МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт искусственного интеллекта
Базовая кафедра 252

КУРСОВАЯ РАБОТА

по дисциплине
«Предупреждение, выявление и установление причин и условий компьютерных инцидентов»

Тема курсовой работы
«Исследование подходов к созданию DLP-систем»

Студент: Никишина Анна Александровна
Группа: ККСО–03–19

Руководитель курсовой работы: Гончаренко Владислав Евгеньевич

Москва
2023

Содержание

1. Анализ текущего состояния в области построения технологий и систем DLP (Data Loss Prevention).

В наше современное информационное общество, где объемы цифровых данных постоянно растут, обеспечение безопасности конфиденциальной информации становится критически важным аспектом деятельности организаций. В этом контексте, системы предотвращения утечек данных (Data Loss Prevention, DLP) занимают центральное место в обеспечении безопасности информации. DLP-системы предназначены для обнаружения, мониторинга и предотвращения утечек конфиденциальных данных, таких как финансовая информация, персональные данные клиентов, интеллектуальная собственность и другие важные корпоративные ресурсы.

1.1. Определение объекта исследований, анализ состава задач предметной области объекта исследований – исследование базовых технологий DLP.

Примеры базовых DLP-технологий

1. Механизмы Классификации Данных

   Одной из основных технологий DLP является механизм классификации данных. Этот подход включает в себя определение и категоризацию информации в соответствии с уровнем ее конфиденциальности. Программные средства автоматической классификации могут использовать ключевые слова, образцы данных или даже машинное обучение для точного определения чувствительных данных.

   Пример: Интегрированные DLP-решения могут обнаруживать и классифицировать конфиденциальные документы, помечая их соответствующим образом и применяя соответствующие политики доступа.

2. Контентный анализ

   Технологии контентного анализа позволяют системам DLP анализировать содержимое файлов и сообщений на наличие чувствительных данных. Это включает в себя поиск определенных шаблонов, распознавание структуры данных и обнаружение угроз на основе контекста.

   Пример: DLP-система, использующая контентный анализ, может предотвратить отправку электронного письма с прикрепленным документом, содержащим финансовые данные, за пределы организации.

3. Мониторинг и анализ поведения пользователей

   Системы DLP также активно используют мониторинг и анализ поведения пользователей для выявления аномалий и потенциальных угроз безопасности. Этот метод позволяет выявлять необычные активности, такие как попытки несанкционированного доступа или передача данных в неразрешенные места.

   Пример: DLP-решение, основанное на мониторинге поведения пользователей, может предупредить об атаке внутреннего угрозы, когда сотрудник пытается загрузить большой объем данных на внешний сервер.

Эти примеры базовых DLP-технологий позволяют нам дать общее представление о том, каким образом данные системы обеспечивают защиту конфиденциальной информации и предотвращают утечку данных. Дальнейший анализ этих технологий позволит более глубоко понять их эффективность и применимость в различных сценариях использования.

1.1.1 Анализ структуры построения существующих базовых технологий DLP.

Существующие базовые технологии DLP включают в себя этапы обнаружения, мониторинга и контроля передачи конфиденциальной информации. Процессы включают анализ данных, обнаружение угроз и принятие мер по предотвращению утечек.

Предварительный анализ позволяет выделить основные модели базовых технологий DLP:

1. Технология механизмов классификации данных.
2. Технология контекстного анализа.
3. Технология мониторинга и анализа поведения пользователей.

Ниже приведём таблицы для разделов, определяющих структуру каждой, выделенной нами, базовой технологии.

Этап	Процесс	Процедура	Действие
Идентификация данных	Сканирование документов	Определение структуры данных	Запуск программы для анализа структуры
			Идентификация различных элементов данных
		Распознавание форматов файлов	Анализ заголовков файлов
			Использование сигнатур для определения формата
	Анализ метаданных	Извлечение метаданных	Использование API для извлечения метаданных
			Анализ заголовков файлов
		Сопоставление с известными шаблонами	Создание базы данных с известными шаблонами
			Сравнение метаданных с шаблонами
Классификация данных	Использование сигнатур	Создание базы сигнатур	Анализ существующих данных для создания сигнатур
			Обновление базы сигнатур при появлении новых данных
		Сравнение сигнатур с данными	Применение сигнатур к потоку данных
			Выявление совпадений с известными сигнатурами
	Машинное обучение	Обучение модели на основе образцов	Подготовка обучающего набора данных
			Обучение модели с использованием алгоритмов машинного обучения
		Применение модели к новым данным	Использование обученной модели для классификации данных
			Анализ результатов и обновление модели при необходимости

Таблица 1: Таблица для разделов, определяющих структуру механизмов классификации данных.

Этап	**Процесс**	**Процедура**	**Действие**
Сбор контекста	Мониторинг сетевой активности	Захват трафика	Установка сетевых датчиков для перехвата трафика
			Шифрование захваченных данных для безопасности
		Анализ пакетов данных	Фильтрация пакетов для удаления шума
			Извлечение информации о источнике, назначении и содержании пакетов
	Слежение за действиями пользователей	Регистрация событий	Определение событий, требующих регистрации
			Логирование событий с указанием времени и пользователя
		Анализ активности пользователей	Сопоставление активности с предопределенными шаблонами
			Выделение аномальной активности для дальнейшего анализа
Оценка контекста	Анализ паттернов поведения	Идентификация нормальных паттернов	Анализ статистики поведения пользователей
			Создание профилей нормального поведения
		Выявление аномалий в поведении	Сравнение активности с нормальными паттернами
			Поднятие тревоги при обнаружении аномалий
	Определение контекстуальных правил	Создание правил на основе контекста	Исследование и анализ данных для определения правил
			Определение пороговых значений для различных параметров
		Применение правил к данным	Внедрение контекстуальных правил в систему мониторинга
			Анализ данных на соответствие установленным контекстным правилам

Таблица 2: Таблица для разделов, определяющих структуру технологии контекстного анализа.

