DOI 10.37882/2223-2966.2025.12.33

# ПРИМЕНЕНИЕ DLP-СИСТЕМ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ: АРХИТЕКТУРА, МЕТОДЫ МОНИТОРИНГА И ОЦЕНКА ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ

## THE USE OF DLP SYSTEMS TO PROTECT CONFIDENTIAL INFORMATION: ARCHITECTURE, MONITORING METHODS, AND EVALUATION OF IMPLEMENTATION EFFECTIVENESS

***T. Rein***

*Summary*. The article analyzes the principles of building data leakage prevention (DLP) systems, their architectural features, methods of monitoring and evaluating the effectiveness of implementation in modern corporate information environments. The paper examines the architecture components of DLP systems, including central management servers, agent modules on workstations and network monitoring points, as well as integration mechanisms with security systems. Special attention is paid to the methods of content, behavioral and network monitoring, revealing the possibilities of timely detection and prevention of information incidents in the context of dynamically changing cyber threats.

Attention is focused on the importance of a comprehensive assessment of the effectiveness of DLP systems implementation, including technical, organizational, and economic parameters, which allows not only to measure the effectiveness of protection, but also to optimize architecture and business processes. It is noted that only a systematic and adaptive approach to the construction, implementation and monitoring of DLP solutions can ensure the sustainability and proactive protection of confidential data.

The presented conclusions emphasize that the effective functioning of DLP systems is possible only if technical means and monitoring methods are integrated with a scientifically based assessment and management measures aimed at continuous improvement of information security tools.

*Keywords*: DLP systems, architecture of DLP systems, monitoring methods, efficiency assessment, information security, integration of security systems, cyber threats.

***Рейн Татьяна Сергеевна***
*кандидат физико-математических наук, доцент,*
*Кемеровский государственный институт*
*tsrein@mail.ru*

*Аннотация*. Статья посвящена анализу принципов построения систем предотвращения утечек данных (DLP), их архитектурных особенностей, методов мониторинга и оценки эффективности внедрения в современных корпоративных информационных средах. В работе рассматриваются компоненты архитектуры DLP-систем, включая центральные серверы управления, агентские модули на рабочих станциях и сетевые точки мониторинга, а также механизмы интеграции с системами обеспечения безопасности. Особое внимание уделено методам контентного, поведенческого и сетевого мониторинга, раскрывающим возможности своевременного выявления и предотвращения информационных инцидентов в условиях динамично изменяющихся киберугроз.

Акцентируется внимание на важности комплексной оценки эффективности внедрения DLP-систем, включающей технические, организационные и экономические параметры, что позволяет не только измерить результативность защиты, но и обеспечить оптимизацию архитектуры и бизнес-процессов. Отмечается, что только систематический и адаптивный подход к построению, реализации и мониторингу DLP-решений способен обеспечить устойчивость и проактивность защиты конфиденциальных данных.

Представленные выводы подчеркивают, что эффективное функционирование DLP-систем возможно лишь при условии интеграции технических средств и методов мониторинга с научно обоснованной оценкой и управленческими мерами, направленными на постоянное совершенствование инструментов информационной безопасности.

*Ключевые слова*: DLP-системы, архитектура DLP-систем, методы мониторинга, оценка эффективности, информационная безопасность, интеграция систем безопасности, киберугрозы.

В условиях возрастающих угроз информационной безопасности в корпоративной среде особую актуальность приобретает проблема предотвращения несанкционированных утечек конфиденциальных данных. В современных научных публикациях акцентируется внимание на том, что на фоне нарастающих киберугроз и прогрессирующей цифровизации бизнес-процессов проблема предотвращения несанкционированных утечек конфиденциальной информации становится фундаментальной задачей корпоративной безопасности [1, 11]. Исходя из этого, участившиеся прецеденты хищения коммерческих данных, персональной

информации и инсайдерские нарушения требуют внедрения таких методов защиты, которые выходят за рамки классических антивирусных и периметровых средств защиты информации.

Одним из ключевых инструментов обеспечения информационной безопасности и снижения рисков информационных потерь выступают DLP-системы (Data Loss Prevention), ориентированные на комплексную защиту корпоративной информации на всех этапах жизненного цикла данных — от их создания до передачи и хранения. В научной литературе указывается, что DLP-системы — это не только главный инструмент в обеспечении реализации требований законодательства и комплекс процедур, но и инструмент поддержание доверия к деятельности организации [10].

