пикнометре быстро доводят до метки, отбирая излишек воды пипеткой, капилляром или свернутой полоской чистой не волокнистой фильтровальной бумаги. Пикнометр снова закрывают пробкой, термостатируют еще 10 мин, проверяют соответствие уровня жидкости метке, протирают снаружи досуха чистой мягкой тканью или фильтровальной бумагой и оставляют на 10 мин за стеклом коробки аналитических весов, а затем снова взвешивают. После этого пикнометр освобождают от воды, затем удаляют остатки эфира продуванием воздуха, заполняют пикнометр испытуемой жидкостью и проводят те же операции, что и с дистиллированной водой. Измерим относительную плотность этилового спирта. Все результаты измерений представлены в таблице (табл. 1).

Таблица 1 – Расчет неопределенности

X_I	x_1	0,5 R_i	k	$u(X_i)$	c_i	$u_i(Y)$
m_1	4,85	$1{,}0\cdot10^{-2}$	2	$5\cdot10^{-3}$	–0,103533	$-5{,}18\cdot10^{-4}$
m_2	6,84	$1{,}0\cdot10^{-2}$	2	$5\cdot10^{-3}$	–0,398980	$-1{,}99\cdot10^{-3}$
m_3	6,43	$1{,}0\cdot10^{-2}$	2	$5\cdot10^{-3}$	0,502512	$2{,}51\cdot10^{-3}$
d	0,79397	–	–	–	–	0,003245

$U(d) = 2\,u(d) = 0{,}00649 = 0{,}007$, $d = 0{,}794 \pm 0{,}007$

Литература

1. Плакс, Д. П. Петрофизика: практикум для студентов специальности 1-51 02 01 «Разработка месторождений полезных ископаемых» / Д. П. Плакс. – Минск: БНТУ, 2021. – 84 с.
2. Arendarski J. Niepewność pomiarów. – Oficyna Wydawnicza Politechniki Warszawskiej, 2003.

УДК 004.056.5

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В DLP-СИСТЕМАХ

Студент гр. ИУ8-122 Мартиросян В. В.
Кандидат техн. наук, доцент Медведев Н. В.
Московский государственный технический университет им. Н. Э. Баумана, Москва, Россия

DLP расшифровывается как «Предотвращение потери данных». Это набор инструментов и технологий, которые помогают организациям предотвратить потерю, кражу или неправомерное использование конфиденциальных данных путем мониторинга и контроля доступа к конфиденциальной информации и шифрования данных для предотвращения несанкционированного доступа [1].

Некоторые популярные решения для предотвращения потери данных могут различаться по функциям, цене и уровню сложности, поэтому важно исследовать и сравнивать варианты, чтобы найти лучшее решение для конкретных потребностей вашей организации.

Основные способы контроля трафика по DLP. Решения для предотвращения потери данных (DLP) обычно контролируют сетевой трафик несколькими способами, в том числе:

Проверка содержимого. Решение DLP сканирует весь входящий и исходящий сетевой трафик для выявления конфиденциальных данных, таких как номера кредитных карт, номера социального страхования и конфиденциальные документы.

Блокировка на основе правил. На основе предопределенных правил решение DLP может автоматически блокировать или разрешать определенные типы трафика в зависимости от их содержимого. Например, он может блокировать отправку электронных писем, содержащих конфиденциальную информацию, за пределы организации.

Шифрование: решения DLP могут шифровать конфиденциальные данные при передаче, чтобы предотвратить несанкционированный доступ, даже если данные перехвачены.

Аутентификация и контроль доступа. Решения DLP могут применять политики аутентификации и контроля доступа, чтобы предотвратить доступ неавторизованных пользователей к конфиденциальным данным.

Отчетность и аудит. Решения DLP создают отчеты и журналы, в которых отображается весь заблокированный или разрешенный трафик, обеспечивая прозрачность использования

данных и помогая организациям выявлять и устранять потенциальные угрозы безопасности.

Это некоторые из основных способов, с помощью которых решения DLP контролируют сетевой трафик для предотвращения потери данных. Конкретные возможности и методы, используемые различными решениями DLP, могут различаться, но обычно они направлены на обеспечение комплексного подхода к защите данных.

Использование ИИ в DLP.Искусственный интеллект (ИИ) становится все более распространенным в области предотвращения потери данных (DLP) и используется несколькими способами для расширения возможностей решений DLP [2]. Вот некоторые из основных способов использования ИИ в DLP:

Классификация контента. Алгоритмы ИИ можно обучить автоматически классифицировать конфиденциальные данные и идентифицировать их в сетевом трафике. Это можно сделать с помощью таких методов, как обработка естественного языка (NLP) и машинное обучение (ML).

Обнаружение угроз: алгоритмы искусственного интеллекта можно использовать для обнаружения потенциальных угроз, таких как вредоносное ПО, фишинговые атаки и попытки кражи данных. Это помогает организациям обнаруживать инциденты безопасности в режиме реального времени и быстро реагировать на них.