Этап	**Процесс**	**Процедура**	**Действие**
Сбор данных о поведении	Захват данных о действиях пользователей	Логирование активности	Установка агентов для отслеживания действий пользователей
			Регистрация информации о каждом действии сотрудника
		Сбор данных о времени использования	Захват данных о времени начала и окончания работы
			Создание логов для анализа паттернов активности
	Сегментация пользователей	Группировка пользователей по профилям	Определение основных характеристик пользователей
			Разделение пользователей на группы по схожести активности
		Анализ схожести поведения в группах	Идентификация общих паттернов внутри групп
			Определение аномалий в поведении отдельных пользователей в группе
Анализ поведения	Выявление аномалий в поведении	Сравнение с образцами нормального поведения	Составление профилей нормального поведения
			Анализ активности сравнением с установленными образцами
		Обнаружение необычных активностей	Использование алгоритмов машинного обучения для выявления аномалий
			Поднятие тревоги при обнаружении необычной активности
	Оценка риска	Присвоение рисковых оценок	Оценка аномальной активности по степени риска
			Классификация уровней риска для принятия дальнейших мер
		Выявление действий, требующих внимания	Выделение конкретных действий, считающихся потенциально опасными
			Системное уведомление или блокировка активности при высоких уровнях риска

	Принятие мер	Автоматические реакции	Задействование автоматических сценариев реагирования на определенные события
			Автоматическое блокирование доступа к ресурсам при высоких уровнях риска
		Ручные реакции	Создание тикетов для ручного анализа и реагирования
			Вовлечение безопасностных аналитиков для проведения дополнительного анализа
	Обучение системы	Актуализация образцов нормального поведения	Использование обратной связи от аналитиков для коррекции образцов
			Автоматическое обновление профилей нормального поведения
		Расширение базы данных аномалий	Добавление новых сценариев аномалий на основе новых данных
			Обучение системы распознавать новые типы аномалий

Таблица 3: Таблица для разделов, определяющих структуру технологии мониторинга и анализа поведения пользователей.

1.1.2 Исследование методологической основы построения базовых технологий DLP.

Методологическая основа включает в себя использование сигнатур, машинного обучения и анализа поведения для обнаружения утечек. Сценарии применения включают защиту корпоративных данных, соблюдение регулирований и предотвращение утечек.

Этап	**Процесс**	**Процедура**	**Действие**	**Методологическая основа**
Идентификация данных	Сканирование документов	Определение структуры данных	Запуск программы для анализа структуры	Использование методов обратной инженерии для разбора структуры данных с целью определения типов, полей и их взаимосвязей.
			Идентификация различных элементов данных	Применение алгоритмов сигнатурного анализа, основанных на характерных последовательностях байт или структур данных, для точной идентификации различных элементов.
		Распознавание форматов файлов	Анализ заголовков файлов	Применение методов статического анализа, включая анализ заголовков файлов и их метаданных для определения типа и формата данных.
			Использование сигнатур для определения формата	Развитие базы сигнатур, основанных на уникальных байтовых последовательностях для точного определения форматов файлов.
	Анализ метаданных	Извлечение метаданных	Использование API для извлечения метаданных	Использование стандартных и внутренних API для извлечения метаданных, обеспечивающих универсальность и совместимость с различными источниками данных.
			Анализ заголовков файлов	Применение методов статического анализа для извлечения метаданных из заголовков файлов и дальнейшего сопоставления с шаблонами.
		Сопоставление с известными шаблонами	Создание базы данных с известными шаблонами	Проведение исследований и анализа для создания базы данных известных шаблонов, включающих в себя метаданные различных типов файлов.
			Сравнение метаданных с шаблонами	Разработка алгоритмов сравнения метаданных с известными шаблонами, обеспечивающих точное сопоставление.

Классификация данных	Использование сигнатур	Создание базы сигнатур	Анализ существующих данных для создания сигнатур	Систематический анализ существующих данных для выделения уникальных характеристик и формирования эффективных сигнатур.
			Обновление базы сигнатур при появлении новых данных	Разработка процессов автоматического обновления базы сигнатур для оперативной адаптации к новым типам данных.
		Сравнение сигнатур с данными	Применение сигнатур к потоку данных	Использование алгоритмов сигнатурного сопоставления для выявления совпадений с известными сигнатурами в потоке данных.
			Выявление совпадений с известными сигнатурами	Разработка стратегий сопоставления и анализа результатов для точного выявления совпадений.
	Машинное обучение	Обучение модели на основе образцов	Подготовка обучающего набора данных	Использование стратегии отбора представительного обучающего набора данных, включающего в себя разнообразные типы данных, представленные в организации.
			Обучение модели с использованием алгоритмов машинного обучения	Применение алгоритмов, таких как метод опорных векторов (SVM), случайные леса или нейронные сети, в зависимости от характеристик данных, для обучения модели классификации.
		Применение модели к новым данным	Использование обученной модели для классификации данных	Реализация интеграции обученной модели в систему классификации данных, обеспечивая эффективное и быстрое применение модели к новым данным.
			Анализ результатов и обновление модели при необходимости	Регулярный анализ результатов классификации, включая оценку точности, полноты и F-меры, а также проведение периодического обновления модели с использованием новых данных для поддержания актуальности.

Таблица 4: Таблица для разделов, определяющих методологическую основу механизмов классификации данных.

Этап	Процесс	Процедура	Действие	Методологическая основа
Сбор контекста	Мониторинг сетевой активности	Захват трафика	Установка сетевых датчиков для перехвата трафика	Применение технологий сетевого мониторинга, включая инструменты packet sniffing, для захвата трафика в режиме реального времени.
			Шифрование захваченных данных для безопасности	Использование протоколов шифрования, таких как SSL/TLS, для обеспечения безопасности передачи и хранения захваченных данных.
		Анализ пакетов данных	Фильтрация пакетов для удаления шума	Разработка фильтров для исключения из анализа шумовых данных и концентрации на существенной информации.
			Извлечение информации о источнике, назначении и содержании пакетов	Применение алгоритмов извлечения метаданных для анализа пакетов и выделения информации об источнике, назначении и содержании данных.
	Слежение за действиями пользователей	Регистрация событий	Определение событий, требующих регистрации	Разработка критериев и правил для определения событий, которые требуют регистрации, с учетом особенностей организации.
			Логирование событий с указанием времени и пользователя	Внедрение системы логирования событий, предоставляющей детализированную информацию о каждом событии, включая временные метки и идентификаторы пользователей.
		Анализ активности пользователей	Сопоставление активности с предопределенными шаблонами	Разработка библиотеки предопределенных шаблонов активности для сопоставления с текущей активностью и выявления событий интереса.
			Выделение аномальной активности для дальнейшего анализа	Применение алгоритмов обработки естественного языка (Natural Language Processing, NLP) для извлечения сущностей и ключевых слов из контекста событий.
Оценка контекста	Анализ паттернов поведения	Идентификация нормальных паттернов	Анализ статистики поведения пользователей	Систематическое сбор и агрегация статистических данных о действиях пользователей в информационных системах организации.

			Создание профилей нормального поведения	Использование аналитических методов, включая среднюю, медианную и стандартную статистику, для создания нормативных моделей поведения пользователей.
		Выявление аномалий в поведении	Сравнение активности с нормальными паттернами	Разработка методов для выявления стандартных паттернов активности пользователей, характерных для их обычной работы.
			Поднятие тревоги при обнаружении аномалий	Внедрение алгоритмов машинного обучения, таких как метод опорных векторов или алгоритмы кластеризации, для обнаружения аномалий в статистике поведения пользователей.
	Определение контекстуальных правил	Создание правил на основе контекста	Исследование и анализ данных для определения правил	Объединение данных из различных источников, таких как журналы системных событий, данные сетевого мониторинга и журналы приложений, для более полного анализа поведения.
			Определение пороговых значений для различных параметров	Разработка методологии для формирования индивидуальных профилей активности пользователей на основе интегрированных данных.
		Применение правил к данным	Внедрение контекстуальных правил в систему мониторинга	Создание системы мониторинга, способной выявлять изменения в статистике активности пользователей, что может указывать на потенциальные угрозы.
			Анализ данных на соответствие установленным контекстным правилам	Применение методов анализа временных рядов для выявления трендов и цикличности в поведении пользователей

Таблица 5: Таблица для разделов, определяющих методологическую основу технологии контекстного анализа.

