مقالهٔ پژوهشی
صفحات ۲۷ - ۵۲

فصلنامه
سیاست‌نامهٔ علم و فناوری
دورهٔ ۱۵، شمارهٔ ۳، پاییز ۱۴۰۴

چهارچوب عوامل مؤثر بر انطباق رفتار کارکنان با سیاست‌های امنیت اطلاعات در نظام بانکی

20.1001.1.24767220.1404.15.3.7.7

سعید کاظم پوریان[۱]
محمدرضا تقوا[۲]
وجه‌الله قربانی‌زاده[۳]
امیر مانیان[۴]

چکیده

با توجه به نقش حیاتی عامل انسانی به‌منزلهٔ یکی از حلقه‌های آسیب‌پذیر در زنجیرهٔ امنیت اطلاعات، پژوهش حاضر با هدف شناسایی، طبقه‌بندی و یکپارچه‌سازی عوامل مؤثر بر انطباق رفتار کارکنان با سیاست‌های امنیت اطلاعات در صنعت بانکداری، به ارائهٔ چهارچوب مفهومی جامع در این حوزه می‌پردازد. این مطالعه از روش تحقیق کیفی فراترکیب بهره برده است. با جست‌وجوی نظام‌مند در پایگاه‌های علمی، ۶۷ مقالهٔ معتبر، که به طور مستقیم به موضوع پژوهش پرداخته بودند، انتخاب و به صورت عمیق به روش تحلیل مضمون مورد تجزیه و تحلیل قرار گرفتند. چهارچوب نظری اصلی برای طبقه‌بندی و یکپارچه‌سازی عوامل مستخرج، مدل رفتار، قابلیت، فرصت و انگیزه (COM-B) بوده است که با مفاهیم کلیدی از نظریه‌های انگیزش محافظت، رفتار برنامه‌ریزی‌شده، خنثی‌سازی و بازدارندگی عمومی تلفیق شد. یافته‌های پژوهش نشان می‌دهد رفتار انطباقی محصول تعامل سه بعد اصلی است. بعد انگیزه با ۱۳ عامل به‌منزلهٔ محوری‌ترین بعد شناسایی شد که در آن نگرش، باورها و ارزیابی هزینه و فایده به ترتیب با ۳۹ و ۲۴ تکرار بیشترین فراوانی را داشتند. در بعد فرصت با ۱۱ عامل، آموزش، آگاهی و هنجارهای اجتماعی با ۲۸ و ۲۱ تکرار قدرتمندترین عوامل محیطی تعیین شدند. در بعد قابلیت نیز، که متشکل از ۱۲ عامل است، عامل خودکارآمدی با ۱۸ تکرار، اهمیت بیشتری از سایر عوامل این دسته دارد. این پژوهش چهارچوبی یکپارچه و چندبعدی ارائه می‌کند که نشان می‌دهد انطباق رفتار کارکنان نظام بانکی با سیاست‌های امنیت اطلاعات بیش از الزام فنی انتخابی شناختی و اجتماعی است. این چهارچوب پیامدهای کاربردی مهمی برای مدیران بانکی دارد؛ از جمله لزوم تغییر تمرکز از راهبردهای ابزارمحور به رویکردهای انسان‌محور، که بر اصلاح نگرش، تقویت خودکارآمدی و پرورش فرهنگ امنیت مثبت تأکید دارند؛ همچنین این چهارچوب به منزلهٔ مبنای نظری جامع مسیرهای تحقیقاتی آتی را برای آزمودن روابط میان این عوامل هموار می‌کند.

واژگان کلیدی: فراترکیب، امنیت اطلاعات، بانک، انطباق، نظریهٔ انگیزش محافظت، نظریهٔ بازدارندگی عمومی، نظریهٔ رفتار برنامه‌ریزی‌شده

تاریخ دریافت: ۲۷ تیر ۱۴۰۴ **تاریخ بازنگری: ۱۵ مرداد ۱۴۰۴** **تاریخ پذیرش: ۲۲ مرداد ۱۴۰۴**

۱. دانشجوی دکتری مدیریت فناوری اطلاعات، دانشکدهٔ مدیریت و حسابداری، دانشگاه علامه طباطبایی، تهران، ایران (نویسندهٔ مسئول)؛ saeed.ka-zem.313@gmail.com
۲. استاد گروه مدیریت فناوری اطلاعات، دانشکدهٔ مدیریت و حسابداری، دانشگاه علامه طباطبایی، تهران، ایران.
۳. استاد گروه مدیریت دولتی، دانشکدهٔ مدیریت و حسابداری، دانشگاه علامه طباطبایی، تهران، ایران.
۴. استاد گروه مدیریت فناوری اطلاعات، دانشکدگان مدیریت، دانشگاه تهران، تهران، ایران.

مقدمه

امروزه امنیت اطلاعات یکی از ارکان اساسی حفظ و توسعهٔ نظام بانکی است و نقشی حیاتی در تضمین اعتماد مشتریان و پایداری سیستم‌های مالی دارد (Petrič and Orehek, 2025). با گسترش فزایندهٔ استفادهٔ سازمان‌ها از فناوری‌های نوین در حوزه‌های گوناگون (Mohammadi et al., 2021) و به دنبال آن افزایش چشمگیر حملات سایبری اهمیت این موضوع، به‌ویژه در نظام بانکی، بیش از پیش نمایان شده است. بر اساس گزارش‌های بین‌المللی و تحقیقات صورت‌گرفته، بانک‌ها و مؤسسات مالی به‌دلیل ماهیت حساس اطلاعاتی که در اختیار دارند و حجم زیاد تراکنش‌های مالی به طور فزاینده‌ای در معرض تهدیدات امنیتی قرار گرفته‌اند (ISACA, 2025; Sullivan, 2025). به گزارش صندوق بین‌المللی پول، بانک‌ها و مؤسسات مالی هدف ۲۰ درصد از کل حملات سایبری هستند (IMF, 2024) و به طور متوسط متحمل خسارتی معادل ۵٫۹۷ میلیون دلار از این رخدادها می‌شوند (Sullivan, 2025). در این راستا، ریشه‌یابی آسیب‌پذیری در برابر این حملات از اهمیت بسزایی برخوردار است؛ همچنین توجه به رفتار و اقدامات کارمندان، به منزلهٔ یکی از مهم‌ترین و تأثیرگذارترین عوامل بر امنیت اطلاعات، ضروری به نظر می‌رسد.

شواهد و گزارش‌های متعدد در سال‌های اخیر حاکی از آن است که بسیاری از حملات سایبری از ضعف‌ها و آسیب‌پذیری‌های موجود در رفتار کارمندان سوءاستفاده می‌کنند (ENISA, 2023; Verizon, 2023). بیشترین نقض‌های امنیتی نیز ناشی از اشتباهات، بی‌توجهی‌ها و رعایت نکردن سیاست‌های امنیتی از سوی کارمندان بوده است (Duncan, 2022; Hadlington et al., 2021). آمارها نشان می‌دهد ۶۷ درصد از نشت یا افشای داده‌ها ناشی از اشتباهات انسانی است (PurpleSec, 2023) و علت ریشه‌ای ۸۲ درصد از این رخدادها نیز به اقدامات و رفتارهای انسانی مرتبط است (Kerner, 2023). این رفتارها تحت تأثیر عوامل مثبت و منفی متعددی قرار می‌گیرند که از جملهٔ آن‌ها می‌توان به پشتیبانی نکردن مدیریت ارشد (Amiri et al., 2015)، آگاهی‌رسانی امنیتی (Li et al., 2019)، تعهد سازمانی (Liu et al., 2020) و عدالت سازمانی (Aebissa et al., 2023) اشاره کرد؛ بنابراین شناسایی و مدیریت عوامل مؤثر بر انطباق رفتار کارمندان با سیاست‌های امنیت اطلاعات در یک سازمان راهبردی کلیدی و پیشگیرانه است که می‌تواند نقش بسزایی در کاهش خطرهای امنیتی و افزایش مقاومت سازمان‌ها در برابر حملات سایبری ایفا کند (Bulgurcu et al., 2010).

پژوهشگران این حوزه تعاریف مختلفی از مفهوم انطباق با سیاست‌های امنیت اطلاعات ارائه داده‌اند. برخی آن را میزان قصد کارکنان برای انطباق با سیاستی امنیتی تعریف می‌کنند (Herath and Rao, 2009; Bulgurcu et al., 2010)؛ همچنین بعضی محققان این مفهوم را به منزلهٔ فرایند حصول اطمینان از تبعیت کارکنان و کل سازمان از استانداردها و مقررات امنیتی می‌دانند (Uchendu et al., 2021). در برخی موارد، این مفهوم با در نظر گرفتن ابعاد فنی تعریف شده و درجهٔ محافظت کارکنان از دارایی‌های اطلاعاتی و فناورانه سازمان در برابر تهدیدات امنیتی با تبعیت از سیاست‌های امنیت اطلاعات تلقی شده است (Alassaf and Alkhalifah, 2021). بعضی از پژوهشگران نیز آن را مفهومی نظری در نظر گرفته‌اند که بر برآورده‌سازی سیاست‌های امنیت اطلاعات تأکید می‌کند و در درجهٔ اول بر رفتار کارکنان تأثیر دارد تا امنیت اطلاعات را بهبود بخشد (Amankwa et al., 2022).

با وجود پژوهش‌های متعدد در حوزه‌هایی مانند بهداشت تاکنون تحقیقات کمتری در زمینهٔ رفتار انطباقی کارمندان با سیاست‌های امنیت اطلاعات در حوزهٔ مالی و بانکی انجام شده است (Alassaf and Alkhalifa, 2021). این تحقیقات مختلف، که بر اساس نظریه‌هایی مانند نظریهٔ انگیزش محافظت (Rogers, 1975; Rogers, 1983)، نظریهٔ کنش منطقی (Ajzen and Fishbein, 1973)، نظریهٔ رفتار برنامه‌ریزی‌شده (Ajzen; ۱۹۸۵)، نظریهٔ بازدارندگی عمومی (Gibbs, 1968; Straub, 1990) و نظریهٔ خنثی‌سازی (Sykes and Matza, 1957) انجام گرفته‌اند، در موارد گوناگونی به نتایج ناسازگار منتهی شده‌اند (Khan et al., 2022)؛ برای مثال، در حالی که در برخی مطالعات ترس از جریمه بر قصد انطباق با سیاست‌های امنیت اطلاعات تأثیرگذار دانسته شده است (D'arcy et al., 2014; Johnston and Warkentin, 2010; Ifinedo, 2016; Vance et al., 2020)، برخی مطالعات دیگر این عامل را بی‌تأثیر دانسته‌اند (Chen et al., 2018; Jacobs, 2010; Menard et al., 2017; Silic et al., 2017)؛ همچنین درک هزینهٔ انطباق با این سیاست‌ها نتایج متفاوتی به همراه داشته است (Bulgurcu et al., 2010; Ogbanufe, 2023; Chen et al., 2018; Ifinedo, 2012). این تفاوت‌ها حاکی از آن است که عوامل مؤثر بر انطباق رفتاری ممکن است در شرایط و بافتارهای مختلف متفاوت باشند.

