УДК 004.056 EDN PGAMXN
https://www.doi.org/10.47813/dnit-III.2024.11.3005

Проблемы и перспективы применения искусственного интеллекта в DLP-системах

А.С. Александров*

Аккредитованное образовательное частное учреждение высшего образования
«Московский финансово-юридический университет МФЮА»
АОЧУ ВО МФЮА, ул. Введенского, 1А, Москва, 117342, Россия

*E-mail: 29395356@s.mfua.ru, alexibb1312@yandex.ru

Аннотация. Доклад посвящён краткому рассмотрению истории внедрения искусственного интеллекта в DLP-решениях. Показаны отдельные наиболее значительные преимущества, которые даёт внедрение искусственного интеллекта на современном этапе развития DLP-систем. Вместе с тем, наличие определённых проблем на этапах жизненного цикла DLP-систем с включёнными механизмами искусственного интеллекта может вызвать недоверие со стороны заказчиков, а также накладывает определённые обязанности на вендоров. Сделаны выводы по условиям и факторам успешного развития механизмов искусственного интеллекта в отечественных DLP-решениях.

Ключевые слова: предотвращение утечки данных, DLP-система, программное обеспечение, ИИ.

Problems and prospects of artificial intelligence application in DLP-systems

A.S. Aleksandrov*

Accredited private educational institution of higher education "Moscow University of Finance and Law MFUA", 1A Vvedenskogo str., Moscow, 117342, Russia

*E-mail: 29395356@s.mfua.ru, alexibb1312@yandex.ru

Abstract. The report focuses on brief review of the history of the introduction of artificial intelligence in DLP solutions. Some of the most significant advantages that the introduction of artificial intelligence provides at the current stage of development of DLP systems are shown. At the same time, the presence of certain problems at the stages of the life cycle of DLP systems with artificial intelligence mechanisms enabled can cause distrust on the part of customers, and also imposes certain responsibilities on vendors. Conclusions are drawn on the conditions and factors of the successful development of artificial intelligence mechanisms in domestic DLP solutions.

Keywords: data leakage prevention, DLP system, software, AI.

1. Введение

DLP-системы с недавнего времени стали неотъемлемой частью современного процесса обеспечения корпоративной информационной безопасности, а искусственный интеллект (далее - ИИ), в свою очередь, становится в настоящий момент неотъемлемой частью этих систем. ИИ давно прижился и качественным образом изменил многие отрасли промышленности и сферы деятельности, такие как банковская или биржевая аналитика, медицина, а в настоящий момент, его применение растёт и в сфере защиты информации.

Основные надежды возлагаются на способность ИИ улучшить возможности DLP-систем по обнаружению и реагированию на угрозы, решая такие вспомогательные задачи, как анализ больших объемов данных, распознавание образов и классификация данных. Он также может быть использован для обучения системы новым паттернам поведения, которые могут указывать на возможные угрозы утечки информации.

В качестве одного из примеров использования ИИ в DLP-системах можно привести анализ контента. При помощи хорошо обученного ИИ можно анализировать содержимое электронных писем и других документов на предмет наличия конфиденциальной информации. Это позволяет системе быстро обнаруживать утечки и, в случае определённой настройки, предпринимать соответствующие действия. Другим примером использования ИИ в DLP-системах является обнаружение аномального поведения пользователя информационной системы. ИИ может использовать алгоритмы машинного обучения для определения того, когда пользователь ведет себя необычно, например, пытается скопировать конфиденциальную информацию на внешний носитель.

Вместе с тем, сам процесс внедрения ИИ в современные DLP-решения за несколько лет прошёл несколько стадий: от энтузиазма к внедрению со стороны вендоров до недоверия и критики со стороны заказчиков, и наоборот - от сомнений и разочарования в эффективности применения до постепенного получения преимуществ в использовании ИИ в рутинных и требующих значительных временных и человеческих ресурсов операций, что открыло ряд новых возможностей для DLP-решений по обнаружению и реагированию на инциденты и угрозы.

Затрагивая тему развития отечественных DLP-решений, стоит упомянуть также наличие и альтернативной концепции развития DLP-решений, которая призвана

составить конкуренцию на рынке для текущей [4, 5]. Однако, данная альтернативная концепция проходит апробацию, в то время как текущая концепция с момента внедрения ИИ уже утратила ряд своих недостатков.

