

УДК 004.056

Анализ функционала реагирования на инциденты в системах предотвращения утечек данных

Романов Вадим Николаевич

roma.vadick@yandex.ru

Мазин Анатолий Викторович

mazin@bmstu.ru

КФ МГТУ им. Н.Э. Баумана, Калуга, Россия

Приведен анализ функционала реагирования на инциденты в системах предотвращения утечки данных (DLP), которые играют важную роль в защите конфиденциальной информации в современных информационных технологиях. Представлены ключевые функции DLP-систем, включая мониторинг, блокировку и анализ данных, а также методы реагирования на инциденты, такие как обнаружение, уведомление и корректирующие действия. Проанализирована работа DLP-системы на предприятии за один месяц, сделаны соответствующие выводы об эффективности ее работы.

Ключевые слова: утечка данных, мониторинг, инцидент, блокировка доступа, уведомление о нарушении, конфиденциальность

В современном мире информационные технологии становятся неотъемлемой частью бизнеса, а утечка конфиденциальной информации может иметь серьезные последствия. В этой связи ключевую роль играют системы предотвращения утечки данных (DLP — Data Loss Prevention). DLP-системы представляют собой программные средства, предназначенные для защиты организаций от несанкционированного доступа к чувствительной информации и ее утечки. Они создают защищенный цифровой «периметр» для анализа и контроля потока данных, как исходящего, так и входящего, что позволяет предотвращать утечки информации [1].

Виды и состав функций DLP. Системы DLP могут функционировать на различных уровнях, включая:

- сетевой уровень: контроль интернет-коммуникаций, включая электронную почту и веб-трафик. DLP-системы могут ограничивать доступ к определенным сайтам или блокировать передачу конфиденциальной информации по сети;
- уровень устройств: мониторинг и ограничение переноса данных на внешние накопители (USB-устройства, внешние жесткие диски) и принтеры. Это предотвращает несанкционированное копирование или печать чувствительной информации;
- уровень приложений: защита данных, обрабатываемых в прикладных системах, путем ограничения функционала программного обеспечения, например, блокировки возможности копирования или сохранения конфиденциальных данных [2].

Функции, на которые распространяется работа DLP, включают, но не ограничиваются:

- мониторинг и анализ данных: отслеживание движения данных внутри и вне сети для выявления признаков утечки;
- блокировка передачи данных: автоматическая остановка передачи конфиденциальной информации по электронной почте, в веб-приложениях, мессенджерах и т. д.;
- ограничение доступа к интернету: фильтрация и блокировка несанкционированного доступа к небезопасным или сомнительным ресурсам;
- контроль доступа к приложениям: настройка политик безопасности, которые запрещают или ограничивают использование определенных программ и функций;
- защита информации на уровне устройств: ограничение использования USB-устройств, принтеров и других периферийных устройств, чтобы предотвратить несанкционированное копирование данных [3].

Реагирование на инциденты DLP-систем. DLP-системы могут реагировать на инциденты с использованием различных подходов, которые обеспечивают многоуровневую защиту конфиденциальной информации. Рассмотрим основные типы реакций:

- *обнаружение*. Этот этап включает использование технологий анализа трафика и поведения пользователей для выявления потенциальных инцидентов. DLP-системы применяют адаптивные алгоритмы, которые постоянно «учатся» на основе предыдущих угроз, что позволяет обеспечить более точное обнаружение аномалий в поведении [2];

- *уведомление*. После обнаружения инцидента система автоматически информирует ответственных сотрудников о возникших угрозах. Уведомления могут быть отправлены через различные каналы (например, электронная почта, мессенджеры) и содержат информацию о характере инцидента [3];

- *блокировка*. Если система определяет, что происходит попытка несанкционированного доступа или утечки данных, она может немедленно заблокировать передачи или доступ к конфиденциальной информации. Это может быть реализовано как на уровне сетевого трафика, так и на уровне дисковых устройств;

- *эскалация*. В случае, если инцидент требует более глубокого анализа или вмешательства со стороны, DLP-система может передать информацию на более высокий уровень управления или специализированным группам. Это позволяет организовать более детальное расследование и оценку последствий инцидента [4];

- *анализ*. После инцидента команда по кибербезопасности проводит систематическое изучение ситуации для выявления причин, масштабов и возможных последствий утечки данных. Анализ может включать изучение лога инцидентов и выявление уязвимостей, которые могли быть использованы злоумышленниками [5];

– *журналирование*. Ведение записей обо всех обнаруженных инцидентах и предпринимаемых мерах является важной частью работы DLP-систем. Эти данные могут использоваться для последующего аудита и анализа, а также для разработки более эффективных процедур реагирования на потенциальные угрозы [3];

– *корректирующие действия*. После завершения анализа инцидента организация может внедрять корректирующие меры, направленные на устранение последствий и предотвращение повторного возникновения аналогичных ситуаций. Это может включать обновление процедур, использование новых технологий и обучение сотрудников;

– *обучение*. Основываясь на результатах анализа инцидента, рекомендуется проводить обучение сотрудников для повышения их осведомленности о безопасности и рисках. Это может помочь снизить вероятность человеческих ошибок и улучшить общую защиту данных в организации [5].

