INTERNATIONAL SCIENTIFIC CONFERENCE
20-22 November 2025
GABROVO

ВЛИЯНИЕ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Биляна Василева, Милко Дочев

Технически колеж – Ловеч, Ловеч, България

IMPACT OF AI ON PERSONAL DATA PROTECTIONITLE

Bilyana Vasileva, Milko Dochev

Technical College - Lovech

Abstract
The report presents the results of the analysis of information on the use of artificial intelligence in the protection of personal data. The aim is to identify the positive and weak sides of its application in order to achieve a certain level of security and protection of personal data in the sphere of private and public life.
Keywords: artificial intelligence, personal data, automated security

ВЪВЕДЕНИЕ

С бурното развитие на дигиталната трансформация изкуственият интелект придоби все по-голяма популярност. Дигиталната трансформация засегна всяка сфера на социално-икономическия живот. От една страна технологичният напредък започна да подобрява качеството на живот на човечеството, като машините започнаха да вършат трудните и монотонни действия, а за хората остава създаването на креативни решения, стимулиращи тяхното въображение и емоции. От друга страна, разпространението на COVID-19 показа, че без напреднички технологични решения и свързаност между трите икономически агента - правителство, фирми и домакинства - бизнесът и социалните процеси буквално ще спрат. От прилагането на маркетингови инструмент с изкуствен интелект, през автоматизирането, подобряването и интелигентизирането на процесите по събирането, анализа, обработката, интерпретирането и прогнозирането на финансови данни до създаването на криптирани системи за сигурност, всичко това е вече реалност и е в услуга на бизнеса и държавната администрация. Тъй като голяма част от процесите вече се дигитализираха, личните данни се оказаха „апетитна хапка" за много престъпни групировки и киберпрестъпления. Сложността и честотата на заплахите изисква комплексни решения и автоматизирано реагиране при инциденти, което да оптимизирана защитните механизми. Обект на настоящия доклад е влиянието на изкуственият интелект /ИИ/ върху защитата на личните данни, защото именно чрез AI системите се създават по-ефективни защитни механизми, които гарантират безопасността на информацията. И обратно, ИИ е мощен инструмент за злонамерени въздействия върху информационните масиви с база данни, особено лични данни в областта на финансите, здравеопазването, застрохователния биз-

Print ISSN: 1313-230X, Online ISSN: 3033-1404

нес и други.

ИЗЛОЖЕНИЕ

Според изложеното в [2] , системите за защита са използвали ИИ за киберзащита най-малко от края на 80-те години, но последните подобрения го правят значително по-ефективен. Първоначално екипите за защита са използвали системи, базирани на правила, за задействане на известявания въз основа на параметри, дефинирани от самите екипи. От началото на 2000 г. постиженията в областта на машинното обучение – подмножество на изкуствен интелект, което анализира и се учи от големи набори от данни – дава възможност на екипите по операциите да разбират типичните модели на трафика и потребителските действия в организацията, за да идентифицират необичайни събития и да отговорят на киберзаплахи. Последното ИИ подобрение е генеративният изкутвен интелект, който създава ново съдържание въз основа на структурата от налични данни. Хората взаимодействат с тези системи, ползвайки естествен език, което позволява на професионалистите по защитата да се задълбочат в много специфични въпроси, без да използват език за заявки [2] .

„Друго ново развитие е използването на агенти, поддържани от изкуствен интелект. Агентите работят съвместно с отделни лица, екипи и организации за автоматизиране на задачи и процеси с висок обем“ [2] .

Но какви всъщност са ключовите предимства на AI за киберсигурността? „Има няколко случая на употреба на изкуственият интелект в областта на сигурността, включително сигурност на данните, управление на самоличността и достъпа, управление на информационни технологии, сигурност в облака, откриване и отговор на заплахи. Изкуственият интелект трансформира киберсигурността, улеснявайки специалистите по защитата в отговора им на растящия брой киберзаплахи. Бъдещите постижения в областта на изкуствения интелект ще продължат да стимулират продуктовата разработка и новите сътрудничества между хора и ИИ системи. Последното ИИ подобрение е генеративният ИИ, който създава ново съдържание въз основа на структурата от налични данни. Хората взаимодействат с тези системи, ползвайки естествен език, което позволява на професионалистите по защитата да се задълбочат в много специфични въпроси, без да използват език за заявки” [2] .

„Изкуственият интелект(AI) помага за бързо откриване на аномалиите. Той анализира много данни от различни източници и това дава по-добра защита. Системите с AI могат да предвиждат заплахи и атаки, да анализират поведението на потребителите и системите, да дават автоматизирани отговори на инциденти, което намалява времето за реакция” [5] .

