ВНЕДРЕНИЕ DLP-СИСТЕМЫ ДЛЯ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ

Сидорук И.С.1, студент гр. 241301

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Дворникова Т.Н. – магистр техн. наук

Аннотация. В статье рассмотрена проблема утечек конфиденциальной информации в корпоративной сети и показана целесообразность применения DLP-систем как инструмента контроля наиболее опасных каналов передачи данных. На основе материалов проанализированы основные угрозы, сравнены механизмы идентификации конфиденциального контента и обоснован выбор Symantec DLP. Отдельное внимание уделено этапам внедрения, интеграции с почтовой системой, прокси-сервером, Active Directory и сервером управления. Сделан вывод о том, что использование DLP повышает прозрачность информационных потоков, снижает риски утечек и упрощает реагирование на инциденты.

Ключевые слова. информационная безопасность, конфиденциальная информация, DLP-система, Symantec DLP, корпоративная сеть, утечка данных.

Введение. Рост цифрового документооборота делает информацию одним из ключевых активов организации. При этом даже хорошо выстроенный набор технических и организационных мер не гарантирует полного исключения утечек, поскольку основная часть инцидентов связана не только с внешними атаками, но и с ошибками сотрудников либо с намеренными действиями внутренних нарушителей. Наиболее уязвимыми остаются каналы электронной почты, веб-доступа, съёмных носителей и локального хранения файлов.

Актуальность задачи защиты данных. Материалы работы показывают, что для корпоративной среды особенно опасны ситуации, в которых конфиденциальная информация передается вне контролируемого периметра или сохраняется в несанкционированных местах. Именно поэтому задача защиты должна решаться комплексно: через политику безопасности, контроль каналов передачи данных и инструменты обнаружения чувствительного контента. В такой архитектуре DLP-система выполняет роль центрального элемента, который фиксирует подозрительные действия, классифицирует инциденты и помогает службе безопасности быстро реагировать на нарушения [1-3].

Таблица 1 – Основные каналы утечки и меры контроля

Канал	Пример риска	Меры контроля
Электронная почта	Отправка вложений внешнему адресату	Контроль SMTP, политика блокировки и журналирование
Web и облачные сервисы	Публикация файлов и выгрузка данных	Инспекция HTTP/HTTPS, контроль web-почты и форм
Съёмные носители	Копирование базы клиентов на флеш-накопитель	Endpoint Prevent, запрет записи и оповещения
Локальное хранение	Сохранение черновиков и копий документов	Сканирование хранилищ и поиск несанкционированных копий

Для практического внедрения важно не только контролировать каналы утечки, но и корректно определить саму конфиденциальную информацию. В ходе работы показано, что DLP-платформа должна сочетать несколько механизмов: поиск по ключевым словам, регулярным выражениям, контексту хранения, цифровым отпечаткам и агентский контроль на рабочих станциях. Такой подход снижает количество ложных срабатываний и позволяет обнаруживать как готовые документы, так и их фрагменты или черновые версии [4-6].

Таблица 2 – Сравнение основных методов идентификации конфиденциальных данных

Метод	Преимущества	Ограничения
Ключевые слова и регулярные выражения	Быстрое обнаружение и понятные правила	Требует постоянной актуализации словарей
Цифровые отпечатки	Хорошо находит новые версии и фрагменты документов	Нужны ресурсы на хранение и настройку
Контекст хранения и агент	Контроль действий пользователя на рабочем месте	Не всегда покрывает черновики вне сети
Ручная разметка	Точный контроль сложных категорий данных	Требует высокой квалификации специалиста

Выбор Symantec DLP в качестве базового решения в работе обоснован тем, что платформа объединяет серверные компоненты, сетевые перехватчики, агентские модули и подсистемы для поиска данных в хранилищах. На уровне сети система позволяет контролировать исходящий трафик, на уровне рабочих станций — фиксировать операции с файлами и съёмными носителями, а на уровне хранилищ — выявлять несанкционированные копии конфиденциальных данных. Центральное управление через Enforce Platform упрощает создание политик, анализ инцидентов и формирование отчетности.

Практическая часть внедрения предполагает интеграцию DLP с корпоративной почтовой системой, прокси-сервером, Active Directory и сетевым оборудованием. Для почтового канала используются скрытые копии исходящих сообщений и транспортные правила. Для веб-канала важна поддержка ICAP и инспекция SSL-трафика. Для идентификации пользователей и рабочих станций система получает актуальные сведения из каталога Active Directory, что позволяет точнее связывать действия с конкретным сотрудником и его ролью [7-10].

С точки зрения организационного эффекта DLP-система повышает дисциплину пользователей и снижает нагрузку на специалистов по информационной безопасности. Вместо ручной проверки большого массива событий служба ИБ получает уже классифицированные инциденты, может быстро определять приоритеты и концентрироваться на действительно опасных случаях. Дополнительным преимуществом становится возможность ретроспективного анализа действий, поскольку система хранит историю событий и отчеты по нарушениям политик.

Заключение. Проведенный анализ показывает, что DLP-система является практическим инструментом защиты корпоративной информации от наиболее вероятных внутренних и внешних угроз. Внедрение Symantec DLP в сети предприятия позволяет контролировать каналы передачи данных, обнаруживать несанкционированное хранение документов и выстраивать управляемую модель реагирования на инциденты. Следовательно, применение DLP обосновано как с точки зрения информационной безопасности, так и с точки зрения экономической эффективности.

Список использованных источников:

1. Государственный стандарт Республики Беларусь СТБ ГОСТ Р 50922–2000: Защита информации. Основные термины и определения.

2. Закон Республики Беларусь «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455–З.

3. Голиков, А.М. Основы информационной безопасности: учеб. пособие / А.М. Голиков. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 288 с.

4. Барабанов, А.В. Предложения по формированию метабазиса оценки соответствия DLP-решений по требованиям безопасности информации / А.В. Барабанов, М.И. Гришин // Материалы XII Международной научно-практической конференции «ИБ-2012». – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 4–11.

5. Умысков, А.В. Рекомендации по внедрению систем предотвращения утечек конфиденциальной информации (DLP-систем) в информационные системы предприятий / А.В. Умысков, А.С. Тимофеев // Молодой учёный. – 2016. – № 13. – С. 231–233.

6. Чернокнижный, Г.М. Защита конфиденциальной информации в корпоративной сети от утечек / Г.М. Чернокнижный // Научные труды SWorld. – 2013. – № 4. – С. 23–27.