22 мая 2025

DLP-системы

В бизнесе любая утечка данных может обернуться не только крупными финансовыми потерями, но и серьезным ударом по репутации компании. С каждым годом количество инцидентов, связанных с несанкционированным доступом к коммерческой, персональной или государственной информации, только растет. Чтобы предотвратить угрозы такого рода, организации внедряют DLP-системы — специализированные решения по контролю и защите данных. В этой статье подробно рассказываем, что это, зачем нужны, как работают и каких результатов позволяют достичь. Также рассмотрим топ-7 российских DLP-систем, их возможности, примеры и советы по внедрению.

ЧТО ТАКОЕ DLP-СИСТЕМА И ЗАЧЕМ ОНА НУЖНА

DLP (Data Loss Prevention, или предотвращение утечек данных) — это комплекс программных и аппаратных средств, который защищает конфиденциальную информацию компании от несанкционированного копирования, передачи, вывода, загрузки вне организации. DLP фиксирует нарушения, автоматически блокирует потенциальные угрозы, уведомляет

службу безопасности и позволяет вести полный аудит работы с данными.

ДЛЯ КАКИХ КОМПАНИЙ И ЗАДАЧ НЕОБХОДИМА DLP

DLP-систему обычно внедряют финансовые и страховые компании, промышленные предприятия, ритейл, IT-сферы, образовательные учреждения, государственные структуры и сервисные B2B-компании. Особенно актуальна такая защита для организаций, работающих с персональными данными (СПДн), коммерческими тайнами, инженерной документацией, технологиями R&D и интеллектуальной собственностью. Главная задача DLP — минимизировать риски утечки данных, снизить штрафы регуляторов и сохранить конкурентные преимущества.

ВИДЫ DLP-СИСТЕМ

1. **Сетевые DLP** анализируют интернет-трафик, корпоративную почту, мессенджеры, веб-приложения, выявляя отправку секретных данных вовне.
2. **Endpoint DLP** устанавливаются на рабочие станции сотрудников и фиксируют любые действия с файлами: копирование на флешки, печать, выгрузку на облака, отправку по Bluetooth.
3. **Cloud DLP** внедряются для контроля данных в облачных сервисах (SaaS, корпоративное облако, электронная почта, CRM/ERP), что особенно актуально для компаний, активно использующих удаленную работу.

КАК РАБОТАЕТ DLP-СИСТЕМА

ПРИНЦИПЫ РАБОТЫ И ОСНОВНЫЕ ФУНКЦИИ

Основной принцип — тотальный контроль всех каналов, по которым возможна утечка данных. DLP-система осуществляет:

- перехват и глубокий анализ сетевого трафика (email, веб, FTP, соцсети, мессенджеры);
- мониторинг локальных операций на компьютерах (копирование, удаление, изменение, перемещение файлов);
- контроль съемных носителей (USB, жесткий диск, смартфон);
- классификацию информации по категориям (личные данные, финансовые документы, разработки);
- поведенческий и лингвистический анализ действий сотрудников;
- запуск автоматических сценариев: блокировка, оповещение, создание инцидента.

КАК DLP ОБНАРУЖИВАЕТ УГРОЗЫ И ЗАЩИЩАЕТ ДАННЫЕ

DLP-система сравнивает передаваемые или изменяемые данные с шаблонами (номера карт, паспорта, договоры, патенты), списками ключевых слов, метками, регулярными выражениями. При обнаружении соответствия политике безопасности она может заблокировать операцию, уведомить администратора и сформировать отчет. Система «учится» на инцидентах — по мере накопления истории точность выявления угроз возрастает.

Основные сценарии использования на предприятиях

- Контроль пересылки и загрузки документов, содержащих коммерческую тайну.
- Защита персональных данных клиентов и сотрудников (соответствие 152-ФЗ, GDPR, PCI DSS).
- Блокировка копирования на неразрешенные устройства или облачные сервисы.
- Выявление инсайдеров и злоупотребления доступом (намеренная или случайная утечка).
- Предотвращение «серых» схем: передачи контактов, цен, коммерческих предложений конкурентам.
- Мониторинг фото- и сканирования документов на рабочих местах.

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ВНЕДРЕНИЯ DLP

Каким бизнесам DLP-системы особенно важны

Группы компаний с критичной информацией обязаны иметь DLP: банки, страховые, ритейлы, промышленные гиганты, энергетика, фармацевтика, госструктуры, high-tech разработчики. DLP становится обязательным элементом комплексной системы информационной безопасности по требованиям регуляторов (ФЗ-152, требования ФСТЭК, GDPR, PCI DSS и др.).

Возможные сложности и ограничения

- DLP требует внимательной настройки политик безопасности, чтобы сократить количество ложных срабатываний.
- Комплекс внедрения и поддержки может быть финансово затратным — особенно для малого и среднего бизнеса;
- Влияет на нагрузку на ИТ-инфраструктуру, возможны легкие замедления работы.
- Иногда встречается сопротивление персонала (восприятие тотального контроля).
- Не все системы поддерживают интеграцию с облачными сервисами или мобильными платформами.