به علاوه، با وجود اینکه تاکنون استانداردها و مدل‌های متنوعی برای انطباق رفتار کارکنان با سیاست‌های امنیتی تدوین شده است، در حوزهٔ بانکی، این چهارچوب‌ها جامعیت و اثربخشی لازم را نداشته‌اند. نمونه‌هایی از رخدادهای امنیت اطلاعات در حوزهٔ بانکی در سال‌های اخیر عبارت‌اند از: حملهٔ باج‌افزاری به بانک صنعتی و تجاری چین (ICBC) به علت اشتباه سهوی کارکنان در کلیک روی لینکی آلوده (Schroeder and Siddiqui, 2023)، نقض سیاست‌های امنیتی بانک اِوُلو (Evolve Bank) آمریکا و افشای اطلاعات میلیون‌ها مشتری (Xie and Gorrivan, 2024) و نقض عمدی سیاست‌های امنیتی توسط یکی از کارمندان سابق بانک ولز فارگو آمریکا با سرقت بیش از ۱ میلیون دلار از مشتریان این بانک (U.S. Department of Justice, 2024). این رخدادهای ناشی از خطای انسانی و رعایت نکردن سهوی یا عمدی سیاست‌های امنیت اطلاعات نشان‌دهندهٔ نیاز مبرم به بازنگری و متناسب‌سازی رویکردهای موجود و توسعه و تدوین چهارچوب‌های جدید در این حوزه است.

بنابراین با توجه به تناقض‌های موجود در نتایج پژوهش‌های پیشین، تعدد نظریه‌های استفاده‌شده و نبود چهارچوبی جامع از عوامل مؤثر بر رفتار کارکنان بانکی در حوزهٔ امنیت اطلاعات هدف اصلی این پژوهش ارائهٔ چهارچوبی جامع و کاربردی برای انطباق رفتار کارمندان با سیاست‌های امنیت اطلاعات در نظام بانکی برای پاسخ به سؤال زیر است:

عوامل مؤثر بر انطباق رفتار کارکنان نظام بانکی با سیاست‌های های امنیت اطلاعات چیست؟

چهارچوب متشکل از این عوامل از طریق اجرای روش فراترکیب و با کاوش در پیشینهٔ پژوهش و استخراج عوامل مؤثر بر این انطباق رفتاری حاصل می‌شود. با توجه به اهمیت چشمگیر مبحث امنیت اطلاعات در نظام بانکی و لزوم پیروی کارکنان از سیاست‌های امنیت اطلاعات به منظور جلوگیری از ایراد خسارت به این سازمان‌ها تدوین این عوامل به صورت ساختارمند می‌تواند به مدیران، رهبران و سایر ذی‌نفعان بانک‌ها کمک کند تا اقداماتی اثربخش را در راستای رعایت سیاست‌های امنیت اطلاعات و جلوگیری از اقدامات مخاطره‌آمیز از سوی کارکنان انجام دهند. به علاوه، یافته‌های این مطالعه می‌تواند به پوشش خلأ دانشی موجود در حوزهٔ انطباق امنیت اطلاعات، تأکید بر اهمیت و ضرورت توجه به این عوامل و رفتارهای متعاقب از سوی کارکنان بانکی آن‌ها کمک شایانی کند.

بر این اساس، به منظور دستیابی به هدف مذکور و پاسخ به سؤال پژوهش ساختار ادامهٔ این مقاله به ترتیب شامل مبانی نظری و بررسی مطالعات انجام‌شده در این زمینه، تشریح روش پژوهش، ارائهٔ یافته‌های پژوهش در قالب چهارچوب پیشنهادی و بحث و نتیجه‌گیری دربارهٔ این چهارچوب می‌شود.

۱. مبانی نظری و پیشینهٔ پژوهش

سیاست‌های امنیت اطلاعات می‌تواند دربرگیرندهٔ طیف وسیعی از مقاصد، جهت‌گیری، الزامات، مستندات، بخش‌نامه‌ها و دستورالعمل سازمان در حوزهٔ امنیت اطلاعات باشد. بعضی از پژوهشگران سیاست‌های امنیت اطلاعات را در قالب مستنداتی تعریف می‌کنند که کنش‌های انسانی را در مورد امنیت اطلاعات تنظیم یا اهداف امنیت اطلاعات سازمان را بیان می‌کنند (Baskerville and Siponen, 2002). برخی دیگر بیان می‌کنند سیاست‌های امنیت اطلاعات مجموعه‌ای فراگیر از اصول بلندمدت، کلی و مستقل از فناوری هستند که هدف اصلی آن‌ها حصول اطمینان از محرمانگی، یکپارچگی و دسترس‌پذیری داده‌های سازمان است (Järveläinen, 2016). در سال‌های اخیر نیز تعاریفی مانند مجموعه‌ای از دستورالعمل‌ها و فرایندهای سازمانی دربارهٔ امنیت اطلاعات (Uchendu et al., 2021) و مستنداتی شامل مقاصد، اصول، قواعد و دستورالعمل‌های امنیتی لازم‌الاجرا برای کارکنان (Khan et al., 2022) ارائه شده است.

انطباق رفتار کارکنان با این سیاست‌ها موضوعی چندوجهی است که در عوامل گوناگون شکل‌دهندهٔ رفتار انسان ریشه دارد. تاکنون پژوهشگران حوزهٔ امنیت اطلاعات تعاریف متنوعی از مفهوم انطباق ارائه داده‌اند. برخی این مفهوم را به صورت میزان قصد کارکنان برای انطباق یا انطباق واقعی با سیاستی امنیتی تعریف می‌کنند (Herath and Rao, 2009; Bulgurcu et al., 2010)؛ در حالی که برخی دیگر آن را مفهومی نظری می‌دانند که بر برآورده کردن معیارهای سیاست‌های امنیت اطلاعات موجود در سازمان‌ها تأکید دارد و در درجهٔ اول بر رفتار کارکنان تأثیر می‌گذارد تا امنیت اطلاعات در سازمان را تقویت کند (Amankwa et al., 2022). با توجه به تعاریف مختلف و چندوجهی بودن این موضوع عوامل مختلفی می‌توانند بر آن تأثیرگذار باشند.

پژوهشگران برای بررسی و تبیین عوامل مؤثر بر انطباق رفتار کارکنان با سیاست‌های امنیت اطلاعات در

نظام بانکی از نظریه‌های مختلفی، به‌ویژه در حوزه‌های روان‌شناسی (McLeod and Dolezel, 2022) و جرم‌شناسی (Bauer and Bernroider, 2017)، بهره برده‌اند. این نظریه‌ها می‌توانند چهارچوبی برای درک انگیزه‌ها، نگرش‌ها و توجیهاتی باشند که رفتار امنیتی کارکنان را در محیط کار شکل می‌دهند. به علاوه، هر یک از این نظریه‌ها با توجه به علم خاستگاه آن‌ها عوامل متفاوتی را معرفی می‌کنند که می‌توانند بر ابعاد مختلف انطباق داشتن یا نداشتن رفتار کارکنان نظام بانکی با سیاست‌های امنیتی تأثیر بگذارند.

نظریهٔ انگیزش محافظت (Rogers, 1975) یکی از نظریه‌های پرکاربرد در این حوزه است (Ali et al., 2021; Rajab and Eydgahi, 2019). این نظریهٔ برخاسته از علم روان‌شناسی در نسخهٔ بازبینی‌شده خود بیان می‌کند که قصد و انگیزهٔ افراد برای رفتار محافظتی (مانند پیروی از سیاستی امنیتی) از طریق دو فرایند ارزیابی شناختی، یعنی ارزیابی تهدید (بررسی پاداش‌های درونی و بیرونی و شدت آسیب‌پذیری) و ارزیابی تقابل (بررسی کارآمدی پاسخ و خودکارآمدی فرد برای انجام آن) شکل می‌گیرد (Rogers, 1983). بنا بر نتایج این نظریه افراد زمانی به رفتار محافظتی روی می‌آورند که تهدید بر انگیزهٔ آن‌ها تأثیر قابل‌توجهی داشته باشد و توانمندی خود را در مقابله با آن مؤثر بدانند.

یکی دیگر از نظریه‌های پرکاربرد در این زمینه نظریهٔ رفتار برنامه‌ریزی‌شده (Ajzen, 1991) است که قصد رفتاری را به منزلهٔ اصلی‌ترین پیش‌بینی‌کنندهٔ رفتار در نظر می‌گیرد. از دیدگاه این نظریه، که در علم روان‌شناسی ریشه دارد، قصد خود تحت تأثیر سه عامل اصلی قرار دارد: نگرش فرد در برابر رفتار، هنجارهای ذهنی (فشار اجتماعی درک‌شده برای انجام دادن یا انجام ندادن رفتار) و کنترل رفتاری درک‌شده (سهولت یا دشواری درک‌شده برای انجام رفتار). این نظریه به‌طور گسترده برای تحلیل قصد کارکنان به منظور انطباق با سیاست‌های امنیتی به کار رفته است (Sulaiman et al., 2022) که قصد خود می‌تواند بر رفتار تأثیرگذار باشد.

علاوه بر روان‌شناسی، در میان نظریه‌های حوزهٔ جرم‌شناسی نیز نظریهٔ بازدارندگی عمومی (Straub, 1990) مورد توجه پژوهشگران بسیاری قرار گرفته است. این نظریه بر این اصل استوار است که انسان‌ها موجوداتی عقلانی هستند و پیش از ارتکاب عمل هزینه‌ها و منافع آن را می‌سنجند (Straub, 1990). بر این اساس می‌توان با اعمال مجازات از رفتارهای نامطلوب جلوگیری کرد. مؤلفه‌های کلیدی این نظریه شامل قطعیت مجازات (احتمال شناسایی و مجازات شدن)، شدت مجازات و شفافیت آن است. در زمینهٔ امنیت اطلاعات این نظریه برای تبیین تأثیر کنترل‌ها و سیاست‌های تنبیهی سازمان بر کاهش تخلفات کارکنان (Merhi and Ahlu-walia, 2024) که و کاهش انگیزه آن‌ها در ارتکاب اعمال متناقض با سیاست‌های امنیتی شود.

در نهایت، نظریهٔ خنثی‌سازی (Sykes and Mat-za, 1957)، که در حوزهٔ جرم‌شناسی مطرح شد، توضیح می‌دهد که چگونه افراد با استفاده از توجیهات شناختی (تکنیک‌های خنثی‌سازی) هنجارهای اجتماعی را به شکلی موقت نادیده می‌گیرند و به خود اجازهٔ ارتکاب رفتار انحرافی را می‌دهند. تکنیک‌هایی مانند انکار مسئولیت، انکار خسارت و محکوم کردن محکوم‌کنندگان به کارکنان این امکان را می‌دهد تا رفتار غیر منطبق با سیاست‌های امنیتی را برای خود منطقی جلوه دهند (Bansal et al., 2021) و انگیزهٔ تکرار این اعمال را در آینده داشته باشند.

بر اساس نظریه‌های فوق، پژوهشگران در مطالعات تجربی خود عوامل مؤثر بر انطباق با سیاست‌های امنیت اطلاعات در نظام بانکی را بررسی و ابعاد مختلفی از این پدیده را روشن کرده‌اند. در زمینهٔ استفاده از نظریه‌های روان‌شناسی، یانسن و فان سخایک با استفاده از نظریهٔ انگیزش محافظت و ترکیب آن با نظریهٔ کنش منطقی (Ajzen and Fishbein, 1973) پژوهشی را در میان کارکنان بانکی کشور هلند انجام دادند (Jansen and Van Schaik, 2017). مدل ترکیبی این پژوهشگران نشان داد رفتارهای احتیاطی آنلاین به شدت تحت تأثیر کارآمدی پاسخ، نگرش به رفتار و خودکارآمدی هستند؛ همچنین یانسن و فان سخایک رفتارهای احتیاطی افراد در مقابله با کلاه‌برداری‌های اینترنتی در زمینهٔ بانکی را هدف قرار دادند و با استفاده از همین نظریه مدلی را طراحی و در کشور هلند آزمایش کردند (Jansen and van Schaik, 2018). پژوهش آن‌ها نشان داد عوامل دخیل در ارزیابی تهدید و ارزیابی تقابل انگیزش محافظت افراد را به درستی پیش‌بینی می‌کنند؛ همچنین کارآمدی پاسخ و خودکارآمدی مهم‌ترین عوامل پیش‌بینی‌کننده اقدامات احتیاطی هستند.

