



انجمن حسابرسان داخلی^۱

چارچوب حسابرسی هوش مصنوعی

مرتضی اسدی
ساناز حجی

مقدمه

هوش مصنوعی (AI) یک اصطلاح گسترده است که برای دربر گرفتن طیف وسیعی از فناوریهای موجود و نوظهور، ساخته شده است. اگرچه تعریف واحد و مورد توافقی برای آن وجود ندارد، اما هوش مصنوعی به طور کلی به "سیستمهایی که دارای فرایندهای فکری با ویژگی انسانی هستند، مانند توانایی استدلال، کشف معنا، تعمیم دادن یا یادگیری از تجربه‌های گذشته" اطلاق می‌شود. رونق کنونی برنامه‌های کاربردی هوش مصنوعی، راه‌های به‌ظاهر بی‌پایانی را نشان می‌دهد که سازمانها می‌توانند از فناوریهای مبتنی بر هوش مصنوعی برای بهبود روش کار خود استفاده کنند؛ در حالی که ریسکهای متعدد و مهمی را ایجاد می‌کند که با توجه به ماهیت این فناوری، طبیعی است.

هوش مصنوعی می‌تواند موضوعی دلهره‌آور برای یک حسابرس داخلی باشد؛ به‌ویژه با توجه به این‌که پذیرش و استفاده از هوش مصنوعی در سازمانها در حال افزایش است. اکنون بیش از هر زمان دیگری، سازمانها برای راهنمایی بیشتر در مورد هوش مصنوعی به حسابرسی داخلی چشم دوخته‌اند. چه به‌عنوان مشاور در مورد ریسکها و کنترل‌های مرتبط با هوش مصنوعی و چه در نقش اطمینان‌بخشی در مورد فرایندهایی که از هوش مصنوعی استفاده می‌کنند یا به آن متکی

بخش اول: مرور کلی

به عنوان مرور کلی بر این موضوع، برای حساب‌رسان داخلی مهم است که شناخت درستی از توسعه تاریخی هوش مصنوعی، نحوه استفاده فعلی از هوش مصنوعی در صنایع مختلف و روندهای نوظهور هوش مصنوعی که حساب‌رسان داخلی باید در نظر بگیرند، داشته باشند. ایده هوش مصنوعی به سال ۱۹۵۰ برمی‌گردد؛ زمانی که آلن تورینگ، ریاضیدان بریتانیایی، در مقاله خود با عنوان "ماشینهای محاسباتی و هوش" این سوال را مطرح کرد: "آیا ماشینها می‌توانند فکر کنند؟" او به عنوان یکی از بنیانگذاران هوش مصنوعی در پیشنهاد این که ماشینها در نهایت قادر به باهوشی شبیه به انسان خواهند بود، در نظر گرفته می‌شود. دو سال بعد، آرتور لی ساموئل، دانشمند علوم کامپیوتر آمریکایی در IBM، برنامه‌ای را ایجاد کرد که می‌توانست با استفاده از مقادیر برنامه‌ریزی شده برای تشخیص بهترین حرکت، بازی چکرز را انجام دهد. پروژه تحقیقاتی تابستانی دارتموث در مورد هوش مصنوعی در سال ۱۹۵۶ یکی از اولین کاربردهای اصطلاح هوش مصنوعی بود که به جان مک‌کارتی، دانشمند علوم کامپیوتر و شناختی آمریکایی نسبت داده می‌شود.

دهه ۱۹۶۰ شاهد پیشرفتهای زیادی در هوش مصنوعی بود؛ از جمله استفاده از رباتیک، برنامه‌های حل مسئله و اولین برنامه کامپیوتری تعاملی (که همچنین به عنوان یک برنامه شناخت زبان طبیعی یا NLP شناخته می‌شود) به نام الیزا (ELIZA)، که توسط جوزف وایزنبوم، دانشمند علوم کامپیوتر و استاد آلمانی-آمریکایی توسعه یافت. الیزا را می‌توان اولین "چت بات" در نظر گرفت که برای شبیه‌سازی مکالمه با یک کاربر انسانی طراحی شده است. توسعه هوش مصنوعی در دهه ۱۹۷۰ شامل اولین ربات هوشمند به نام وابوت (WABOT) بود که توسط دانشکده علوم و مهندسی دانشگاه واسدا در توکیو ایجاد شد و همچنین ادامه کار بر روی NLP ها توسط راج ردی، دانشمند علوم کامپیوتر هندی-آمریکایی. پیشرفتهای دهه ۱۹۸۰ شامل ساخت یک ون مرسدس بنز بدون راننده در سال ۱۹۸۶ تحت نظارت ارنست دیکمانس، رهبر آلمانی فناوری رانندگی خودران بود. دهه ۱۹۹۰ شاهد پیشرفتهایی در فناوریهای مرتبط با هوش مصنوعی بود،

