10th International Conference on Interdisciplinary Studies in Management & Engineering (ICISME-2024) SEPTEMBER 21, 2024 | TEHRAN
دهمین کنفرانس بین المللی مطالعات بین رشته‌ای در مدیریت و مهندسی
۳۱ شهریور ۱۴۰۳ – تهران

چالش‌های امنیتی در اطلاعات شخصی کارکنان و راهکارهای مقابله

حسین بیرامی

کارشناس ارشد مدیریت دولتی توسعه منابع انسانی دانشگاه آزاد اسلامی واحد تهران شمال،تهران،ایران
beyrami.hossein@yahoo.com

چکیده

امنیت داده‌های شخصی کارکنان در عصر دیجیتال یک مسأله حیاتی است که با وابستگی فزاینده به فناوری‌های اطلاعات و ارتباطات (ICT) و گذار به دورکاری تشدید می‌شود. این مطالعه چالش‌های امنیتی کلیدی مرتبط با حفاظت از اطلاعات شخصی کارکنان را بررسی می‌کند، اقدامات متقابل مؤثر را شناسایی کرده و رویکردهای نوآورانه برای افزایش امنیت داده‌ها را مورد بحث قرار می‌دهد. چالش‌های اصلی شناسایی شده عبارتند از: دسترسی غیرمجاز، نقض داده‌ها، تهدیدات داخلی، پیچیدگی‌های دورکاری، عدم آگاهی کارکنان، موانع انطباق با مقررات و آسیب‌پذیری‌های فناوری. اقدامات متقابل مؤثری مانند رمزگذاری، کنترل‌های دسترسی قوی، فناوری‌های جلوگیری از از دست دادن داده‌ها (DLP)، سیستم‌های تشخیص و جلوگیری از نفوذ (IDPS) و آموزش جامع آگاهی امنیتی برای کاهش این تهدیدات ضروری هستند. علاوه بر این، راه‌حل‌های نوآورانه مانند تکنیک‌های رمزگذاری پیشرفته، معماری Zero Trust، هوش مصنوعی و یادگیری ماشین برای تشخیص تهدید، فناوری بلاک چین، بازی‌وارسازی در آموزش امنیتی، فناوری‌های بهبود حریم خصوصی (PETs)، Secure Access Service Edge (SASE)، بیومتریک رفتاری و رمزنگاری کوانتومی پیشرفت‌های امیدوارکننده‌ای را در امنیت اطلاعات ارائه می‌دهند. یافته‌ها بر ضرورت یک رویکرد جامع تأکید می‌کنند که راه‌حل‌های فناوری را با عوامل انسانی و سیاست‌های سازمانی ادغام کند. پیامدهای عملی شامل نیاز به به‌روزرسانی مداوم اقدامات امنیتی، پایبندی به مقررات حفاظت از داده‌ها و سرمایه‌گذاری در فناوری‌های نوظهور است. این مطالعه بینش‌ها و توصیه‌های ارزشمندی را برای سازمان‌ها جهت افزایش اقدامات امنیتی اطلاعات آنها و تضمین حفاظت از داده‌های شخصی کارکنان در برابر تهدیدات در حال تحول ارائه می‌دهد.

واژگان کلیدی: امنیت اطلاعات، داده‌های شخصی کارکنان، نقض داده‌ها، اقدامات متقابل امنیت سایبری، فناوری‌های امنیتی نوآورانه

۱- مقدمه

در عصر دیجیتال امروزی، امنیت داده‌های شخصی کارکنان به یک دغدغه مهم برای سازمان‌ها تبدیل شده است .وابستگی فزاینده به فناوری‌های اطلاعات و ارتباطات (ICT) در عملیات تجاری، اجرای اقدامات امنیتی اطلاعات قوی را برای محافظت از داده‌های حساس در برابر دسترسی غیرمجاز، نقض‌ها و سایر تهدیدات سایبری ضروری کرده است .اهمیت ایمن‌سازی اطلاعات شخصی کارکنان با پیامدهای احتمالی نقض داده‌ها، از جمله ضررهای مالی، آسیب به شهرت و پیامدهای قانونی برای سازمان‌ها، مورد

تاکید قرار گرفته است (Jevtić & Alhudaidi, 2023). داده‌های شخصی کارکنان، مانند شماره‌های شناسایی، اطلاعات تماس، اطلاعات بهداشتی و سوابق مالی، دارایی‌های ارزشمندی هستند که نیاز به اقدامات حفاظتی دقیق دارند .ادغام فناوری‌های دیجیتال در فرآیندهای محل کار، حجم داده‌های شخصی جمع‌آوری‌شده، ذخیره شده و پردازش شده توسط کارفرمایان را به طور تصاعدی افزایش داده است .در نتیجه، تضمین محرمانه بودن، یکپارچگی و در دسترس بودن این داده‌ها برای حفظ اعتماد و انطباق با چارچوب‌های نظارتی بسیار مهم است (Knowen et al., 2023). سفر تحول دیجیتال بسیاری از سازمان‌ها، که با پذیرش مدل‌های دورکاری تسریع شده است، نیاز به استراتژی‌های جامع امنیت سایبری را بیشتر برجسته کرده است .حفاظت از داده‌های کارکنان نه تنها یک الزام قانونی است، بلکه یک جزء حیاتی از تاب‌آوری و رقابت سازمانی است (Dvojmoč & Verboten, 2022).

۱-۱- بیان مسئله

با وجود پیشرفت‌های قابل توجه در فناوری‌های امنیت اطلاعات، سازمان‌ها همچنان با چالش‌های قابل توجهی در حفاظت از داده‌های شخصی کارکنان مواجه هستند .تهدیدات سایبری در پیچیدگی و فراوانی در حال تکامل هستند و محافظت از اطلاعات حساس را برای سازمان‌ها به طور فزاینده‌ای دشوار می‌کند .یکی از چالش‌های اصلی، آسیب‌پذیری ذاتی عناصر انسانی در زیرساخت امنیتی است .عدم آگاهی کارکنان و عدم رعایت سیاست‌های امنیتی از عوامل اصلی نقض داده‌ها هستند (Indah et al., 2022). علاوه بر این، استفاده گسترده از دستگاه‌های شخصی برای اهداف حرفه‌ای (BYOD - Bring Your Own Device) بردارهای جدیدی را برای نقض داده‌ها معرفی کرده است، زیرا این دستگاه‌ها اغلب فاقد اقدامات امنیتی سختگیرانه‌ای هستند که در محیط‌های شرکتی اجرا می‌شوند .پیچیدگی مدیریت پروتکل‌های امنیتی متنوع در دستگاه‌ها و پلتفرم‌های مختلف، لایه دیگری از دشواری را برای تیم‌های امنیت اطلاعات ایجاد می‌کند (Hewitt & White, 2021). چشم‌انداز نظارتی همیشه در حال تغییر نیز چالشی را برای سازمان‌هایی که در تلاش برای انطباق با قوانین حفاظت از داده‌ها هستند، ایجاد می‌کند . مقرراتی مانند مقررات عمومی حفاظت از داده‌ها (GDPR) در اروپا، الزامات سختگیرانه‌ای را در مورد مدیریت و حفاظت از داده‌های شخصی اعمال می‌کند و مستلزم به‌روزرسانی مداوم شیوه‌ها و سیاست‌های امنیتی است (Gusarov & Melnyk, 2023).

۲-۱- اهداف

اهداف اصلی این تحقیق عبارتند از:

- شناسایی و تجزیه و تحلیل چالش‌های امنیتی کلیدی مرتبط با حفاظت از اطلاعات شخصی کارکنان در سازمان‌ها.
- ارزیابی اثربخشی اقدامات متقابل فناوری و رویه‌ای فعلی در کاهش این چالش‌ها.
- بررسی رویکردهای نوآورانه و بهترین شیوه‌ها برای افزایش امنیت داده‌های شخصی کارکنان.
- ارائه توصیه‌های عملی برای سازمان‌ها برای بهبود چارچوب‌ها و سیاست‌های امنیت اطلاعات خود.