Статистика работы DLP-системы. Для более глубокого понимания эффективности работы системы предотвращения утечек данных (DLP) необходимо проанализировать статистику ее работы на некотором предприятии за прошедший месяц. Этот анализ позволит выявить основные направления работы системы, ее надежность в предотвращении инцидентов и уровень реагирования на различные угрозы. В приведенной ниже таблице представлены собранные данные о типах инцидентов, с которыми столкнулась DLP-система, а также мерах реагирования на них (см. таблицу).

Статистика работы DLP-системы за 1 месяц

Тип инцидента	Количество	Мера реагирования
Отправка документа по электронной почте	272	Уведомление отправителя и дальнейший анализ
Попытка доступа к запрещенным веб-сайтам	86	Блокировка доступа и логирование события
Копирование данных на сетевой ресурс	113	Логирование события
Попытка сканирования документов, содержащих конфиденциальные данные	2	Блокировка сканирования и анализ инцидента
Неправильное использование служебных документов	4	Уведомление и повторное обучение сотрудников
Необоснованная попытка доступа к системам с конфиденциальной информацией	17	Блокировка доступа и дальнейший анализ

По результатам анализа статистики DLP-системы за месяц было зафиксировано 494 инцидента. Основная часть из них связана с передачей доку-

ментации по электронной почте — это 272 случая, что составило более половины всех инцидентов. В таких случаях сработали меры уведомления отправителя и инициирование дальнейшего анализа.

На втором месте — случаи попыток доступа к запрещенным веб-сайтам, которые составляют 86 инцидентов. Все они были заблокированы, а события задокументированы, что подтверждает активное использование механизма блокировки DLP-системы.

Результаты также показывают значительное количество попыток копирования данных на сетевые ресурсы — 113 инцидентов, к которым была применена мера логирования, что позволяет сохранить информацию для последующего анализа, но требует более активных мер для предотвращения возможных утечек информации в будущем.

Таким образом, результаты подчеркивают важность использования DLP-систем не только для блокировки инцидентов, но и для активного мониторинга и анализа поведения пользователей. Повышение осведомленности сотрудников об использовании служебных документов также необходимо, учитывая 4 инцидента неправильного использования, что указывает на необходимость регулярного обучения. Эти данные могут служить основой для корректировки политики безопасности и обеспечения более высокой защитой конфиденциальной информации в организации.

Литература

- [1] Рябова Г. *Автоматизация мониторинга и расследования инцидентов в DLP-системе*. URL: <https://www.securitylab.ru/analytics/475554.php> (дата обращения 17.10.2024).
- [2] Коржов В. *DLP на пути к расследованию инцидентов*. URL: <https://www.osp.ru/os/2014/08/13043489> (дата обращения 17.10.2024).
- [3] *DLP: как работа системы предотвращает утечку информации*. URL: <https://it2bsns.ru/articles/dlp-kak-rabota-sistemy-predotvrashhaet-utechku-informaczii/> (дата обращения 20.10.2024).
- [4] Бирюков А. *Как уберечься от инсайда*. URL: <https://bit.samag.ru/archive/article/1076> (дата обращения 21.10.2024).
- [5] Степанов И. *Сравнительный обзор средств предотвращения утечек данных (DLP)*. URL: <https://safe-surf.ru/specialists/article/5233/609990/> (дата обращения 21.10.2024).

Analysis of incident response functionality in data leak prevention systems

Romanov V.N.

roma.vadick@yandex.ru

Mazin A.V.

mazin@bmstu.ru

BMSTU (KB), Kaluga, Russia

The article examines the analysis of the incident response functionality in data leakage prevention (DLP) systems, which play an important role in protecting confidential information in modern information technologies. The key functions of DLP systems are presented, including monitoring, blocking and data analysis, as well as incident response methods such as detection, notification and corrective actions. The work of the DLP system at the enterprise for one month was analyzed, and appropriate conclusions were drawn about the effectiveness of its work.

Keywords: data leakage, monitoring, incident, access blocking, violation notification, confidentiality