هستند، ضروری است که حساب‌رسان داخلی دانش خود را در مورد موضوع هوش مصنوعی افزایش دهند. از حساب‌رسان داخلی انتظار می‌رود که فعالیتهای اطمینان بخشی را پیرامون فرایندهایی ارائه دهند که می‌توانند از تراکتهای تجاری ساده تا رویه‌های بسیار پیچیده که نیاز به درک عمیق دارند، متغیر باشند. گستره و عمق سواد هوش مصنوعی مورد نیاز برای پشتیبانی از فعالیتهای اطمینان بخشی، چالشهای مستمری را برای حساب‌رسان داخلی ایجاد می‌کند که باید به طور مداوم دانش خود را از هوش مصنوعی توسعه دهند تا به طور کامل ریسکها و عملکرد آن را درک کرده و مشاوره و اطمینان بخشی آگاهانه ارائه دهند. هوش مصنوعی به عنوان یک موضوع حسابرسی، چالشهای منحصر به فرد خود را دارد و تکامل آن به این معنی است که حساب‌رسان داخلی باید ریسک و کاهش ریسک را در محیط هوش مصنوعی دوباره ارزیابی کنند. حال، حساب‌رسان داخلی از قبل مهارتهای اساسی مهمی مانند تفکر انتقادی، ترسیم فرایندها، ارزیابی ریسک، ارزیابی کنترل‌های فناوری اطلاعات، شناخت راهبردهای سازمانی و ارائه اطمینان بخشی مستقل به عملکرد ارکان راهبری را دارند. هدف از ارائه چارچوب حسابرسی هوش مصنوعی از سوی انجمن حساب‌رسان داخلی (IIA) کمک به حساب‌رسان داخلی در شناخت ریسک و تشخیص بهترین شیوه‌ها و کنترل‌های داخلی برای هوش مصنوعی است. این چارچوب به حساب‌رسان داخلی در توسعه دانش پایه کمک خواهد کرد.

این چارچوب، که از جنبه‌های مدل سه خطی انجمن حساب‌رسان داخلی بهره می‌برد، شامل ارجاعهایی به چارچوب بین‌المللی اجرای حرفه‌ای (IPPF) خواهد بود که مبنایی برای الزامهای اجباری و اصول راهنما برای حرفه حسابرسی داخلی ارائه می‌دهد. استانداردهای قابل اجرا باید برای اطلاعات بیشتر بررسی شوند. رهنمودهای مرتبط انجمن حساب‌رسان داخلی، مانند رهنمودهای جهانی حسابرسی فناوری^۲ (GTAGs)، برای ارائه محتوای خاص موضوعی ارجاع داده شده‌اند. سایر چارچوبهای مرتبط، مانند چارچوب مدیریت ریسک هوش مصنوعی (NIST AI RMF 1.0)، به عنوان منابع اضافی برای فعالان حسابرسی داخلی فهرست شده‌اند.

سال ۲۰۲۳ سال افزایش پذیرش مدل‌های زبانی بزرگ (LLM)

مانند چت جی بی تی (ChatGPT) بود که قابلیت‌های هوش مصنوعی را از

پیش‌بینی صرف نتایج به انواع مختلف تولید محتوا ارتقا داده است

دیدگاه‌های مختلفی در مورد نحوه گروه‌بندی اشکال مختلف هوش مصنوعی وجود دارد، بخش زیر خلاصه‌ای مختصر از اشکال رایج هوش مصنوعی ارائه می‌دهد که یا هم اکنون در حال استفاده هستند (ماشین واکنش‌پذیر و حافظه محدود) یا فقط نظری (نظریه ذهن و خودآگاه) هستند.

ماشین واکنش‌پذیر: هوش مصنوعی بدون حافظه که بر اساس ورودی یا آموزش انسانی کار می‌کند. این سیستم‌ها، گاهی اوقات هوش مصنوعی باریک یا ضعیف نامیده می‌شوند، برای هدایت ماشین در مورد نحوه عمل مستقل، به برنامه‌نویسی "انسان در حلقه" متکی هستند. این برنامه‌نویسی به‌طور معمول به‌عنوان "الگوریتم" یا مجموعه‌ای از محاسبات شامل جنبه‌هایی از علوم کامپیوتر و ریاضیات یا آمار شناخته می‌شود. دیپ بلو "Deep Blue" یک مثال است. برخی از کاربردهای یادگیری ماشین ذکر شده‌اند اما به‌تفصیل شرح داده نشده‌اند.

حافظه محدود: هوش مصنوعی با حافظه محدود که از تجربه‌های گذشته برای تصمیم‌گیری استفاده می‌کند. این نوع هوش مصنوعی از حافظه برای بهبود قابلیت‌های پیش‌بینی خود در طول زمان استفاده می‌کند.

نظریه ذهن: هوش مصنوعی با درک از احساسات و افکار دیگران. این هوش مصنوعی، هنوز یک مفهوم فقط نظری است.