۳-۱- اهمیت مطالعه

پرداختن به چالش‌های امنیتی مرتبط با اطلاعات شخصی کارکنان به چند دلیل بسیار مهم است .اولاً، حفاظت از داده‌های شخصی یک حق اساسی است و سازمان‌ها از نظر قانونی و اخلاقی موظف به حفاظت از این اطلاعات هستند .عدم انجام این کار می‌تواند منجر به مجازات‌های قانونی شدید و آسیب به شهرت سازمان شود (Pant, 2023). ثانیاً، اقدامات موثر امنیت اطلاعات برای حفظ اعتماد و اطمینان کارکنان بسیار مهم است .زمانی که کارکنان احساس کنند اطلاعات شخصی‌شان امن است، احتمالاً مولدتر و متعهدتر خواهند بود .این اعتماد برای ایجاد یک فرهنگ سازمانی مثبت و افزایش عملکرد کلی ضروری است (Đukić & Vuletić, 2022). علاوه بر این، شیوه‌های امنیتی داده قوی برای کاهش خطرات مالی حیاتی هستند .نقض داده‌ها می‌تواند به دلیل جریمه‌های نظارتی، هزینه‌های اصلاحی و از دست دادن کسب و کار منجر به ضررهای مالی قابل توجهی شود .سازمان‌ها با سرمایه‌گذاری در استراتژی‌های امنیتی جامع می‌توانند از این تأثیرات مالی بالقوه محافظت کنند (Srivastav, 2020). در نهایت، این مطالعه با تاکید بر اهمیت یک رویکرد جامع که راه‌حل‌های فناوری، آموزش کارکنان و سیاست‌های سازمانی را ادغام می‌کند، قصد دارد به مجموعه دانش موجود در مورد امنیت اطلاعات کمک کند .این تحقیق بینش‌های ارزشمندی را برای سیاست‌گذاران، متخصصان و دانشگاهیان در زمینه امنیت اطلاعات فراهم می‌کند (Alshanfari et al., 2022).

۲- مرور ادبیات

۲-۱- مروری بر چالش‌های امنیتی

حفاظت از داده‌های شخصی کارکنان چالش‌های امنیتی متعددی را به همراه دارد که سازمان‌ها برای اطمینان از یکپارچگی، محرمانه بودن و در دسترس بودن اطلاعات حساس باید به آن‌ها بپردازند. تهدیدات امنیتی کلیدی شامل دسترسی غیرمجاز، نقض داده‌ها و تهدیدات داخلی است.

دسترسی غیرمجاز: دسترسی غیرمجاز به داده‌های شخصی کارکنان یک تهدید قابل توجه است که اغلب در نتیجه کنترل‌های دسترسی ناکافی و مکانیزم‌های احراز هویت ضعیف رخ می‌دهد. این تهدید می‌تواند منجر به نقض داده‌ها، سرقت هویت و سایر فعالیت‌های مخرب شود. افزایش استفاده از دستگاه‌های شخصی برای اهداف کاری، این خطر را تشدید می‌کند زیرا ممکن است این دستگاه‌ها به اندازه دستگاه‌های شرکتی امنیت نداشته باشند (Gusarov & Melnyk, 2023).

نقض داده‌ها: نقض داده‌ها زمانی اتفاق می‌افتد که اطلاعات حساس بدون مجوز قابل دسترسی یا افشا می‌شود. چنین حوادثی می‌تواند عواقب شدیدی از جمله خسارات مالی، مجازات‌های قانونی و آسیب به شهرت سازمان در پی داشته باشد. روند افزایش دیجیتالی شدن و اتکا به خدمات ابری، نقض داده‌ها را به یک تهدید دائمی تبدیل کرده است (Hewitt & White, 2021).

تهدیدات داخلی: تهدیدات داخلی شامل کارکنان یا پیمانکارانی می‌شود که از دسترسی خود به داده‌های شرکت برای مقاصد مخرب سوء استفاده می‌کنند. این می‌تواند شامل سرقت اطلاعات حساس، خرابکاری سیستم‌ها یا افشای داده‌های محرمانه باشد. تهدیدات داخلی به ویژه به دلیل اینکه افراد داخلی اغلب به داده‌هایی که از آنها سوء استفاده می‌کنند دسترسی قانونی دارند، به سختی قابل شناسایی و پیشگیری هستند (Al-Harrasi et al., 2021).

۲-۲- اقدامات متقابل فنی

برای کاهش این تهدیدات، سازمان‌ها راه‌حل‌های فناوری مختلفی را برای محافظت از داده‌های شخصی کارکنان در برابر دسترسی و نقض غیرمجاز پیاده‌سازی کرده‌اند.

رمزگذاری: رمزگذاری یک اقدام امنیتی اساسی است که با تبدیل داده‌ها به فرمتی ناخوانا که تنها توسط طرف‌های مجاز با کلید صحیح قابل رمزگشایی است، از داده‌ها محافظت می‌کند. این تضمین می‌کند که حتی اگر داده‌ها رهگیری یا بدون مجوز به آنها دسترسی پیدا شود، نامفهوم باقی می‌ماند (Knowen et al., 2023).

کنترل‌های دسترسی: پیاده‌سازی مکانیسم‌های قوی کنترل دسترسی، مانند احراز هویت چند عاملی (MFA) و کنترل دسترسی مبتنی بر نقش (RBAC)، به محدود کردن دسترسی داده‌ها فقط به افراد مجاز کمک می‌کند. این کنترل‌ها در جلوگیری از دسترسی غیرمجاز و کاهش خطر تهدیدات داخلی بسیار مهم هستند (Woldemichael, 2020).

جلوگیری از دست دادن داده (DLP): فناوری‌های DLP انتقال داده‌ها را برای جلوگیری از اشتراک‌گذاری یا انتقال غیرمجاز اطلاعات حساس نظارت و کنترل می‌کنند. این راه‌حل‌ها با اطمینان از اینکه داده‌های حساس نمی‌توانند بدون مجوز مناسب سازمان را ترک کنند، به محافظت در برابر نقض داده‌ها کمک می‌کنند (Janjua et al., 2020).

سیستم‌های تشخیص و جلوگیری از نفوذ (IDPS): راه‌حل‌های IDPS فعالیت‌های مشکوک و نقض‌های امنیتی بالقوه را شناسایی و به آن‌ها پاسخ می‌دهند. با نظارت بر ترافیک شبکه و فعالیت‌های سیستم، این سیستم‌ها می‌توانند تهدیدات را قبل از اینکه آسیب قابل توجهی ایجاد کنند، شناسایی و کاهش دهند (Ameen et al., 2020).

۲-۳- عوامل انسانی در امنیت اطلاعات

رفتار انسان نقش مهمی در اثربخشی اقدامات امنیتی اطلاعات دارد. آگاهی کارکنان، آموزش و پایبندی به سیاست‌های امنیتی، اجزای ضروری یک چارچوب امنیتی قوی هستند.

آموزش آگاهی امنیتی: برنامه‌های آموزشی منظم برای آموزش کارکنان در مورد اهمیت امنیت اطلاعات، تهدیدات رایج و بهترین شیوه‌ها برای محافظت از داده‌های حساس ضروری است. آموزش موثر به کاهش خطر خطای انسانی و افزایش وضعیت کلی امنیت کمک می‌کند (Chen et al., 2021).

تجزیه و تحلیل رفتاری: سازمان‌ها به طور فزاینده‌ای از تجزیه و تحلیل رفتاری برای نظارت و تجزیه و تحلیل فعالیت‌های کارکنان برای تشخیص ناهنجاری‌هایی که ممکن است نشان دهنده تهدیدات امنیتی باشند، استفاده می‌کنند. با درک الگوهای رفتاری معمولی، تیم‌های امنیتی می‌توانند فعالیت‌های غیرعادی یا مشکوک را شناسایی و به آنها پاسخ دهند (Rauf et al., 2023).

برنامه‌های تهدید داخلی: توسعه برنامه‌های جامع تهدیدات داخلی که شامل عناصر فناوری و انسانی است برای کاهش خطرات بسیار مهم است. این برنامه‌ها باید شامل اقداماتی مانند نظارت بر رفتار کارکنان، انجام ممیزی‌های منظم و ایجاد فرهنگ آگاهی امنیتی باشد (Oyebisi & Njenga, 2020).

۴-۲- اقدامات سیاستی و سازمانی

سیاست‌ها و فرهنگ سازمانی تأثیر قابل توجهی بر اثربخشی استراتژی‌های امنیت اطلاعات دارند. ایجاد سیاست‌های روشن و تقویت یک فرهنگ آگاه به امنیت برای محافظت از داده‌های شخصی کارکنان ضروری است.

