УДК: 004.056.55:004.423.24

Аскарбеков Руслан Нуркожоевич *к.ф.-м.н., И. Раззаков атындагы Кыргыз мамлекеттик техникалык университетинин К. Курманалиев атындагы «Полиграфия» кафедрасынын доценти. Кыргызстан 720044, Бишкек шаары. Ч. Айтматов проспектиси, 66, e-mail:* askarbekov@kstu.kg.
Байгазиев Мирбек Сагымбаевич *т.и.к., И. Раззаков атындагы Кыргыз мамлекеттик техникалык университетинин К. Курманалиев атындагы «Полиграфия» кафедрасынын доценти. Кыргызстан 720044, Бишкек шаары. Ч. Айтматов проспектиси, 66, e-mail:* mirbek-1985@kstu.kg.
Агибаев Мухаммед Абдулхаевич *И. Раззаков атындагы Кыргыз мамлекеттик техникалык университетинин К. Курманалиев атындагы «Полиграфия» кафедрасынын ага окутуучу. Кыргызстан 720044, Бишкек шаары. Ч. Айтматов проспектиси, 66, e-mail:* agibaev137@gmail.com

ЭФФЕКТИВНОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ АЛГОРИТМОВ В СИСТЕМАХ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ

Аннотация. В данной статье проводится комплексный анализ ключевых алгоритмов, применяемых в системах предотвращения утечек данных. Рассматриваются четыре основных класса алгоритмов: детерминированные методы на основе регулярных выражений, контентный анализ с использованием цифровых отпечатков, статистический анализ и методы машинного обучения для поведенческого анализа. Целью данной статьи является сравнительная оценка указанных методов и эффективности в обнаружении инцидентов информационной безопасности. В работе представлены результаты симуляционного моделирования, демонстрирующие компромисс между точностью обнаружения и уровнем ложных срабатываний.

Ключевые слова: DLP, информационная безопасность, машинное обучение, цифровые отпечатки, регулярные выражения, поведенческий анализ

Введение

В условиях цифровой трансформации и роста объемов корпоративных данных защита конфиденциальной информации становится критически важной задачей. Системы предотвращения утечек данных (Data Loss Prevention или кратко DLP) являются одним из ключевых инструментов для решения этой задачи. Они предназначены для мониторинга, обнаружения и блокировки несанкционированной передачи чувствительной информации. Современные DLP-решения используют широкий спектр алгоритмов, от простых детерминированных правил до сложных моделей искусственного интеллекта [1, 4].

В условиях роста числа инцидентов информационной безопасности возрастает роль централизованных подсистем сбора, корреляции и анализа событий, интегрируемых в архитектуру SOC, что позволяет повысить эффективность обнаружения и реагирования на утечки данных [8].

Как показывает статистика, большинство утечек происходит по вине внутренних сотрудников, а не внешних хакеров. DLP помогает выявить и заблокировать злоумышленные действия. Например, если сотрудник пытается скопировать клиентскую базу на флешку или отправить стратегический план конкурентам через личную почту, система останавливает непреднамеренные утечки. Классический пример: бухгалтер по ошибке отправляет ведомость с зарплатами не коллеге, а внешнему подрядчику. DLP распознает конфиденциальный документ и заблокирует отправку. Многие отрасли строго регулируются в части обработки данных [5]. Компании обязаны защищать персональные данные клиентов, пациентов и сотрудников. DLP — это технический инструмент, доказывающий, что компания приняла меры по защите данных, как того требуют законы (например, GDPR в Европе, PCI DSS для банковских карт). Система автоматически отслеживает данные,

подпадающие под регуляцию (например, номера паспортов, данные карт), и применяет к ним политики безопасности. Для многих компаний их главный актив — это интеллектуальная собственность: уникальные разработки, формулы, чертежи, бизнес-стратегии, исходный код. DLP гарантирует, что ваши ноу-хау не окажутся у конкурентов. Система позволяет безопасно работать с фрилансерами и партнерами, давая им доступ к данным, но не позволяя их скопировать или переслать [2].

Многие руководители даже не представляют, как на самом деле сотрудники работают с информацией. DLP дает полную картину. Если утечка все же произошла, DLP предоставляет архив всех событий. Служба безопасности может точно и быстро определить, *кто, что, когда* и *куда* отправил. Анализ отчетов DLP показывает, какие бизнес-процессы небезопасны, и помогает их оптимизировать (например, если сотрудники массово используют личные мессенджеры для рабочей переписки) [5, 6]. Утечка данных клиентов или партнеров — это мощнейший удар по доверию. Клиенты охотнее работают с компанией, которая доказывает, что может защитить их данные. Новость об утечке моментально попадает в СМИ, отпугивая инвесторов и партнеров. Предотвратить утечку гораздо дешевле, чем восстанавливать репутацию.