ВНЕДРЕНИЕ И ИСПОЛЬЗОВАНИЕ DLP-СИСТЕМ

Как выбрать подходящую DLP-систему

Оценивайте:

- локальное или облачное решение,
- совместимость с ОС и бизнес-приложениями,
- широту каналов контроля (почта, мессенджеры, облака, соцсети),
- глубину анализа (контекст, образы, лексический разбор, OCR, поведенческий профиль),
- качество технической поддержки, наличие российского сертификата,
- гибкость политики и интеграцию с SIEM/IDM/CMDB.

Этапы внедрения в организации

1. Анализ и аудит бизнес-процессов, рисков, моделей угроз.

2. Согласование требований безопасности и подбор подходящей DLP-системы.

3. Пилотное тестирование, внедрение на ограниченной группе.

4. Разработка детализированных политик контроля для каналов передачи.

5. Обучение персонала, настройка процедур реагирования на инциденты.

6. Постоянный мониторинг, корректировка политик, регулярная проверка эффективности.

Советы по эффективной эксплуатации

Систему важно регулярно обновлять: пополнять словари, учитывать изменившиеся бизнес-процессы, настраивать интеграцию с другими компонентами ИБ. Особое внимание — работе с персоналом: важно объяснять цель и задачи системы, привлекать к обучению, иначе DLP воспринимается как «шпионаж» и происходит пассивное или активное

противодействие.

РЕЙТИНГ РОССИЙСКИХ DLP-СИСТЕМ: ТОП-7 РЕШЕНИЙ

1. СёрчИнформ Контур

Основные характеристики:

- Поддержка контроля переписки (почта, современные мессенджеры, соцсети);
- Анализ всей структуры хранилища файлов;
- Глубокий лингвистический и поведенческий анализ персонала;
- Готовые шаблоны для обнаружения ПДн, финансовых данных, коммерческих секретов;
- Централизованное управление, гибкая настройка политик.

Особенности:

Простое внедрение, ориентированность на российские реалии, продуманные механизмы расследований.

2. Falcongaze SecureTower

Основные характеристики:

- Универсальный контроль всех каналов обмена (почта, приложения, веб, принтеры, устройства);
- Автоматическое выявление угроз на основе предикативной аналитики;
- Собственный аналитический движок DLP+SOC.

Возможности:

- Выявление инцидентов как по ключевым словам, так и по поведенческим моделям;
- Богатые возможности аудита и отчетности.

3. InfoWatch Traffic Monitor

Основные характеристики:

- Глубокий анализ контента (тексты, изображения, речь);
- Масштабируемое решение для крупных предприятий и холдингов;
- Широкая интеграция с другими системами ИБ (SIEM);
- Интеллектуальный анализ больших данных (Big Data).

Особенности:

Точность обнаружения утечек, поддержка сложных, «скользящих» шаблонов.

4. Dallas Lock DLP

Основные характеристики:

- Соответствие требованиям ФСТЭК и ФСБ РФ;
- Защита рабочих станций, аудит всех действий пользователя.
- Быстрое внедрение, невысокая стоимость для среднего бизнеса.

Особенности:

Хорошо работает в госсекторе, проста в администрировании.

5. Solar Dozor

Основные характеристики:

- Интеграция с другими продуктами Solar Security, в том числе SOC;
- Контроль электронных писем, мессенджеров, облачных сервисов;
- Гибкие механизмы расследований.

Особенности:

Ориентация на крупные корпоративные внедрения, адаптация под отрасль.

6. Zecurion DLP

Основные характеристики:

- Контроль всех каналов утечки — от e-mail до фото с экранов;
- Высокая производительность, интеграция с корпоративными БД;
- Широкие возможности по автоматизации политик.

Особенности:

Внедрение под ключ, быстрая настройка под конкретные задачи.

7. DeviceLock DLP

Основные характеристики:

- Максимум возможностей по контролю внешних устройств (USB, Bluetooth, принтеры);
- Предотвращение несанкционированного копирования данных;
- Микроуровень настройки для пользователей и групп.

Особенности:

Эффективна для компаний с частым использованием внешних носителей и периферии.

ЗАКЛЮЧЕНИЕ

DLP-система — основа комплексной ИБ организации. Ее правильный выбор и внедрение защищает бизнес от утечек, штрафов, сбережет клиентскую базу и репутацию. Важно фокусироваться на глубине анализа, регулировке политик, работе с сотрудниками и сочетать DLP с другими средствами защиты.

Ответы на популярные вопросы о DLP-системах (FAQ)

Что такое DLP-система простыми словами?

Инструмент контроля и предотвращения утечек ценных или секретных данных из компании.

Для чего нужна DLP-система в организации?

Для защиты персональных, финансовых и коммерческих данных от случайных либо умышленных утечек.

Какие бывают виды DLP-систем?

Сетевые, endpoint («на компьютерах»), облачные и их гибридные варианты.

Сколько стоит внедрить DLP-систему?

Минимальная стоимость — от нескольких сотен тысяч рублей, зависит от комплектации и числа пользователей.

Какой DLP выбрать для российского рынка?

Лучшие варианты: СёрчИнформ, Falcongaze, InfoWatch, Solar Dozor, Zecurion, DeviceLock — решение зависит от масштабов и задач.