И.В. Алябьев, З.З. Шарипов
Ташкентский университет информационных технологий им. Мухаммада Аль-Хорезми, г. Ташкент
УДК 004.056.5

ПОСТРОЕНИЕ ПОДРОБНОЙ МОДЕЛИ СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ

Аннотация. В статье описана модель системы предотвращения утечек информации.

Ключевые слова: предотвращение утечек информации, модель системы.

Предотвращение утечек информации является одной из самых актуальных проблем информационной безопасности на сегодняшний день. Под утечкой информации, в данной статье, понимается случайная или преднамеренная передача конфиденциальных данных неавторизованному лицу[1]. В данной статье описана модель системы предотвращения утечек информации (Data loss/leak prevention, далее DLP), а также рекомендации по разработке DLP-системы используя данную модель.

Пример распределения системы предотвращения утечек информации в корпоративной сети предприятия показан на рис.1.

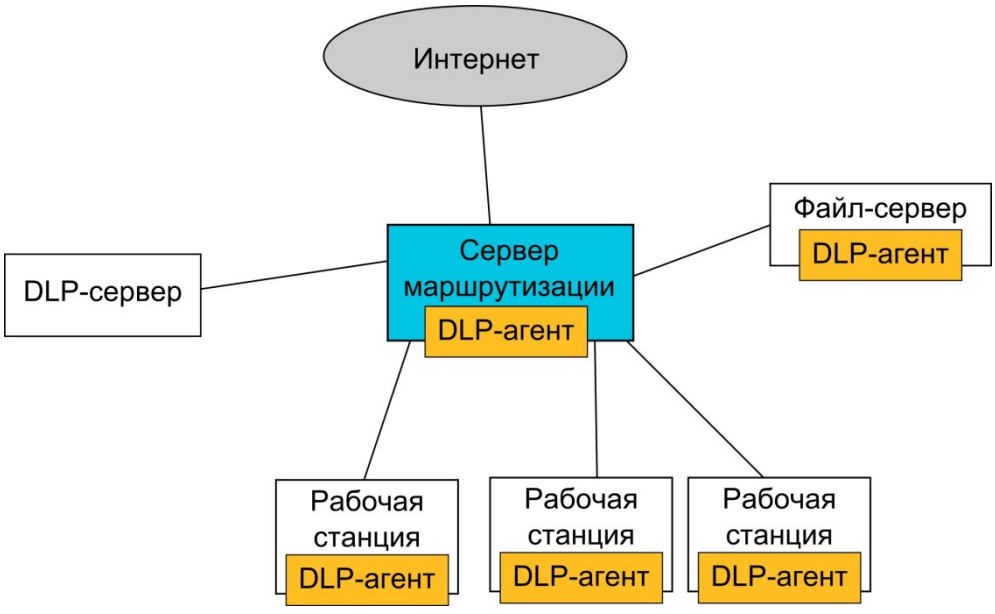

Рис. 1. DLP-система в корпоративной сети предприятия.

DLP-агент (клиент) – программа, устанавливаемая на компьютеры пользователей, на сервера хранения данных (например, файл-сервер) и в качестве межсетевого экрана. DLP-сервер предназначен для распространения политик, показывает статистику по событиям на компьютерах пользователей. DLP-агент выполняет свои функции даже в случае отключения от сервера.

На рис.2. изображена общая модель DLP-агента, включающая 3 уровня: уровень обмена сообщениями, уровень мониторинга (логирования) и уровень DLP. Назначение уровня обмена сообщениями состоит в том, чтобы обеспечить клиент-серверное взаимодействие между DLP-сервером и DLP-агентом. Уровень мониторинга предназначен для сбора данных о действиях пользователя, состоянии файловой системы, свойствах компьютера и т. п. Кроме того, логирование работы самого DLP-клиента (вне контекста DLP) также обеспечивается данным уровнем. Уровень DLP разрешает или блокирует те или иные действия.