2. Постановка задачи

В данной статье предлагается кратко рассмотреть историю внедрения ИИ в DLP-решения, преимущества, которые даёт внедрение ИИ, текущие проблемы использования ИИ в DLP-решениях, а также на основании этих данных сделать прогноз развития ИИ в сфере информационной безопасности.

3. История внедрения ИИ в DLP-решения

На протяжении десяти прошедших лет разработчики DLP-решений активно внедряют в свои программные продукты механизмы ИИ. Одним из основных сопутствующих факторов внедрения данных механизмов совершенно справедливо является появление достаточных вычислительных мощностей в информационных системах.

Изначально на волне энтузиазма о применении ИИ в информационной безопасности начали говорить все участники рынка, представляя преимущества от его применения как новую ступень развития средств защиты информации. Однако, ИИ на своём раннем этапе не являлся достаточно развитой технологией, что мешало вывести решения на его основе, которые тогда предлагались в качестве прототипа, на рынок технологий информационной безопасности уже в составе готового продукта. Указанное обстоятельство, во многом, привело к нарастанию недоверия заказчиков к данной технологии [1, 2, 6].

Первые решения на основе ИИ формально использовали нейронные сети и машинное обучение (далее - ML), однако технологии были освоены на недостаточно качественном уровне, отличались сложностями в использовании, а также дороговизной сопровождения. Это, прежде всего, было обусловлено тем, что технология ИИ требует много различных компетенций и времени, что, в конечном счёте, создавало негативный опыт у заказчиков.

Недоверие к ИИ в средствах защиты информации существует и сейчас. Однако конкуренция на рынке DLP-решений позволила укрепить позиции ИИ в таких задачах, как автоматическая генерация лингвистических словарей, распознавание изображений,

классификация документов, выявление аномального поведения сотрудников, автоматизация процесса обнаружения защищаемых данных в компании, о которых будет подробно указано при описании преимуществ применения ИИ [1, 2].

4. Преимущества внедрения ИИ для DLP-систем

Сам ИИ по определению – это выполнение машинами тех процессов, которые ассоциируются с когнитивными способностями человека [3].

В данный момент ИИ в DLP-решениях занят распознаванием образов (скриншотов, изображений и документов, содержащих изображения) при помощи механизмов машинного зрения: в потоке трафика обнаруживается графическая информация, которая может представлять собой информацию ограниченного распространения.

Помимо этого, ИИ применяется для решения задач работы в области «Big data». Как показывает практика, доля неразмеченных серых событий может достигать до 80% от всего заблокированного трафика. Это связано на прямую с тем, что описать известные документы и события при помощи политик информационной безопасности в ручном режиме в существующих DLP-решениях не представляется возможным, а разбор подобных неразмеченных событий представляет собой трудоёмкую задачу. В связи с этим, на решение подобного рода задач ориентировано применение ИИ в настоящий момент. Таким образом, ИИ в DLP-решениях используются также для разметки и классификации серых неразмеченных данных [1].

Равнозначная по важности задача - автоматическая генерация лингвистических словарей. При помощи ИИ она работает по принципу анализа примеров документов или первичной документации, что позволяет значительно ускорить генерацию готового лингвистического словаря с десятками тысяч терминов.

Следующим важным вариантом применения искусственного интеллекта является поиск черновиков и других редакций конфиденциальных документов, а также составления перечня лиц, работавшим над созданием и редактированием этих документов. Для этого вводится процедура отслеживания редакции документов и лиц, которые с ним работали. Она происходит предварительно, не в момент пересечения документом периметра контролируемой зоны ИС [1]. Стоит заметить, что описанное решение в указанном исполнении довольно близко пересекается с идеями

альтернативной концепции развития DLP-систем, однако существует ряд различий, о которых пойдёт речь описании проблем использования ИИ [4, 5].

5. Текущие проблемы использования ИИ в DLP-решениях

Развитие технологий ИИ в информационной безопасности достаточно наукоемкий и дорогостоящий процесс, который несомненно требует привлечения специалистов с опытом разработки и внедрения в области «Data science» и лингвистике. Более того, технологии, созданные на базе ИИ и ML, требуют больше испытаний и этапов тестирования (как на этапе разработки, так и на этапе внедрения), чем какие-либо предопределённые (детерминированные) алгоритмы. Только после прохождения всего пути испытаний и тестирования можно внедрять технологию на инфраструктуре (информационной системе) заказчика [3].