خودآگاه: هوش مصنوعی با خودآگاهی که فراتر از توانایی‌های انسان است. این هوش مصنوعی، یک شکل فرضی از هوش مصنوعی است که دارای آگاهی درونی غنی است و به‌طور بالقوه از توانایی‌های انسان فراتر می‌رود. این نوع هوش مصنوعی ارتباط نزدیکی با بحث‌های جاری در مورد هوش

از جمله نرم‌افزار تشخیص گفتار در ویندوز مایکروسافت، آی. بی. ام. (IBM) هوش مصنوعی بسیار موثری مانند دیپ بلو "Deep Blue" را توسعه داد که در سال ۱۹۹۷ زمانی که گری کاسپاروف، استاد بزرگ شطرنج را شکست داد، خبرساز شد. در دهه ۲۰۰۰، هوش مصنوعی به بخشی از زندگی روزمره ما تبدیل شد، از جمله برنامه‌هایی مانند Alexa آمازون، Siri اپل و Google Assistant. سال ۲۰۲۳ سال افزایش پذیرش مدل‌های زبانی بزرگ (LLM) مانند چت جی بی تی (ChatGPT) بود که قابلیت‌های هوش مصنوعی را از پیش‌بینی صرف نتایج به انواع مختلف تولید محتوا ارتقا داده است.

سطوح پذیرش

بر اساس شاخص جهانی پذیرش هوش مصنوعی (IBM) در سال ۲۰۲۳، معادل ۴۲ درصد از شرکتهای مورد بررسی، گزارش دادند که از هوش مصنوعی در تجارت خود استفاده می‌کنند و ۴۰ درصد دیگر گزارش دادند که در حال بررسی هوش مصنوعی هستند. گسترش مداوم هوش مصنوعی نشان می‌دهد که چرا حساب‌رسان داخلی باید اطمینان حاصل کنند که حساب‌رسان در حال گنجاندن ریسک‌های مربوط به هوش مصنوعی در برنامه‌ریزی حساب‌رسی‌های خود هستند. علاوه بر این، حساب‌رسان داخلی باید به‌طور مداوم دانش خود را در مورد هوش مصنوعی توسعه دهند. بخش دوم (آغاز به‌کار) به بررسی عمیق‌تر ملاحظات می‌پردازد که یک حساب‌رسان داخلی می‌تواند از آن‌ها برای تشخیص استفاده از هوش مصنوعی در سازمان خود استفاده کند. همانطور که چشم‌انداز هوش مصنوعی به تکامل خود ادامه می‌دهد، روش‌های دسته‌بندی هوش مصنوعی نیز تغییر می‌کنند. در حالی که

که یک انسان نمی‌تواند به‌طور منطقی با همان سهولت یا سرعت پردازش کند. با توجه به توانایی هوش مصنوعی در دریافت سریع و پاسخگویی به مقادیر زیادی از مجموعه‌های داده‌های متنوع، معماری، عملکرد و دقت الگوریتم‌های درگیر بسیار مهم است. الگوریتم‌ها در ابتدا توسط انسان‌ها توسعه داده می‌شوند، بنابراین خطاهای انسانی و سوگیری‌ها (هم عمدی و هم غیرعمدی) می‌توانند بر عملکرد الگوریتم تأثیر بگذارند. بخش سوم این چارچوب جزئیات بیشتری را در مورد ریسک‌های مربوط به خطاها و سوگیری‌های الگوریتم ارائه می‌دهد. خارج از هوش مصنوعی، بسیاری از سازمان‌ها در حال حاضر استراتژی برای جمع‌آوری، ذخیره‌سازی، استفاده، مدیریت و حفاظت از داده‌ها تدوین کرده‌اند. هوش مصنوعی مانند سایر برنامه‌های کاربردی داده‌محور است، به این معنا که همان جنبه‌های مهم در مورد داده‌ها مرتبط است و باید در نظر گرفته شوند، که شامل یکپارچگی، حریم خصوصی، محرمانه‌بودن، اعتبار، صحت و کامل بودن است.

کلان داده‌ها به معنای بیش از فقط مقادیر زیادی از داده‌ها است - کلان داده‌ها به داده‌هایی اشاره دارد که به حجم، تنوع، سرعت و تغییرپذیری بسیار بالایی می‌رسند که سازمان‌ها در معماری‌های سیستم، ابزار و رویه‌هایی سرمایه‌گذاری می‌کنند که به‌طور خاص برای مدیریت داده‌ها طراحی شده‌اند. بسیاری از این داده‌ها ممکن است توسط خود سازمان تولید شوند، در حالی که سایر داده‌ها ممکن است در دسترس عموم باشند یا از منابع خارجی خریداری شوند. برای راهنمایی جامع در مورد شناخت و حسابرسی کلان داده‌ها، از جمله بحث در مورد فرصت‌ها و ریسک‌ها و یک برنامه کاری نمونه، به "رهنمود حسابرسی فناوری اطلاعات (GTAG): شناخت و حسابرسی کلان داده‌ها" انجمن حساب‌رسان داخلی مراجعه کنید.

