Предотвращение утечек ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Data Leak Prevention, DLP*) — [технологии](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F) предотвращения [утечек конфиденциальной информации](https://ru.wikipedia.org/wiki/%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B0_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) из [информационной системы](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) вовне, а также технические устройства ([программные](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) или программно-аппаратные) для предотвращения утечек.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При [детектировании](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%82%D0%B5%D0%BA%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Используются также следующие термины, обозначающие приблизительно то же самое:

* Data Loss Prevention (DLP);
* Data Leak Prevention (DLP);
* Data Leakage Protection (DLP);
* [Information Protection and Control](https://ru.wikipedia.org/wiki/Information_Protection_and_Control) (IPC);
* Information Leak Prevention (ILP);
* Information Leak Protection (ILP);
* Information Leak Detection & Prevention (ILDP);
* Content Monitoring and Filtering (CMF);
* Extrusion Prevention System (EPS).

Из этой группы пока не выделился один термин, который можно было бы назвать основным или самым распространённым.

Необходимость защиты от внутренних угроз была очевидна на всех этапах развития средств [информационной безопасности](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). Однако первоначально внешние угрозы считались более опасными. В последние годы на внутренние угрозы стали обращать больше внимания, и популярность DLP-систем возросла. Необходимость их использования стала упоминаться в стандартах и нормативных документах (например, раздел «12.5.4 Утечка информации» в стандарте ГОСТ Р ИСО/МЭК 27002-2012). Специализированные технические средства для защиты от внутренних угроз стали массово выпускаться только после 2000 года.

Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением [хеш-функции](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F)) и анализом контента. Первый способ позволяет избежать [ложных срабатываний](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B6%D0%BD%D0%BE%D0%B5_%D1%81%D1%80%D0%B0%D0%B1%D0%B0%D1%82%D1%8B%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) (ошибок первого рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т. д. Пропуски конфиденциальной информации (ошибки второго рода) при этом методе вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются.

В состав DLP-систем входят компоненты (модули) сетевого уровня и компоненты уровня хоста. Сетевые компоненты контролируют трафик, пересекающий границы информационной системы. Обычно они стоят на [прокси-серверах](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D0%B8-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80), серверах электронной почты, а также в виде отдельных серверов. Компоненты уровня хоста стоят обычно на персональных компьютерах работников и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т. п. Хостовые компоненты также стараются отслеживать изменение сетевых настроек, инсталляцию программ для туннелирования, [стеганографии](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) и другие возможные методы для обхода контроля. DLP-система должна иметь компоненты обоих указанных типов плюс модуль для централизованного управления.

Основной задачей DLP-систем, что очевидно, является предотвращение передачи конфиденциальной информации за пределы информационной системы. Такая передача (утечка) может быть намеренной или ненамеренной. Практика показывает, что большая часть ставших известными утечек (порядка 75%) происходит не по злому умыслу, а из-за ошибок, невнимательности, безалаберности, небрежности работников[[1]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8#cite_note-IW_analit1-1). Выявлять подобные утечки проще. Остальная часть связана со злым умыслом операторов и пользователей информационных систем. Понятно, что инсайдеры, как правило, стараются преодолеть средства DLP-систем. Исход этой борьбы зависит от многих факторов. Гарантировать успех здесь невозможно.

Кроме основной перед DLP-системой могут стоять и вторичные (побочные) задачи. Они таковы:

* архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;
* предотвращение передачи вовне не только конфиденциальной, но и другой нежелательной информации (обидных выражений, спама, эротики, излишних объёмов данных и т. п.);
* предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы;
* предотвращение использования работниками казённых информационных ресурсов в личных целях;
* оптимизация загрузки каналов, экономия трафика;
* контроль присутствия работников на рабочем месте.

Практически во всех странах охраняется законом [право на тайну связи](https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D0%B9%D0%BD%D0%B0_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8) и право на [тайну частной жизни](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B8%D0%BA%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D1%87%D0%B0%D1%81%D1%82%D0%BD%D0%BE%D0%B9_%D0%B6%D0%B8%D0%B7%D0%BD%D0%B8) (приватность, privacy). Использование DLP-систем может противоречить местным законам в некоторых режимах или требовать особого оформления отношений между работниками и работодателем. Поэтому при внедрении DLP-системы необходимо привлекать юриста на самом раннем этапе проектирования.

Взаимоотношения DLP-систем с российским законодательством рассмотрены в ряде работ[[2]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8#cite_note-fnn_tszi-2)[[3]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8#cite_note-polik-3).

Информационная безопасность также описывается в [ГОСТ](https://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2), например, в ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

Согласно обзору «Российский рынок DLP-систем 2021. Проблемы и решения» от ICT-Online.ru основные игроки и решения на российском рынке DLP[[4]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8#cite_note-4):

* [StaffCop Enterprise](https://www.staffcop.ru/)
* Falcongaze [SecureTower](https://ru.wikipedia.org/wiki/SecureTower" \o "SecureTower)
* [DeviceLock](https://ru.wikipedia.org/wiki/DeviceLock) DLP
* [Infowatch](https://ru.wikipedia.org/wiki/InfoWatch) Traffic Monitor DLP
* [Zecurion](https://ru.wikipedia.org/wiki/Zecurion) DLP
* [Ростелеком Solar](https://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC-%D0%A1%D0%BE%D0%BB%D0%B0%D1%80) Dozor DLP
* [SearchInform](https://ru.wikipedia.org/wiki/SearchInform) DLP
* Гарда Предприятие
* [Kaspersky](https://ru.wikipedia.org/wiki/%D0%9B%D0%B0%D0%B1%D0%BE%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%D0%9A%D0%B0%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%BA%D0%BE%D0%B3%D0%BE) DLP

Зарубежные решения:

* [Symantec](https://ru.wikipedia.org/wiki/Symantec) DLP
* [Forcepoint](https://ru.wikipedia.org/wiki/Forcepoint) DLP
* [McAfee](https://ru.wikipedia.org/wiki/McAfee) DLP
* [Sophos](https://ru.wikipedia.org/wiki/Sophos) Endpoint Protection
* Digital Guardian