سیاست‌های امنیت اطلاعات: سیاست‌های جامع امنیت اطلاعات، قوانین و دستورالعمل‌هایی را برای مدیریت و محافظت از داده‌های حساس تعریف می‌کنند. این سیاست‌ها باید جنبه‌هایی مانند دسترسی به داده‌ها، استفاده، ذخیره‌سازی و دفع را پوشش دهند و باید به‌طور منظم مورد بازبینی و به‌روزرسانی قرار گیرند تا تهدیدات نوظهور را برطرف کنند (Fedocenko & Spitsyna, 2023).

انطباق با مقررات: رعایت الزامات قانونی و نظارتی مانند مقررات عمومی حفاظت از داده‌ها (GDPR) و سایر قوانین حفاظت از داده‌ها برای اطمینان از پردازش و حفاظت قانونی از داده‌های شخصی کارکنان بسیار مهم است. انطباق به سازمان‌ها کمک می‌کند از مجازات‌های قانونی اجتناب کنند و اعتماد کارکنان و ذی‌نفعان را افزایش دهند (Dvojmoč & Verboten, 2022).

فرهنگ سازمانی: فرهنگ امنیتی قوی در سازمان، کارکنان را تشویق می‌کند که در فعالیت‌های روزانه خود اولویت را به امنیت بدهند. رهبری نقش حیاتی در تعیین لحن شیوه‌های امنیتی و اطمینان از اجرای مداوم سیاست‌های امنیتی ایفا می‌کند (Lutsenko, 2023).

طرح‌های واکنش به حادثه: تدوین و آزمایش منظم طرح‌های واکنش به حادثه تضمین می‌کند که سازمان‌ها می‌توانند به سرعت و به طور مؤثر به نقض‌های امنیتی پاسخ دهند. این طرح‌ها باید مراحلی را که باید در صورت نقض داده‌ها انجام شود، از جمله روش‌های اطلاع‌رسانی، استراتژی‌های کاهش و تلاش‌های بازیابی، مشخص کنند (Afanasyeva et al., 2023).

۳- روش‌شناسی

طراحی تحقیق این مطالعه از روش تحقیق کتابخانه‌ای برای جمع‌آوری، بررسی و تجزیه و تحلیل سیستماتیک منابع موجود در مورد چالش‌های امنیتی مرتبط با اطلاعات شخصی کارکنان و اقدامات متقابل برای مقابله با این چالش‌ها استفاده می‌کند . تحقیقات کتابخانه‌ای که به عنوان تحقیقات ثانویه نیز شناخته می‌شود، شامل جمع‌آوری و ترکیب اطلاعات از منابع موجود مانند کتاب‌ها، مجلات دانشگاهی، مقالات کنفرانس و پایگاه‌های اطلاعاتی آنلاین می‌شود .این روش به ویژه برای به دست آوردن بینش

در مورد موضوعات به خوبی تحقیق شده و شناسایی روندها، شکاف‌ها و بهترین شیوه‌ها در زمینه امنیت اطلاعات موثر است. فرآیند تحقیق با شناسایی موضوعات و مفاهیم کلیدی مرتبط با موضوع، از جمله تهدیدات امنیتی رایج، راه حل‌های فناوری، عوامل انسانی و سیاست‌های سازمانی آغاز شد .این مضامین، جستجوی منابع مرتبط را هدایت کرد و یک بررسی جامع و متمرکز را تضمین کرد.

۳-۱- منابع داده

برای جمع آوری منابع مرتبط، از چندین پایگاه داده و مجله کلیدی استفاده شد .این منابع بر اساس شهرتشان برای انتشار تحقیقات با کیفیت بالا و peer-review شده در زمینه امنیت اطلاعات انتخاب شدند .پایگاه‌های داده و مجلات اصلی عبارتند از:

- **IEEE Xplore Digital Library**: به دلیل مجموعه گسترده از منابع فنی در مهندسی و فناوری، به ویژه در امنیت اطلاعات، شناخته شده است.
- **ACM Digital Library**: یک منبع جامع برای تحقیقات محاسباتی و فناوری اطلاعات، ارائه دسترسی به طیف گسترده‌ای از مقالات و مجموعه مقالات کنفرانس.
- **ScienceDirect**: دسترسی به مجموعه وسیعی از مقالات تحقیقاتی علمی و فنی، از جمله مقالاتی که بر امنیت اطلاعات و امنیت سایبری تمرکز دارند را فراهم می‌کند.
- **Google Scholar**: یک موتور جستجوی پرکاربرد برای منابع دانشگاهی، ارائه دسترسی به مقالات، پایان‌نامه‌ها، کتاب‌ها و مقالات کنفرانس در رشته‌های مختلف.
- **SpringerLink**: دسترسی به طیف گسترده‌ای از اسناد علمی، از جمله مقالات مجلات و فصول کتاب در زمینه امنیت اطلاعات را ارائه می‌دهد.
- **JSTOR**: یک کتابخانه دیجیتال برای مجلات دانشگاهی، کتاب‌ها و منابع اولیه، ارائه دیدگاه‌های تاریخی و معاصر در مورد موضوعات امنیت اطلاعات.

۳-۲- جمع آوری و تجزیه و تحلیل داده‌ها

فرآیند جمع‌آوری داده‌ها شامل چندین مرحله برای اطمینان از جامعیت و ارتباط منابع بررسی شده بود:

- **جستجوی کلمات کلیدی :**کلمات کلیدی مرتبط با موضوع تحقیق شناسایی و برای جستجوی پایگاه‌های داده انتخاب شده استفاده شد .کلمات کلیدی شامل "امنیت داده‌های شخصی کارکنان"، "تهدیدات امنیت اطلاعات"، "نقض داده‌ها"، "تهدیدات داخلی"، "اقدامات متقابل امنیتی"، "سیاست‌های امنیت سایبری" و "عوامل انسانی در امنیت اطلاعات" می‌شد.
- **معیارهای شمول و حذف :**برای اصلاح نتایج جستجو، معیارهای ورود و خروج خاصی اعمال شد .معیارهای شمول شامل:
  - انتشارات از سال ۲۰۲۰ به بعد برای اطمینان از گنجانده شدن جدیدترین تحقیقات.
  - مقالات مجلات peer-review شده، مقالات کنفرانس و کتاب‌ها.

- مطالعات با تمرکز بر امنیت اطلاعات شخصی کارکنان و اقدامات متقابل مرتبط.
- معیارهای حذف شامل:
  - مقالاتی که متن کامل آنها در دسترس نیست.
  - انتشاراتی که ارتباط مستقیمی با موضوع تحقیق ندارند.
- **غربالگری و انتخاب :**نتایج جستجوی اولیه با بررسی عناوین و چکیده مقالات برای ارزیابی ارتباط آنها با موضوع تحقیق بررسی شد .مقالاتی که معیارهای ورود را داشتند برای بررسی متن کامل انتخاب شدند.
- **استخراج و ترکیب داده‌ها :**اطلاعات کلیدی از مقالات انتخاب شده استخراج شد، از جمله اهداف تحقیق، روش‌ها، یافته‌ها و نتیجه‌گیری‌ها .این اطلاعات برای شناسایی موضوعات، روندها و شکاف‌های مشترک در تحقیقات موجود ترکیب شدند.
- **تحلیل انتقادی :**منابع جمع‌آوری‌شده برای ارزیابی استحکام و قابلیت اطمینان یافته‌ها مورد تجزیه و تحلیل انتقادی قرار گرفت .این شامل ارزیابی طرح تحقیق، روش‌شناسی، حجم نمونه و ارتباط نتایج با اهداف تحقیق بود.

با پیروی از این رویکرد سیستماتیک، مطالعه تضمین کرد که بررسی منابع جامع، مرتبط و بازتاب دهنده وضعیت فعلی تحقیق در مورد چالش‌های امنیتی و اقدامات متقابل مرتبط با اطلاعات شخصی کارکنان است.