یکی دیگر از جنبه‌های مهم هم در استفاده از داده‌ها و هم در برنامه‌های کاربردی مرتبط با هوش مصنوعی، این است که آیا داده‌ها توسط طرفی خارج از سازمان میزبانی یا پردازش می‌شوند یا خیر. حساب‌رسان داخلی باید همیشه ریسک‌های مربوط به معاملات شخص سوم (و چهارم) را در نظر بگیرند، زیرا محیط‌های کنترل داخلی فروشندگان ممکن است به اندازه محیط سازمان (یا چارچوب کنترلی محیط کنترل هوش

مصنوعی عمومی (AGI) دارد. در حالی که این موضوع در حال حاضر مورد بحث است، احتمال عملکرد هوش مصنوعی در این سطح همچنان موضوع بحث است.

بخش دوم: آغاز به کار

این بخش به نیاز حساب‌رسان داخلی برای مشارکت فعال در پیاده‌سازی هوش مصنوعی در سازمان‌ها اشاره دارد. در این مرحله، حساب‌رسان داخلی باید موارد زیر را انجام دهند:

- در رابطه با هوش مصنوعی در سازمان خود تحقیق و منابع خارجی را بررسی کنند.
- گفتگوهای اولیه هوش مصنوعی را با مدیریت، از جمله گروه هوش مصنوعی/علم داده‌ها یا مدیریت فناوری اطلاعات (یا هر دو) و گروه رهبری اجرایی (CFO، CISO، CIO و ...) انجام دهند.

- با مدیریت در بررسی یا تدوین یک فهرست برای ثبت نحوه استفاده از هوش مصنوعی (یا برنامه‌ریزی برای استفاده در آینده) همکاری کنند.

- فرایند شناخت این که چه راهبری برای هوش مصنوعی وجود دارد را آغاز کنند.

انجام این چهار کار نشان می‌دهد که حساب‌رسی داخلی اولین گام‌ها را در ایجاد یک دانش پایه از هوش مصنوعی در سازمان برداشته است. این کار همچنین فرصتی را برای حساب‌رسی داخلی فراهم می‌کند تا هرگونه مشاهده‌های فوری را که باید به موقع به مدیریت اطلاع داده شود، برجسته کند.

داده‌ها: پس از این که حساب‌رسان داخلی شناخت اساسی از نحوه استفاده از هوش مصنوعی پیدا کردند، باید دانش قوی‌تری در مورد استفاده از هوش مصنوعی در سازمان ایجاد کنند. از آنجایی که الگوریتم‌های مورد استفاده برای پشتیبانی از هوش مصنوعی به حجم زیادی از داده‌ها (که "کلان داده‌ها" نیز نامیده می‌شود) وابسته است، تعیین این که چه داده‌های سازمانی در یک برنامه کاربردی هوش مصنوعی معین استفاده می‌شود و نحوه مدیریت این داده‌ها بسیار مهم است. یک الگوریتم مجموعه‌ای از قوانین برای پیروی هوش مصنوعی است و همان چیزی است که یک ماشین را قادر می‌سازد تا به سرعت مقادیر عظیمی از داده‌ها را پردازش کند

مصنوعی فروشنده مورد نظر) جامع نباشد. رهنمود اجرایی "حسابرسی مدیریت ریسک شخص سوم هوش مصنوعی" رویکردی دقیق تر در مورد ریسکهای مربوط به استفاده از فروشندگان خارجی در اختیار حسابسان داخلی قرار می دهد. یکی دیگر از جنبه های مهم داده ها، دسترسی کاربر است. شناخت این که چه کسی می تواند داده ها را ویرایش یا تغییر دهد، حیاتی است؛ زیرا دستکاری مجموعه داده ها از منظر ورودی، به طور قطع می تواند بر خروجی پایین دستی هوش مصنوعی تاثیر بگذارد. شناخت و مستندسازی دسترسی کاربر مدیر به داده های متکی به هوش مصنوعی نیز ضروری است. "رهنمود حسابرسی فناوری اطلاعات (GTAG) : حسابرسی هویت و مدیریت دسترسی هوش مصنوعی" انجمن حسابسان داخلی، نگاهی دقیق تر به ملاحظات حسابرسی داخلی مربوط به نحوه اطمینان سازمان از دسترسی مناسب کاربران به منابع فناوری اطلاعات ارائه می دهد.