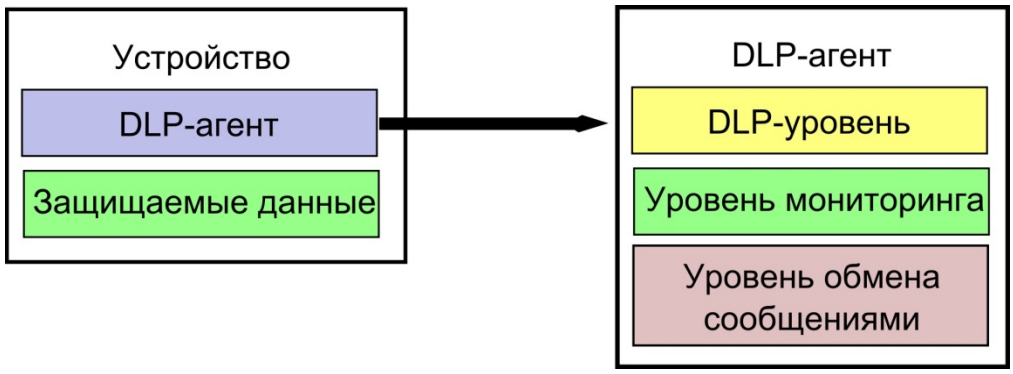

Рис. 2. Общая модель DLP-агента.

Уровень обмена сообщениями включает в себя две основные функции – это авторизация и базовый обмен сообщениями. Каждый агент при подключении к серверу проходит авторизацию. Кроме того, может быть реализован механизм установления подлинности сервера на агенте при подключении. Это необходимо, т.к. данные, передаваемые с DLP-агента на DLP-сервер сами по себе могут представлять интерес для злоумышленника. Базовый обмен сообщениями предоставляет соответствующий механизм для

взаимодействия агента и сервера. Существуют различные типы сообщений, основанные на базовом типе сообщений. В структуру базового сообщения входит уникальный идентификатор, отправитель и временной штамп. Остальные типы сообщений создаются в зависимости от назначения: для синхронизации политик – свой тип, для каждой DLP-функции – свой. В зависимости от конкретной реализации, уровень обмена сообщениями может являться ядром, обеспечивающим также и взаимодействие с остальными частями DLP-агента, может являться модулем, вызываемым остальными модулями программы для взаимодействия с сервером, или же может быть распределен по всем модулям, являясь отдельной частью каждого (это не касается функции авторизации, т.к. она относится к DLP-агенту в целом, а сообщения от разных модулей производится в общей сессии после авторизации).

На рис.3. представлена модель DLP-агента, при котором уровень мониторинга является основным. В данном случае DLP-агент собирает данные об активности пользователя и состоянии компьютера, а сервер обрабатывает эти данные и представляет результат в удобном виде, в то время, как активные DLP-функции могут отсутствовать (блокирование неразрешенных действий), а разбирательства по утечке могут происходить в организационном порядке на предприятии. В описанном контексте, ядро подсистемы мониторинга отвечает за запуск и остановку отдельных модулей, а также их конфигурирование в соответствии с политиками, устанавливаемыми сервером. Модули уровня мониторинга собирают данные в соответствующих их назначению областях, а именно: работа со съемными носителями (характеристики устройства, данные, считанные или записанные на устройство и т.п.), печать документов, файловая система (создание, изменение, удаление файлов), логирование работы самого приложения и др. Следует отметить, что в данном случае наличие сервера является обязательным и должен быть реализован механизм, обеспечивающий отложенную отправку данных на сервер в случае отключения агента от сервера. Кроме того, должны быть продуманы рамки накопления данных на агенте.