۴- یافته‌ها

۴-۱- چالش‌های امنیتی شناسایی شده

۱. **دسترسی غیرمجاز :**دسترسی غیرمجاز به داده‌های شخصی کارکنان همچنان یک تهدید قابل توجه است .این اغلب به دلیل مکانیسم‌های احراز هویت ضعیف، کنترل‌های دسترسی ناکافی و استفاده فزاینده از دستگاه‌های شخصی برای اهداف کاری رخ می‌دهد .همانطور که توسط Gusarov و Melnyk (2023) برجسته شده است، افزایش استفاده از سیستم‌های مخابراتی و پایگاه‌های داده خودکار، خطرات دسترسی غیرمجاز و نقض داده‌ها را افزایش داده است .مدیریت نامناسب دستگاه‌های شخصی، که ممکن است اقدامات امنیتی قوی نداشته باشند، این مشکل را تشدید می‌کند.

۲. **نقض داده‌ها :**نقض داده‌ها یک نگرانی عمده است که باعث خسارات مالی، پیامدهای قانونی و آسیب به شهرت می‌شود . مطالعه Hewitt and White (2021) تأکید می‌کند که نقض داده‌ها می‌تواند ناشی از کارکنانی باشد که از دستگاه‌های محاسبات شخصی بدون اقدامات امنیتی کافی استفاده می‌کنند .فراوانی بالای نقض داده‌ها بر نیاز به پروتکل‌های امنیتی دقیق برای محافظت از اطلاعات حساس تاکید می‌کند.

۳. **تهدیدات داخلی :**تهدیدات داخلی شامل کارمندان یا پیمانکارانی است که از دسترسی خود به داده‌های شرکت سوء استفاده می‌کنند .شناسایی و جلوگیری از این تهدیدات به ویژه دشوار است زیرا افراد داخلی اغلب به اطلاعات حساس دسترسی قانونی دارند. Al-Harrasi et al. (2021) به بحث در مورد چگونگی تهدیدات داخلی می‌پردازند که می‌تواند منجر به سرقت داده، کلاهبرداری مالی و خرابکاری زیرساخت‌های فناوری اطلاعات شود و خطرات قابل توجهی برای سازمان‌ها ایجاد کند.

۴. **چالش‌های دورکاری :**تغییر به دورکاری چالش‌های امنیتی منحصربه‌فردی را به همراه داشته است، از جمله تضمین حریم خصوصی داده‌ها و مدیریت دسترسی ایمن به منابع سازمانی. Livshitz (2022) خاطرنشان می‌کند که دورکاری پیچیدگی حفظ حریم خصوصی و امنیت داده‌ها را افزایش داده است، زیرا کارکنان از محیط‌های متنوع و اغلب ناامن به سیستم‌های شرکتی دسترسی دارند.

۵. **عدم آگاهی کارکنان :**بسیاری از حوادث امنیتی به دلیل عدم آگاهی کارکنان در مورد سیاست‌های امنیتی و بهترین شیوه‌ها رخ می‌دهد. Khando et al. (2021) تاکید می‌کنند که آگاهی ناکافی از امنیت اطلاعات (ISA) در بین کارکنان یک عامل مهم منجر به نقض‌های امنیتی است .عنصر انسانی همچنان یک حلقه ضعیف در زنجیره امنیت است و نیازمند برنامه‌های جامع آگاهی و آموزش است.

۶. **چالش‌های انطباق و نظارتی :**سازمان‌ها در انطباق با قوانین در حال تحول حفاظت از داده‌ها مانند GDPR با چالش‌هایی مواجه هستند. Fedocenko and Spitsyna (2023) به پیچیدگی‌های تنظیم مقررات قانونی برای حفاظت از داده‌های شخصی می‌پردازند و بر نیاز به چارچوب‌های انطباق قوی برای مطابقت با استانداردهای بین‌المللی تأکید می‌کنند.

۷. **آسیب‌پذیری‌های فناوری :**آسیب‌پذیری‌های فناوری، از جمله نرم‌افزارهای قدیمی، روش‌های رمزگذاری ضعیف و شبکه‌های ناامن، به خطرات امنیتی کمک می‌کنند. Mannebäck and Padyab (2021) چندین چالش فنی را که توسط همه‌گیری COVID-19 تشدید شده است، شناسایی می‌کنند، که بسیاری از سازمان‌ها را مجبور کرد تا به سرعت اقدامات امنیتی خود را برای محیط‌های دورکاری تطبیق دهند.

۲-۴- اقدامات متقابل مؤثر

۱. **رمزگذاری :**رمزگذاری یک اقدام متقابل اساسی است که تضمین می‌کند داده‌ها برای کاربران غیرمجاز غیرقابل خواندن باقی می‌مانند .این محرمانه بودن اطلاعات حساس را با تبدیل آن به یک فرمت امن محافظت می‌کند. Knowen et al. (2023) بر اهمیت رمزگذاری در حفاظت از داده‌های شخصی در سازمان‌های بیمه تأکید می‌کنند.

۲. **کنترل‌های دسترسی :**پیاده‌سازی مکانیسم‌های قوی کنترل دسترسی، مانند احراز هویت چند عاملی (MFA) و کنترل دسترسی مبتنی بر نقش (RBAC)، به محدود کردن دسترسی به داده‌های حساس تنها به پرسنل مجاز کمک می‌کند .این کنترل‌ها برای جلوگیری از دسترسی غیرمجاز و کاهش تهدیدات داخلی ضروری هستند (Woldemichael, 2020).

۳. **جلوگیری از دست دادن داده‌ها (DLP):** فناوری‌های DLP انتقال داده‌ها را برای جلوگیری از اشتراک‌گذاری یا انتقال غیرمجاز اطلاعات حساس نظارت و کنترل می‌کنند .این راه‌حل‌ها با اطمینان از اینکه داده‌های حساس نمی‌توانند بدون مجوز مناسب سازمان را ترک کنند، به محافظت در برابر نقض داده‌ها کمک می‌کنند(Janjua et al., 2020).

۴. **سیستم‌های تشخیص و جلوگیری از نفوذ (IDPS):** راه‌حل‌های IDPS فعالیت‌های مشکوک و نقض‌های امنیتی بالقوه را شناسایی و به آنها پاسخ می‌دهند .با نظارت بر ترافیک شبکه و فعالیت‌های سیستم، این سیستم‌ها می‌توانند تهدیدات را قبل از اینکه آسیب قابل توجهی ایجاد کنند، شناسایی و کاهش دهند(Ameen et al., 2020).

۵. **آموزش آگاهی امنیتی :**برنامه‌های آموزشی منظم برای آموزش کارکنان در مورد اهمیت امنیت اطلاعات، تهدیدات رایج و بهترین شیوه‌ها برای محافظت از داده‌های حساس ضروری است .آموزش موثر به کاهش خطر خطای انسانی و افزایش وضعیت کلی امنیت کمک می‌کند(Chen et al., 2021).

۶. **تجزیه و تحلیل رفتاری :**سازمان‌ها به طور فزاینده‌ای از تجزیه و تحلیل رفتاری برای نظارت و تجزیه و تحلیل فعالیت‌های کارکنان برای تشخیص ناهنجاری‌هایی که ممکن است نشان دهنده تهدیدات امنیتی باشند، استفاده می‌کنند .با درک الگوهای رفتاری معمولی، تیم‌های امنیتی می‌توانند فعالیت‌های غیرعادی یا مشکوک را شناسایی و به آنها پاسخ دهند(Rauf et al., 2023) .

۷. **برنامه‌های تهدید داخلی :**توسعه برنامه‌های جامع تهدیدات داخلی که شامل عناصر فناوری و انسانی است برای کاهش خطرات بسیار مهم است .این برنامه‌ها باید شامل اقداماتی مانند نظارت بر رفتار کارکنان، انجام ممیزی‌های منظم و ایجاد فرهنگ آگاهی امنیتی باشد(Oyebisi & Njenga, 2020).

۸. **اقدامات سیاستی و سازمانی :**ایجاد سیاست‌های روشن امنیت اطلاعات و تقویت فرهنگ آگاه به امنیت برای محافظت از داده‌های شخصی کارکنان ضروری است .این سیاست‌ها باید جنبه‌هایی مانند دسترسی به داده‌ها، استفاده، ذخیره‌سازی و دفع را پوشش دهند و باید به‌طور منظم مورد بازبینی و به‌روزرسانی قرار گیرند تا تهدیدات نوظهور را برطرف کنند(Fedocenko & Spitsyna, 2023) .