К основным проблемам использования ИИ на текущем этапе их развития можно отнести следующие:

- требовательность ИИ к качеству исходных данных;
- проблема обеспечения безопасности модели данных;
- контроль за исключением подмены ценностных установок и критериев при обучении модели данных;
- проблема интерпретации результатов и обеспечения валидации корректности принимаемых решений, отображения результатов анализа и причин реагирования на те или иные события;
- частое отсутствие собственных исследований в области ИИ у разработчиков средств обеспечения информационной безопасности с механизмами ИИ;
- требование к обязательному наличию инструментов для обучения модели, которые подойдут под ту или иную специфику работы или категорию информации заказчика;
- существует вопрос обеспечения процесса по сертификации решений в области информационной безопасности, которые используют ИИ.

Данные проблемы, как вместе, так и по отдельности, в результате своего проявления способны серьёзным и непредсказуемым образом снизить эффективность применения DLP-системы, что, в конечном итоге, может подорвать доверие заказчика. Вместе с тем, ряд проблем, такие как обеспечение безопасности модели данных, подмена ценностных установок и критериев при обучении модели данных, реализуют достаточно

серьёзные уязвимости, которые могут привести к остановке бизнес-процессов в информационной системе.

6. Выводы

Исходя из истории внедрения ИИ, наличия как объективных преимуществ и предоставления новых возможностей по обеспечению защиты информации, так и текущих проблем внедрения и использования ИИ в DLP-решениях, можно сделать очевидный вывод о том, что успешное внедрение механизмов ИИ в DLP-решения и в области информационной безопасности в целом будет зависеть от соблюдения следующих важных правил и факторов:

- ответственного подхода вендоров к собственным исследованиям в области ИИ, разработке, апробации и тестированию решений, основанных на данной технологии;
- тщательному контролю за исходными данными и обеспечения безопасности самой модели данных с целью защиты от подмена ценностных установок;
- активного обсуждения результатов исследований и внедрения ИИ в научном сообществе в области информационной безопасности с участием представителей пользователей/заказчиков;
- наличия предпосылок сертификации решений, основанных на механизмах ИИ;
- общих тенденций, популярности и распространения ИИ в различных областях и сферах профессиональной деятельности, в том числе, в области обеспечения безопасности.

Список литературы

1. Клевцов А. «Искусственный интеллект в DLP-решениях InfoWatch№ доклад / А. Клевцов // конференция «BIS SUMMIT» 2023 «Индустрия защиты информации. Версия 6.0». – 21.09.2023
2. Естехин В. ИИ как предсказатель утечек данных / В. Естехин // [Электронный ресурс] // журнал Information Security: [сайт]. – URL: https://www.itsec.ru/articles/ii-kak-predskazatel-utechek-dannyh?ysclid=lsrvixuga9234391808 (дата обращения: 22.02.2024)

3. Тушканов В. «Машинное обучение в сфере информационной безопасности», доклад / В. Тушканов // конференция «BIS SUMMIT» 2023 «Индустрия защиты информации. Версия 6.0». – 21.09.2023
4. Минзов А.С. Новые подходы к предупреждению утечек информации в корпоративных информационных системах / А.С. Минзов, А.С. Александров, В.А. Мещерский // Информатизация инженерного образования: Труды Международной научно-практической конференции - ИНФОРИНО-2016, Москва, 12–13 апреля 2016 года. – Москва: Издательский дом МЭИ, 2016. – С. 172-177
5. Александров А.С. Преимущества практической реализации альтернативной концепции развития DLP-систем / А.С. Александров // Достижения науки и технологий-ДНиТ-11-2023: Сборник научных статей по материалам II Всероссийской научной конференции, Красноярск, 27–28 февраля 2023 года. Том Выпуск 7. – Красноярск: Общественное учреждение "Красноярский краевой Дом науки и техники Российского союза научных и инженерных общественных объединений". – 2023. – С. 389-394. – https://www.doi.org/10.47813/dnit-II.2023.7.389--394. – EDN MMSXSZ
6. Петренко С.А. Развитие DLP в России: история, тенденции и перспективы / С.А. Петренко // Аналитический банковский журнал. – 2014. – Т. 221. – № 09 [Электронная версия] – URL: https://iteranet.ru/press/publications/razvitie-dlp-v-rossii-istoriya-tendentsii-i-perspektivy/?ysclid=lecygphgmr145884598