Обнаружение аномалий. Алгоритмы ИИ можно использовать для обнаружения необычных моделей поведения в сетевом трафике, таких как необычные передачи данных или попытки доступа. Это может помочь организациям обнаруживать потенциальные утечки данных и другие инциденты безопасности.

Применение политик: алгоритмы искусственного интеллекта можно использовать для автоматического применения политик DLP и предотвращения утечек данных. Например, решение DLP можно настроить на автоматическую блокировку электронных писем, содержащих конфиденциальную информацию, если они отправляются за пределы организации.

Это некоторые из основных способов использования ИИ для расширения возможностей решений DLP и помощи организациям в лучшей защите конфиденциальных данных. Поскольку технологии искусственного интеллекта продолжают развиваться, вполне вероятно, что в будущем они будут играть еще большую роль в области DLP.

Интеграция ИИ с DLP с технической точки зрения. С технической точки зрения ИИ можно интегрировать с защитой от потери данных (DLP) несколькими способами, в том числе:

Интеграция API: решения DLP могут интегрироваться с платформами ИИ с помощью API, что позволяет двум системам обмениваться данными и инициировать действия. Например, решение DLP может использовать API для отправки данных на платформу ИИ для анализа и получения результатов обратно в режиме реального времени.

Модели машинного обучения. Решения DLP могут интегрировать модели машинного обучения для классификации конфиденциальных данных и обнаружения угроз. Модели можно обучать на больших наборах данных, а затем развертывать в решении DLP для выполнения анализа сетевого трафика в реальном времени.

Интеграция озера данных: решения DLP могут интегрироваться с озером данных, централизованным хранилищем для хранения больших объемов данных, чтобы предоставить алгоритмам ИИ необходимые данные для выполнения их анализа.

Облачная интеграция: решения DLP также можно интегрировать с облачными платформами искусственного интеллекта, что позволяет организациям использовать возможности искусственного интеллекта без необходимости в специализированном оборудовании или опыте.

Вот некоторые из способов интеграции ИИ с DLP с технической точки зрения. Конкретный метод интеграции будет зависеть от конкретных требований организации и возможностей используемых решений DLP и AI. Однако цель интеграции – предоставить DLP-решению интеллектуальные возможности и возможности, необходимые для лучшей защиты конфиденциальных данных.

Интеграция ИИ с DLP по API. Интеграция ИИ с предотвращением потери данных (DLP) с помощью API может быть выполнена в несколько этапов:

Выберите платформу ИИ. Выберите платформу ИИ, которая предоставляет API для анализа данных, например Google Cloud AI, Amazon Web Services (AWS) AI или Microsoft Azure AI.

Определите интерфейс API: определите интерфейс API между платформой ИИ и решением DLP, включая формат данных и методы связи.

Создайте ключ API: создайте ключ API или токен доступа, который позволит решению DLP получить доступ к API платформы ИИ.

Внедрение вызовов API. Внедрение вызовов API в решении DLP для отправки данных на платформу ИИ для анализа и получения результатов обратно. Это можно сделать с помощью таких языков программирования, как Python или Java.

Протестируйте интеграцию. Протестируйте интеграцию между решением DLP и платформой ИИ, чтобы убедиться, что вызовы API работают правильно, а данные анализируются должным образом.

Разверните интеграцию: разверните интеграцию в производственной среде, отслеживайте ее и вносите необходимые коррективы.

Это общие шаги по интеграции ИИ с DLP с помощью API. Конкретная реализация будет зависеть от конкретных требований организации и возможностей используемого решения DLP и платформы ИИ. Однако цель интеграции – предоставить DLP-решению интеллектуальные возможности и возможности, необходимые для лучшей защиты конфиденциальных данных.

ИИ в постановке математической задачи использования DLP. Использование искусственного интеллекта (ИИ) для предотвращения потери данных (DLP) можно математически сформулировать как задачу оптимизации. Цель задачи оптимизации – найти оптимальное решение для защиты конфиденциальных данных при минимизации влияния на поток информации внутри организации.

Обычный подход к постановке этой проблемы состоит в том, чтобы определить набор ограничений, представляющих политики защиты конфиденциальных данных, а затем найти оптимальное решение, удовлетворяющее этим ограничениям. Например, ограничения могут включать правила для обнаружения и блокировки конфиденциальных данных в сообщениях электронной почты или для управления доступом к конфиденциальным данным, хранящимся на серверах.

После определения ограничений задачу оптимизации можно сформулировать как задачу линейного программирования, целью которой является минимизация риска потери данных при максимальном увеличении потока информации внутри организации. Затем задача линейного программирования может быть решена с использованием алгоритмов оптимизации, таких как симплексный алгоритм, метод внутренней точки или метод ветвей и границ.