۹. **انطباق با مقررات :**رعایت الزامات قانونی و نظارتی، مانند مقررات عمومی حفاظت از داده‌ها (GDPR)، برای اطمینان از پردازش و حفاظت قانونی از داده‌های شخصی کارکنان بسیار مهم است .انطباق به سازمان‌ها کمک می‌کند از مجازات‌های قانونی اجتناب کنند و اعتماد کارکنان و ذی‌نفعان را افزایش دهند (Dvojmoč & Verboten, 2022).

۱۰. **طرح‌های واکنش به حادثه :**تدوین و آزمایش منظم طرح‌های واکنش به حادثه تضمین می‌کند که سازمان‌ها می‌توانند به سرعت و به طور مؤثر به نقض‌های امنیتی پاسخ دهند .این طرح‌ها باید مراحلی را که باید در صورت نقض داده‌ها انجام شود، از جمله روش‌های اطلاع‌رسانی، استراتژی‌های کاهش و تلاش‌های بازیابی، مشخص کنند (Afanasyeva et al., 2023).

۳-۴- رویکردهای نوآورانه

۱. **تکنیک‌های رمزنگاری پیشرفته:** تکنیک‌های رمزنگاری نوظهور، مانند رمزگذاری هومومورفیک، به داده‌ها اجازه می‌دهند تا در حین رمزگذاری پردازش شوند، در نتیجه امنیت را بدون به خطر انداختن عملکرد افزایش می‌دهند. این رویکرد به ویژه برای محافظت از داده‌های حساس در محیط‌های ابری مفید است (Knowen et al., ۲۰۲۳).

۲. **معماری Zero Trust**: Zero Trust یک مدل امنیتی است که فرض می‌کند تمام ترافیک شبکه به طور پیش فرض غیرقابل اعتماد است. این مدل نیاز به تأیید دقیق برای هر کاربر و دستگاهی دارد که تلاش می‌کند به منابع دسترسی پیدا کند و خطر دسترسی غیرمجاز را به حداقل می‌رساند. سازمان‌ها به طور فزاینده‌ای اصول Zero Trust را برای افزایش وضعیت امنیتی خود اتخاذ می‌کنند (Woldemichael, ۲۰۲۰).

۳. **هوش مصنوعی و یادگیری ماشین:** از فناوری‌های هوش مصنوعی و یادگیری ماشین برای افزایش قابلیت‌های تشخیص و پاسخ به تهدیدات استفاده می‌شود. این فناوری‌ها می‌توانند حجم وسیعی از داده‌ها را برای شناسایی الگوها و

ناهنجاری‌هایی که ممکن است نشان دهنده تهدیدات امنیتی باشند تجزیه و تحلیل کنند و امکان اقدامات دفاعی فعال را فراهم کنند (Janjua et al, ۲۰۲۰).

۴. **بلاکچین برای امنیت داده‌ها:** فناوری بلاک چین یک روش غیرمتمرکز و مقاوم در برابر دستکاری برای ذخیره و اشتراک گذاری داده‌ها ارائه می‌دهد. با استفاده از بلاک چین، سازمان‌ها می‌توانند امنیت و یکپارچگی داده‌های شخصی کارکنان را افزایش دهند و اطمینان حاصل کنند که بدون مجوز نمی‌توان آنها را تغییر داد یا به آنها دسترسی پیدا کرد (Ameen et al., ۲۰۲۰).

۵. **بازی‌وارسازی در آموزش‌های امنیتی:** بازی‌وارسازی شامل گنجاندن عناصر بازی مانند در برنامه‌های آموزشی برای جذاب‌تر و موثرتر کردن یادگیری است. نشان داده شده است که این رویکرد مشارکت کارکنان و حفظ بهترین شیوه‌های امنیتی را بهبود می‌بخشد (Khando et al., ۲۰۲۱).

۶. **تکنولوژی‌های بهبود حریم خصوصی (PETs):** PETs، مانند حریم خصوصی تفاضلی و محاسبات امن چند جانبه، به سازمان‌ها اجازه می‌دهد تا داده‌ها را بدون به خطر انداختن حریم خصوصی فردی تجزیه و تحلیل کنند. این فناوری‌ها به ویژه برای انجام تحقیق و تجزیه و تحلیل در مجموعه داده‌های حساس در عین حال که از انطباق با مقررات حفظ حریم خصوصی اطمینان حاصل می‌کنند، مفید هستند (Livshitz, ۲۰۲۲).

۷. **Secure Access Service Edge (SASE):** SASE یک چارچوب امنیتی مبتنی بر ابر است که قابلیت‌های شبکه گسترده (WAN) را با خدمات امنیتی شبکه ترکیب می‌کند. این رویکرد صرف نظر از مکان کاربر، دسترسی ایمن به برنامه‌ها و داده‌ها را فراهم می‌کند و آن را برای محیط‌های دورکاری ایده‌آل می‌سازد (Fedocenko & Spitsyna, ۲۰۲۳).

۸. **بیومتریک رفتاری:** بیومتریک رفتاری الگوهای رفتار کاربر، مانند ریتم تایپ و حرکات ماوس را برای تأیید هویت تجزیه و تحلیل می‌کند. این رویکرد نوآورانه با نظارت مداوم بر رفتار کاربر و تشخیص ناهنجاری‌هایی که ممکن است نشان دهنده دسترسی غیرمجاز باشد، امنیت را افزایش می‌دهد (Chen et al., ۲۰۲۱).

۹. **رمزنگاری کوانتومی:** رمزنگاری کوانتومی از اصول مکانیک کوانتومی برای ایجاد کانال‌های ارتباطی امن استفاده می‌کند. این فناوری پیشرفته وعده می‌دهد با ارائه رمزگذاری غیرقابل شکستن، امنیت داده‌ها را متحول کند (Rauf et al., ۲۰۲۳).

۱۰. **Cybersecurity Mesh:** یک شبکه امنیت سایبری یک رویکرد غیرمتمرکز برای امنیت است که امکان حفاظت مقیاس‌پذیر و انعطاف‌پذیر از دارایی‌ها را صرف نظر از مکان آنها فراهم می‌کند. این مدل به ویژه در محیط‌های پویا و توزیع‌شده مانند محیط‌های ایجاد شده توسط دورکاری مؤثر است (Njenga & Oyebisi, ۲۰۲۰).

۵- بحث

۵-۱- تجزیه و تحلیل یافته‌ها

بررسی منابع چندین یافته کلیدی را در مورد چالش‌های امنیتی و اقدامات متقابل مؤثر مرتبط با محافظت از اطلاعات شخصی کارکنان نشان داد .این یافته‌ها با تحقیقات قبلی همسو و گسترش می‌یابد و هم موضوعات ثابت و هم بینش‌های جدید را برجسته می‌کند.