کاتازی و بولگورجو[1] (۲۰۱۳) به بررسی انطباق کارکنان با الزامات امنیتی از منظر تشدید تعهد پرداختند. آن‌ها با بهره‌گیری از نظریهٔ رفتار برنامه‌ریزی‌شده و نظریهٔ نمایندگی مدلی متشکل از عوامل موانع کاری، تقارن نداشتن اطلاعات، ایمنی منابع و آگاهی از امنیت اطلاعات برای تبیین نگرش کارکنان دربارهٔ انطباق با سیاست‌های امنیت اطلاعات ارائه دادند. ویلیامز[2] و همکاران (۲۰۱۹) نیز با تکیه بر این نظریه و ادغام آن با نظریهٔ خودکارآمدی (Bandura, 1977) عوامل رفتاری داخلی و خارجی تأثیرگذار بر انطباق با استانداردها و سیاست‌های امنیت اطلاعات را در بانک‌های نیجریه بررسی کردند. در این پژوهش، عوامل داخلی شامل اثربخشی درک‌شده، آگاهی از تهدیدات امنیت اطلاعات و سوگیری‌های ادراکی و عوامل خارجی شامل شدت جریمه، قطعیت تشخیص و باورهای هنجاری بودند. نظری[3] (۲۰۲۰) در پژوهشی به بررسی عوامل اثرگذار بر پذیرش سیاست‌های امنیت اطلاعات در میان کارمندان بانک تجارت پرداخت. او نظریهٔ رفتار برنامه‌ریزی‌شده و نظریهٔ کنش منطقی را در کنار هم به کار گرفت و نشان داد طرز تفکر کارکنان دربارهٔ سیاست‌های امنیت اطلاعات، هنجارهای ذهنی و توصیفی، تعهد سازمانی و خودباوری بر پذیرش سیاست‌های امنیت اطلاعات از سوی این کارمندان تأثیر دارد. هاشم‌زاده اقدم[4] (۲۰۲۱) نیز تأثیر حمایت مدیریتی بر رفتار انطباقی کارکنان بانک‌های استان آذربایجان شرقی را با نقش میانجی اعتماد درک‌شده و خودکارآمدی سنجید. بنیان پژوهش او نیز بر همین نظریه بود و نشان داد حمایت مدیریتی بر اعتماد درک‌شده و خودکارآمدی تأثیر مثبتی دارد و در نتیجه سبب تقویت رفتار انطباقی کارکنان بانک‌ها خواهد شد.

در زمینهٔ استفاده از نظریه‌های جرم‌شناسی، ته[5] و همکاران (۲۰۱۵) با استفاده از ترکیبی از نظریهٔ خنثی‌سازی و نظریهٔ مبادلهٔ اجتماعی (Homans, 1958) در صنعت بانکداری، به بررسی عوامل مؤثر بر به‌کارگیری تکنیک‌های خنثی‌سازی توسط کارکنان پرداختند. یافته‌های آن‌ها نشان می‌دهد تعهد سازمانی تأثیر منفی و تعارض نقش تأثیر مثبتی بر استفاده از این توجیهات برای نقض سیاست‌های امنیتی دارد. به علاوه، باوئر[6] و همکاران (۲۰۱۷) با اشاره به نظریهٔ خنثی‌سازی بر موضوع تأثیر آگاهی‌رسانی امنیت اطلاعات بر ارتقای رفتارهای منطبق با سیاست‌های امنیت اطلاعات تمرکز کردند و تأثیر روش‌های ترکیبی آگاهی‌رسانی، راهبرد بلندمدت برنامهٔ آگاهی‌رسانی، ارتباط دوطرفه غیر تکنوکراتیک (با بیان ساده و قابل درک برای کاربران عادی) و تمایز قائل شدن در مخاطبان هدف بر انطباق رفتاری و همچنین تأثیر برنامه‌های آگاهی‌رسانی بر کاهش استفاده از تکنیک‌های خنثی‌سازی را بررسی کردند. بائر و برنرویدر[7] (۲۰۱۷) نیز در تحقیقی، که با ترکیب نظریه‌های کنش منطقی و خنثی‌سازی در بانکی بین‌المللی انجام دادند، نشان دادند نگرش به انطباق با سیاست‌های امنیتی مهم‌ترین متغیر پیش‌بینی‌کنندهٔ رفتار انطباقی کارکنان است. این یافته بر اهمیت شکل‌دهی به نگرش مثبت کارکنان از طریق برنامه‌های آگاهی‌رسانی و ارتباطات مؤثر تأکید دارد.

علاوه بر نظریه‌ها و تحقیقات ذکرشده پژوهشگران دیگری با استفاده از سایر نظریه‌ها به بررسی عوامل تأثیرگذار بر انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات پرداخته‌اند. چوی و یو[8] (۲۰۱۴) در مطالعه‌ای مبتنی بر نظریهٔ مبادلهٔ اجتماعی (Homans, 1958) در بانک‌های کرهٔ جنوبی، تأثیر شیوه‌های مدیریت منابع انسانی را بر انطباق با سیاست‌های حریم خصوصی اطلاعات بررسی کردند. آن‌ها دریافتند اقداماتی مانند پاداش منصفانه، ارزیابی توسعه‌گرا و آموزش فراگیر از طریق تقویت تعهد سازمانی به افزایش قصد کارکنان برای انطباق با سیاست‌ها منجر می‌شود. فان در کلی[9] و همکاران (۲۰۲۰) بر این باورند که فناوری به تنهایی نمی‌تواند از وقوع رخدادهای امنیتی جلوگیری کند. سازمان‌ها نیز نیازمند پیروی کاربران از سیاست‌های امنیتی‌اند. آن‌ها در پژوهش خود دربارهٔ پیشگیری از نشت داده‌ها، که در میان کارکنان دو بانک بین‌المللی در هلند انجام شد، مدلی از نحوهٔ تعامل سازه‌های روانی ظرفیت (دانش)، فرصت و انگیزه ارائه می‌دهند. نتایج این پژوهش نشان می‌دهد ظرفیت بر رفتار پیشگیرانه و انگیزه و فرصت بر ظرفیت تأثیر دارند.

1. Kajtazi and Bulgurcu
2. Williams
3. Nazari
4. Hashemzadeh Aghdam
5. Teh
6. Bauer
7. Bauer and Bernroider
8. Choi and Yoo
9. Van der Kleij

کام[1] و همکاران (۲۰۲۱) نیز با بهره‌گیری از مدل ارزش‌های رقابتی به بررسی تأثیر فرهنگ سازمانی بر انطباق در صنعت بانکداری پرداختند. نتایج تحقیق آن‌ها حاکی از آن بود که فرهنگ‌های سلسله‌مراتبی و منطقی، که بر کنترل و ثبات تأکید دارند، به‌خوبی می‌توانند هنجارهای ذهنی امنیتی را میان کارکنان تقویت کنند. در مقابل، فرهنگ‌های کارآفرینانه و تیمی در این زمینه تأثیرگذاری کمتری دارند. این یافته بر نقش حیاتی ساختار و فرهنگ رسمی سازمان در پیشبرد اهداف امنیتی دلالت دارد. بوتلر و براون[2] (۲۰۲۳) با بهره‌گیری از نظریهٔ فرهنگ سازمانی نحوهٔ تأثیر اختلالات محیطی ناشی از همه‌گیری بیماری کووید-۱۹ بر فرهنگ امنیت اطلاعات و فرهنگ سازمانی و تأثیر این دو بر رفتارهای منطبق بر سیاست‌های امنیت اطلاعات کارمندان را در شرکت فناوری مالی بررسی کردند. آن‌ها نشان دادند پیامدهای این همه‌گیری سبب کنترل بیشتر و انعطاف‌پذیری بالاتر در فرهنگ امنیت اطلاعات و فرهنگ سازمانی می‌شود و این موارد بر ارتقای انطباق رفتار کارمندان با سیاست‌های امنیت اطلاعات نیز تأثیر معناداری دارد.

عواملی که هر یک از پژوهشگران گزارش کرده‌اند ممکن است بر ابعاد مختلف تعیین‌کنندهٔ رفتارهای امنیتی تأثیر بگذارد. بر اساس سیستم COM-B مؤلفه‌های اساسی لازم برای درک و طراحی مداخلات تغییر رفتار را می‌توان به سه دستهٔ قابلیت، فرصت و انگیزه تقسیم کرد (Michie et al., 2011). مؤلفهٔ قابلیت به مهارت‌های فیزیکی و روان‌شناختی اشاره دارد که در پژوهش حاضر می‌تواند شامل آگاهی، دانش و مهارت‌های کارکنان در حوزهٔ امنیت اطلاعات باشد. مؤلفهٔ فرصت شامل شرایط محیطی و اجتماعی است که انجام رفتار را تسهیل یا از ارتکاب آن ممانعت می‌کند و در پژوهش حاضر می‌تواند شامل حمایت‌های مدیران سازمان و وجود نظام‌های پاداش تنبیه باشد. مؤلفهٔ انگیزه نیز دربرگیرندهٔ انگیزهٔ بازتابی (فرایندهای خودآگاه و عمدی) و انگیزش خودکار (پاسخ‌های ناخودآگاه و عاطفی) است که فرد را به انجام دادن رفتارهای مشخص سوق می‌دهد و در این پژوهش عواملی مانند تعهد سازمانی و نگرش کارکنان می‌توانند در این دسته قرار گیرند. این سیستم را می‌توان مرجعی برای دسته‌بندی هر یک از عوامل معرفی‌شده در مطالعات پیشین در حوزهٔ رفتارهای امنیت اطلاعات قرار داد.

با وجود پژوهش‌های متعدد در زمینهٔ انطباق رفتار کارکنان با سیاست‌های امنیت اطلاعات همچنان به چهارچوبی جامع برای بررسی این موضوع در نظام بانکی نیاز است. ادبیات موضوعی بدون چهارچوبی جامع از عوامل تأثیرگذار بر انطباق رفتار کارکنان با سیاست‌های امنیت اطلاعات در نظام بانکی است. تدوین آن نیز به بهره‌گیری از سیستم COM-B می‌تواند در شناسایی و دسته‌بندی عوامل مؤثر بر رفتارهای امنیتی، بهبود رفتارهای امنیتی کارکنان و به دنبال آن ارتقای فرهنگ امنیت اطلاعات در بانک‌ها نقش مهمی ایفا کند. در بخش بعدی، نحوهٔ تدوین چهارچوب انطباق رفتار کارکنان نظام بانکی با سیاست‌های امنیت اطلاعات با استفاده از روش فراترکیب ارائه خواهد شد.

۲. روش‌شناسی

در پژوهش حاضر، برای بررسی عوامل تأثیرگذار بر انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات از الگوی تفسیری، رویکرد کیفی و روش فراترکیب بهره گرفته شده است. روش فراترکیب مرور و مطالعهٔ نظام‌مند یافته‌های کیفی موجود در مطالعات مرتبط، مقایسهٔ انواع مختلف داده‌ها با توجه به کیفیت و قابلیت کاربرد آن‌ها و همچنین ترکیب و تفسیر یافته‌های پژوهشی مربوط به پدیده‌ای یکسان است (Dawson, 2019). این روش می‌تواند تصویری جامع و ارزشمند از یافته‌های موجود ارائه دهد، دیدگاه‌های نوینی در خصوص موضوعی خاص فراهم کند (Edwards and Kaimal, 2016) و به منزلهٔ الگویی ساختاریافته برای تحلیل یافته‌های کیفی و استخراج مفاهیم است (Afshari et al., 2024).