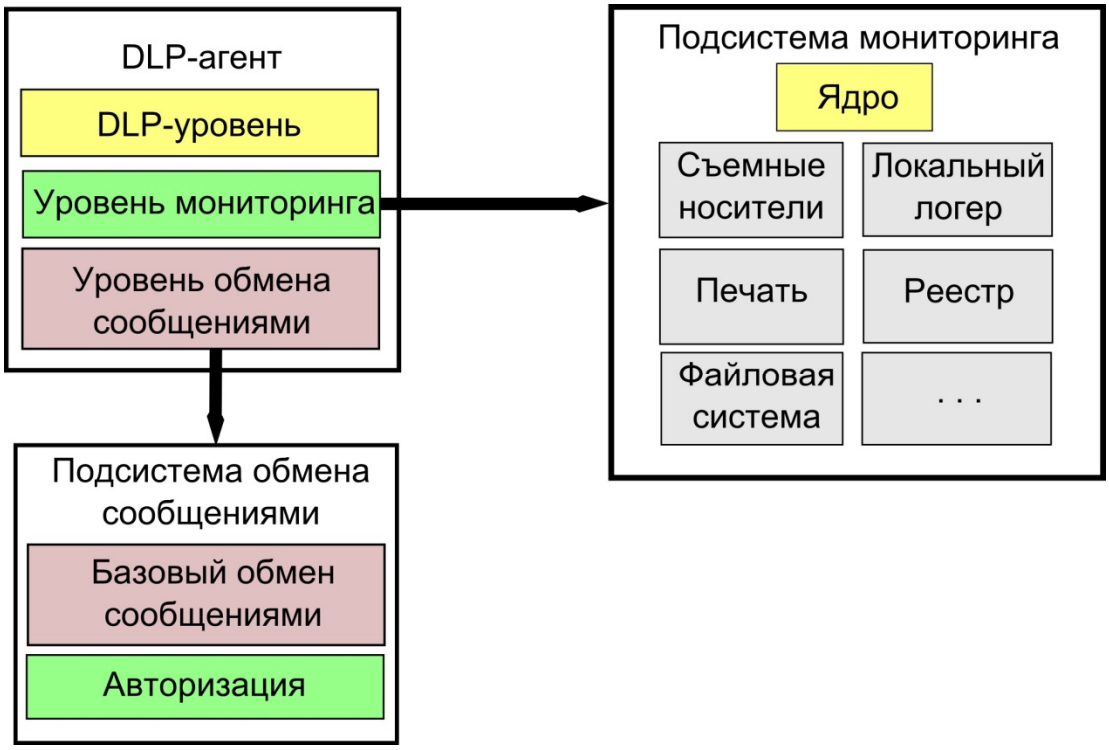

Рис.3. Модель DLP-агента с подсистемой мониторинга в качестве основной.

На рис.4. представлена модель DLP-агента, при котором уровень DLP является основным.