До внедрения DLP (Высокий риск)	После внедрения DLP (Риск под контролем)
Данные уходят бесконтрольно (на флешки, в облака).	Передача данных на внешние носители и в сеть контролируется.
Утечки обнаруживаются постфактум, часто из СМИ.	Попытки утечки блокируются в реальном времени.
Невозможно доказать вину сотрудника или факт утечки.	Все инциденты фиксируются, есть доказательная база.
Высокий риск штрафов от регуляторов (НБ КР, Госагентство по защите персональных данных и др.).	Требования законов и правил выполняются.
Коммерческая тайна и клиентские базы уязвимы.	Ключевые активы компании защищены от кражи.

Классификация и описание алгоритмов DLP

Алгоритмы, используемые в DLP-системах, можно условно разделить на четыре основные группы [3].

1. Детерминированные алгоритмы. Основаны на поиске точных совпадений по заранее заданным шаблонам. Регулярные выражения: используются для поиска структурированной информации, такой как номера кредитных карт, паспортные данные, ИНН.

   Пример: Шаблон для номера кредитной карты Visa: \b4[0-9]{12}(?:[0-9]{3})?\b.

   Преимущества: Высокая скорость работы, предсказуемость, низкое количество ложных срабатываний для строго формализованных данных.

   Недостатки: Неспособность обнаруживать неструктурированный контент (например, фрагменты коммерческой тайны в свободной форме).
2. Алгоритмы контентного анализа. Анализируют содержимое файлов и документов целиком или по частям. Цифровые отпечатки: с защищаемого документа или базы данных снимается набор хэш-сумм (отпечатков). Агент ищет точные или частичные совпадения этих отпечатков в исходящем трафике.

   Принцип работы: Документ разбивается на фрагменты, для каждого вычисляется хэш. Система ищет совпадения по этим хэшам.

   Преимущества: Высочайшая точность для защиты конкретных документов и структурированных данных (например, клиентских баз), устойчивость к незначительным изменениям.

   Недостатки: Требует предварительной каталогизации защищаемых данных.
3. Статистические методы. Применяют математические модели для анализа данных. Байесовские классификаторы: часто используются для категоризации текстов (например,

«спам» / «не спам»). В DLP могут классифицировать документы как «конфиденциальные» или «публичные» на основе частоты встречаемости определенных терминов. Статистический анализ метаданных: Анализ не самого контента, а его атрибутов (размер, тип файла, отправитель, получатель).

4. Машинное обучение и поведенческий анализ. Наиболее продвинутая группа алгоритмов, направленная на выявление аномалий. Система строит профиль «нормального» поведения для каждого пользователя (типичное время работы, объемы передаваемых данных, используемые приложения). Отклонения от этого профиля (аномалии) помечаются как потенциальные инциденты.

   Пример: Сотрудник, который никогда не работал с CRM, внезапно пытается выгрузить из нее всю базу клиентов в 3 часа ночи.

   Преимущества: Способность обнаруживать ранее неизвестные угрозы и инсайдерскую активность.

   Недостатки: Требует длительного периода обучения, более высокий процент ложных срабатываний на начальном этапе, высокая ресурсоемкость.

Рассмотрим базовые сценарии: DLP-система сработает, если обнаружит попытку передачи фрагмента кода, содержащего чувствительную информацию или цифровой отпечаток всего проекта.

Сценарий 1: Утечка аутентификационных данных

```
// Пример кода, который DLP может заблокировать из-за обнаружения 'SECRET_KEY'
public class PaymentGateway {
    private static final String API_KEY =
"sk_live_v2_f8d7g0a9b3c4e5f6h7j0k1l2m3n4p5r6"; // <--- СЕКРЕТНЫЙ КЛЮЧ
    private static final String DB_PASS = "admin123#prod_2025"; // <--- ПАРОЛЬ

    public void processPayment(double amount) {
        // Логика обработки платежа...
        System.out.println("Connecting to API with key: " + API_KEY);
    }
}
```

Как DLP это обнаруживает: С помощью регулярных выражений, настроенных на поиск шаблонов, похожих на ключи (например, `sk_live_...` или `[A-Za-z0-9]{32}`), а также на основе ключевых слов (`API_KEY`, `DB_PASS`, `password`, `secret`).

Сценарий 2: Утечка исходного кода с цифровым отпечатком

```
/*
* [FILE: LicenseHeader.cs]
* Proprietary Code of Acme Corp. (c) 2025.
* This code is subject to the terms of the Corporate Source License Agreement.
* DO NOT SHARE OR REPLICATE. [Project_ID: AX-747-BETA] <--- УНИКАЛЬНЫЙ ОТПЕЧАТОК
*/

// Фрагмент кода, который был скопирован и отправлен на личную почту
public void CalculateAnnualBonus()
{
    // ...
    double bonus = (salesRevenue - costs) * 0.05;
    // ...
}
```

Как DLP это обнаруживает: Используя технологию цифровых отпечатков, которая сравнивает отправляемый контент с эталонным набором конфиденциальных документов, даже если был скопирован только небольшой, но уникальный фрагмент.