در پژوهش حاضر، به دلیل تعدد و تنوع مطالعات در زمینهٔ انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات، روش فراترکیب انتخاب شده است که امکان یکپارچه‌سازی و ارائهٔ چهارچوبی جامع از یافته‌های کیفی موجود دربارهٔ عوامل مؤثر بر انطباق و رفتار امنیتی را فراهم می‌کند. با استفاده از این روش، امکان تلفیق و بررسی یافته‌های مطالعات کیفی فراهم می‌آید و درکی عمیق و چهارچوبی جامع از عوامل مؤثر در این حوزه حاصل می‌شود. در این راستا، روش هفت‌مرحله‌ای سندلوفسکی و باروسو[3] (۲۰۰۷) برای انجام فراترکیب به کار گرفته شده است. خلاصهٔ این هفت مرحله در شکل ۱ آمده است.

1. Kam
2. Butler and Brown
3. Sandelowski and Barroso

شکل ۱: مراحل اجرای فراترکیب

۲-۱. بیان مسئله، سؤال و اهداف تحقیق

با توجه به نبود چهارچوبی جامع برای انطباق رفتار کارکنان با سیاست‌های امنیت اطلاعات و به منظور نیل به هدف اصلی این پژوهش، یعنی شناسایی عوامل مؤثر بر انطباق رفتار کارکنان با سیاست‌های امنیت اطلاعات در نظام بانکی، سؤال اصلی این پژوهش به شرح زیر مطرح شد:

عوامل مؤثر بر انطباق رفتار کارکنان نظام بانکی با سیاست‌های امنیت اطلاعات چیست؟

۲-۲. جست‌وجوی منابع

برای شناسایی و گردآوری مطالعات مرتبط جست‌وجویی نظام‌مند در پایگاه‌های اطلاعاتی بین‌المللی بدون محدودیت زمانی انجام شد. شامل:

ScienceDirect, Web of Science, Google Scholar , Scopus

فرایند جست‌وجو با استفاده از کلیدواژه‌های اصلی مرتبط با حوزهٔ پژوهش به شرح زیر و جست‌وجو در قسمت‌های عنوان، چکیده و کلیدواژه‌های مقالات موجود در پایگاه‌های مذکور صورت گرفت:

(information security OR cybersecurity OR cyber-security OR cyber security) AND (policy OR policies OR governance OR management OR audit OR procedure OR process OR instruction OR strateg OR practice OR guideline OR rule OR law OR regulat OR legislat) AND (culture OR compli OR behavior OR conform OR adopt OR adhere OR comply) AND (bank OR financ)

برای انتخاب مقالات مرتبط با موضوع این پژوهش از دستورالعمل PRISMA استفاده شد (Page et al., 2021) که روشی مرسوم برای گزینش مقالات واحد شرایط در مقالات مروری و فراترکیب است (Pourkarimi, 2025). معیارهای ورود به این مطالعه شامل همهٔ اسناد علمی (اعم از کیفی و کمی) منتشرشده به زبان انگلیسی در پایگاه‌های ذکرشده بود که به بررسی عوامل مؤثر بر انطباق رفتار کارکنان با سیاست‌های امنیت اطلاعات در صنعت بانکداری پرداخته بودند. مقالات مروری، مجموعه مقالات کنفرانس و مطالعاتی که در صنایعی غیر از بانکداری انجام شده بودند، از فرایند بررسی حذف شدند.

جست‌وجوی اولیه به شناسایی ۱۹۵۰ مقاله منتهی شد. پس از حذف ۹۰۲ مورد فاقد معیارهای شمول اولیه (زبان انگلیسی و متعلق به مجلات)، ۱۰۴۸ مورد از مجموع پایگاه‌های مختلف باقی ماند که پس از حذف ۲۰۳ مورد تکراری، عناوین و چکیده ۸۴۵ مقالهٔ باقی‌مانده بر اساس میزان ارتباط با موضوع پژوهش غربالگری شدند. در نهایت،

شکل ۲: مراحل انتخاب مقالات بر اساس دستورالعمل PRISMA

متن کامل مقالاتی که ارتباط احتمالی با موضوع داشتند به دقت ارزیابی شدند و ۷۴ مقاله برای تحلیل نهایی در فرایند فراترکیب انتخاب شدند. خلاصهٔ نتایج فرایند غربالگری در شکل ۲ آمده است.

۲-۳. ارزیابی کیفیت

کیفیت مطالعات منتخب با استفاده از ابزار استاندارد ارزیابی انتقادی (CASP) سنجیده شد. این ابزار با بررسی طرح، روش و شیوهٔ گزارش‌دهی مطالعات منتخب، به ارزیابی نظام‌مند روایی، پایایی و ارتباط یافته‌های هر مطالعه با اهداف پژوهش کمک می‌کند (Nadelson and Nadelson, 2014). این روش شامل ۱۰ سؤال ۵ امتیازی است که پژوهشگر را در تحلیل کیفیت، دقت، اهمیت و اعتبار مقالات یافت‌شده یاری می‌دهد تا با حذف مقالات بدون کیفیت مناسب‌ترین مقالات را برای پژوهش خود برگزیند (Campbell et al., 2003). در این پژوهش، مقالاتی که حداقل ۳۰ امتیاز از ۵۰ امتیاز ممکن در این روش را کسب کردند واجد شرایط تشخیص داده شدند. بدین ترتیب، ۷ مقاله از ۷۴ مقاله انتخاب‌شده در مرحلهٔ قبل امتیازی کمتر از ۳۰ کسب کردند؛ بنابراین با حذف آن‌ها در نهایت ۶۷ مقاله برای تجزیه و تحلیل یافته‌ها و استخراج مطالب مرتبط با این پژوهش انتخاب شدند.

۲-۴. طبقه‌بندی یافته‌های گزارش‌ها

در این مرحله، یافته‌های حاصل از گزارش‌های بررسی‌شده و منتخب به دسته‌های مختلف تقسیم شدند تا انتخاب روش مناسب برای ترکیب آن‌ها در گام بعدی تسهیل شود. این فرایند، که به نوع‌شناسی یافته‌ها اشاره دارد، داده‌ها را بر مبنای میزان تغییر و تبدیل آن‌ها گروه‌بندی می‌کند (Sandelowski and Barroso, 2007). در این تحقیق، ابتدا داده‌ها از محتوای آشکار مطالعات به صورت اسمی و موضوعی استخراج و در قالب جدولی اولیه سازمان‌دهی شدند که می‌توان آن را به‌منزلهٔ مرحلهٔ زمینه‌سازی موضوعی تلقی کرد. در گام بعد، با تحلیل عمیق‌تر الگوهای پنهان و مضامین مشترک شناسایی شدند و داده‌ها به شکلی نظام‌مندتر سازمان‌دهی و مرتب شدند که معادل زمینه‌سازی مضمونی است. پس از آن، داده‌ها با تکیه بر نظریه‌های انگیزش محافظت، کنش منطقی و بازدارندگی بازتفسیر و در قالب مفاهیم کلیدی ترکیب شدند. این مرحله با عنوان توصیف مفهومی شناخته می‌شود. در نهایت به منظور ارائهٔ تبیینی‌تفسیری، یافته‌ها با نظریه‌های موجود تطبیق داده و در قالب چهارچوبی منسجم ارائه شدند.

۲-۵. ترکیب یافته‌ها

در این پژوهش از رویکرد فراترکیب کیفی برای ترکیب یافته‌ها استفاده شد. مفاهیم برگرفته از نظریه‌های بنیادین مرتبط با انطباق رفتاری کارکنان با سیاست‌های امنیت اطلاعات در صنعت بانکداری تحلیل شدند. تلفیق ارتباطات معنایی میان این عوامل نیز در قالب چهارچوب مفهومی یکپارچه صورت گرفت. این چهارچوب را می‌توان توسعه‌ای مرکب از نظریه‌های پیشین به شمار آورد. بر همین اساس، در این مطالعه از روش تحلیل طبقه‌بندی سندلوفسکی و باروسو در فراترکیب کیفی به منظور تلفیق و ترکیب نظام‌مند یافته‌ها بهره گرفته شده است. به علاوه، از روش تحلیل مضمون و نرم‌افزار مکس‌کیودا[1] ۲۰۲۴ برای مدیریت کدگذاری، تحلیل و یکپارچه‌سازی داده‌های استخراج‌شده استفاده شد (Braun and Clarke, 2006).

۲-۶. روایی یافته‌ها

روایی پژوهش‌های فراترکیب از روش‌های گوناگونی قابل بررسی است. برای ارزیابی و تضمین روایی فرایند این پژوهش از روش‌های مسیر حسابرسی و روایی توافقی مذاکره‌شده استفاده شد (Sandelowski and Barroso, 2007). روش مسیر حسابرسی از طریق مستندسازی کامل تمام مراحل و تصمیم‌ها انجام شد. به علاوه حصول روایی توافقی مذاکره‌شده اعضای تیم پژوهش با برگزاری جلسات حضوری برای بررسی این اسناد، همهٔ مستندات را بررسی کردند تا برای عبور از هر مرحلهٔ پژوهش توافق میان تمامی اعضای تیم شکل گیرد. در نهایت، کدهای استخراجی، مفاهیم شاخته‌شده و دسته‌بندی‌های ایجادشدهٔ پژوهشگران با نظر دو خبره مستقل مقایسه شد تا روایی و کیفیت نتایج پژوهش تضمین شود (Leung, 2015).

۲-۷. ارائهٔ یافته‌ها

در این گام، خروجی‌های نهایی حاصل از تحلیل‌های صورت‌پذیرفته در قالب جدول‌ها و نمودارها ارائه شده‌اند. جدول‌های خروجی شامل محل یافتن کدها در مقالات منتخب، فراوانی کدهای شمارش‌شده و ترکیب آن‌ها برای ساختن مضامین‌اند؛ همچنین نمودارهای نقشهٔ ارتباط کدها و مضامین و ابر کدها در نرم‌افزار مکس‌کیودا ۲۰۲۴ برای ارائهٔ بصری از تحلیل یافته‌ها استفاده شدند. به علاوه، برای ترسیم ابر کلمات پرتکرار از نرم‌افزار ان‌ویوو[2] ۲۰ استفاده شد (Lu and Phillips, 2018). خروجی این تحلیل‌ها شامل جدول‌ها و نمودارهای مربوط در بخش بعدی با ذکر جزئیات ارائه می‌شوند.