DLP-системы предназначены для защиты информации на всех этапах жизненного цикла данных: от их формирования и обработки до передачи, хранения и уничтожения. Ключевой задачей DLP-систем, как отмечается, является предотвращение ситуаций, связанных с несанкционированным использованием данных, либо их защита в том случае, когда они могут стать объектом внешних и внутренних угроз — как случайных, так и целенаправленных [3, 5]. Особая роль при этом отводится борьбе с инсайдерскими рисками и ошибками работников организации, на которые приходится большая доля современных утечек [2, 6, 7].

Методологические подходы к практическому применению DLP-систем включают использование: интеллектуальных инструментов анализа (контентного, контекстного, поведенческого, корреляционного), механизмов предотвращения и регистрации инцидентов в реальном времени, комплексной интеграции с другими сегментами корпоративной защиты (система управления сбора информации (SIEM), система управления идентификации доступом (IAM), центра безопасности операций (SOC) и др.), автоматизированного управления политиками обработки информации и реагирования на выявленные аномалии.

Анализ многочисленных научных работ показывает, что эффективность DLP-систем подтверждается снижением инцидентов, связанных с несанкционированным распространением и утратой данных, а сами системы становятся обязательным элементом инфраструктуры любой современной компании независимо от масштаба и отраслевой принадлежности. Кроме того, развитие DLP-технологий опирается на использование искусственного интеллекта и машинного обучения, что позволяет перехватывать даже сложные схемы передачи информации и опережать современные киберугрозы [4].

Таким образом, DLP-системы в свете современных исследований выступают не только как средства минимизации технологических и правовых рисков, но и как стратегически значимый инструмент формирования культуры обращения с данными и повышения конкурентоспособности хозяйствующих субъектов в условиях цифровой трансформации.

Современные DLP-системы реализуются в виде многоуровневых программных комплексов, интегрированных в единую корпоративную инфраструктуру информационной безопасности. К их основным архитектурным особенностям относятся:

— поддержка гибридных схем, сочетающих агентский и централизованный подход (размещение агентов на рабочих станциях и точках передачи данных, централизованный анализ сетевого трафика);
— мультиканальность, то есть контроль всех основных каналов утечки — электронной почты, облачных сервисов, мессенджеров, USB-носителей и других внешних устройств;
— обеспечение унифицированного управления политиками безопасности и инцидентами в рамках единой консоли [1, 10, 11].

Для лучшего понимания архитектуры DLP-системы необходимо ее представить в обобщенном виде (рисунок 1). Архитектура DLP-системы, представленная на рисунке, включает в себя три ключевых уровня взаимодействия, обеспечивающие комплексную защиту корпоративной информации на всех этапах ее жизненного цикла: сервер (сервер управления); агенты на рабочих станциях, точки мониторинга (мониторинг сетевого трафика).

Сервер управления является центральным компонентом, отвечающим за настройку политик безопасности, обработку предупреждений и инцидентов, хранение и анализ событий, централизованное управление агентами и точками контроля. На сервере настраиваются правила, отчеты, проводится аудит и расследование инцидентов.

Агенты на рабочих станциях — это своего рода программные модули, устанавливаемые на персональные компьютеры, ноутбуки или другие конечные устройства работников организации. Они контролируют все локальные действия с информацией: перемещение, копирование, печать, выгрузку на внешние носители, изменение сетевых настроек, запуск подозрительных приложений. Агенты могут обнаруживать попытки обхода контроля с помощью туннелирования, шифрования и других методов.

Точки мониторинга сетевого трафика представляют собой специализированные сетевые шлюзы, прокси-серверы, почтовые серверы или точки зеркалирования