امنیت سایبری: امنیت سایبری نیز باید مورد توجه قرار گیرد؛ زیرا مربوط به محدود کردن کاربران غیرمجاز از دسترسی به داده ها و اطمینان از حریم خصوصی، محرمانه بودن و محافظت از داده ها است. پذیرش و تکامل هوش مصنوعی، سازمانها را مجبور می کند تا بر قابلیت های انعطاف پذیری سایبری خود تاکید مجدد کنند. از آنجایی که هوش مصنوعی قدرتمندتر می شود و تصمیم های بیشتری به الگوریتم های جدید، پیچیده و مبهم با استفاده از مجموعه های داده های بزرگ سپرده می شود، محافظت از این سیستمها در برابر نیروهای خارجی و مخرب برای موفقیت سازمانی حیاتی است. انعطاف پذیری سایبری برای هر سازمانی که از هوش مصنوعی استفاده می کند حیاتی است. حسابسان داخلی به طور معمول در آزمون اثربخشی کنترل های داخلی فناوری اطلاعات دخیل اند. این آشنایی با نحوه پیاده سازی کنترل های داخلی مرتبط با امنیت سایبری توسط سازمان می تواند به حسابسان داخلی در تایید این که همان کنترلها برای محافظت از داده های مرتبط با هوش مصنوعی استفاده می شوند، کمک کند. نمونه هایی از کنترل های امنیت سایبری عبارتند از:

• استفاده از رمزگذاری.

• وجود نرم افزار ضدویروس.

- استفاده از سیستم های پیشگیری/تشخیص نفوذ.
- ثبت رویدادهای امنیتی هم درخواستها و هم پاسخها.
- اطمینان از این که یک آزمون نفوذ به طور دوره ای برای جستجوی فعالانه آسیب پذیرها انجام می شود.
- آموزش کارکنان در بهترین شیوه ها برای تشخیص و جلوگیری از فیشینگ^۲، اسمیشینگ^۳ یا سایر طرح های مهندسی اجتماعی.

برای جزییات بیشتر، به "رهنمود حسابرسی فناوری اطلاعات (GTAG) : حسابرسی عملیات امنیت سایبری: پیشگیری و تشخیص" انجمن حسابسان داخلی مراجعه کنید. حسابسان داخلی باید تعیین کنند که داده های متکی به هوش مصنوعی کجا ذخیره می شوند (داخلی، خارجی یا هر دو) و در نظر بگیرند که چه کنترل های امنیت سایبری در آنجا وجود دارد. برای داده های ذخیره شده به صورت خارجی، گزارش شرکت خدمات بازرسی سازمانی (SOC) باید برای آگاهی از محیط کنترلی فروشنده به دست آید. مدیریت باید از هرگونه نقص کنترلی که در گزارش شرکت خدمات بازرسی سازمانی (SOC) یافت می شود، آگاه باشد و اطمینان حاصل کند که این نقصها داده های متکی به هوش مصنوعی را در معرض خطر قرار نمی دهند. توافق نامه های سطح خدمات (SLA) با فروشندگان باید شامل یک بند "حق حسابرسی" باشد.

بخش سوم: چارچوب حسابرسی هوش مصنوعی

اولین نسخه چارچوب حسابرسی هوش مصنوعی در سال ۲۰۱۷ منتشر شد. این چارچوب رویکردی را برای انجام خدمات مشاوره و اطمینان بخشی هوش مصنوعی به شیوه ای سیستماتیک و منظم در اختیار متخصصان حسابرسی داخلی قرار داد. این نسخه به روزرسانی شده چارچوب، محتوا را با مثالهایی از محیط هوش مصنوعی فعلی مدرن سازی می کند، در حالی که جزییات بیشتری را برای کمک به حسابسان داخلی هم به عنوان مشاور و هم به عنوان ارائه دهنده اطمینان بخشی ارائه می دهد. این چارچوب دارای سه حوزه است:

• ارکان راهبری

• مدیریت

• حسابرس داخلی

این چارچوب به مدل سه خط هوش مصنوعی مرتبط است:

در حالی که از حسابرسان داخلی انتظار نمی‌رود که

تمام ویژگیهای فنی و جزییات الزامهای هوش مصنوعی را بدانند

آن‌ها باید دانش اولیه‌ای از منابع فناوری اطلاعات (IT) داشته باشند

منابع مورد نیاز برای آموزش کارکنان در مورد این خط‌مشی‌های جدید برنامه‌ریزی کنند تا اطمینان حاصل شود که کارکنان برای پذیرش و رعایت نقش‌ها، کنترل‌ها و مسئولیت‌های تازه تعریف‌شده مرتبط با استفاده از هوش مصنوعی آماده‌اند.