۵-۲- چالش‌های امنیتی

- **دسترسی غیرمجاز :**افزایش استفاده از دستگاه‌های شخصی و محیط‌های دورکاری، خطر دسترسی غیرمجاز به داده‌های کارکنان را افزایش داده است .این یافته با مطالعات قبلی مطابقت دارد که بر اهمیت کنترل‌های دسترسی قوی و مکانیسم‌های احراز هویت برای کاهش این خطر تأکید کرده‌اند(Gusarov & Melnyk, 2023).
- **نقض داده‌ها :**نقض داده‌ها همچنان یک تهدید قابل توجه است و پیامدهای مالی، قانونی و اعتباری برای سازمان‌ها دارد .روند مداوم دیجیتالی شدن و استفاده از سرویس‌های ابری به عنوان عوامل مؤثر در تداوم نقض داده‌ها شناسایی شده‌اند(Hewitt & White, 2021) .
- **تهدیدات داخلی :**تهدیدات داخلی همچنان یک نگرانی عمده است، زیرا شامل افرادی در سازمان می‌شود که از دسترسی خود به داده‌های حساس سوء استفاده می‌کنند .این با تحقیقات قبلی که بر دشواری شناسایی و جلوگیری از تهدیدات داخلی به دلیل دسترسی مشروع آنها تاکید می‌کند، همسو است(Al-Harrasi et al., 2021).
- **چالش‌های دورکاری :**تغییر به دورکاری چالش‌های امنیتی جدیدی را به ویژه در تضمین حریم خصوصی داده‌ها و دسترسی ایمن به سیستم‌های شرکتی به همراه داشته است .این یافته نشان دهنده اهمیت روزافزون تطبیق اقدامات امنیتی برای پشتیبانی از محیط‌های دورکاری است(Livshitz, 2022).
- **عدم آگاهی کارکنان :**یک موضوع تکراری در منابع، نقش حیاتی آگاهی کارکنان در جلوگیری از نقض‌های امنیتی است .بسیاری از حوادث به عدم درک و پایبندی به سیاست‌های امنیتی نسبت داده می‌شود (Khando et al., 2021).
- **چالش‌های انطباق و نظارتی :**پیچیدگی‌های انطباق با قوانین در حال تحول حفاظت از داده‌ها، مانندGDPR ، چالش‌های مداومی را برای سازمان‌ها ایجاد می‌کند .این بر نیاز به چارچوب‌های انطباق قوی برای مطابقت با استانداردهای بین‌المللی تأکید می‌کند(Fedocenko & Spitsyna, 2023).
- **آسیب‌پذیری‌های فناوری :**نرم‌افزارهای قدیمی، روش‌های رمزگذاری ضعیف و شبکه‌های ناامن از عوامل مهم در خطرات امنیتی هستند .این بیماری همه‌گیر، این آسیب‌پذیری‌ها را بیشتر برجسته کرده و نیاز به به‌روزرسانی مداوم اقدامات امنیتی را ضروری کرده است(Mannebäck & Padyab, 2021).

۳-۵- اقدامات متقابل موثر:

- **رمزگذاری :**رمزگذاری همچنان یک اقدام متقابل اساسی برای محافظت از محرمانه بودن داده‌ها است .این تضمین می‌کند که داده‌های رهگیری شده برای کاربران غیرمجاز غیرقابل خواندن باقی می‌مانند (Knowen et al., 2023).
- **کنترل دسترسی :**مکانیسم‌های قوی کنترل دسترسی، مانند احراز هویت چند عاملی و کنترل دسترسی مبتنی بر نقش، برای محدود کردن دسترسی به داده‌های حساس و کاهش تهدیدات داخلی ضروری هستند (Woldemichael, 2020).
- **جلوگیری از دست دادن داده‌ها (DLP):** فناوری‌هایDLP ، انتقال داده‌ها را برای جلوگیری از اشتراک‌گذاری غیرمجاز اطلاعات حساس نظارت و کنترل می‌کنند و به طور مؤثر خطر نقض داده‌ها را کاهش می‌دهند (Janjua et al., 2020)
- **سیستم‌های تشخیص و جلوگیری از نفوذ(IDPS)** : راه حل‌های IDPS برای شناسایی و پاسخ به فعالیت‌های مشکوک و جلوگیری از نقض‌های امنیتی بالقوه بسیار مهم هستند (Ameen et al., 2020).
- **آموزش آگاهی امنیتی :**برنامه‌های آموزشی منظم برای آموزش کارکنان در مورد تهدیدات امنیتی و بهترین شیوه‌ها، کاهش خطر خطای انسانی و افزایش وضعیت کلی امنیت بسیار مهم است (Chen et al., 2021).
- **تجزیه و تحلیل رفتاری :**استفاده از تجزیه و تحلیل رفتاری برای نظارت و تجزیه و تحلیل فعالیت‌های کارکنان به شناسایی ناهنجاری‌هایی که ممکن است نشان دهنده تهدیدات امنیتی باشد کمک می‌کند (Rauf et al., 2023).
- **برنامه‌های تهدید داخلی :**برنامه‌های جامع تهدید داخلی که شامل عناصر فناوری و انسانی می‌شود در کاهش خطرات مرتبط با تهدیدات داخلی موثر هستند(Oyebisi & Njenga, 2020).
- **اقدامات سیاستی و سازمانی :**ایجاد سیاست‌های روشن امنیت اطلاعات و پرورش فرهنگ آگاه به امنیت برای حفاظت از داده‌های شخصی کارکنان ضروری است(Fedocenko & Spitsyna, 2023).
- **انطباق با مقررات :**پایبندی به مقررات حفاظت از داده‌ها، مانند GDPR، برای اطمینان از پردازش و حفاظت قانونی از داده‌های شخصی کارکنان بسیار مهم است(Dvojmoč & Verboten, 2022).
- **طرح‌های واکنش به حادثه :**آزمایش و به‌روزرسانی منظم طرح‌های واکنش به حادثه تضمین می‌کند که سازمان‌ها می‌توانند به طور مؤثر به نقض‌های امنیتی پاسخ دهند(Afanasyeva et al., 2023) .

۴-۵- رویکردهای نوآورانه:

- **تکنیک‌های رمزگذاری پیشرفته :**تکنیک‌های رمزگذاری نوظهور، مانند رمزگذاری هومومورفیک، امنیت پیشرفته را بدون به خطر انداختن عملکرد، به ویژه در محیط‌های ابری ارائه می‌دهند (Knowen et al., 2023).
- **معماری Zero Trust:** مدل Zero Trust که فرض می‌کند تمام ترافیک شبکه به طور پیش فرض غیرقابل اعتماد است، یک چارچوب قوی برای به حداقل رساندن دسترسی غیرمجاز ارائه می‌دهد(Woldemichael, 2020) .
- **هوش مصنوعی و یادگیری ماشین :**فناوری‌های هوش مصنوعی و یادگیری ماشین با تجزیه و تحلیل حجم وسیعی از داده‌ها برای شناسایی الگوها و ناهنجاری‌ها، قابلیت‌های تشخیص و پاسخ به تهدیدات را افزایش می‌دهند (Janjua et al., 2020).

- **بلاکچین برای امنیت داده‌ها :**فناوری بلاک چین یک روش غیرمتمرکز و مقاوم در برابر دستکاری برای ذخیره و اشتراک گذاری داده‌ها ارائه می‌دهد که امنیت و یکپارچگی داده‌های شخصی کارکنان را افزایش می‌دهد (Ameen et al., 2020).
- **بازی‌وارسازی در آموزش‌های امنیتی :**بازی‌وارسازی، آموزش امنیتی را جذاب‌تر و مؤثرتر می‌کند و مشارکت کارکنان و حفظ بهترین شیوه‌های امنیتی را بهبود می‌بخشد(Khando et al., 2021).
- **فناوری‌های بهبود حریم خصوصی(PETs) :** PETs، مانند حریم خصوصی تفاضلی، امکان تجزیه و تحلیل داده‌ها را بدون به خطر انداختن حریم خصوصی فردی فراهم می‌کند و انطباق با مقررات حفظ حریم خصوصی را تضمین می‌کند (Livshitz, 2022).
- **Secure Access Service Edge (SASE):** SASE قابلیت‌های شبکه گسترده (WAN) را با خدمات امنیتی شبکه ترکیب می‌کند و دسترسی ایمن به برنامه‌ها و داده‌ها را در محیط‌های دورکاری فراهم می‌کند (Fedocenko & Spitsyna, 2023).
- **بیومتریک رفتاری :**بیومتریک رفتاری با نظارت مداوم بر رفتار کاربر و تشخیص ناهنجاری‌ها، امنیت را افزایش می‌دهد و یک لایه امنیتی اضافی را فراهم می‌کند(Chen et al., 2021).
- **رمزنگاری کوانتومی :**رمزنگاری کوانتومی رمزگذاری غیرقابل شکستن را ارائه می‌دهد و نویدبخش انقلاب در امنیت داده‌ها است(Rauf et al., 2023).
- **Cybersecurity Mesh:** مدل شبکه امنیت سایبری، محافظت مقیاس‌پذیر و انعطاف‌پذیر از دارایی‌ها، به ویژه در محیط‌های پویا و توزیع‌شده ایجاد شده توسط دورکاری را فراهم می‌کند(Oyebisi & Njenga, 2020).