„AI системите подобряват киберсигурността чрез бързо откриване на заплахи. Те анализират поведението на потребителите, като това позволява да се реагира бързо на потенциални инциденти” [5] . От друга страна обаче, хакерите също използват AI за по-сложни атаки. „Тези заплахи включват автоматизирани атаки, които се адаптират в реално време, използване на дълбочинно обучение за генериране на зловреден софтуер, идентифициране на уязвимости в защитата на данните чрез AI алгоритми” [5] .

Правното основание за обработка на лични данни според [6] е :

„Според чл. 6, пар. 1-ви от ОРЗД обработката на лични данни е законосъобразна, само когато е налице законово основание за тази обработка по смисъла на ОРЗД. OpenAI изцяло се позовава на своя „легитимен интерес“ (чл. 6, пар. 1, б. „е“ от ОРЗД) да събира от интернет лични данни на трети лица за разработката, подобряването и/или популяризирането своите чатботове.

Това правно основание в практиката обаче остава най-спорното и в този смисъл най-рисковото, доколкото прилагането му налага винаги да се съобразяват

(на предварителен етап) правата и интересите на тези субекти на данните, които ще бъдат засегнати от обработката. Изисква се съществуването на балансиращ тест, известен още и като оценка на въздействието („legitimate interest impact assessment“), за която OpenAI твърди, че е изначало подготвило. Същата следва да обоснове и докаже преимущество на интересите на разработчика на софтуера пред тези на засегнатите лица.

Въпреки въвеждането на възможност от OpenAI всеки потребител да подаде възражение срещу обработката на неговите личните данни, т.н. „opt-out" формуляр, това не гарантира законосъобразността на подхода, възприет при обучението на чатботовете и трябва да се изследва още в неговото начало. Още повече, личните данни на всеки етап вече са послужили за развитието на технологията, а това е необратимо.

Макар OpenAI да не продава или да не използва за директен маркетинг личните данни на трети лица, изключително трудно за много от практиците по защита на данните е да си представят, че интересът на OpenAI да използва въпросните данни може да надделее над този на лицата, без да предоставят своето съгласие. Защитава се едва ли не идеята, че субектите на данните могат разумно да очакват, че личните им данни, понеже са направени публично достояние, ще бъдат използвани за всякакви цели (включително обучение на изкуствен интелект), още повече и без да бъдат предварително информирани за тях" [6].

„Регламентирането на AI е ключово за съответствието с GDPR. Бизнесите трябва да проверят дали не нарушават правата на потребителите. За да се спазват регулациите, трябва да се защитават данните. Това увеличава доверието към клиентите. Анализирането на събраната информация и обработката на данни, стратегиите за реакция при киберинциденти подпомагат GDPR и правят дигиталния свят безопасен. Така се намалят рисковете и се осигурява устойчивост. GDPR съответствието трябва да осигури, че данните се събират и обработват правилно. Това включва правото на личен живот и прозрачност при обработка на данни" [5].

„Данните могат да съдържат чувствителна (и силно регулирана) информация за клиенти или служители, разкриваща самоличността (лични данни), интелектуална собственост и търговски тайни, счетоводна информация, данни за доставчика на продукт или услуга. Участниците в заплахите могат да намерят готов пазар за всяко от изброените по-горе в подземните киберпрестъпления. Измамниците могат да използват личните данни в последващи измами и измами със самоличност" [1] .

В [1] е посочено, че организациите трябва да търсят сигурност, ориентирана към данните, която защитава, като същевременно поддържа полезността на данните. Това е от решаващо значение, тъй като бизнес потребителите трябва да могат да извлекат предвидените ползи от AI анализа, като едновременно с това осигурят достатъчно надеждна безопасност в боравенето с основните данни. Стъпките на най-добрите практики за внедряване на ориентирани към данните мерки за сигурност в AI и аналитични среди трябва да включват:

- автоматизирано откриване и класифициране на данни за идентифициране и категоризиране на данни;
- шифроване, както в покой, така и при транзит, и/или токенизация – една от най-ефективните стратегии. Те са от съществено значение за защитата на данните чрез замяна на чувствителни елементи от данни с нечувствителни еквиваленти.
- стабилен контрол на достъпа, като ролеви контрол на достъпа (RBAC) и многофакторно удостоверяване (MFA), заедно с решения за предотвратяване на загуба на данни (DLP) и стратегии за нулево доверие за предотвратяване на неоторизиран достъп и изтичане на данни.
- непрекъснато наблюдение, одит в ре-

ално време и поддържане на подробни регистрационни файлове за подпомагане на бързо откриване и реакция на инциденти със сигурността.
- изчерпателна рамка за управление на данните, редовно обучение по сигурността и програми за осведоменост и спазване на нормативните изисквания.
Следвайки този план, организациите могат да защитят чувствителните данни и да намалят риска от съответствие, като същевременно използват AI и анализи за иновации, прозрения и растеж [1].