Этап	Процесс	Процедура	Действие	Методологическая основа
Сбор данных о поведении	Захват данных о действиях пользователей	Логирование активности	Установка агентов для отслеживания действий пользователей	Разработка стратегии установки агентов, включая выбор точек интеграции (например, на уровне ОС, приложений или сетевого уровня) и обеспечение совместимости с общими стандартами безопасности.
			Регистрация информации о каждом действии сотрудника	Определение области регистрации действий, включая выбор уровня детализации (например, файловые операции, запросы к базе данных, сетевая активность) и чувствительность данных.
		Сбор данных о времени использования	Захват данных о времени начала и окончания работы	Разработка механизмов для точного захвата времени начала и окончания работы пользователя с системой, включая синхронизацию с часовыми серверами и учет временных зон.
			Создание логов для анализа паттернов активности	Разработка формата логов, включая необходимую информацию о пользователях, времени событий и типах активности, для последующего анализа паттернов и выявления аномалий.
	Сегментация пользователей	Группировка пользователей по профилям	Определение основных характеристик пользователей	Исследование и определение основных характеристик пользователей, таких как должность, отдел, уровень доступа, для создания базы для группировки.
			Разделение пользователей на группы по схожести активности	Разработка алгоритмов и критериев схожести активности для эффективной группировки пользователей с учетом их поведенческих паттернов.
		Анализ схожести поведения в группах	Идентификация общих паттернов внутри групп	Разработка алгоритмов и инструментов для выявления общих паттернов поведения внутри каждой группы пользователей.

			Определение аномалий в поведении отдельных пользователей в группе	Применение методов машинного обучения для выявления аномалий в поведении отдельных пользователей в группе и определение потенциальных угроз безопасности.
Анализ поведения	Выявление аномалий в поведении	Сравнение с образцами нормального поведения	Составление профилей нормального поведения	Использование аналитических методов для создания профилей нормального поведения, учитывая сезонные и временные изменения.
			Анализ активности сравнением с установленными образцами	Применение алгоритмов сравнения для анализа текущей активности с установленными образцами нормального поведения.
		Обнаружение необычных активностей	Использование алгоритмов машинного обучения для выявления аномалий	Применение алгоритмов, таких как методы кластеризации или классификации, для обнаружения аномальных паттернов.
			Поднятие тревоги при обнаружении необычной активности	Разработка системы уведомлений и тревожных сигналов для оперативного реагирования на обнаруженные аномалии.
	Оценка риска	Присвоение рисковых оценок	Оценка аномальной активности по степени риска	Использование шкалы оценок для выражения степени риска, основанной на характеристиках каждой аномалии.
			Классификация уровней риска для принятия дальнейших мер	Разработка системы классификации уровней риска для определения необходимости дополнительных мер безопасности.
		Выявление действий, требующих внимания	Выделение конкретных действий, считающихся потенциально опасными	Определение конкретных действий, которые могут свидетельствовать о наличии угрозы безопасности, среди обнаруженных аномалий.
			Системное уведомление или блокировка активности при высоких уровнях риска	Разработка механизмов системного уведомления и автоматической блокировки активности при высоких уровнях риска для оперативного реагирования.
	Принятие мер	Автоматические реакции	Задействование автоматических сценариев реагирования на определенные события	Определение конкретных сценариев реагирования, которые могут быть автоматизированы для оперативного контроля ситуации.

			Автоматическое блокирование доступа к ресурсам при высоких уровнях риска	Разработка механизмов автоматической блокировки доступа к ресурсам при высоких уровнях риска
		Ручные реакции	Создание тикетов для ручного анализа и реагирования	Установление стандартов и процедур для создания тикетов с подробной информацией о каждой обнаруженной аномалии, требующей ручного анализа.
			Вовлечение безопасностных аналитиков для проведения дополнительного анализа	Установление процедур и критериев для вовлечения безопасностных аналитиков в случае необходимости дополнительного анализа и реагирования на сложные или неоднозначные ситуации.
	Обучение системы	Актуализация образцов нормального поведения	Использование обратной связи от аналитиков для коррекции образцов	Создание механизмов для систематического получения обратной связи от безопасностных аналитиков относительно корректности образцов нормального поведения.
			Автоматическое обновление профилей нормального поведения	Разработка системы автоматического обновления профилей нормального поведения на основе новых данных и обратной связи.
		Расширение базы данных аномалий	Добавление новых сценариев аномалий на основе новых данных	Разработка процессов и критериев для внедрения новых сценариев аномалий, выявленных в процессе мониторинга, в систему анализа поведения.
			Обучение системы распознавать новые типы аномалий	Разработка системы обучения и адаптации для обучения системы распознавать новые типы аномалий и включения их в общую базу данных.

Таблица 6: Таблица для разделов, определяющих методологическую основу технологии мониторинга и анализа поведения пользователей.

1.1.3 Построение структурно – функциональной схемы систем и средств. Исследование существующих систем, комплексов и средств, реализующих базовые технологии DLP.

Составим общую структурно – функциональную схему системы DLP.