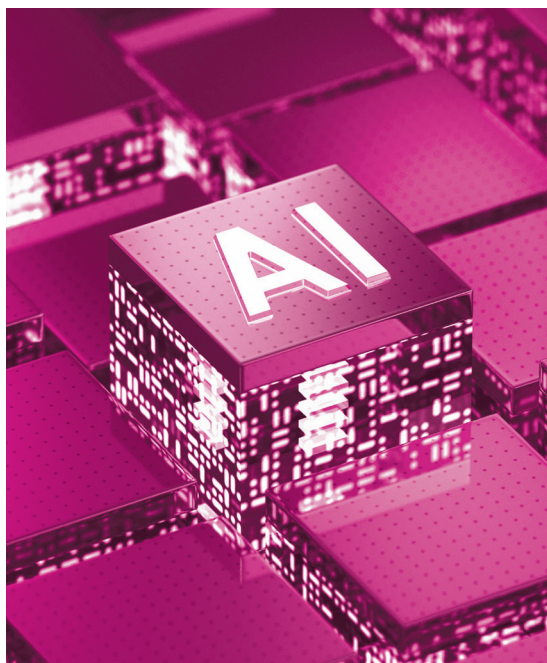
منابع فناوری اطلاعات برای پشتیبانی از هوش مصنوعی

بهینه‌سازی منابع فناوری اطلاعات برای پشتیبانی از طرح‌های هوش مصنوعی مورد نیاز است و باید بر این اساس توسط مدیریت بودجه‌بندی شود. استفاده از هوش مصنوعی نیازمند عملکرد فشرده دارایی‌های رایانه‌ای برای پایداری است. **پردازش قابل اعتماد.** نمونه‌هایی از قابلیت‌های منابع فناوری اطلاعات (IT) مورد استفاده برای پشتیبانی از طرح‌های هوش مصنوعی یک سازمان عبارتند از:

- **واحدهای پردازش مرکزی (CPU)** - "مغز" رایانه؛ پردازنده‌هایی که دستورالعمل‌ها را اجرا می‌کنند.
- **واحدهای پردازش گرافیکی (GPU)** - مغزهای توان‌تر که می‌توانند قطعات زیادی از داده‌ها را به‌طور همزمان با قابلیت‌های ریاضی اضافی پردازش کنند؛ قادر به تولید گرافیک و تصاویراند و بیشتر در هوش مصنوعی تولید خلاق رایج‌اند.
- **ذخیره‌سازی** - محل داده‌هایی که برای پردازش توسط هوش مصنوعی مورد نیاز است. ذخیره‌سازی به‌طور معمول بر حسب ترابایت (۱۰۰۰ گیگابایت) یا پتابایت (۱۰۰۰ ترابایت) اندازه‌گیری می‌شود. به‌عنوان مثال، یک ویدیوی ۵ تا ۱۰ دقیقه‌ای، کیفیتی حدود یک گیگابایت (۱ میلیارد بایت) اندازه دارد. سرورهای میزبانی شده در محل یا راه‌حل‌های مبتنی بر

ارکان راهبری بر مدیریت (خطوط اول و دوم) نظارت دارد؛ در حالی که نقش حسابرسی داخلی در حوزه سوم پوشش داده می‌شود، که شامل هر دو فعالیت اطمینان‌بخشی مستقل (خط سوم) و مشاوره‌ای است. بر این اساس، خط‌مشی‌ها و رویه‌هایی که انتظارها و دستورالعمل‌ها را برای اشخاص ثالث درگیر در طرح‌های هوش مصنوعی روشن می‌کنند نیز مهم است. هماهنگی بین گروه‌هایی که هوش مصنوعی را مدیریت می‌کنند و گروه سازمان که روابط شخص سوم را مدیریت می‌کند (مانند حقوقی)، روابط سازگار با فروشندگان هوش مصنوعی را ترویج می‌کند. از آنجا که اشخاص سوم، امتدادی از فرایندهای سازمان هستند، شناخت خوب داشتن از محیط‌های کنترل فروشندگان بسیار مهم خواهد بود. در صورت وجود، مدیریت باید گزارش‌های شرکت خدمات بازرسی سازمانی (SOC) فروشندگان هوش مصنوعی را برای شناخت فرایندهای کنترلی آن‌ها و آگاهی از هرگونه نگرانی مانند یافته‌های حسابرسی، دریافت کند. استفاده از هر شخص سوم مرتبط با توسعه قابلیت‌های هوش مصنوعی یا پشتیبانی مداوم از طرح‌های هوش مصنوعی باید به وضوح تعریف و نظارت شود، از جمله توافق‌نامه‌های سطح خدمات (SLA) که شامل حق حسابرسی است.

هنگامی که این خط‌مشی‌ها و رویه‌ها مشخص شدند، سازمان‌ها می‌توانند با به‌اشتراک گذاشتن اسناد خط‌مشی سازمانی پیش‌نویس شده مانند خط‌مشی استفاده قابل قبول در بین تمام کارکنان و دعوت از بازخورد در طول یک دوره اظهار نظر آزاد، خرید متقابل عملکردی خط‌مشی‌ها و رویه‌های هوش مصنوعی را ترویج دهند. سازمان‌ها همچنین باید برای



ابر نمونه‌هایی از مکان‌هایی است که داده‌ها ممکن است در آن ذخیره شوند.