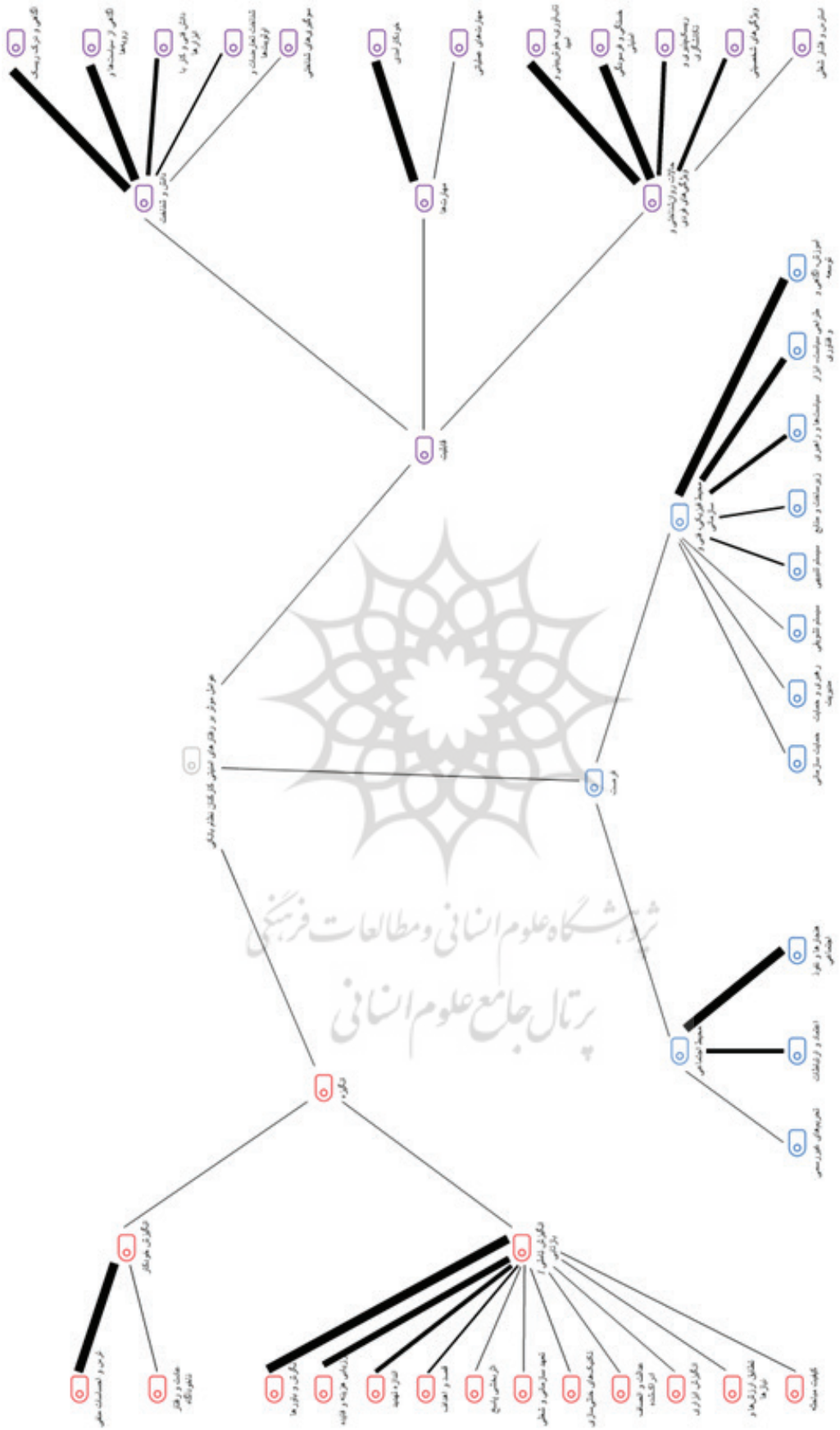
۳. یافته‌ها

این پژوهش با بهره‌گیری از روش فراترکیب و تحلیل عمیق ۶۷ مطالعهٔ منتخب به شناسایی و طبقه‌بندی عوامل مؤثر بر انطباق رفتار کارکنان نظام بانکی با سیاست‌های امنیت اطلاعات پرداخته است. به منظور ایجاد چهارچوبی یکپارچه و جامع عوامل مستخرج بر اساس مدل رفتار COM-B، که رفتار را محصول تعامل سه بعد اصلی قابلیت، فرصت و انگیزه می‌داند، سازمان‌دهی شدند. جدول ۱ خلاصه‌ای از این یافته‌ها را به همراه منابع مرجع و تعداد تکرار آن‌ها در این منابع ارائه می‌دهد که در ادامهٔ این بخش به تفصیل تشریح می‌شوند.

برای درک بهتر روابط و اهمیت این عوامل نقشه‌ای مفهومی با استفاده از نرم‌افزار مکس‌کیودا ترسیم شد (شکل ۳). در این نقشه، هر مفهوم (کد) به صورت یک گره نمایش داده شده و ضخامت خطوط ارتباطی میان گره‌ها،

1. MaxQDA

2. Nvivo



شکل ۳: نقشهٔ ارتباط کدها و مضامین مرتبط با عوامل مؤثر بر رفتارهای امنیتی کارکنان نظام بانکی

متناسب با فراوانی تکرار آن‌ها در منابع است. این نمایش بصری به روشنی بیانگر این است که ابعاد انگیزه و فرصت به مراتب وزن بیشتری از بعد قابلیت در ادبیات داشته‌اند. به طور خاص، مضامین نگرش و باورها (در بعد انگیزه)، آموزش، آگاهی و توسعه (در بعد فرصت)، ارزیابی هزینه و فایده (در بعد انگیزه) و هنجارها و نفوذ اجتماعی (در بعد فرصت) کانون‌های اصلی و پرتکرار این شبکهٔ مفهومی‌اند که در ادامه با ذکر جزئیات ارائه می‌شوند.

۳-۱. قابلیت: فراتر از دانش

بعد قابلیت به دانش و شناخت، مهارت‌ها و حالات روان‌شناختی و ویژگی‌های فردی کارکنان برای رفتار منطبق با سیاست‌های امنیت اطلاعات اشاره دارد. تحلیل یافته‌های پژوهش نشان می‌دهد دو مضمون فرعی آگاهی و درک ریسک و آگاهی از سیاست‌ها و رویه‌ها هر یک با ۱۳ تکرار بیشترین فراوانی را میان مؤلفه‌های زیرمجموعهٔ دانش و شناخت به خود اختصاص داده‌اند. این هم‌وزنی تأکیدی است بر این نکتهٔ کلیدی که تنها آگاه کردن کارکنان از ریسک‌های امنیت اطلاعات کافی نیست، بلکه آن‌ها باید به همان اندازه با رویه‌های عملیاتی سازمان برای مقابله با این خطرها نیز آشنا باشند. این دو مضمون در کنار دانش فنی (با ۷ تکرار)، بنیان قابلیت‌های شناختی را تشکیل می‌دهند.

با این حال، مهم‌ترین یافته در بعد قابلیت امتیاز چشمگیر مضمون خودکارآمدی با ۱۸ تکرار است. این فراوانی زیاد گویای این است که انطباق امنیتی تنها مسئله‌ای دانشی نیست، بلکه به شکلی عمیق به باور و اعتماد کارکنان به توانایی خود برای اجرای موفقیت‌آمیز رفتارهای امنیتی وابسته است. کارمندی که حتی با وجود دانش کافی خود را در برابر تهدیدات ناتوان ببیند، ظرفیت بیشتری برای بروز رفتار نامنطبق از خود دارد. علاوه بر این، مفاهیم نوظهوری مانند خستگی و فرسودگی امنیتی (۴ تکرار) و تاب‌آوری (۴

جدول ۱: کدها و مضامین اصلی و فرعی انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات

ابعاد مفهومی	مضامین اصلی	مضامین فرعی	منابع*	مجموع تعداد یافت‌شده
قابلیت	دانش و شناخت	آگاهی و درک ریسک	۵ و ۹ و ۱۰ و ۱۶ و ۲۱ و ۲۴ و ۲۸ و ۳۳ و ۳۵ و ۴۵ و ۴۶ و ۶۰ و ۶۳	۱۳
		آگاهی از سیاست‌ها و رویه‌ها	۱۱ و ۱۳ و ۱۶ و ۱۷ و ۲۰ و ۲۶ و ۳۳ و ۴۲ و ۴۴ و ۴۵ و ۴۹ و ۵۴ و ۵۶	۱۳
		دانش فنی و کار با ابزارها	۵ و ۴۸ و ۴۹ و ۵۰ و ۵۳ و ۶۳ و ۶۶	۷
		شناخت تعارضات و اولویت‌ها	۱۰ و ۱۲ و ۲۱ و ۲۳	۴
		سوگیری‌های شناختی	۲۸ و ۵۱	۲
	مهارت‌ها	مهارت‌های عملیاتی	۶ و ۷ و ۲۱ و ۵۹	۴
		خودکارآمدی	۲ و ۶ و ۷ و ۹ و ۱۰ و ۱۹ و ۲۱ و ۲۷ و ۲۹ و ۳۳ و ۳۹ و ۴۹ و ۵۳ و ۵۵ و ۵۸ و ۵۹ و ۶۲ و ۶۳	۱۸
	حالات روان‌شناختی و ویژگی‌های فردی	تاب‌آوری، خوش‌بینی و امید	۶ و ۲۱ و ۴۹ و ۵۹	۴
		خستگی و فرسودگی امنیتی	۵ و ۳۴ و ۴۹ و ۶۶	۴
		استرس و فشار شغلی	۶۶	۱
		ریسک‌پذیری و تکانش‌گری	۳ و ۴۱	۲
		ویژگی‌های شخصیتی	۴۱ و ۵۹	۲

ابعاد مفهومی	مضامین اصلی	مضامین فرعی	منابع*	مجموع تعداد یافت‌شده
فرصت	محیط فیزیکی، فنی و سازمانی	زیرساخت و منابع	۱۰ و ۱۴ و ۱۸ و ۲۰ و ۲۱ و ۲۴ و ۳۱ و ۳۵ و ۳۷ و ۵۴ و ۵۹ و ۶۰ و ۶۶	۱۳
		طراحی سیاست، ابزار و فناوری	۱ و ۵ و ۱۱ و ۲۰ و ۲۳ و ۲۴ و ۲۵ و ۳۵ و ۳۶ و ۴۷ و ۴۹ و ۵۰ و ۵۳ و ۵۹ و ۶۰ و ۶۱ و ۶۶ و ۶۷	۱۸
		سیاست‌ها و راهبری	۱ و ۱۵ و ۱۹ و ۲۳ و ۲۴ و ۳۱ و ۳۴ و ۳۷ و ۳۸ و ۴۰ و ۴۳ و ۴۵ و ۴۷ و ۵۲ و ۵۷ و ۵۹ و ۶۷	۱۷
		رهبری و حمایت مدیریت	۱۹ و ۲۴ و ۲۵ و ۳۰ و ۴۵ و ۴۷ و ۵۴	۷
		آموزش، آگاهی و توسعه	۱ و ۵ و ۱۰ و ۱۱ و ۱۲ و ۱۳ و ۲۲ و ۲۳ و ۲۴ و ۲۵ و ۳۱ و ۳۳ و ۳۷ و ۳۸ و ۳۹ و ۴۰ و ۴۲ و ۴۳ و ۴۵ و ۴۸ و ۵۴ و ۵۶ و ۵۷ و ۵۹ و ۶۰ و ۶۵ و ۶۶ و ۶۷	۲۸
		سیستم تنبیهی	۴ و ۵ و ۶ و ۱۴ و ۱۷ و ۱۹ و ۲۱ و ۲۳ و ۲۵ و ۲۷ و ۵۹ و ۶۱ و ۶۴	۱۳
		سیستم تشویقی	۳ و ۱۰ و ۱۴ و ۲۳ و ۲۵ و ۴۳ و ۵۷ و ۵۸ و ۶۰ و ۶۷	۱۰
		حمایت سازمانی	۲ و ۱۵ و ۱۶ و ۲۲	۴
	محیط اجتماعی	هنجارها و نفوذ اجتماعی	۱۷ و ۱۸ و ۱۹ و ۲۱ و ۲۲ و ۲۳ و ۲۴ و ۲۷ و ۳۲ و ۳۵ و ۳۹ و ۴۰ و ۴۴ و ۴۶ و ۴۷ و ۵۳ و ۵۵ و ۵۹ و ۶۱ و ۶۲ و ۶۴	۲۱
		تحریم‌های غیررسمی	۴ و ۳۹ و ۶۱	۳
		اعتماد و ارتباطات	۳۳ و ۳۸ و ۴۵ و ۴۶ و ۴۷ و ۴۸ و ۵۴ و ۵۹ و ۶۰ و ۶۴ و ۶۶	۱۱
انگیزه	انگیزش تأملی / بازتابی	نگرش و باورها	۱ و ۲ و ۵ و ۷ و ۸ و ۹ و ۱۰ و ۱۱ و ۱۲ و ۱۵ و ۱۶ و ۱۷ و ۱۸ و ۱۹ و ۲۱ و ۲۲ و ۲۳ و ۲۴ و ۲۵ و ۲۶ و ۲۸ و ۳۰ و ۳۱ و ۳۲ و ۳۶ و ۳۷ و ۴۰ و ۴۲ و ۴۴ و ۴۶ و ۴۷ و ۴۸ و ۵۰ و ۵۳ و ۵۴ و ۵۵ و ۵۶ و ۵۹ و ۶۲	۳۹
		قصد و اهداف	۷ و ۹ و ۲۰ و ۲۱ و ۲۳ و ۲۵ و ۳۶ و ۴۳ و ۴۴ و ۴۶ و ۴۸ و ۵۵ و ۵۷ و ۵۸ و ۶۱ و ۶۲ و ۶۳	۱۷
		ارزیابی هزینه و فایده	۲ و ۳ و ۵ و ۱۲ و ۱۸ و ۱۹ و ۲۱ و ۲۳ و ۲۵ و ۲۶ و ۲۷ و ۲۸ و ۳۰ و ۳۲ و ۳۳ و ۳۴ و ۳۶ و ۳۹ و ۴۲ و ۴۷ و ۴۹ و ۵۱ و ۵۸ و ۵۹	۲۴
		اندازهٔ تهدید	۲ و ۳ و ۵ و ۶ و ۷ و ۱۰ و ۱۳ و ۱۹ و ۲۳ و ۲۷ و ۲۹ و ۳۳ و ۴۴ و ۵۰ و ۵۱ و ۵۳ و ۵۵ و ۵۸ و ۵۹ و ۶۲	۲۰
		اثربخشی پاسخ	۲ و ۶ و ۷ و ۲۹ و ۳۳ و ۴۹ و ۵۸ و ۵۹ و ۶۴	۹
		تطابق ارزش‌ها و نیازها	۴۷	۱
		عدالت و انصاف ادراک‌شده	۸ و ۱۲	۲
		تعهد سازمانی و شغلی	۴۳ و ۴۸ و ۵۲ و ۵۹ و ۶۰	۵
		انگیزش ابزاری	۵۹ و ۶۴	۲
		تکنیک‌های خنثی‌سازی	۷ و ۳۴ و ۴۵ و ۴۶ و ۵۲	۵
		کیفیت مباحثه	۲۹	۱
	انگیزش خودکار	ترس و احساسات منفی	۲ و ۵ و ۷ و ۱۰ و ۱۴ و ۱۸ و ۲۱ و ۲۳ و ۲۴ و ۳۴ و ۴۰ و ۵۰	۱۲
		عادت و رفتار ناخودآگاه	۱۱ و ۲۳ و ۵۸ و ۵۹	۴

