Немаловажным фактором, влияющим на развитие DLP-систем, является также распространение ноутбуков и нетбуков в корпоративных средах. Специфика лэптопов (работа вне корпоративной среды, возможность кражи информации вместе с самим устройством и т.д.) заставляет производителей DLP-систем разрабатывать принципиально новые подходы к защите портативных компьютеров. Стоит отметить, что сегодня лишь немногие вендоры готовы предложить заказчику функцию контроля ноутбуков и нетбуков своей DLP-системой.

Применение DLP в Беларуси

В Беларуси DLP-системы применяются в сравнительно небольшом числе организаций, но их количество до начала кризиса уверенно росло. Тем не менее, собранную с помощью DLP-систем информацию белорусские организации вовсе не спешат предавать огласки, преследуя виновных в утечках информации сотрудников в судебном порядке. Несмотря на то, что белорусское законодательство содержит в себе нормы, позволяющие наказывать распространителей корпоративных секретов, подавляющее большинство организаций, использующих DLP-системы, предпочитают ограничиваться внутренними разбирательствами и дисциплинарными взысканиями, в крайнем случае увольняя провинившихся в особо крупных размерах сотрудников. Впрочем, традиция «не выносить сор из избы» характерна для всего постсоветского пространства, в отличие от западных стран, где об утечке данных сообщают всем, кто мог от неё пострадать.

Вадим Станкевич

Сравнительные характеристики DLP систем представленных на рынке РБ. Параметры. Функциональность системы

Название торговой марки, название продукта	**Security Curator**	**LanAgent Bel**	**Falcongaze SecureTower**	**КИБ SearchInform**
Разработчик	ООО «Атом Парк», РФ, С.-Петербург	«Нетворк Профи», РФ, ООО «Нейрон-М», РБ	Falcongaze, РФ, г. Москва	SEARCHINFORM, РФ, г. Москва
Представитель в РБ	ООО «Нейрон-М» 220119, г. Минск, ул. Тикоцкого, 16, оф. 75в www.neuron-m.by E-mail: info@neuron-m.by, kv_home@mail.ru Тел.: (029) 142-45-18 Виторский Иван, (029) 661-49-63 Никифоров Сергей	ООО «Нейрон-М» 220119, г. Минск, ул. Тикоцкого, 16, оф.75в www.neuron-m.by E-mail: info@neuron-m.by, kv_home@mail.ru Тел.: (029) 142-45-18 Виторский Иван, (029) 661-49-63 Никифоров Сергей	ИООО "ДПА Бел" 220116, г. Минск, пр-т Дзержинского, 104, офис 503 www.dpa.by E-mail: info@dpa.by (017) 277-26-37, (029) 195-11-15 Караневич Иван	ООО «НПТ» 220012, г. Минск, ул. К. Чорного, 5А www.searchinform.ru Тел. (017) 288-41-29 моб.: (029) 649-77-79 ICQ: 39941848 Skype: hazasoft
Сертификаты	На стадии завершения сертификации ФСТЭК	На стадии сертификации ФСТЭК	На стадии завершения сертификации ФСТЭК	ФСТЭК России, Газпросет
Архитектура продукта	Агент — Сервер (Администратор)	Агент — Сервер	Серверные компоненты (сервер перехвата, сервер обработки данных, сервер контроля агентов), агенты на раб.станциях, клиентские приложения (консоль администратора, клиентская консоль)	Агент/зеркалирование трафика
Централизованная настройка системы	+	+	+ (из одной консоли)	+
Запоминание запуска и закрытие программ	+	+	+	-
Определение подключения и отключения носителей информации	+	+	-	+
Снимки экранов мониторов	+	+	+	+
Кейлоггер	+	+	-	-
Перехват сообщений — ICQ, Mail.ru Agent	+	+	+	+
Перехват и анализ трафика по шифрованным протоколам			+	+
Контроль мобильных рабочих мест			+	+
Резервное копирование данных			+	+
Контроль содержимого буфера обмена	+	+	-	-
Перехват посещённых сайтов	+	+	+	+
Учет соединений с интернет	+	+	-	-
Установка и удаление программ	+	+	-	-
Статистика создания и удаления файлов	+	+	-	+
Учет документов, отправленных на печать на принтер	+	+	+	+
Включение/выключение компьютера	+	+	-	-
Вся информация хранится централизованно в базе	+	+	+	+
Автоматическое получение статистики от контролируемых компьютеров	+	+	+	+
Возможность отправки текстовых сообщений на компьютер пользователя	+	+	-	-
Статистика и отчеты	+	+	+	+
Контроль Skype	+	+	Перехват текстовых сообщений и голосовых звонков	Перехват текстовых сообщений, голосовых звонков и файлов
Поиск информации по критериям	+	+	+	+
Уведомления	+	+	+	+
Блокирование действий на компьютере — агенте	+	+	-	+
Мониторинг изменения баз данных	+	+	+	+
Граф-анализатор связей	+	+	+	+
Фильтры:	+	+	+	+
Средства анализа перехваченного контента на предмет утечек данных	Поиск по ключевым словам, фразам	Поиск по ключевым словам, фразам	Контекстный и контентный анализ (ключевые слова и выражения с учетом русской морфологии, регулярные выражения, цифровые отпечатки документов и БД)	Ключевые слова и выражения с учетом русской морфологии и расстояний между словами и фразами, регулярные выражения и цепочки регулярных выражений, цифровые отпечатки документов и БД, поиск похожих документов
Анализ статистики использования сети пользователями			+ (с отправкой уведомлений в случае превышения лимитов)	+
Требования к компьютерной технике	Компьютер хранения базы: PIV-1 гБайт RAM, HDD- 300-400 гБайт	Компьютер базы: PIV-1 гБайт RAM, HDD- 300-400 гБайт	**Рекомендуемые для контроля 100 раб.станций:** Pentium® 2+ ГГц (2-ядра и более); 2 сетевых адаптера: 100 Мбит/1 Гбит; RAM не менее 4 Гб; HDD 150 Мб	CPU: Intel Core 2 Duo E6600, RAM: 6Gb, HDD 500Gb+, Ethernet: 100Mbps
Стоимость:	70-80 у.е. на одно рабочее место (компьютер)	60-70 у.е. на одно рабочее место (компьютер)	В зависимости от размера и конфигурации сети	В зависимости от количества пользователей
За сервер	-	-	В зависимости от размера и конфигурации сети	-
За агент на 1 компьютер	-	-	В зависимости от размера и конфигурации сети	-