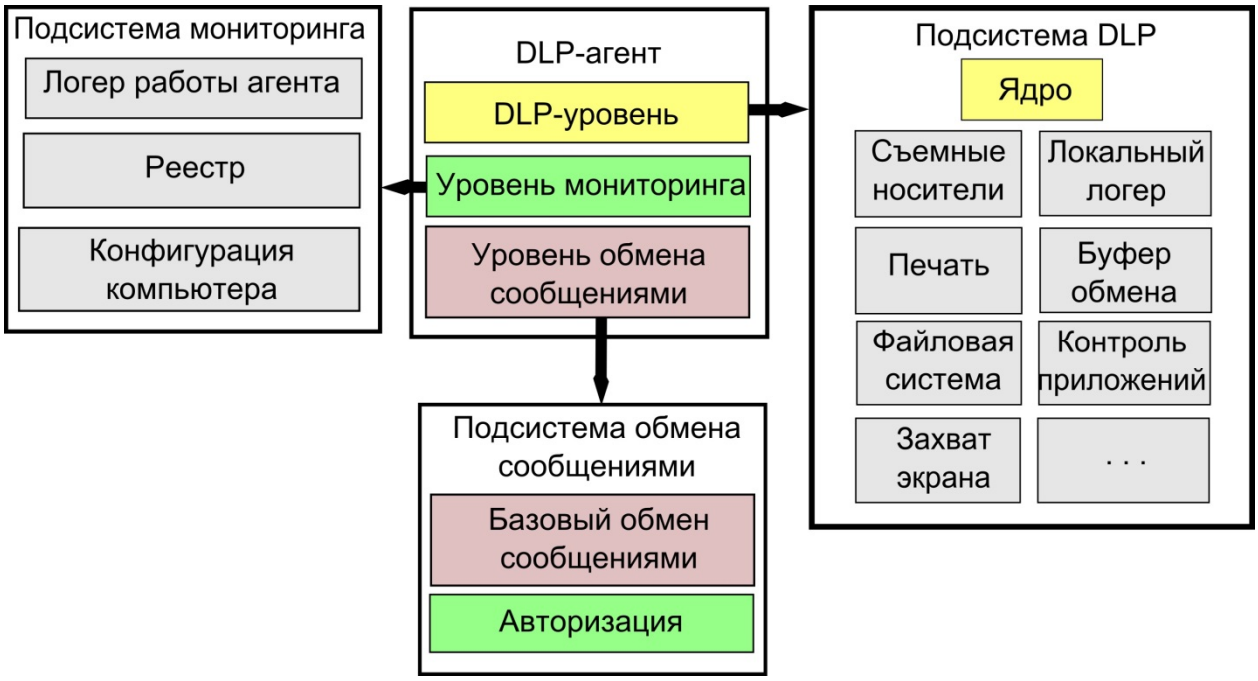

Рис.4. Модель DLP-агента с подсистемой DLP в качестве основной.

Подсистема мониторинга собирает данные, непосредственно не связанные с контекстом DLP, такие как логирование работы самого агента, изменения системного реестра и т.п. Подсистема DLP, в свою очередь обеспечивает предотвращение утечек по каналам, покрытым конкретной реализацией DLP-системы.

Ключевым отличием от варианта с доминирующей системой мониторинга является то, что в данном случае DLP-система предпринимает активные действия, такие как блокирование действий, шифрование разделов управление доступом и т.д., в то время как функционал мониторинга ограничивается наблюдением. Также следует отметить, что в некоторых случаях необязательно иметь сервер, т.к. большинство функций DLP выполняются локально и не требуют подключения агента к серверу, так же и политики могут конфигурироваться локально.

На рис.5. изображена общая модель DLP-сервера. Основным назначением сервера является конфигурирование и распространение политик.

Рис. 5. Модель DLP-сервера.

Обработка получаемых от агентов данных, в самом простом случае, нужна для вывода статистики по деятельности пользователей рабочих станций. Кроме того, на основе результатов анализа получаемых сервером данных можно конфигурировать политики более рационально.

Подобное разделение на уровни продиктовано следующим. Для предприятия, по тем или иным причинам, может быть невыгодно приобретение одного из предлагаемых на рынке DLP-решений. Зачастую, предприятию достаточно лишь определенного набора DLP-утилит – инструментов, обрабатывающих какой-либо конкретный канал утечек информации (съемные носители, печать и т.п.). В подобном случае, может быть целесообразно разрабатывать соответствующую ограниченному набору требований DLP-систему с нуля. При использовании методологии разработки с частыми релизами, данный подход является более рентабельным, т.к. уровни могут разрабатываться независимо друг от друга, а функции программного обеспечения могут добавляться от релиза к релизу начиная с реализации самых критичных для предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Shabtai A, Elovici Y, Rokach R. A Survey of Data Leakage Detection and Prevention Solutions. SpringerBriefs in Computer Science, 2012, 92 стр.
2. Alneyadi S, Sithirasenan E, Muthukkumarasamy V. A survey on data leakage prevention systems. Journal of Network and Computer Applications, 2016, том 62, стр. 137–152.