۵-۵- پیامدهای عملی

یافته‌های این تحقیق پیامدهای عملی متعددی برای سازمان‌ها دارد:

- **استراتژی‌های امنیتی جامع :**سازمان‌ها باید استراتژی‌های امنیتی جامعی را اتخاذ کنند که هم راه‌حل‌های فناوری و هم عوامل انسانی را ادغام کند .این شامل آموزش منظم آگاهی امنیتی و اقدامات کنترل دسترسی قوی است.
- **سازگاری با دورکاری :**با افزایش شیوع دورکاری، سازمان‌ها باید اقدامات امنیتی خود را برای پشتیبانی از دسترسی ایمن به سیستم‌های شرکتی از محیط‌های مختلف تطبیق دهند .این شامل پیاده‌سازی راه‌حل‌هایی مانند SASE و معماری Zero Trust است.
- **به‌روزرسانی‌ها و آزمایش‌های منظم :**به‌روزرسانی و آزمایش مداوم اقدامات امنیتی و طرح‌های واکنش به حادثه برای حفظ وضعیت امنیتی موثر و تضمین واکنش سریع به نقض‌های احتمالی بسیار مهم است.
- **پایبندی به انطباق و مقررات :**رعایت مقررات حفاظت از داده‌ها برای جلوگیری از مجازات‌های قانونی و حفظ اعتماد با ذی‌نفعان ضروری است .سازمان‌ها باید چارچوب‌های انطباق خود را به طور منظم بررسی و به‌روز کنند.
- **سرمایه گذاری در فناوری‌های نوظهور :**سرمایه گذاری در فناوری‌های نوظهور مانند هوش مصنوعی، بلاک چین و رمزنگاری کوانتومی می‌تواند اقدامات امنیتی پیشرفته را ارائه دهد و سازمان‌ها را در برابر تهدیدات در حال تحول مقاوم کند.

- **تمرکز بر رفتار کارکنان :**پرداختن به عنصر انسانی در امنیت اطلاعات از طریق برنامه‌های آموزشی جامع و تجزیه و تحلیل رفتاری می‌تواند به طور قابل توجهی خطر حوادث امنیتی را کاهش دهد.

۶-۵- توصیه‌ها

بر اساس یافته‌ها و پیامدهای آنها، توصیه‌های زیر برای بهبود شیوه‌های امنیت اطلاعات ارائه می‌شود:

۱. **ارتقاء آموزش کارکنان:** برنامه‌های آموزشی آگاهی امنیتی منظم و جامع را برای آموزش کارکنان در مورد تهدیدات امنیتی و بهترین شیوه‌ها اجرا کنید. برای جذاب‌تر کردن آموزش، بازی‌وارسازی را در آن بگنجانید.
۲. **اتخاذ رمزگذاری پیشرفته:** از تکنیک‌های رمزگذاری پیشرفته مانند رمزگذاری هومومورفیک و رمزنگاری کوانتومی برای افزایش حفاظت از داده‌ها، به‌ویژه در محیط‌های ابری استفاده کنید.
۳. **پیاده‌سازی معماری Zero Trust:** مدل امنیتی Zero Trust را برای اطمینان از تأیید دقیق برای هر کاربر و دستگاهی که تلاش می‌کند به منابع سازمانی دسترسی پیدا کند، اتخاذ کنید تا خطر دسترسی غیرمجاز به حداقل برسد.
۴. **استفاده از هوش مصنوعی و یادگیری ماشین:** از فناوری‌های هوش مصنوعی و یادگیری ماشین برای افزایش قابلیت‌های تشخیص و پاسخ به تهدیدات با تجزیه و تحلیل مجموعه داده‌های بزرگ برای شناسایی الگوها و ناهنجاری‌ها استفاده کنید.
۵. **استقرار تجزیه و تحلیل رفتاری:** تجزیه و تحلیل رفتاری را برای نظارت و تجزیه و تحلیل فعالیت‌های کارکنان پیاده‌سازی کنید، رفتارهای غیرعادی یا مشکوکی را که ممکن است نشان دهنده تهدیدات امنیتی باشد شناسایی و به آنها پاسخ دهید.
۶. **تقویت برنامه‌های تهدید داخلی:** برنامه‌های جامع تهدیدات داخلی را توسعه دهید که شامل هر دو راه‌حل فناوری و عناصر انسانی برای کاهش مؤثر خطرات مرتبط با تهدیدات داخلی باشد.
۷. **به‌روزرسانی و آزمایش منظم اقدامات امنیتی:** به‌روزرسانی و آزمایش مداوم اقدامات امنیتی و طرح‌های واکنش به حادثه را برای حفظ وضعیت امنیتی موثر و اطمینان از واکنش سریع به نقض‌های احتمالی تضمین کنید.
۸. **اطمینان از انطباق با مقررات:** چارچوب‌های انطباق را به‌طور منظم بررسی و به‌روز کنید تا به مقررات حفاظت از داده‌ها مانند GDPR پایبند باشید، از مجازات‌های قانونی اجتناب کنید و اعتماد ذی‌نفعان را حفظ کنید.
۹. **سرمایه گذاری در فناوری‌های نوظهور:** روی فناوری‌های نوظهور مانند بلاک چین و PETs سرمایه گذاری کنید تا امنیت داده‌ها را افزایش دهید و از انطباق با مقررات حفظ حریم خصوصی اطمینان حاصل کنید.
۱۰. **ترویج فرهنگ آگاه به امنیت:** با تعیین لحن از سوی رهبری و اطمینان از اجرای مداوم سیاست‌های امنیتی، یک فرهنگ آگاه به امنیت را در سازمان ایجاد کنید.

۶- نتیجه‌گیری

محافظت از داده‌های شخصی کارکنان یک چالش مهم در چشم انداز دیجیتال امروزی است که با افزایش اتکا به فناوری‌های اطلاعات و ارتباطات (ICT) در عملیات تجاری ایجاد می‌شود. این مطالعه چالش‌های امنیتی کلیدی، اقدامات متقابل مؤثر و رویکردهای نوآورانه برای افزایش امنیت اطلاعات برای داده‌های کارکنان را بررسی کرده است. یافته‌ها بر پیچیدگی و ماهیت چندوجهی امنیت اطلاعات تأکید می‌کند و بر نیاز به استراتژی‌های جامعی که راه‌حل‌های فناوری، عوامل انسانی و سیاست‌های سازمانی را ادغام می‌کند، تأکید می‌کند.

۶-۱- چالش‌های امنیتی کلیدی

این تحقیق چندین چالش امنیتی فراگیر را شناسایی کرد، از جمله دسترسی غیرمجاز، نقض داده‌ها، تهدیدات داخلی، چالش‌های دورکاری، عدم آگاهی کارکنان، موانع انطباق و نظارتی، و آسیب‌پذیری‌های فناوری. دسترسی غیرمجاز همچنان یک تهدید قابل توجه است که اغلب با استفاده از دستگاه‌های شخصی و کنترل‌های دسترسی ناکافی تشدید می‌شود. نقض داده‌ها همچنان خطرات شدیدی را به همراه دارد و پیامدهای مالی، قانونی و اعتباری برای سازمان‌ها دارد. تهدیدات داخلی به دلیل دسترسی قانونی افراد داخلی به داده‌های حساس، به ویژه چالش برانگیز هستند. تغییر به دورکاری چالش‌های امنیتی جدیدی را به همراه داشته است و نیازمند راه حل‌های قوی برای تضمین حریم خصوصی داده‌ها و دسترسی ایمن به سیستم‌های شرکتی است. یک مسئله اساسی مهم در بسیاری از این چالش‌ها، عدم آگاهی کارکنان و پایبندی به سیاست‌های امنیتی است.

۶-۲- اقدامات متقابل مؤثر

برای کاهش این تهدیدات، چندین اقدام متقابل مؤثر شناسایی شد. رمزگذاری یک ابزار اساسی برای اطمینان از محرمانه بودن داده‌ها است و داده‌ها را به فرمتی غیرقابل خواندن تبدیل می‌کند که فقط برای کاربران مجاز قابل دسترسی است. کنترل‌های دسترسی قوی، مانند احراز هویت چند عاملی (MFA) و کنترل دسترسی مبتنی بر نقش (RBAC)، برای جلوگیری از دسترسی غیرمجاز و کاهش تهدیدات داخلی ضروری هستند. فناوری‌های جلوگیری از از دست دادن داده‌ها (DLP) انتقال داده‌ها را کنترل و نظارت می‌کنند و از اشتراک‌گذاری غیرمجاز اطلاعات حساس جلوگیری می‌کنند. سیستم‌های تشخیص و جلوگیری از نفوذ (IDPS) برای شناسایی و پاسخ به فعالیت‌های مشکوک و در نتیجه جلوگیری از نقض‌های احتمالی بسیار مهم هستند. برنامه‌های آموزشی منظم آگاهی امنیتی برای آموزش کارکنان در مورد تهدیدات امنیتی و بهترین شیوه‌ها، کاهش خطر خطای انسانی و افزایش وضعیت کلی امنیت حیاتی هستند. تجزیه و تحلیل رفتاری و برنامه‌های جامع تهدید داخلی با نظارت و تجزیه و تحلیل فعالیت‌های کارکنان برای شناسایی ناهنجاری‌ها، امنیت را بیشتر افزایش می‌دهند.