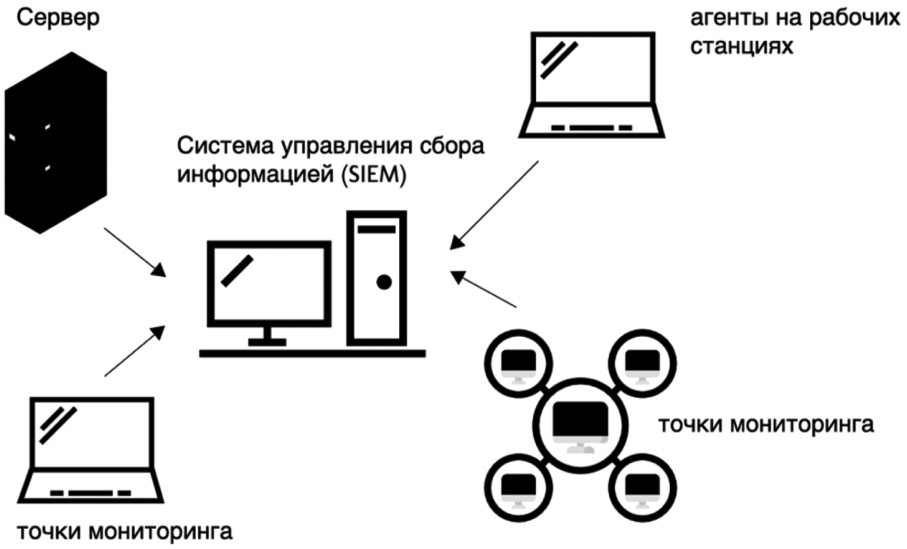


Рис. 1. Обобщенная схема архитектуры DLP-системы

(SPAN-порты). Точки мониторинга контролируют «данные в движении», анализируя электронную почту, вебтрафик, пересылку файлов, сообщения в мессенджерах и другие сетевые коммуникации между пользователями и внешними адресатами. Этот компонент обеспечивает предиктивную блокировку и регистрацию передачи конфиденциальной информации по внешним каналам.

Интеграция с системой управления собора информацией (SIEM) осуществляется за счет того, что DLP-система передает информацию о событиях и инцидентах в корпоративные аналитические и мониторинговые платформы, что позволяет решать задачи быстрого реагирования, глубокой аналитики, корреляции событий и согласования с политиками безопасности на уровне всей организации.

Таким образом, архитектура DLP-системы организована по модульному принципу: все компоненты взаимосвязаны, реализуют сбор, анализ и контроль информации на сетевом и локальном уровнях, а их взаимодействие через сервер управления и интеграционные шлюзы с внешними аналитическими модулями позволяет построить единую линию обороны против утечек данных.

В научной литературе методы мониторинга в DLP-системах рассматриваются как совокупность технологий и процедур, обеспечивающих всесторонний контроль за обработкой, передачей и хранением корпоративных данных.

К основным подходам мониторинга относят: контентный анализ, поведенческий анализ пользователей, сетевой мониторинг и аудит событий [5, 8, 11]. Контентный анализ направлен на автоматическое выявление признаков конфиденциальных данных, по ключевым словам, регулярным выражениям, шаблонам документов и цифровых отпечаткам. Актуальным направлением является расширение семантического анализа, позволяющего выявлять нетипичные проявления обработки чувствительной информации.

Поведенческий анализ пользователей имеет другое назначение — он позволяет осуществлять построение профилей типичного поведения работников организации, анализ аномалий и подозрительных операций, использование машинного обучения для выделения инсайдерских рисков и несанкционированных попыток передачи данных.

Сетевой мониторинг и аудит событий обеспечивает слежение за всеми каналами передачи информации (почта, облако, мессенджеры, и др.), построение графов связей и комплексную корреляцию событий безопасности в рамках интеграции с системой управления собора информацией SIEM и другими аналогичными системами.

Таким образом, как и сами DLP-системы, методы их мониторинга являются многоуровневыми, поскольку формируют систему защиты на нескольких уровнях, где каждый компонент дополняет другие, обеспечивая надежный и адаптивный контроль информационных потоков. Комплексное применение этих методов является ключевым условием повышения эффективности предотвращения утечек данных. При этом успех реализации DLP-механизмов во многом определяется не только технологическими возможностями, но и глубиной интеграции с бизнес-процессами и культурами информационной безопасности внутри организации. В перспективе развитие интеллектуальных аналитических инструментов и повышение автоматизации мониторинга станет определяющим фактором для создания проактивных и высокоэффективных систем предотвращения утечек информации.

Вместе с тем успешное функционирование DLP-системы заключается не только в построении ее архитектуры, но и в тщательной и систематической оценке эффективности внедрения такой системы. Обусловлено это тем, что без объективных критериев и метрик невозможно определить реальный уровень защиты, а также провести необходимую диагностику для оптимизации DLP-системы при ее практическом применении.

Оценка эффективности внедрения DLP-систем представляет собой сложный процесс, направленный на количественную и качественную оценку степени реализации поставленных целей по сохранению конфиденциальности корпоративной информации. Эффективная оценка требует системного подхода, сочетающего технические, организационные и экономические аспекты.

Технический аспект оценки включает количественный анализ событий безопасности до и после внедрения DLP-системы, что позволяет определить уровень снижения инцидентов, связанных с утечками данных. Важной метрикой является коэффициент обнаружения и предотвращения несанкционированного распространения информации, а также показатель ложных срабатываний, отражающий качество алгоритмов классификации данных и минимизацию помех для бизнес-процессов. Значительное внимание уделяется показателям производительности системы, влиянию на нагрузку, на ИТ-инфраструктуру и способность своевременно реагировать на инциденты.