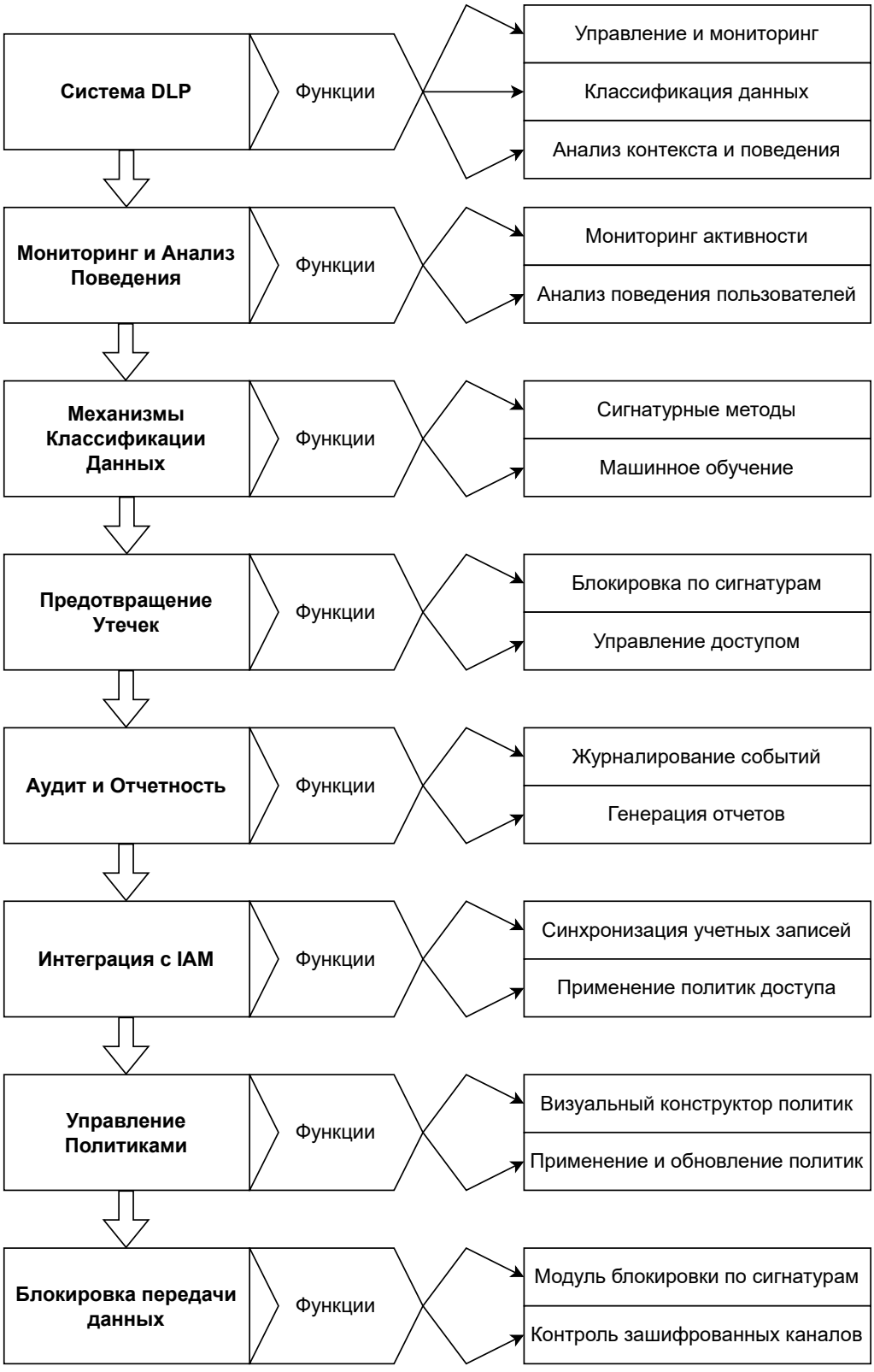

Рис. 1.1.1: Общая структурно – функциональная схема системы DLP.

Составим обзор некоторых известных систем и решений DLP, которые широко используются в отрасли.

Symantec Data Loss Prevention (DLP):	Symantec DLP предоставляет обширные возможности для обнаружения и предотвращения утечек конфиденциальных данных. Включает в себя механизмы классификации данных, контроль за передачей информации и мониторинг поведения пользователей.
McAfee Total Protection for Data Loss Prevention:	McAfee предлагает решение DLP, которое включает сигнатурные методы, анализ контекста, мониторинг активности и интеграцию с другими системами безопасности. Решение также поддерживает шифрование и управление доступом.
Forcepoint Data Loss Prevention:	Forcepoint DLP предоставляет защиту от утечек данных через контентный анализ и анализ поведения пользователей. Это решение также включает в себя инструменты классификации данных и механизмы предотвращения утечек.
Digital Guardian:	Digital Guardian предоставляет решение для управления и защиты конфиденциальных данных. Включает в себя функции контроля за передачей данных, мониторинга активности и предотвращения утечек.
Varonis Data Security Platform:	Varonis предоставляет решение для мониторинга и защиты данных, включая анализ контекста, анализ поведения пользователей и контроль доступа. Помимо DLP, предоставляет средства обеспечения безопасности данных в целом.
Symplified DLP:	Symplified DLP предоставляет решение для защиты данных с помощью методов классификации, мониторинга активности и предотвращения утечек. Имеет возможности интеграции с существующими системами безопасности.
Microsoft Azure Information Protection:	Платформа Azure Information Protection предоставляет средства классификации и шифрования данных для предотвращения утечек. Интегрируется с другими продуктами Microsoft для обеспечения полной защиты данных.

1.2. Анализ состава задач в области построения технологий DLP. Анализ предмета исследований – исследование существующих прикладных технологий DLP.

Рассмотрим три конкретных примера прикладных технологий DLP:

1. Шифрование данных:

   - *Описание:* Технология шифрования используется для защиты конфиденциальных данных при их передаче или хранении. Шифрование преобразует информацию в непонятный для посторонних вид в случае несанкционированного доступа.
   - *Пример применения:*
     Шифрование электронной почты: Использование шифрования для защиты содержимого электронных писем, чтобы предотвратить утечку конфиденциальных данных в процессе их передачи.

2. Мониторинг и защита конфиденциальной информации в облачных хранилищах:

   - *Описание:* Технологии, позволяющие мониторить и защищать конфиденциальные данные, хранящиеся в облачных сервисах. Это включает в себя контроль доступа, аудит и предотвращение утечек в облаке.
   - *Пример применения:*
     Контроль доступа к облачным файлам: Установка политик, определяющих, кто и как может получить доступ к файлам в облачных хранилищах, и мониторинг этих действий.

3. Контроль использования съемных устройств:

   - *Описание:* Технологии, ограничивающие или контролирующие использование съемных устройств, таких как USB-накопители, для предотвращения утечек данных через подобные устройства.
   - *Пример применения:*
     Блокировка USB-устройств: Установка политики, которая запрещает или ограничивает использование USB-накопителей на компьютерах в корпоративной сети с целью предотвращения копирования конфиденциальной информации.

1.2.1 Анализ структуры построения существующих прикладных технологий DLP и их составляющих (этапов, процессов, процедур, действий и т.п.).

Проведен анализ структуры прикладных технологий DLP, выявлены следующие основные этапы:

Этап	**Процесс**	**Процедура**	**Действие**
Разработка политик шифрования	Определение категорий данных	Идентификация чувствительных данных	Проведение аудита данных
			Маркировка данных в соответствии с их чувствительностью
		Классификация данных	Группировка данных по уровню чувствительности
			Установка категорий для каждой группы данных
	Разработка политик шифрования	Определение методов шифрования	Исследование современных методов шифрования
			Выбор оптимальных методов для каждой категории данных
		Установка правил применения шифрования	Определение условий, при которых применяется шифрование
			Настройка параметров шифрования
Реализация и мониторинг шифрования	Внедрение системы шифрования	Установка шифровальных средств на сервера и устройства	Проведение тестирования средств шифрования
			Развёртывание средств на всех уровнях инфраструктуры
	Мониторинг шифрованных данных	Определение метрик мониторинга	Выбор параметров для отслеживания (активность, производительность)
			Настройка системы мониторинга
		Реагирование на инциденты	Автоматическое уведомление при обнаружении нарушений
			Ручное вмешательство при необходимости

Таблица 8: Таблица для разделов, определяющих структуру технологии шифрования данных.