Компаниите, работещи с лични данни, трябва да следват някои правила. Това включва: изрично информиране на потребителите каква информация се събира, правила за съхранение и обработка на лични данни, възможности за потребителите да контролират как се използват техните данни. Затова инвестирането в по-добра защита на личните данни е важно. Същевременно трябва да се защитават личните данни, без да се жертват удобствата. Законите са само началото в процеса на защита на лични данни. AI в организациите предлага нови възможности, но също и рискове.

Важно е да се създадат подходящи мерки за справяне с тези предизвикателства. Организациите трябва да следват някои ключови стратегии за защита на данните. Това включва:
- Определяне на ясни отговорности за защита на данните.
- Идентификация на информацията, която трябва да бъде защитена.
- Разработка на политики за прозрачност и достъп до данни.
- Внедряване на модерни технологии за защита, базирани на AI.

От друга страна, потребителите също имат ключова роля в защитата на данните. Те трябва да бъдат информирани за своите права и задължения относно личните данни, да използват сложни пароли и редовно да ги обновяват, да бръщат внимание на условията за ползване на различни платформи и услуги, да сигнализират при съмнение за неразрешен достъп до своите данни.

“Изкуственият интелект променя начинът, по който живеем, работим и учим. Той може да автоматизира задачи, подобрява здравеопазването, прави транспорта по-безопасен и дори помага в науката” [7]. Технологиите се развиват бързо и трябва да се създадат ясни стратегии за защита на данните. Тези стратегии трябва да намалят рисковете и да увеличат ползите от AI. Така ще се осигури безопасност и конфиденциалност в дигиталната ера. „Организациите, разработчиците и потребителите трябва да сътрудничат, за да осигурят защитата на личните данни. Сътрудничеството е ключово за използването на AI без да се компрометира сигурността на данните. Така се постигат положителни промени за общото благо“ [5].

„Изкуственият интелект за киберсигурност се отнася за използването на технологии и техники за изкуствен интелект за подобряване защитата от кибернападения на компютърни системи, мрежи и данни“ [2]. ИИ помага като автоматизира откриването на заплахи, анализира големи обеми от данни, идентифицира модели и отговаря в реално време на инциденти по защитата.

„Основните приложения на ИИ за защита включват откриване на аномалии, на злонамерен софтуер, отчитане на проникване, предотвратяване на измами, резюмета за инциденти, отчитане на заинтересовани лица, изграждане и обратно инженерство на скриптове“ [2]. Като използва машинно обучение, задълбочено обучение и обработка на естествен език, ИИ непрекъснато се учи от новите данни, подобрявайки способността си да идентифицира и смекчава възникващите заплахи, да намалява грешните положителни резултати и да мащабира по-ефективно защитата.

„Машинното обучение е подвид изкуствен интелект, ползващ алгоритми, за да се учи от данни и да прави прогнози. Тази възможност е използвана в киберзащитата, за да разкрива и автоматично

да отговаря на потенциални заплахи при различни устройства, потребители и мрежи. В дълбоко обучение, по-сложно разклонение на машинното обучение ИИ системите обработват сложни структури от данни чрез многослойни невронни мрежи, които наподобяват невронните пътища в човешкия мозък.

Дълбокото обучение и невронните мрежи обикновено са по-ефективни от традиционното машинно обучение при анализирането на големи набори от данни с много измерения и се използват в киберсигурността, за да откриват и реагират на сложни заплахи“ [2].

Друга заплаха за сигурността на личните данни са технологиите за разпознаване на лица. Всъщност какви рискове носи употребата на технологии за разпознаване на лица?

„Технологиите за разпознаване на лица предизвикват нови рискове за личния живот. Те могат да нарушават поверителността и да влияят негативно на репутацията на хората” [5].

Мястото на лицевото разпознаване поражда етични опасения, тъй като събира и съхранява биометрични данни, понякога без съгласие. Като например, „някои магазини на дребно използват технологията за разпознаване на лица, за да проследят поведението на клиентите, което води до опасения относно наблюдението и личните свободи“ [3]. Други недостатъци от използването на технологиите за лицево разпознаване са погрешни обвинения, културни и полови пристрастия, уязвимости на информационната сигурност и личната безопасност.