• **حافظه** – همچنین به‌عنوان رم RAM (حافظه دسترسی تصادفی) نامیده می‌شود. مکانی که داده‌های کوتاه‌مدت در آن ذخیره میشوند و سریعتر از داده‌های ذخیره‌سازی در دسترس‌اند. بر حسب گیگابایت اندازه‌گیری می‌شود؛ جایی که ایستگاه‌های کاری رایانه‌ای منفرد دارای ۸ تا ۴۸ گیگابایت رم است. هرچه هوش مصنوعی در حال اجرا پیچیده‌تر باشد، رم بیشتری مورد نیاز است.

• **ابرایانه‌ها** – سریعترین رایانه‌های پردازشی که برای محاسبات با کارایی بالا استفاده می‌شوند و دارای CPU های متعددی هستند.

• **ایستگاه‌های کاری** – شامل رایانه‌های رومیزی و لپ‌تاپ با ویژگی‌های فنی است که از الزامات هوش مصنوعی مورد استفاده پشتیبانی می‌کند.

• **نرم افزار** – پلتفرم‌ها و برنامه‌هایی که برای توسعه، استقرار و مدیریت هوش مصنوعی استفاده می‌شوند. نرم‌افزار توسعه مانند Microsoft Azure AI، IBM Watsonx.ai و Google Cloud AI Platform. نرم‌افزار استقرار، که برای ادغام هوش مصنوعی در برنامه‌های موجود استفاده می‌شود. مانند Docker و MLflow.

• **اتصال شبکه** – این یک دسته‌بندی گسترده است که شامل سخت‌افزار، نرم‌افزار و خدماتی است که به کاربران اجازه می‌دهد منابع دیجیتال را به‌اشتراک بگذارند و اطلاعات را مبادله کنند؛ مانند سرورهای فایل و روترها.

در حالی که از حساب‌رسان داخلی انتظار نمی‌رود که تمام ویژگی‌های فنی و جزییات الزامات هوش مصنوعی را بدانند، آنها باید دانش اولیه‌ای از منابع فناوری اطلاعات (IT) داشته باشند.

• **کارگزینی و آموزش** : کارگزینی مناسب یک عنصر مهم در استراتژی هوش مصنوعی یک سازمان است. منابع انسانی باید با مدیریت همکاری کند تا اطمینان حاصل شود که کارمندان با تجربه هوش مصنوعی مورد نیاز در سراسر سازمان استخدام می‌شوند. تجربه هوش مصنوعی باید نه تنها برای کارمندان که وظیفه مدیریت جنبه‌های روزمره هوش مصنوعی را برعهده دارند، بلکه برای رهبری که طرح‌های

هوش مصنوعی را هدایت می‌کنند، در اولویت قرار گیرد. از آنجا که هوش مصنوعی به‌سرعت در حال توسعه است، مهم است که کارکنان سازمان از پیشرفت‌ها و ریسک‌های مربوط آگاه باشند. سازمان‌ها باید اطمینان حاصل کنند که آموزش عمومی آگاهی از هوش مصنوعی به همه کارکنان ارائه می‌شود و فرصت‌های آموزشی فنی بیشتری مانند سمینارها، آموزش برخط یا دوره‌های آموزشی در اختیار کارمندان که بر طرح‌های هوش مصنوعی تمرکز دارند، قرار می‌گیرد.

اجرای آموزش در مورد سیاست رسمی استفاده قابل قبول از هوش مصنوعی و گنجاندن هوش مصنوعی در دفترچه راهنمای کارمند و در توجیه کارمندان جدید، راه‌های خوبی برای افزایش آگاهی سازمانی از هوش مصنوعی همراه با ریسک‌های احتمالی است. با ادغام طرح‌های آموزشی متمرکز بر هوش مصنوعی و سواد دیجیتال، سیاست‌ها و رویه‌های سازمانی و فرصت‌های ارتقای مهارت، سازمان‌ها می‌توانند از طریق سرمایه‌گذاری مستقیم در اعضای فعلی و جدید کارکنان از طرح‌های هوش مصنوعی پشتیبانی کنند. اجرا و نتایج این طرح‌ها باید توسط حساب‌رسان داخلی به‌عنوان بخشی از کنترل‌های هوش مصنوعی یک سازمان نظارت شود.

اطلاعات مرتبط برای حفظ قابلیت ردیابی ضروری است. اجرای یک پروژه هوش مصنوعی مستلزم اطمینان از شفافیت، قابلیت توضیح، مسئولانه و قابلیت حسابرسی است.