DLP-системы используют комбинацию технологий для классификации и защиты данных:

Технология обнаружения	*Что ищет DLP (пример "кода")*
Регулярные выражения (RegEx)	*Номера кредитных карт, ИНН, БИК:* `(\d{4}[- ]?){4}`
Ключевые слова/словари	*Слова или фразы, сигнализирующие о конфиденциальности:* `"КОММЕРЧЕСКАЯ ТАЙНА"`, `"НЕ ДЛЯ ПУБЛИКАЦИИ"`, `"PROJECT"`.
Цифровые отпечатки	*Уникальные последовательности текста или данных, соответствующие внутренним базам документов (исходники, патенты, финансовые отчеты).*
Классификация (AI/ML)	*Файлы или сообщения, которые по контексту или поведению (например,* `.zip` *архив с 1000* `.java` *файлов) классифицируются как "Исходный код".*

Методология сравнительного анализа

Для оценки эффективности и производительности алгоритмов было проведено симуляционное моделирование. Были сгенерированы три набора данных:

1. Набор А (Структурированные данные): 10 000 документов, содержащих персональные данные в формализованном виде.
2. Набор Б (Неструктурированные данные): 5 000 документов, содержащих фрагменты текста, относящиеся к коммерческой тайне.
3. Набор В (Чистые данные): 20 000 документов без конфиденциальной информации.

Каждый алгоритм был протестирован на этих наборах для определения двух ключевых метрик: True Positive Rate — доля корректно выявленных утечек, и False Positive Rate — доля ложных срабатываний.

Таблица 1 – Сравнительные показатели точности алгоритмов DLP

Алгоритм	Тестовый набор	TPR (Точность обнаружения)	FPR (Ложные срабатывания)
Регулярные выражения	Набор А (Структур.)	99.5%	0.1%
	Набор Б (Неструктур.)	15.2%	1.0%
Цифровые отпечатки	Набор А (Структур.)	98.9%	0.05%
	Набор Б (Неструктур.)	95.7%	0.5%
Статистический анализ	Набор А (Структур.)	85.0%	5.5%
	Набор Б (Неструктур.)	88.3%	4.2%
Машинное обучение	Любой тип данных	94.5%	3.0%

- **Регулярные выражения** показывают почти идеальный результат на структурированных данных, но практически бесполезны для анализа неструктурированных текстов.
- **Цифровые отпечатки** являются наиболее сбалансированным и точным методом для защиты известных данных, демонстрируя крайне низкий уровень ложных срабатываний.
- **Машинное обучение** показывает высокую эффективность на всех типах данных, но ценой более высокого FPR, что требует дополнительной верификации инцидентов со стороны офицера безопасности.

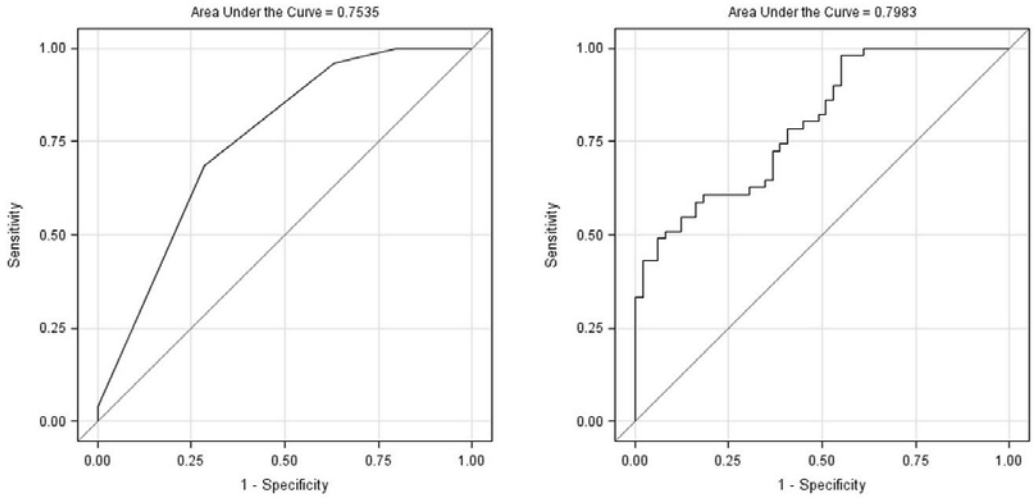

График 1 – ROC-кривая для модели машинного обучения (компромисс между TPR и FPR)

По горизонтальной оси X отложен FPR – доля ложных срабатываний, а по вертикальной оси Y – TPR, или полнота обнаружения. Каждая точка на кривой представляет собой соотношение TPR и FPR при определенном пороговом значении чувствительности модели. Идеальная точка для DLP-системы, отражающая максимально эффективный баланс, находится в левом верхнем углу (координаты 0,1). Эта точка соответствует 100% полноте обнаружения TPR=1 при 0% ложных срабатываний FPR=0. Реальные модели стремятся приблизиться к этой точке, как показано на кривой. Площадь под кривой - служит единым количественным показателем эффективности модели, где ее значение близкое к 1.0 означает превосходную производительность. ROC (Receiver Operating Characteristic) – кривая означает Характеристика Оператора Приемника.