Этап	**Процесс**	**Процедура**	**Действие**
Интеграция с облачными сервисами	Определение облачных сервисов	Идентификация используемых облачных платформ	Анализ текущих облачных решений в организации
			Определение степени использования каждого сервиса
		Оценка рисков облачного хранения данных	Определение уровня конфиденциальности для данных в облаке
			Оценка мер безопасности облачных провайдеров
	Разработка стратегии мониторинга	Определение параметров мониторинга	Выбор критериев мониторинга (доступ, изменения, сетевая активность)
			Установка пороговых значений для оповещений
		Разработка мер безопасности в облаке	Настройка средств мониторинга в облаке
			Разработка автоматизированных реакций на обнаружение угроз
Мониторинг и адаптация стратегии	Непрерывный мониторинг облачных сред	Отслеживание активности пользователей в облаке	Мониторинг логов доступа к облачным ресурсам
			Анализ нештатных ситуаций и подозрительной активности
		Мониторинг изменений в структуре данных	Отслеживание изменений в файлах и папках облачного хранилища
			Реагирование на несанкционированные изменения
	Анализ данных и оптимизация стратегии	Сбор и агрегация данных мониторинга	Формирование отчётов по результатам мониторинга
			Анализ трендов и выявление основных угроз
		Оптимизация стратегии мониторинга	Внесение корректив в параметры мониторинга
			Повышение эффективности мер безопасности в зависимости от выявленных угроз

Таблица 9: Таблица для разделов, определяющих структуру технологии мониторинга и защиты конфиденциальной информации в облачных хранилищах.

Этап	**Процесс**	**Процедура**	**Действие**
Планирование и настройка контроля	Определение политик использования съемных устройств	Классификация съемных устройств	Определение различных типов съемных устройств (USB, внешние HDD)
			Выделение уровней разрешений для каждого типа устройств
		Установка правил доступа	Определение пользовательских групп и их прав доступа
			Настройка ограничений на основе времени, местоположения и типа устройства
	Развёртывание средств контроля	Выбор средств контроля	Исследование и выбор специализированных утилит для контроля
			Интеграция выбранных средств в существующую инфраструктуру
		Настройка оповещений и журналирования	Установка механизмов оповещения о несанкционированных попытках
			Конфигурирование системы журналирования для анализа инцидентов
Мониторинг и реагирование на события	Непрерывный мониторинг съемных устройств	Отслеживание подключения и использования устройств	Мониторинг логов подключения устройств
			Выявление несанкционированных действий с устройствами
		Мониторинг передачи данных на съемных устройствах	Контроль записи и копирования данных на съемные устройства
			Реагирование на попытки утечки конфиденциальной информации

	Реагирование на инциденты	Автоматическое реагирование на нарушения	Запрет доступа при обнаружении несанкционированного подключения
			Отправка уведомлений администратору о нарушениях
		Ручное вмешательство и анализ	Проверка ложных срабатываний и ложных событий
			Проведение дополнительного анализа в случае неясных инцидентов

Таблица 10: Таблица для разделов, определяющих структуру технологии контроля использования съемных устройств.

1.2.2 Исследование теоретических аспектов построения прикладных технологий DLP, определение сценариев применения теоретической основы построения существующих прикладных технологий.

Теоретические аспекты построения прикладных технологий DLP:

1. Шифрование данных:

   - *Основы шифрования:* Рассматриваются принципы симметричного и асимметричного шифрования, методы генерации ключей, и выбор подходящих алгоритмов для обеспечения конфиденциальности данных.
   - *Управление ключами:* Теоретические основы управления ключами, включая генерацию, обмен, хранение и ротацию ключей для обеспечения безопасности шифрованных данных.

2. Мониторинг и защита конфиденциальной информации в облачных хранилищах:

   - *Принципы обнаружения угроз:* Разбор методов обнаружения угроз, включая мониторинг сетевой активности, анализ пользовательского поведения и использование средств машинного обучения.
   - *Контроль доступа в облаке:* Теоретическая основа построения стратегий контроля доступа, включая определение ролей, настройку правил доступа и механизмы аудита.

3. Контроль использования съемных устройств:

   - *Политики использования устройств:* Рассмотрение методов классификации съемных устройств, установка политик доступа, и определение сценариев блокировки и разрешения использования устройств.
   - *Механизмы предотвращения утечки данных:* Теоретические основы механизмов контроля передачи данных на съемных устройствах, включая блокировку и мониторинг записи информации.

1.2.3 Построение структурно – функциональной схемы и Информационно – алгоритмической модели систем и средств. Исследование существующих систем, комплексов и средств, реализующих прикладные технологии DLP.

- Технология обнаружения угроз в электронной почте:

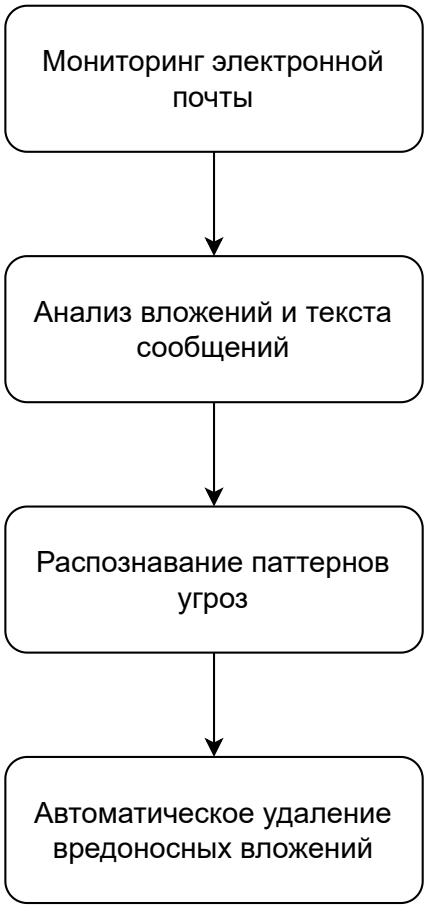

Рис. 1.2.2: Структурно – функциональная схема технологии обнаружения угроз в электронной почте.