تکرار) دلالت بر اهمیت فزایندهٔ مضامین مربوط به حالات روان‌شناختی کارکنان در محیط کاری پرتنش بانکی دارند که می‌توانند قابلیت این کارکنان را در انطباق با سیاست‌های امنیتی تقویت یا تضعیف کنند.

۳-۲. فرصت: اهمیت بسترهای سازمانی و اجتماعی

بعد فرصت به عوامل محیطی خارج از فرد می‌پردازد که رفتار را ممکن یا محدود می‌کنند. یافته‌های پژوهش نشان می‌دهد سازمان‌ها نقشی حیاتی در شکل‌دهی به این فرصت‌ها دارند. مضمون آموزش، آگاهی و توسعه با ۲۸ تکرار پرتکرارترین عامل در این بعد است که زیرمجموعهٔ محیط فیزیکی، فنی و سازمانی قرار می‌گیرد. این موضوع بیانگر آن است که در ادبیات علمی، برنامه‌های آموزشی یکی از مهم‌ترین ابزارهای سازمانی برای توانمندسازی و فراهم کردن فرصت برای رفتار امن کارکنان بانکی شناخته می‌شوند. پس از آن، طراحی سیاست، ابزار و فناوری (۱۸ تکرار) و سیاست‌ها و راهبری (۱۷ تکرار) قرار دارند که نشان می‌دهند کیفیت، وضوح و کاربرپسند بودن سیاست‌ها و ابزارهای امنیتی در کنار سیاست‌های مطرح در زمینهٔ هدایت و راهبری کلان سازمان تأثیری مستقیم بر امکان‌پذیری انطباق دارند.

در حوزهٔ محیط اجتماعی نیز مضمون هنجارها و نفوذ اجتماعی با ۲۱ تکرار عاملی قدرتمند است. این یافته تأیید می‌کند رفتار همکاران و مدیران و فرهنگ غالب در نهاد مالی و بانکی می‌تواند به مراتب تأثیرگذارتر از دستورالعمل‌های رسمی باشد. انطباق داشتن یا نداشتن رفتار کارمند اغلب تحت تأثیر رفتار گروهی، انتظارات و تحریم‌های غیر رسمی از سوی همکارانش شکل می‌گیرد. این امر اهمیت ایجاد فرهنگ امنیت را به منزلهٔ فرصتی اجتماعی برجسته می‌کند.

۳-۳. انگیزه: کانون تأثیرگذاری بر انطباق

بعد انگیزه شامل فرایندهای مغزی است که به رفتار کارکنان جهت و نیرو می‌بخشد. یافته‌های این پژوهش نشان می‌دهد این بعد پیچیده‌ترین و کلیدی‌ترین حوزه در تبیین رفتار انطباقی آن‌ها است. مضمون نگرش و باورها در این بعد با ۳۹ تکرار بیشترین فراوانی را میان تمام عوامل شناسایی‌شده در پژوهش دارد. این یافته قاطعانه نشان می‌دهد هستهٔ اصلی مسئلهٔ انطباق در ذهنیت، باورها و نگرش کارکنان به اهمیت امنیت اطلاعات نهفته است.

این نگرش‌ها در کنار تأثیر سایر مضامین تأثیرگذار از منظر انگیزش قرار می‌گیرند. مضامین ارزیابی هزینه و فایده (۲۴ تکرار)، اندازهٔ تهدید (۲۰ تکرار) و قصد و اهداف (۱۷ تکرار) می‌توانند تشکیل‌دهندهٔ سه ضلع مثلث انگیزشی را در زیرمجموعهٔ انگیزش تأملی/بازتابی تشکیل می‌دهند. کارکنان به صورت آگاهانه یا ناخودآگاه شدت و احتمال وقوع تهدید را می‌سنجند، هزینه‌ها (مانند اتلاف وقت و پیامدهای مالی) را در برابر مزایای انطباق ارزیابی می‌کنند و بر اساس این محاسبات قصد رفتاری خود را شکل می‌دهند. نکتهٔ جالب توجه حضور تکنیک‌های خنثی‌سازی (۵ تکرار) در این بعد است. این مفهوم نشان می‌دهد کارکنان چگونه با توجیهاتی مانند مسئولیت‌پذیر نبودن یا آسیب نرساندن به دیگران، انطباق نداشتن رفتار خود را از نظر اخلاقی منطقی جلوه می‌دهند و انگیزهٔ خود را برای رفتار صحیح تضعیف می‌کنند.

در نهایت، بخش انگیزش خودکار با مضامینی چون ترس و احساسات منفی (۱۲ تکرار) و عادت (۴ تکرار) نشان می‌دهد بخشی از رفتارهای کارکنان در حوزهٔ امنیت اطلاعات در واکنش‌های آنی و غیر تأملی آن‌ها ریشه دارد؛ در حالی که ترس می‌تواند محرکی کوتاه‌مدت باشد، هدف غایی سازمان‌ها باید تبدیل رفتارهای امن به عادت‌های ناخودآگاه باشد تا بار شناختی تصمیم‌گیری از دوش کارکنان برداشته و این موضوع به اخلاق و جزئی از فرهنگ آن‌ها تبدیل شود.

برای نمایش بصری وزن مفاهیم تحلیلی مستخرج ابر کدها (شکل ۴) با استفاده از نرم‌افزار ترسیم شد. این شکل فراوانی مضامین فرعی را به تصویر می‌کشد و خلاصه‌ای از نتایج تحلیلی پژوهش ارائه می‌دهد. در این ابر، برجستگی و غلبهٔ مشخص نگرش و باورها بر سایر مفاهیم به شکلی انکارناپذیر مشهود است. پس از آن، کدهای آموزش، آگاهی و توسعه، ارزیابی هزینه و فایده، هنجارها و نفوذ اجتماعی و اندازهٔ تهدید به ترتیب بیشترین برجستگی را دارند. این تصویر به وضوح نشان می‌دهد از منظر پژوهش‌های انجام‌شده، سنگ‌بنای چهارچوب انطباق نه‌تنها دانش یا مهارت، بلکه مجموعه‌ای از ساختارهای روان‌شناختی مرتبط با انگیزه و عوامل اجتماعی است. این ابر کد به مثابه نقشهٔ راه بصری عمل می‌کند و به مدیران و سیاست‌گذاران نشان می‌دهد برای تغییر پایدار در رفتار امنیتی کارکنان مداخلات باید در درجهٔ اول بر اصلاح نگرش‌ها، بهبود تحلیل هزینه-فایده، تقویت آموزش‌های هدفمند و مدیریت هنجارهای اجتماعی متمرکز شوند.

به منزلهٔ مکملی برای ابر کدها و به منظور کاوش در محتوای خام و بدون ساختار متون ۶۷ مطالعهٔ منتخب

شکل ۴: ابر کدهای مرتبط با عوامل مؤثر بر انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات

شکل ۵: ابر کلمات مرتبط با عوامل مؤثر بر انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات

ابر کلمات (شکل ۵) از کل داده‌های متنی استخراج شد. این نمودار، که در آن اندازهٔ هر کلمه بازتاب‌دهندهٔ فرکانس تکرار آن است، تأییدی بر ماهیت انسان‌محور مسئلهٔ امنیت اطلاعات است. پس از intentions (قصد) که از بیشترین تکرار در مقالات برخوردار است، اندازهٔ واژگانی همچون awareness (آگاهی)، attitudes (نگرش‌ها) و motives (انگیزه‌ها) در تصویر تأییدی بر این است که کانون اصلی بحث در این پژوهش‌ها دنیای ذهنی و درونی کارکنان است. نکتهٔ قابل تأمل دیگر در این نمودار هم‌نشینی بصری مفاهیم کنترلی و بازدارنده مانند threats (تهدیدها)، controls (کنترل‌ها) و sanctions (تنبیه‌ها) با مفاهیم توانمندساز و اجتماعی نظیر culture (فرهنگ)، support (حمایت) و -social ly (اجتماعی) است. این هم‌جواری گویای دوگانگی راهبردی در این حوزه است: از یک سو تلاش برای مهار رفتارهای نامنطبق از طریق ابزارهای کنترلی و از سوی دیگر، تلاش برای شکل‌دهی به آن‌ها از طریق فرهنگ و حمایت. این ابر کلمات به صورت بصری نشان می‌دهد در گفتمان امنیت، صحبت از فناوری و کنترل بدون در نظر گرفتن نگرش و فرهنگ و ابعاد انسانی و بالعکس ناقص است و این دو رشته به طور جدایی‌ناپذیری در هم تنیده‌اند.

به طور خلاصه، تحلیل یافته‌های حاصل از فراترکیب نشان می‌دهد انطباق امنیتی رفتار کارکنان در نظام بانکی پدیده‌ای تک‌بعدی نیست، بلکه محصول مجموعه‌ای پیچیده از تعاملات میان قابلیت‌های فردی، فرصت‌های محیطی و فرایندهای انگیزشی است که در آن، نگرش‌ها و باورهای کارکنان نقشی محوری ایفا می‌کنند.