Приемник: Это сама модель классификации (алгоритм машинного обучения), которая «принимает» данные и принимает решение — является ли событие утечкой данных (положительный класс) или нет (отрицательный класс).

Характеристика: Это график, который показывает, как изменяется способность модели обнаруживать истинные положительные случаи TPR в зависимости от частоты ложных срабатываний FPR при изменении порога принятия решения. ROC-кривая визуализирует компромисс между двумя ключевыми метриками TPR – чувствительность (Sensitivity) или полнота. Это доля правильно идентифицированных положительных случаев (например, реальных утечек данных).

$$TPR = \frac{\text{Истинно положительные}}{\text{Истинно положительные+Ложно отрицательные}},$$

FPR – доля ложно идентифицированных положительных случаев (например, легитимные действия, ошибочно помеченные как утечка).

$$FPR = \frac{\text{Ложно положительные}}{\text{Ложно положительные+Истинно отрицательные}},$$

ROC – кривая помогает выбрать оптимальный порог для модели DLP, чтобы максимизировать обнаружение угроз TPR при минимизации помех и блокировок легитимного трафика FPR.

Заключение

Проведенное исследование показало, что не существует единого «лучшего» алгоритма для систем DLP. Выбор конкретной технологии должен основываться на типе защищаемых данных и приоритетах организации. Для защиты строго формализованных данных наиболее эффективны регулярные выражения. Для защиты конкретных документов и баз данных (коммерческая тайна, интеллектуальная собственность) оптимальным выбором являются цифровые отпечатки. Для выявления инсайдерских угроз и сложных, ранее неизвестных сценариев утечек, необходимо использовать поведенческий анализ на основе машинного обучения. Наилучшие результаты демонстрируют современные гибридные DLP-системы, которые комбинируют несколько алгоритмов, применяя наиболее подходящий в зависимости от контекста операции. Дальнейшие исследования могут быть направлены на изучение методов оптимизации производительности машинного обучения – ее моделей и разработку адаптивных алгоритмов, автоматически выбирающих метод анализа.

Литература

1. Алексеева Е.Ю., Бутин А.А. DLP-системы. Методология и продукты // Информационные технологии и проблемы математического моделирования сложных систем. — 2016. — № 17. — С. 23–28. — EDN IDVXUM.
2. Антонов А.Е., Матвеев В.В. Обеспечение экономической безопасности с использованием DLP-системы (искусственного интеллекта) // Теоретические и прикладные вопросы комплексной безопасности: Материалы V Междунар. науч.-практ. конф. (Санкт-Петербург, 23 марта 2022 г.). — СПб.: …, 2022. — С. 251–257. — EDN DEOZZA.
3. Зверев И.Н. Сравнительный обзор методов категоризации, применяемых в DLP-системах // Актуальные вопросы современной науки. — 2014. — № 35. — С. 108–117. — EDN SIEBRV.
4. Калиберда Е.А., Шабалин А.М. Использование современных систем виртуализации… // Наука о человеке: гуманитарные исследования. — 2020. — Т. 14, № 2. — С. 118–122. — DOI 10.17238/issn1998-5320.2020.14.2.20. — EDN WUCZCP.
5. Сипатров Н.А., Крылова С.Л. Аспекты эффективности DLP-систем // WORLD SCIENCE: PROBLEMS AND INNOVATIONS… — Пенза, 2017. — Ч. 1. — С. 102–106. — EDN YHXWRB.
6. Яблоков Д.С. Обзор системы Zecurion DLP 11… // Тенденции развития науки и образования. — 2024. — № 115–15. — С. 157–163. — DOI 10.18411/trnio-11-2024-722. — EDN GBHMJX.
7. Gartner. Market Guide for Data Loss Prevention. — 2025. — URL: https://www.gartner.com/en/documents/6342779 (дата обращения: укажите свою).
8. Корякина Ю.С., Айтбаев Ш.Т., Зимин И.В. Аналитический обзор методов реализации подсистем сбора, обработки, хранения и визуализации данных для SOC (Security Operations Center) // Проблемы автоматики и управления. — 2025. — № 2(53). — С. 29–40.