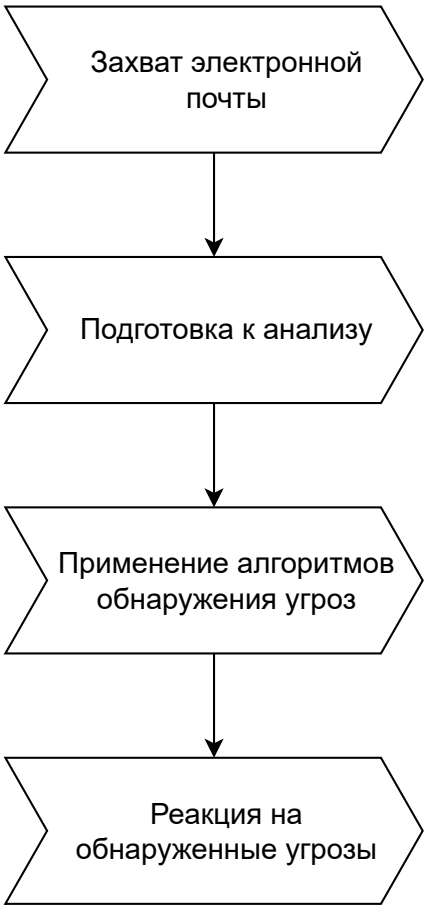

Рис. 1.2.3: Информационно – алгоритмическая модель технологии обнаружения угроз в электронной почте.

- Технология контроля утечек через внешние устройства:

Рис. 1.2.4: Структурно – функциональная схема технологии контроля утечек через внешние устройства.

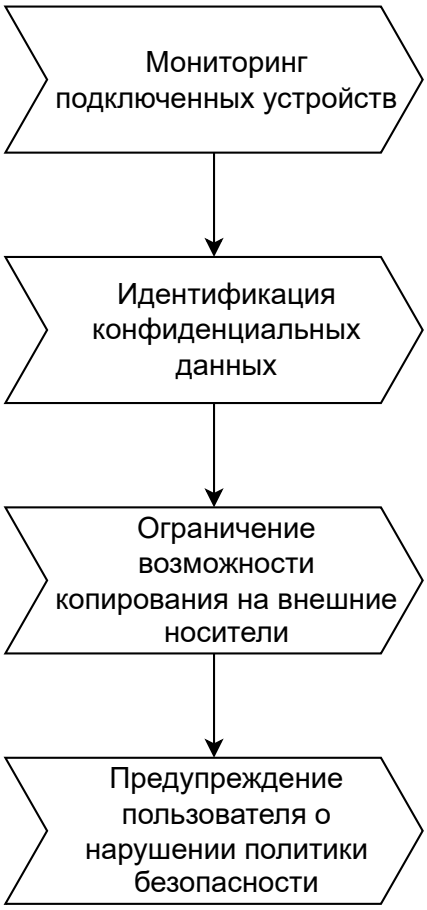

Рис. 1.2.5: Информационно – алгоритмическая модель технологии контроля утечек через внешние устройства.

- Технология мониторинга файловых хранилищ:

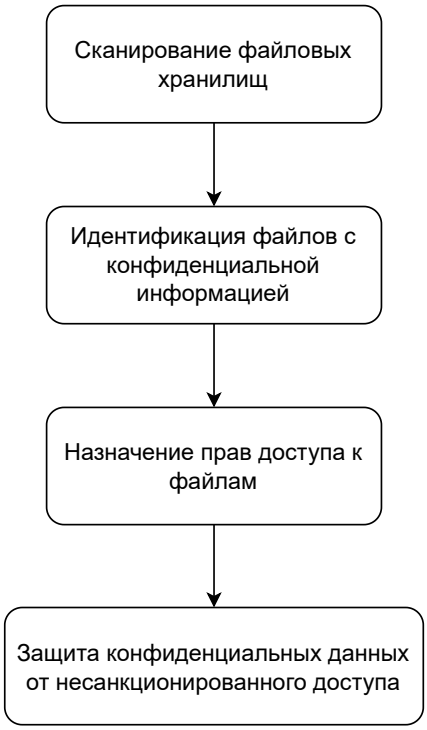

Рис. 1.2.6: Структурно – функциональная схема технологии мониторинга файловых хранилищ.

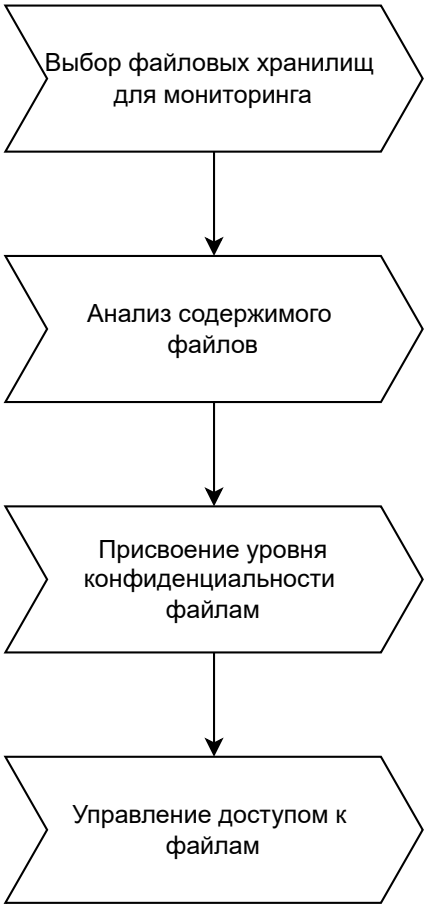

Рис. 1.2.7: Информационно – алгоритмическая модель технологии мониторинга файловых хранилищ.

2. Анализ ограничений существующих прикладных технологий DLP, проведение их классификации. Формирование требований по разработке современной технологии DLP, их классификация и обоснование.

2.1. Классификация ограничений существующих технологий DLP:

1. Технические ограничения:

   - *Проблемы совместимости:* Некоторые системы DLP могут сталкиваться с проблемами совместимости с определенными операционными системами или приложениями.
   - *Ограниченные возможности анализа:* Некоторые технологии DLP могут неэффективно обнаруживать и анализировать новые методы утечек данных.

2. Ограничения в области производительности:

   - *Замедление сетевого трафика:* Использование технологий DLP может вызывать замедление сетевого трафика, особенно в случае обширного мониторинга и анализа.

2.2. Формирование требований по разработке современной технологии DLP, их классификация и обоснование:

1. Требования к производительности:

   - *Минимальное воздействие на сетевой трафик:* Разработка технологии DLP с минимальным влиянием на производительность сети.

2. Требования к точности обнаружения:

   - *Эффективное обнаружение новых методов утечек:* Разработка алгоритмов, способных эффективно обнаруживать новые методы утечек данных.

3. Требования к совместимости:

   - *Максимальная совместимость с различными ОС и приложениями:* Разработка технологии, которая может эффективно работать на различных платформах.

3. Разработка методических рекомендаций по построению современной технологии DLP.