Разпознаването на лица е сравнително нова технология и има и своите положителни страни:

- повишена обществена безопасност: полицейските управления използват лицево разпознаване за идентифициране на изчезнали лица и издирвани престъпници;

-защитени транзакции: много банки и платежни системи използват лицево разпознаване, за да направят транзакциите си по-безопасни, като по този начин се намаляват случаите на измама и се предоставя удобство при безкасовите плащания;

-по-добро здравеопазване: болниците са внедрили системи за разпознаване на лица за безпроблемен достъп до указателите на пациентите и за ускоряване на процеса на регистрация. Някои системи дори откриват физическа болка или емоционални смущения на пациентите, като по този начин позволяват на лекарите да предоставят по-добри грижи;

- сигурност: технологията за лицево разпознаване промени завинаги сигурността на смартфоните. Въпреки че Face ID на Apple не само отключва телефона, той също така дава възможност за защита на чувствителни приложения, като цифрови портфейли и банкови приложения“ [3].

„Събирането на лицеви данни е в основата за работата на всеки софтуер за лицево разпознаване. Предоставя ценна информация като дължина на носа, ширината на челото, формата на устата, ушите, лицето и много други. Използвайки данни за обучение на AI, автоматизираните системи за разпознаване на лица могат точно да идентифицират лице сред голяма тълпа в динамично променяща се среда въз основа на техните черти на лицето” [3].

„Всяка една обработка, независимо на какво правно основание се извършва (легитимен интерес или съгласие), трябва да бъде прозрачна спрямо субекта на данните. Това е и изискването на чл. 12 от ОРЗД, който предписва на субектите на данните да бъде предоставяна изрично информация относно обработването на личната им информация своевременно, в разбираема и лесно достъпна форма. Обработката на данните, извършвана от OpenAI за целите на обучението на чатботовете, информирането на отделните засегнати лица не се извършва своевременно, а и на практика изобщо” [6].

Заради строгите регулаторни мерки на органите за защита на личните данни,

ChatGPT пък трябва да се използва със завишено внимание, особено докато единодушно на Европейско ниво не бъде установена сигурността му. В тази връзка е препоръчително, когато се представя информация за използване от ChatGPT или други езикови модели, личните данни да бъдат винаги заличавани (имена, уникални идентификатори, адреси, други обстоятелства от естество да идентифицират физически лица), съответно да бъдат разработени и използвани инструментите за възразяване срещу обработката на данните и ограничаване на съхраняването на информация от предходна чат кореспонденция. Освен за лични данни, компаниите трябва внимателно да следят и дали техни служители не предоставят информация в ChatGPT (обикновено с цел да си послужат с подготвянето на някое работно „мемо“, резюме на презентация, или проектен имейл), която може да съдържа търговска тайна, ноу-хау и друга по-чувствителна информация, обект на авторско право [6].

В противен случай, тази информация е възможно да „изтече“ в някакъв последващ момент, инцидентно или не, под формата на генериран текст-отговор от ChatGPT, разкриващ неправомерно данни за дадена компания, нейните служители (субекти на данните), което да бъде свързано както с нарушение на ОРЗД, така и с възникване на вреди [6].

ЗАКЛЮЧЕНИЕ

Бъдещето на AI оставя много въпроси без отговор, но най-важният от всички е свързан с поверителността на личните данни.

С развитието на AI расте и нуждата от правни регулации. За това свидетелства и Регламент 2024/1689 на Европейския парламент и на Съвета за установяване на хармонизирани правила относно изкуствения интелект от 13 юни 2024г. За да се гарантира безопасността трябва сътрудничество между технологичните компании, правителствата и потребителите.

Намерението да се подобри бъдещето на AI в защитата на личните данни е в минимизирането на злоупотребите от използването му и това трябва да се прави с грижа за обществото.

Докладът се публикува във връзка с резултатите от изпълнение на дейностите по договор ***№ НИП 2025 -3 / 25.02.2025*** *г. по ФНИ на ТУ- Габрово.*

ЛИТЕРАТУРА

[1] https://www.nikrama.bg/data-centric-security-is-a-critical-foundation-for-ai-powered-analytics/.
[2] https://www.microsoft.com/bg-bg/security/business/security-101/what-is-ai-for-cybersecurity.
[3] https://bg.shaip.com/blog/data-collection-for-facial-recognition-models/
[4] https://penkov- arkov.eu/bg/articles/chatgpt-i-zashhita-na-licnite-danni
[5] https://chatbotbg.com/kak-ai-vliyae-na-poveritelnostta-i-zasthitata-na-dannite/
[6] ChatGPT и защита на личните данни
[7] https://learning.fnts.bg/%D0%BA%D0%B0%D0%BA%D0%B2%D0%BE-%D1%82%D1%80%D1%8F%D0%B1%D0%B2%D0%B0-%D0%B4%D0%B0-%D0%B7%D0%BD%D0%B0%D0%B5%D0%BC-%D0%B7%D0%B0-%D0%B8%D0%B7%D0%BA%D1%83%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%B8%D1%8F-%D0%B8/