Организационный аспект основан на оценке степени вовлеченности сотрудников, их обученности и соблюдения внутренних политик безопасности, что является критически важным для снижения человеческого фактора при утечках. Оценка охватывает процесс внедрения политик обеспечения информационной безопасности, мониторинга и реагирования, а также адаптивность политики в условиях изменяющейся бизнес-среды.

Экономическая оценка эффективности рассматривает соотношение затрат на внедрение и поддержку DLP-системы с уменьшением финансовых потерь, репутационных рисков и возможных штрафных санкций за нарушение требований законодательства по защите персональных данных и коммерческой тайны. Анализ затрат включает прямые расходы на лицензирование, оборудование, обучение и поддержку, а также косвенные расходы, связанные с минимизацией простоев и защитой интеллектуальной собственности.

В совокупности комплексная оценка эффективности внедрения DLP-систем формирует основу для принятия управленческих решений о дальнейшем развитии и совершенствовании информационной безопасности, обеспечивая оптимизацию ресурсов и повышение устойчивости организации к современным киберугрозам. При этом систематический подход к мониторингу, адаптация к специфике бизнеса и интеграция с другими ИТ-системами являются ключом к достижению максимального эффекта от внедрения DLP-систем.

Подводя итог, следует отметить, что архитектурные решения и набор методов мониторинга в DLP-системах не могут рассматриваться в качестве окончательной цели внедрения DLP-систем. Эффективность этих технических компонентов реализуется лишь в контексте систематической и научно обоснованной оценки результата их внедрения. Лишь путем комплексного анализа ключевых показателей — от точности обнаружения утечек до экономической целесообразности — возможно сформировать объективное представление о значении и роли DLP-системы в обеспечении информационной безопасности организации. В этом смысле оценка эффективности становится критерием не только технологической состоятельности, но и управленческой зрелости хозяйствующего субъекта, отражая уровень адаптации защиты к динамично меняющимся условиям и требованиям современного киберпространства.

Таким образом, интегральный подход, объединяющий инновационные архитектурные решения, современные аналитические методы и регулярный мониторинг эффективности, является базисом формирования проактивной, устойчивой и адаптивной системы предотвращения утечек данных, способной отвечать вызовам времени и обеспечивать надежную защиту корпоративных информационных ресурсов.

ЛИТЕРАТУРА

1. Андриянова Т.А., Саломатин С.Б. Использование адаптированной DLP-системы для Блокирования утечек информации // Системный анализ и прикладная информатика. 2017. №4. С. 52–57.
2. Артюшкина Е.С., Скакун О.О., Гузь А.Р. Использование искусственного интеллекта в DLP-системах // Прикладные экономические исследования. 2023. №2. С. 123–129.
3. Аусилова Н.М., Зарынбеков А.Б., Ахмет Г.Б. Применение DLP-систем как инструмента обеспечения информационной безопасности // НИР/S&R. 2023. №1 (13). С. 93–96.
4. Гречанная А.Ю., Тастенов А.Д. DLP-системы и их роль в защите от утечек конфиденциальной информации // Наука и техника Казахстана. 2015. №3–4. С. 23–27.

5. Глушков В.А. Классификация данных в DLP-системах: пробелы в локальном регулировании и правовые последствия // Новый юридический журнал. 2025. №1. С. 43–49.
6. Жинкин Д.Р., Журилко Г.С. Сравнительный анализ методов обнаружения утечек конфиденциальной информации в текстовых сообщениях // Вестник науки. 2025. №4 (85). С. 658–668.
7. Кабанцов Ю.Е., Лапшин Д.В., Баулин А.В. Предотвращение утечки конфиденциальной информации с использованием DLP систем // Синергия наук. 2018. № 26. С. 292–298.
8. Королев В.В. Использование методов анализа контента в DLP системах // Проблемы науки. 2016. №10 (11). С. 16–20.
9. Мавринская Т.В., Лошкарёв А.В., Чуракова Е.Н. DLP-системы и тайна личных переписок // Интерактивная наука. 2017. №14. С. 181–183.
10. Страхов А.А., Дубинина Н.М. Об утечке данных и DLP-системах // Криминологический журнал. 2022. №4. С. 226–232.
11. Firoz Mohammed Ozman. Implementing Data Loss Prevention (DLP). World Journal of Advanced Engineering Technology and Sciences, 2025, 15(02), 2427–2436.


Журнал «Современная наука: актуальные проблемы теории и практики»