3.1. Выбор структуры построения современной технологии DLP

Исходя из анализа существующих технологий и их ограничений, мне кажется наиболее оптимальным решением – выбрать модульную структуру, где каждый модуль отвечает за определенный функционал. На мой взляд, модель многоуровневой защиты должна включать следующие ключевые компоненты:

Рис. 3.1.8: Ключевые компоненты модели многоуровневой защиты.

3.2. Определение методических, алгоритмических и технологических решений в области построения этапов, процессов, процедур и т.п. современной технологии DLP, а также формирование сценариев применения методологической основы построения современной прикладной технологии и реализующей ее системы.

1. Уровень мониторинга:
   - *Этап*: Активный мониторинг сетевого трафика
     - *Процесс*: Захват пакетов данных на сетевом уровне.
     - *Процедура*: Фильтрация трафика для анализа целевых данных.

- *Действие*: Определение подозрительной активности в сети.

- *Этап*: Анализ активности пользователей
  - *Процесс*: Мониторинг действий пользователей.
  - *Процедура*: Идентификация аномалий в поведении.
  - *Действие*: Предупреждение администратора при обнаружении необычной активности.

2. Уровень обнаружения и предотвращения:

   - *Этап*: Обнаружение угроз и аномалий
     - *Процесс*: Анализ данных на предмет угроз.
     - *Процедура*: Применение алгоритмов обнаружения угроз.
     - *Действие*: Автоматическое срабатывание предупреждений при обнаружении угроз.
   - *Этап*: Применение политик безопасности для блокировки угроз
     - *Процесс*: Принятие решений на основе политик безопасности.
     - *Процедура*: Автоматическая блокировка доступа при обнаружении угрозы.
     - *Действие*: Изоляция угрозы для предотвращения дальнейшего распространения.

3. Уровень реагирования:

   - *Этап*: Уведомление администраторов о событиях
     - *Процесс*: Формирование уведомлений по приоритету.
     - *Процедура*: Отправка уведомлений на заранее определенные каналы связи.
     - *Действие*: Быстрое реагирование на критические события.
   - *Этап*: Логирование и анализ инцидентов
     - *Процесс*: Запись сведений о произошедших инцидентах.
     - *Процедура*: Анализ логов для выявления причин и последствий инцидентов.
     - *Действие*: Совершенствование политик безопасности на основе опыта прошлых событий.

3.3. Определение порядка использования методических рекомендаций по построению технологии и системы DLP:

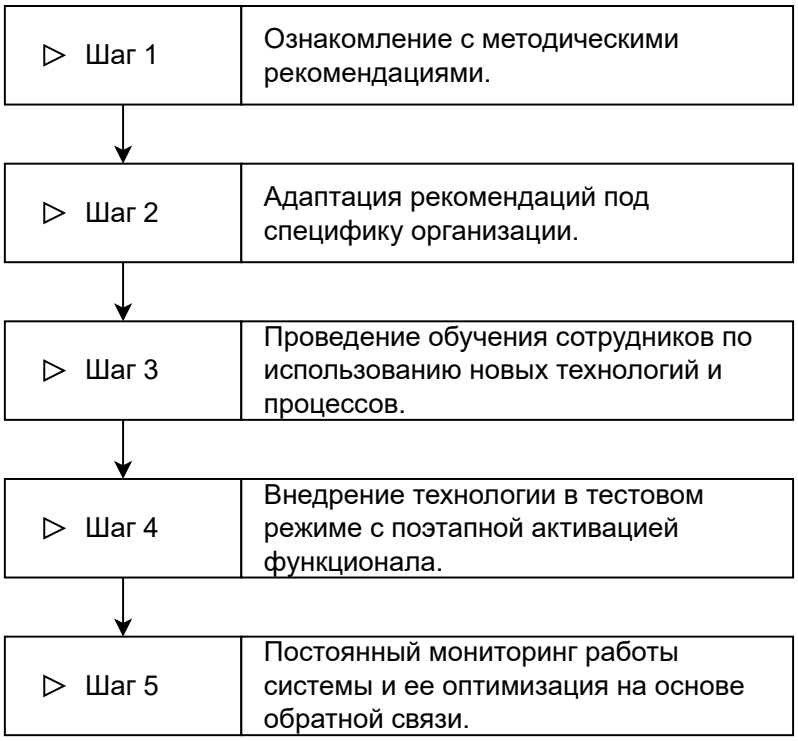

Рис. 3.3.9: Порядок использования методических рекомендаций по построению технологии и системы DLP.

4. Выбор архитектуры построения системы DLP

4.1. Построение структурно – функциональной схемы

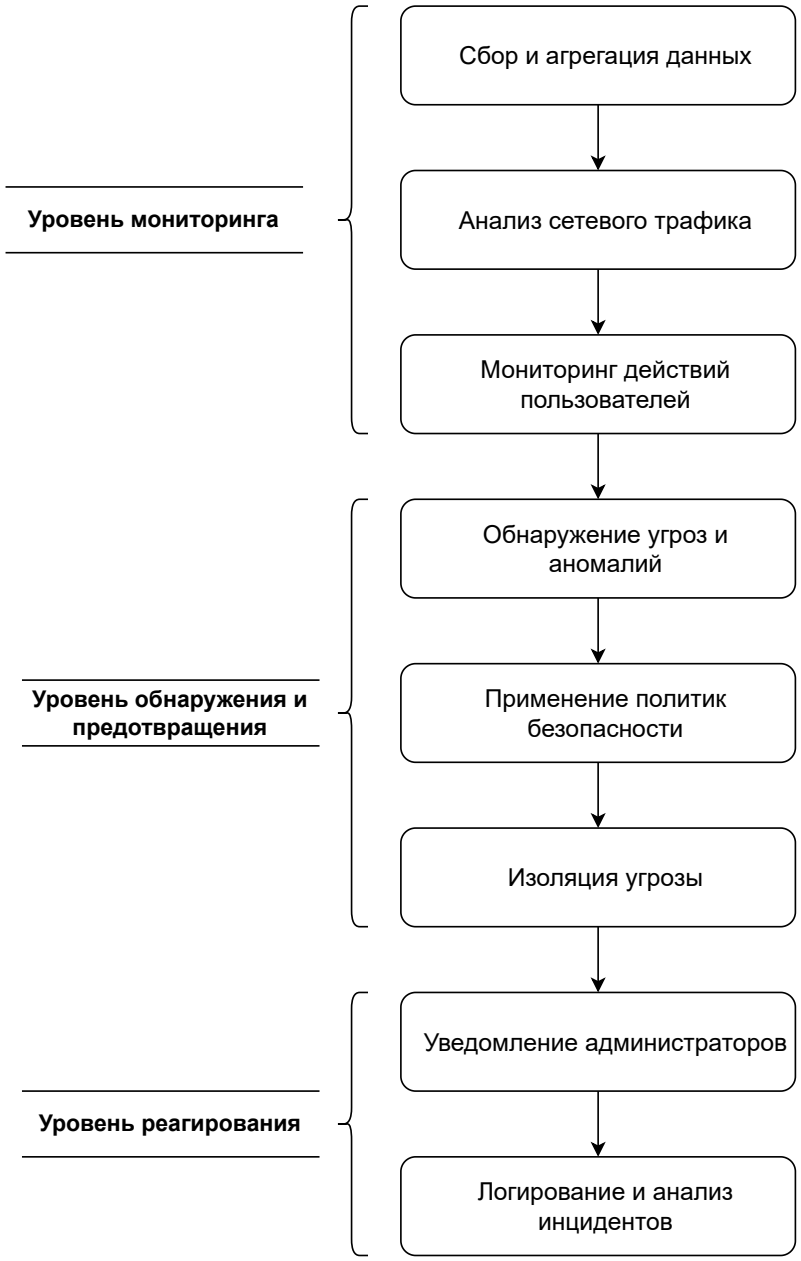

Рис. 4.1.10: Структурно – функциональная схема DLP.