بحث و نتیجه‌گیری

این پژوهش با هدف ارائهٔ چهارچوبی جامع از عوامل مؤثر بر انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات از طریق روش فراترکیب انجام شد. چهارچوب حاصل (شکل ۶)، که بنیان آن بر مدل رفتار COM-B سازمان‌دهی مبتنی شده است، نشان می‌دهد این انطباق با سیاست‌های امنیتی پدیده‌ای پیچیده و چندوجهی است که از تعامل قابلیت‌های فردی، فرصت‌های محیطی و اجتماعی و انگیزه‌های روان‌شناختی افراد نشئت می‌گیرد.

برجسته‌ترین یافتهٔ پژوهش حاضر مرکزیت و اکثریت بلامنازع بعد انگیزه و به طور خاص مضمون نگرش و باورها با ۳۹ تکرار است. این یافته هم‌راستایی قدرتمندی با ستون‌های اصلی نظریهٔ رفتار برنامه‌ریزی‌شده دارد که در آن نگرش به منزلهٔ یکی از پیش‌بین‌های اصلی قصد رفتاری و در نهایت خود رفتار در نظر گرفته می‌شود (Alraja et al., 2023; Cram et al., 2020; Bélanger et al., 2017; Siponen et al., 2014). یافته‌های مطالعهٔ حاضر نشان می‌دهد در حوزهٔ امنیت اطلاعات بانکی نگرش مثبت یا منفی کارمندان به سیاستی امنیتی و همچنین نگرش‌ها و باورهای آن‌ها در سایر زمینه‌های مرتبط بیش از هر عامل دیگری تعیین‌کنندهٔ پایبندی یا نبود پایبندی ایشان به این سیاست‌ها است. این نگرش می‌تواند محصول فرایندهای ارزیابی‌های پیچیده‌تری باشد. فراوانی بالای کدهای ارزیابی هزینه و فایده (۲۴ تکرار) و ارزیابی اندازهٔ تهدید (۲۰ تکرار) این موضوع را تأیید می‌کند. این امر با ارکان کلیدی نظریهٔ انگیزش محافظت نیز کاملاً سازگار است، که بر اساس آن افراد زمانی رفتار محافظتی را در پیش می‌گیرند که تهدید را جدی (ارزیابی تهدید) و راهکار ارائه‌شده را مؤثر و کم‌هزینه (ارزیابی مقابله) بدانند (Ogbanufe et al., 2023; Asfoor et al., 2023; Ameen et al., 2021; Vance et al., 2012)؛ بنابراین چهارچوب ارائه‌شده نشان می‌دهد کارکنان بانک‌ها بازیگرانی منطقی‌اند که پیش از ارتکاب رفتارهای امنیتی به تحلیل هزینه-فایدهٔ عقلانی و شناختی اقدام می‌کنند.

با این حال، این عقلانیت محدودیت‌هایی دارد. شناسایی تکنیک‌های خنثی‌سازی (۵ تکرار)، به منزلهٔ عامل انگیزشی، لایهٔ جدیدی به این تحلیل می‌افزاید. این یافته، که با نظریهٔ خنثی‌سازی هم‌خوانی دارد، نشان می‌دهد کارکنان می‌توانند با توجیهاتی مانند ایراد نداشتن خسارت جدی یا رفتار دیگران باورهای اخلاقی خود را موقت به حالت تعلیق درآورند و رفتار ناامن را منطقی جلوه دهند (Alraja et al., 2023; D'Arcy and Teh, 2019; Bauer and Bernroider, 2017; Teh et al., 2015). این بدان معناست که انطباق نداشتن همیشه ناشی از نبود انگیزهٔ مثبت نیست، بلکه گاهی محصول فعال‌سازی انگیزهٔ منفی و فرایند توجیه‌گرانه است.

در بعد فرصت، یافته‌ها نقش مهم محیط سازمانی و اجتماعی را برجسته می‌کنند. آموزش، آگاهی و توسعهٔ سرمایهٔ انسانی (۲۸ تکرار) پرتکرارترین عامل در این بعد و نشان‌دهندهٔ اجماع گستردهٔ ادبیات موضوع بر سر اهمیت آن است؛ اما نکتهٔ جالب‌تر قدرت هنجارها و نفوذ اجتماعی (۲۱ تکرار) است، که هم‌راستا با مفهوم هنجارهای ذهنی در نظریهٔ رفتار برنامه‌ریزی‌شده،

شکل ۶: چهارچوب عوامل مؤثر بر انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات

نشان می‌دهد فشار و رفتار همکاران می‌تواند به اندازهٔ سیاست‌های رسمی یا حتی بیشتر بر رفتار کارکنان تأثیر بگذارد (Jaeger et al., 2021; Posey and Folger, 2020; Chen et al., 2018; Herath and Rao; 2009). در کنار آن، وجود سیستم تنبیهی (۱۳ تکرار) و مفهوم تحریم‌های غیر رسمی (۳ تکرار) مؤید اصول نظریهٔ بازدارندگی عمومی‌اند که بر نقش قطعیت و شدت تنبیه در پیشگیری از رفتار نامطلوب تأکید دارند (Hengstler et al., 2023; Asfoor et al., 2023; Jaeger et al., 2021; Hovav and D'Arcy, 2012). با این حال فراوانی بیشتر هنجارهای اجتماعی در برابر سیستم تنبیهی رسمی ممکن است حاکی از آن باشد که در محیط‌های بانکی بازدارندگی غیر رسمی (ترس از قضاوت همکاران) از بازدارندگی رسمی (ترس از تنبیه سازمانی و مدیریتی) اثربخش‌تر است.

در نهایت در بعد قابلیت، در حالی که درک و آگاهی از خطرها و سیاست‌های امنیتی (هر کدام با ۱۳ تکرار) به منزلهٔ عوامل ضروری تأیید می‌شود، یافتهٔ کلیدی خودکارآمدی (۱۸ تکرار) است. این یافته نیز با نظریهٔ رفتار برنامه‌ریزی‌شده هم‌راستا است و نشان می‌دهد دانش به تنهایی کافی نیست. کارمندان باید باور داشته باشند که توانایی فنی و عملی برای اجرای رفتار امن را دارند (Ogbanufe et al., 2023; Tam et al., 2022; Ameen et al., 2020; Rhee et al., 2009). این امر اهمیت طراحی کاربرپسند سیاست‌ها و ابزارها را دوچندان می‌کند؛ زیرا ابزارهای پیچیده می‌توانند

مستقیم خودکارآمدی را تضعیف کنند و به انطباق نداشتن رفتار کارکنان منجر شوند.

این پژوهش با ترکیب و یکپارچه‌سازی بدنهٔ گسترده‌ای از ادبیات چهارچوبی جامع، منسجم و چندبعدی را برای تبیین انطباق رفتار کارکنان بانکی با سیاست‌های امنیت اطلاعات ارائه داده است. نتیجهٔ اصلی این است که انطباق رفتار رویدادی منفرد نیست، بلکه اکوسیستمی رفتاری است که در آن عوامل فردی (قابلیت)، سازمانی (فرصت) و روان‌شناختی (انگیزه) مداوم با یکدیگر تعامل دارند. این چهارچوب، که مبتنی بر مدل COM-B است، با نظریه‌های کلاسیک رفتاری غنی‌شده می‌تواند ابزاری تشخیصی و راهنمای عملی برای مدیران و پژوهشگران این حوزه باشد.

پژوهش حاضر از لحاظ نظری چندین پیامد مهم دارد. نخست اینکه این پژوهش نشان می‌دهد مدل COM-B می‌تواند چهارچوبی قدرتمند برای یکپارچه‌سازی نظریه‌های به ظاهر رقیب مانند نظریهٔ انگیزش محافظت، نظریهٔ رفتار برنامه‌ریزی‌شده، نظریهٔ بازدارندگی عمومی و نظریهٔ خنثی‌سازی در حوزهٔ امنیت اطلاعات باشد. این مدل به جای تمرکز بر نظریه‌ای خاص به پژوهشگران اجازه می‌دهد عوامل مختلف را در جایگاه منطقی خود قرار دهند؛ همچنین این فراترکیب با نمایش فراوانی نسبی عوامل به وزن‌دهی تجربی سازه‌های نظری مختلف کمک می‌کند؛ برای مثال نتایج این پژوهش نشان می‌دهد سازه‌های مرتبط با نگرش و هنجارهای اجتماعی (از رفتار برنامه‌ریزی‌شده) در ادبیات موجود بازتاب گسترده‌تری از سازهٔ شدت تنبیه (از بازدارندگی عمومی) داشته‌اند. این امر می‌تواند راهنمای پژوهشگران برای تمرکز بر متغیرهای مهم‌تر باشد.

در حوزهٔ عملی و کاربردی نیز چهارچوب ارائه‌شده نقشهٔ راه عملی برای مدیران ارشد، مدیران امنیت اطلاعات و مدیران منابع انسانی در نظام بانکی فراهم می‌آورد. این چهارچوب بیان می‌کند تمرکز مدیران بر کمپین‌های آگاهی‌رسانی به تنهایی کافی نیست. فراتر از آگاهی‌رسانی که می‌تواند مبتنی بر شبیه‌سازی حملات سایبری برای کارکنان ستاد و شعب مجزا باشد، مداخلات باید بر اصلاح نگرش‌ها و باورهای کارکنان متمرکز شوند. این امر می‌تواند از طریق نمایش پیامدهای واقعی نقض‌های امنیتی (تقویت ارزیابی تهدید) و برجسته‌سازی مزایای انطباق برای فرد و سازمان (تقویت ارزیابی فایده) انجام شود. البته در موضوع توانمندسازی، آموزش و آگاهی‌رسانی نیز می‌توان از روش‌های متنوع مانند ایجاد تیم‌های متشکل از نیروهای امنیت اطلاعات و سایر کارکنان برای بازنگری سیاست‌ها و اطمینان از اجرایی بودن آن‌ها، استفاده از بازی‌سازی برای جذب و علاقه‌مند کردن کارکنان به این حوزه و تعریف نقش سفیر امنیت برای هر مدیر میانی در زیرمجموعهٔ خود بهره برد؛ همچنین در طراحی سیاست‌ها و ابزارهای امنیتی باید محدودیت‌های شناختی و شغلی کارکنان در نظر گرفته شود. در صورت استفادهٔ بانک‌ها از سیستم‌های پیچیده هزینهٔ انطباق بیشتر و خودکارآمدی کمتر می‌شود و کارکنان به سمت یافتن راه‌های میان‌بر ناامن سوق داده می‌شوند؛ بنابراین طراحی امنیت به شیوهٔ انسان‌محور می‌تواند گزینهٔ خوبی برای بهبود این موضوع باشد. علاوه بر این، به جای اتکای صرف به تهدید و تنبیه بانک‌ها باید بر ایجاد فرهنگ امنیت مثبت سرمایه‌گذاری کنند. شناسایی و تقویت قهرمانان امنیت در هر واحد سازمانی، ترویج داستان‌های موفقیت‌آمیز، تشویق گفت‌وگوی باز در مورد مسائل امنیتی و تخصیص مشوق‌های مالی یا نمادین (مانند لوح تقدیر یا نشان سازمانی) به افرادی که بهترین عملکرد را در این حوزه دارند می‌تواند هنجارهای مطلوب را تقویت کند. در نهایت مدیران باید از تکنیک‌های خنثی‌سازی آگاه باشند و به طور فعال با آن‌ها مقابله کنند. شفاف‌سازی مسئولیت فردی هر کارمند و نشان دادن اینکه حتی تخلفات کوچک نیز می‌توانند پیامدهای جدی داشته باشند، راهی برای برخورد با این توجیه‌ها است.