دو نکته مهم برای برنامه‌ریزی راهبرد هوش مصنوعی

رویکرد تکراری: برنامه‌ریزی راهبرد هوش مصنوعی یک رویداد یکباره نیست، بلکه یک فرایند مداوم است. حسابرسی داخلی و مدیریت باید برای ایجاد برنامه‌ای به‌منظور بررسی دوره‌ای راهبرد هوش مصنوعی با یکدیگر همکاری کنند. **راهبرد جامع:** راهبرد هوش مصنوعی نباید مجزا باشد. به‌دلیل دامنه منابع داده و موارد استفاده بالقوه، راهبردهای هوش مصنوعی سازمانی باید چندوجهی باشد. به‌دلیل اهمیت حیاتی هوش مصنوعی، احتمال دخالت و نظارت در سطح هیئت‌مدیره وجود دارد؛ زیرا هوش مصنوعی پتانسیل تغییر یا اصلاح قابل توجهی در راهبردهای تجاری دارد.

پرداختن به این نکته‌ها اطمینان می‌دهد که برنامه‌های هوش مصنوعی با اهداف کلی سازمان همسو است. 

پانوشته‌ها:

1- The Institute Of Internal Auditors (IIA)

2- Global Technology Audit Guides (GTAG)

۳- فیشینگ (Phishing) نوعی حمله سایبری است که در آن از پیوندهای (لینک‌های) مخرب (شامل پیوندهای دانلود بدافزار یا پیوندهای صفحه‌های وب ناامن) با روش‌هایی مثل ایمیل، پیامک، شبکه‌های اجتماعی و... برای مخاطب ارسال و از روش‌های مهندسی اجتماعی (social engineering) استفاده می‌شود تا مخاطب را ترغیب به کلیک کردن روی پیوند ناامن کند.

۴- اسمیشینگ (Smishing) یک نوع حمله فیشینگ است که از پیام‌های متنی به‌عنوان یک بردار حمله استفاده می‌کند. می‌تواند برای کلاهبرداری از افراد به مهندسی اجتماعی، پیوسته‌های مخرب و وب‌سایت‌های جعلی متکی باشد.

منبع:

• The Institute of Internal Auditors, (2024) **THE IIA'S Artificial Intelligence Auditing Framework**, <https://www.theiia.org/globalassets/site/content/tools/professional/aiframework-sept-2024-update.pdf>

اجرای مدیریت ریسک توسط خطوط اول و دوم

همانطور که ملاحظه شد بخش دوم در مورد اهمیت تشخیص ریسک‌های هوش مصنوعی مربوط به امنیت، یکپارچگی، حریم خصوصی و محرمانه‌بودن داده‌ها بحث کرد و رسیدگی به این نگرانی‌ها باید در حین اجرای پروژه‌های هوش مصنوعی توسط سازمان مورد توجه قرار گیرد. الگوریتم‌های هوش مصنوعی به داده‌های دقیق و قابل اعتماد متکی است و گروه‌های پروژه باید داده‌های ورودی را از نزدیک نظارت کنند. سازمان‌ها راه‌های متعددی برای اعتبارسنجی کامل بودن داده‌های مورد استفاده در پروژه‌های هوش مصنوعی دارند. شامل حصول اطمینان از تطابق جمع کل رکوردها و تجزیه و تحلیل گزارش خطا هنگام انتقال داده‌ها بین سیستم‌ها. مدیریت باید کنترل‌های داخلی را طراحی و نظارت کند که ناهنجاری‌ها را در کیفیت یا کامل بودن داده‌ها تشخیص دهد. سایر ملاحظات مهم داده‌ها شامل محدود کردن دسترسی کاربران فقط به کارمندانی است که روی یک پروژه هوش مصنوعی کار می‌کنند، که شامل دسترسی مدیر سیستم نیز می‌شود. تعیین نقش‌های کاربری و اطمینان از تفکیک وظایف مناسب نیز بسیار مهم است. به‌عنوان مثال، مدیران پایگاه داده‌ها بر داده‌های ورودی زیربنایی نظارت می‌کنند و نباید به تغییر الگوریتم‌هایی که آن داده‌ها را پردازش می‌کنند، دسترسی داشته باشند. وظیفه‌ای که به‌طور سنتی برعهده یک توسعه‌دهنده است. هنگامی که یک پروژه هوش مصنوعی در حال پیاده‌سازی است، مهم است که سازمان اطمینان حاصل کند که پروژه شفاف، قابل توضیح، مسئولانه و قابل حسابرسی است:

- **شفافیت** - قادر به شناخت آسان هدف هوش مصنوعی یا الگوریتم با اصطلاحات ساده،
- **قابلیت توضیح** - قادر به توضیح سازوکارها، محاسبات یا نتایج پردازش شده توسط هوش مصنوعی یا الگوریتم،
- **مسئولانه** - استفاده از هوش مصنوعی یا الگوریتم‌ها به شیوه‌ای اخلاقی، ایمن، منصفانه و قابل اعتماد و
- **قابل حسابرسی** - حسابرسی بسیار مهم است زیرا هوش مصنوعی ممکن است فرایندهای انطباق یا کسب‌وکار کلیدی را جایگزین یا بهبود بخشد. گزارش‌های حسابرسی موثر یا