4.2. Формирование Информационно – алгоритмической модели

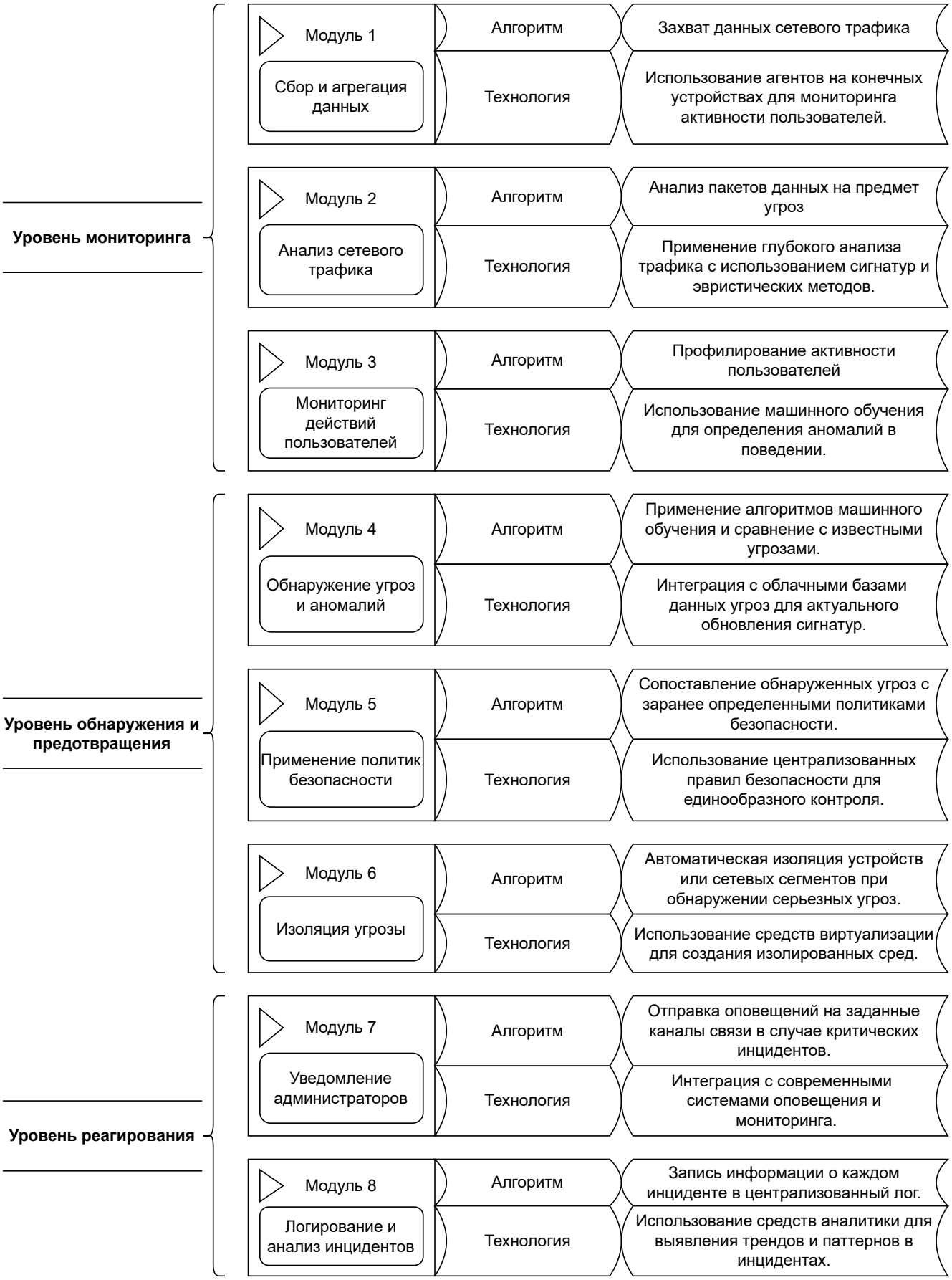

Рис. 4.2.11: Информационно – алгоритмическая модель DLP.

5. Определение перспективных направлений исследований в данной предметной области

В рамках перспективных направлений исследований в области DLP технологий я выделила:

Развитие алгоритмов машинного обучения:	Исследование новых методов обучения моделей на основе поведенческих анализов пользователей и сетевого трафика для повышения точности обнаружения угроз.
Улучшение анализа контента:	Исследование и внедрение продвинутых алгоритмов анализа контента для более точной идентификации конфиденциальной информации в различных типах данных.
Интеграция с технологией блокчейн:	Исследование возможности применения технологии блокчейн для обеспечения более надежной системы хранения логов и обеспечения целостности данных.
Расширение возможностей анализа угроз:	Разработка интеграции с искусственным интеллектом для автоматического определения и анализа новых видов угроз.

Эти направления исследований направлены на повышение эффективности DLP систем и обеспечение их адаптации к постоянно меняющейся угрозовой среде.

6. Список источников и литературы

1. «Информационная безопасность в корпоративных сетях» – Карасёв П.А.
2. «Анализ проблем информационной безопасности в корпоративных сетях» – Табилова А.З., Коннов А.Л.
3. «Защита информации»: учебник для вузов – В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе
4. «Безопасность и управление доступом в информационных системах»: учебное пособие – А. В. Васильков, И. А. Васильков.
5. https://searchinform.ru/products/kib/
6. «Информационная безопасность в корпоративных системах: практические аспекты» – Сергей Симонов для https://www.itweek.ru
7. "Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft"by Eric Cole.
8. "Data Protection and Information Lifecycle Management"by Tom Petrocelli.
9. "Enterprise Data Center Design and Methodology"by Rob Snevely.
10. "Network Security Essentials: Applications and Standards"by William Stallings.
11. "Security Engineering: A Guide to Building Dependable Distributed Systems"by Ross J. Anderson.