۶-۳- رویکردهای نوآورانه

فناوری‌های نوظهور و رویکردهای نوآورانه، راه حل‌های امیدوارکننده‌ای را برای افزایش امنیت اطلاعات ارائه می‌دهند. تکنیک‌های رمزگذاری پیشرفته، مانند رمزگذاری هومومورفیک، امنیت پیشرفته را بدون به خطر انداختن عملکرد، به ویژه در محیط‌های ابری فراهم می‌کنند. مدل امنیتی Zero Trust، که فرض می‌کند تمام ترافیک شبکه به طور پیش فرض غیرقابل اعتماد است، یک چارچوب قوی برای به حداقل رساندن دسترسی غیرمجاز ارائه می‌دهد. فناوری‌های هوش مصنوعی و یادگیری ماشین با تجزیه و

تحلیل حجم وسیعی از داده‌ها برای شناسایی الگوها و ناهنجاری‌ها، قابلیت‌های تشخیص و پاسخ به تهدیدات را افزایش می‌دهند. فناوری بلاک چین یک روش غیرمتمرکز و مقاوم در برابر دستکاری برای ذخیره و اشتراک گذاری داده‌ها ارائه می‌دهد و امنیت و یکپارچگی داده‌های شخصی کارکنان را تضمین می‌کند. بازی‌وارسازی در آموزش‌های امنیتی، آموزش را جذاب‌تر و موثرتر می‌کند و مشارکت کارکنان و حفظ بهترین شیوه‌های امنیتی را بهبود می‌بخشد. فناوری‌های بهبود حریم خصوصی (PETs)، مانند حریم خصوصی تفاضلی، امکان تجزیه و تحلیل داده‌ها را بدون به خطر انداختن حریم خصوصی فردی فراهم می‌کنند. Secure Access Service Edge (SASE) قابلیت‌های شبکه گسترده (WAN) را با خدمات امنیتی شبکه ترکیب می‌کند و دسترسی ایمن به برنامه‌ها و داده‌ها را در محیط‌های دورکاری فراهم می‌کند. بیومتریک رفتاری و رمزنگاری کوانتومی به ترتیب با نظارت مداوم بر رفتار کاربر و ارائه رمزگذاری غیرقابل شکستن، لایه‌های امنیتی اضافی را ارائه می‌دهند.

۴-۶- پیامدها و توصیه‌ها:

یافته‌های این مطالعه پیامدهای قابل توجهی برای عمل دارد. سازمان‌ها باید استراتژی‌های امنیتی جامعی را اتخاذ کنند که هم راه‌حل‌های فناوری و هم عوامل انسانی را ادغام کند. به‌روزرسانی و آزمایش منظم اقدامات امنیتی، اطمینان از انطباق با مقررات حفاظت از داده‌ها و سرمایه گذاری در فناوری‌های نوظهور گام‌های مهمی برای افزایش امنیت هستند. پرورش فرهنگ آگاه به امنیت در سازمان و تعیین لحن از سوی رهبری برای اطمینان از اجرای مداوم سیاست‌های امنیتی ضروری است. در پایان، حفاظت از داده‌های شخصی کارکنان نیازمند یک رویکرد چندوجهی است که هم عناصر فناوری و هم عناصر انسانی را در بر می‌گیرد. با اجرای اقدامات متقابل شناسایی شده و اتخاذ رویکردهای نوآورانه، سازمان‌ها می‌توانند وضعیت امنیت اطلاعات خود را به میزان قابل توجهی افزایش دهند و از داده‌های حساس کارکنان در برابر تهدیدات در حال تحول محافظت کنند.

۷- منابع

1. Afanasyeva, S. V., Cherepanova, E., & Shekhova, N. V. (2023). Innovative methods for cyber threats prevention to ensure the economic security of organizations.
2. Al-Harrasi, A. S., Shaikh, A., & Al-Badi, A. (2021). Towards protecting organisations' data by preventing data theft by malicious insiders.
3. Ameen, N., Tarhini, A., Shah, M., Madichie, N., Paul, J., & Choudrie, J. (2020). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce.
4. Chen, Y., Galletta, D., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model.
5. Dvojmoč, M., & Verboten, M. T. (2022). Cyber (In)security of Personal Data and Information in Times of Digitization.
6. Fedocenko, N., & Spitsyna, H. (2023). Current issues of international legal regulation of the protection of personal data of employees.
7. Gusarov, S. M., & Melnyk, K. Y. (2023). Protection of personal data of the employee.
8. Janjua, F., Masood, A., Abbas, H., & Rashid, I. (2020). Handling Insider Threat Through Supervised Machine Learning Techniques.
9. Khando, K., Gao, S., Islam, S., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review.
10. Knowen, C., Ronoh, L., & Mugalavai, A. (2023). Prioritizing Personal Data Protection in Insurance Organizations.

11. Livshitz, I. (2022). Data privacy assurance for remote work.
12. Mannebäck, E., & Padyab, A. (2021). Challenges of Managing Information Security during the Pandemic.
13. Oyebisi, D., & Njenga, K. (2020). Behaviour of Outsourced Employees as Sources of Information System Security Threats.
14. Rauf, U., Mohsen, F., & Wei, Z. (2023). A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations.
15. Woldemichael, H. T. (2020). Emerging Cyber Security Threats in Organization.
16. Hassandoust, F., & Techatassanasoontorn, A. (2018). Understanding users' information security awareness and intentions.
17. Dong, L., Peng, X., Zhuang, Y., Zhu, Z., Xu, H., Zhen, L., Gao, H., & Zhang, Y. (2020). Research on Computer Security Protection Technology Based on Information.
18. Kondratenko, N. (2021). Study of Information Security of the Information Services Market.
19. Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach.
20. Obidenko, A. V., & Shaburova, A. (2021). Justification of the Need to Ensure Information Security of an Enterprise in the Era of Digitalization.
21. Sukhov, A. N. (2022). Socio-psychological analysis of the information security threats.
22. Andriishena, H., Chunakov, R., Zaitsev, M., & Shyshatskyi, A. (2023). Developing a methodological approach to assessing state information security.
23. Ahsan, M., Asif, A., & Naseer, S. (2020). Design of a Cyber Security Research Lab.
24. Zakoldaev, D., & Grishentsev, A. (2021). Methodology for Modeling and Ensuring Information Security in Resource Management.
25. Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers.
26. Schinagl, S., & Shahim, A. (2020). What do we know about information security governance?
27. Nweke, L. O., & Wolthusen, S. (2020). Ethical Implications of Security Vulnerability Research for Critical Infrastructure Protection.
28. Khetagurova, T. G., Khetagurova, I. Y., Soskieva, Z. V., & Bagieva, M. G. (2023). Information Security in the Digital Economy.
29. Ziro, A., Toibayeva, S., Gnatyuk, S., Imanbayev, A., Iavich, M., & Zhaybergenova, Z. (2023). Research of the Information Security Audit System in Organizations.
30. Hooper, V. A., & Blunt, C. J. (2020). Factors influencing the information security behaviour of IT employees.
31. Moustafa, A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management.
32. Ramirez, R., Yano, T., Shimaoka, M., & Magata, K. (2020). Knowledge-Base Practicality for Cybersecurity Research Ethics Evaluation.
33. Lyashenko, H., Shemendiuk, O., Bokhno, T., & Cherednychenko, O. (2023). Developing a methodological approach to assessing state information security.
34. Singh, N., Krishnaswamy, V., & Zhang, Z. (2022). Intellectual structure of cybersecurity research in enterprise information systems.