В дополнение к линейному программированию для решения проблемы ИИ в DLP также можно использовать другие методы оптимизации, такие как деревья решений, машины опорных векторов и нейронные сети. Эти методы можно использовать для выполнения комплексного анализа данных и прогнозирования вероятности утечки данных, позволяя решению DLP принимать обоснованные решения о том, как защитить конфиденциальные данные.

Математическая формулировка ИИ в DLP может помочь организациям лучше понять компромиссы, связанные с защитой конфиденциальных данных, и принимать более обоснованные решения о политиках и технологиях, которые они используют для защиты своих данных.

Задание математических зависимостей. Использование ИИ в предотвращении потери данных (DLP) может включать в себя различные математические формулировки, включая линейное программирование, деревья решений, машины опорных векторов и нейронные сети. Конкретные используемые математические формулы будут зависеть от конкретных требований решения DLP и типа используемых методов искусственного интеллекта.

Например, если в решении DLP используется подход линейного программирования, задачу оптимизации можно сформулировать в виде линейной программы, целью которой является минимизация риска потери данных при максимальном увеличении потока информации внутри организации. Линейная программа может быть записана в матричной форме как:

свести к минимуму $c'x$
при условии $Ax <= b$
$x >= 0$,

где c – вектор коэффициентов, представляющих затраты, связанные с защитой конфиденциальных данных, x – вектор переменных, представляющих решения, принятые решением DLP,

A – матрица ограничений, представляющая политики защиты конфиденциальных данных, a, b – вектор значений правой части.

Если решение DLP использует деревья решений, математическая формулировка может включать создание деревьев решений на основе исторических данных и использование деревьев для прогнозирования вероятности утечки данных. Деревья решений могут быть записаны в виде серии правил принятия решений, представленных в виде утверждений «если-то», которые определяют условия, при которых данные должны быть защищены.

В случае машин опорных векторов математическая формулировка может включать использование набора обучающих данных для создания границы, которая разделяет данные на разные классы. Затем эту границу можно использовать для классификации новых данных и прогнозирования вероятности утечки данных. Математическая формула для машины опорных векторов может быть записана как:

$$f(x) = w'x + b\ . \qquad (1)$$

где w – вектор весов, представляющих важность каждого признака, x – вектор признаков, представляющих анализируемые данные, a, b – член смещения.

Наконец, если решение DLP использует нейронные сети, математическая формулировка может включать создание сети искусственных нейронов, которые можно обучить делать прогнозы о вероятности утечки данных. Математические формулы для нейронных сетей могут быть сложными и включать большое количество переменных и параметров и обычно выражаются с использованием матричной алгебры и векторного исчисления.

Это всего лишь несколько примеров математических формулировок, которые можно использовать в контексте ИИ в DLP. Конкретные используемые математические формулы будут зависеть от конкретных требований решения DLP и типа используемых методов искусственного интеллекта.

Литература

1. What is Data Loss Prevention [Электронный ресурс]. – Режим доступа: https://www.fortinet.com/resources/cyberglossary/dlp. – Дата доступа: 14.02.2023.

2. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В DLP [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/resources/blog/iskustvenniy-intellekt-v-dlp-i-kak-ne-dat-sebya-obmanut. – Дата доступа: 25.02.2023.

УДК 519.718.2

АВТОМАТИЗИРОВАННАЯ БАЗА ЗНАНИЙ СОСТОЯНИЙ СИСТЕМ АВТОМАТИКИ ЭНЕРГЕТИЧЕСКОГО ОБОРУДОВАНИЯ АЭС

Магистрант гр. 1-438001 Мацук А. С.
Кандидат техн. наук, доцент Савкова Е. Н.
Белорусский национальный технический университет, Минск, Беларусь

Системы автоматики энергетических предприятий направлены на обеспечение эффективного выполнения рабочих процессов и их безопасности. Несмотря на многообразие выполняемых функций, данные системы состоят из однотипных простейших узлов, которые подразделяются на воспринимающие, преобразующие, исполнительные, задающие и корректирующие органы, элементы сложения и вычитания сигналов.

Неисправности в системе автоматики сводятся к ограниченному числу элементарных событий: 1) обрывы цепей; 2) короткое замыкание; 3) нарушение функции контактов; 4) неисправность электрических элементов; 5) неисправность механической части аппаратуры. В некоторых случаях при отказе элемента системы автоматики возможно изменение состояния объекта на неработоспособное, нерабочее, предельное или опасное.

Таким образом, создание базы знаний опасных событий и их потенциальных причин позволит повысить надежность систем автоматики. Удобным инструментом является реестр рисков, представляющий собой гибкую, модульную автоматизированную систему, включающую базы данных взаимосвязанных энергетических процессов, опасных событий, последствий, ущерба и вероятностей возникновения с функциями комплексирования и документирования.