این پژوهش با وجود نقاط قوت تشریح‌شده با محدودیت‌هایی نیز روبه‌رو بوده است. نخست اینکه به منزلهٔ پژوهشی فراترکیب چهارچوب ارائه‌شده ماهیتی مفهومی دارد و روابط علی و معلولی میان متغیرهای شناسایی‌شده را به صورت تجربی نیازموده است. دوم اینکه تمرکز این پژوهش بر رفتار انطباقی کارکنان بوده و ابعاد دیگر رفتار امنیتی مانند رفتار شهروندی امنیت سایبری کمتر مدنظر قرار گرفته است. بر این اساس، برخی مسیرهای پژوهشی برای مطالعات آتی در این زمینه پیشنهاد می‌شود. اولین و مهم‌ترین پیشنهاد توسعهٔ ابزار سنجش (مانند پرسشنامه) بر اساس چهارچوب پیشنهادی و آزمایش تجربی آن در صنعت بانکداری ایران است. استفاده از مدل‌سازی معادلات ساختاری می‌تواند روابط و مسیرهای تأثیرگذاری میان ابعاد قابلیت، فرصت و انگیزه و مضامین فرعی زیرمجموعهٔ آن‌ها را به صورت کمی مشخص کند؛ همچنین بومی‌سازی چهارچوب ارائه‌شده

بر اساس شرایط صنعت بانکداری ایران نیز می‌تواند مدنظر پژوهشگران قرار گیرد. به علاوه رتبه‌بندی این عوامل با استفاده از فنونی مانند روش‌های تصمیم‌گیری چندمعیاره می‌تواند موضوع مطالعاتی پژوهشگران باشد. افزون بر این، پژوهش‌های آتی می‌توانند نقش متغیرهای جمعیت‌شناختی (مانند سن و سابقهٔ کار) و سازمانی (مانند اندازهٔ بانک، دولتی یا خصوصی بودن) را به منزلهٔ تعدیل‌گر در روابط مدل بررسی کنند؛ همچنین با توجه به ماهیت پویای فرایند انطباق مطالعات طولی در این زمینه می‌تواند چگونگی تغییر نگرش‌ها، قابلیت‌ها و رفتار کارکنان را در طول زمان و در پاسخ به مداخلات مختلف (مانند کمپین آموزشی جدید) ردیابی کند. مضاف بر این، بررسی چهارچوب‌های ارائه‌شده توسط مراجع معتبر بانکی (مانند مقررات Basel III) و ریسک‌های مربوط به آموزش و آگاهی‌رسانی خطاهای انسانی و رفتار نادرست، که در چهارچوب خطرهای عملیاتی نظام بانکی قرار می‌گیرند، می‌تواند زمینه‌ساز پژوهش‌هایی با رویکرد عملیاتی باشد؛ همچنین با توجه به امکان تأثیر عوامل مادی در نقض سیاست‌های امنیت اطلاعات در نظام بانکی و اهمیت این موضوع در بروز کلاه‌برداری‌ها این موضوع می‌تواند توجه پژوهشگران را به خود جلب کند. در نهایت می‌توان چهارچوب حاضر را با ادغام مفاهیم و نظریه‌های دیگر مانند نظریهٔ شکل‌گیری عادت (چگونگی تبدیل رفتار امن به کنش خودکار) غنی‌تر کرد.

منابع

Aebissa, B., Dhillon, G., and Meshesha, M. (2023). "The Direct and Indirect Effect of Organizational Justice on Employee Intention to Comply With Information Security Policy: The Case of Ethiopian Banks". *Computers and Security*, 130, p. 103248. https://doi.org/10.1016/j.cose.2023.103248

Afshari, P., Bayazidi, S., and Yazdani, S. (2024). "Meta-Synthesis As an Original Method to Synthesize Qualitative Literature in Chronic Diseases: A Narrative Review. *Jundishapur Journal of Chronic Disease Care*, 13(2). p.e 139621. https://doi.org/10.5812/jjcdc-139621

Ajzen, I. (1985). *From Intentions to Actions: A Theory of Planned Behavior* (pp. 11-39). Springer Berlin Heidelberg.

Ajzen, I., and Fishbein, M. (1973). "Attitudinal and Normative Variables as Predictors of Specific Behavior". *Journal of personality and Social Psychology,* 27(1), pp. 41–57. https://psycnet.apa.org/doi/10.1037/h0034440

Alassaf, M. and Alkhalifah, A. (2021). "Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review". *IEEE Access,* 9, pp. 162687-162705. https://doi.org/10.1109/ACCESS.2021.3132574

Alraja, M. N., Butt, U. J., and Abbod, M. (2023). "Information Security Policies Compliance in a Global Setting: An Employee's Perspective". *Computers and Security*, 129, p. 103208. https://doi.org/10.1016/j.cose.2023.103208

Amankwa, E., Loock, M., and Kritzinger, E. (2022). "The Determinants of an Information Security Policy Compliance Culture in Organisations: the Combined Effects of Organisational and Behavioural Factors. *Information and Computer Security*, 30(4), pp. 583-614. https://doi.org/10.1108/ICS-10-2021-0169

Ameen, N., Tarhini, A., Shah, M. H., and Madichie, N. O. (2020). "Employees' Behavioural Intention to Smartphone Security: A Gender-Based, Cross-National Study". *Computers in Human Behavior*, 104, p. 106184. https://doi.org/10.1016/j.chb.2019.106184

Amiri, M., Roozbehani, K., and Zamanian, M. (2015). "Identifying the Failure of Implementation of Information Security Management Systems (ISMS) With a Focus on Iranian Organizations". *Science and Technology Policy Letters*, 05(2), pp. 69-76.

Asfoor, A. H., Latif, A. B. A., and Rahim, F. B. A. (2023). "Investigate the Roles of Sanctions, Psychological Capital, and Organizational Security Resources Factors in Information

Security Policy Violation". *Asia pacific journal of information systems*, 33(4), pp. 863-898. https://doi.org/10.14329/apjis.2023.33.4.863

Bandura, A. (1977). "Self-efficacy: Toward a Unifying Theory of Behavioral Change". *Psychological review,* 84(2), pp. 191-215. https://psycnet.apa.org/doi/10.1037/0033-295X.84.2.191

Bansal, G., Muzatko, S., and Shin, S. I. (2021). "Information System Security Policy Noncompliance: the Role of Situation-Specific Ethical Orientation". *Information Technology and People*, 34(1), pp. 250-296. https://doi.org/10.1108/ITP-03-2019-0109

Baskerville, R., and Siponen, M. (2002). "An Information Security Meta-Policy for Emergent Organizations. *Logistics Information Management,* 15(5/6), pp. 337-346. https://doi.org/10.1108/09576050210447019

Bauer, S., and Bernroider, E. W. (2017). "From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 48(3), pp. 44–68. https://doi.org/10.1145/3130515.3130519

Bauer, S., Bernroider, E. W., and Chudzikowski, K. (2017). "Prevention is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-Compliance with Information Security Policies in Banks". *Computers and Security*, 68, pp. 145-159. https://doi.org/10.1016/j.cose.2017.04.009

Begishev, I. R., Khisamova, Z. I., and Mazitova, G. I. (2019). "Information Infrastructure of Safe Computer Attack. *Helix*, 9(5), pp. 5639-5642. https://doi.org/10.29042/2019-5639-5642

Bélanger, F., Collignon, S., Enget, K., and Negangard, E. (2017). "Determinants of Early Conformance with Information Security Policies. *Information and Management*, 54(7), pp. 887-901. https://doi.org/10.1016/j.im.2017.01.003

Braun, V., and Clarke, V. (2006). "Using Thematic Analysis in Psychology. *Qualitative Research in Psychology,* 3(2), pp. 77-101. http://dx.doi.org/10.1191/1478088706qp063oa

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34(3), pp. 523-548. https://doi.org/10.2307/25750690

Butler, K. J., and Brown, I. (2023). "COVID-19 Pandemic-Induced Organisational Cultural Shifts and Employee Information Security Compliance Behaviour: a South African Case Study. *Information and Computer Security*, 31(2), pp. 221-243. https://doi.org/10.1108/ICS-09-2022-0152

Campbell, R., Pound, P., Pope, C., Britten, N., Pill, R., Morgan, M., and Donovan, J. (2003). "Evaluating Meta-Ethnography: a Synthesis of Qualitative Research on Lay Experiences of Diabetes and Diabetes Care. *Social Science and Medicine*, 56(4), pp. 671-684. https://doi.org/10.1016/S0277-9536(02)00064-3

Chen, X., Wu, D., Chen, L., and Teng, J. K. (2018). "Sanction Severity and Employees' Information Security Policy Compliance: Investigating Mediating, Moderating, and Control Variables. *Information and Management*, 55(8), pp. 1049-1060. https://doi.org/10.1016/j.im.2018.05.011

Choi, Y., and Yoo, T. (2014). "Influence of HRM Practices on Privacy Policy Compliance Intention: a Study Among Bank Employees in Korea". *International Journal of Security and Its Applications*, 8(1), pp. 9-18. https://doi.

org/10.14257/IJSIA.2014.8.1.02

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. (2020). "Maximizing Employee Compliance with Cybersecurity Policies". *MIS Quarterly Executive*, 19(3), pp. 183–198. http://dx.doi.org/10.17705/2msqe.00032

D'Arcy, J., Herath, T., and Shoss, M. K. (2014). "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of management information systems,* 31(2), pp. 285-318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., and Teh, P. L. (2019). "Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-Related Stress, Emotions, and Neutralization". *Information and Management*, 56(7), p. 103151. https://doi.org/10.1016/j.im.2019.02.006

Dawson, A. J. (2019). *Meta-synthesis of Qualitative Research*. In P. Liamputtong (Ed.), *Handbook of Research Methods in Health Social Sciences* (pp. 785-804). Springer. https://doi.org/10.1007/978-981-10-5251-4_112

Duncan, C. (2022). *Cyber Security in Banking*. Retrieved from https://www.alert-software.com/blog/cybersecurity-in-banking.

Edwards, J., and Kaimal, G. (2016). "Using Meta-Synthesis to Support Application of Qualitative Methods Findings in Practice: A Discussion of Meta-Ethnography, Narrative Synthesis, and Critical Interpretive Synthesis. *The Arts in Psychotherapy*, 51, pp. 30-35. https://doi.org/10.1016/j.aip.2016.07.003

ENISA. (2023). *ENISA threat Landscape Report 2023*. Hearklion: European Network and Information Security Agency (ENISA), Retrieved from www.enisa.europa.eu/topics/cyber-threats/threats-and-trends.

Gibbs, J. P. (1968). "Crime, Punishment and Deterrence". *The Southwestern Social Science Quarterly*, 48(4), pp. 515-530.

Hadlington, L., Binder, J., and Stanulewicz, N. (2021). "Exploring the Role of Moral Disengagement and Counterproductive Work Behaviours in Information Security Awareness. *Computers in Human Behavior,* 114, p. 106557. https://doi.org/10.1016/j.chb.2020.106557

Hashemzadeh Aghdam, N. (2021). "Data Security Policies: The Indirect Role of Management Support on Users' Adjustment Behavior of Banks' Data Systems". *Quarterly Studies in Banking Management and Islamic Banking*, 7(16), pp. 77-98. https://doi.org/10.22034/jifb.2022.153329 {In Persian}

Hengstler, S., Kuehnel, S., Masuch, K., Nastjuk, I., and Trang, S. (2023). "Should i Really do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior". *Computers and Security*, 133, p. 103370. https://doi.org/10.1016/j.cose.2023.103370

Herath, T., and Rao, H. R. (2009). "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems*, 47(2), pp. 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Homans, G. C. (1958). "Social Behavior as Exchange. *American journal of sociology,* 63(6), pp. 597-606. https://doi.org/10.1086/222355

Hovav, A., and D'Arcy, J. (2012). "Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the US and South Korea. *Information and Management*, 49(2), pp. 99-110. https://doi.org/10.1016/j.im.2011.12.005

Ifinedo, P. (2012). "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers and Security,* 31(1), pp. 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2016). Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance with IS Security Policy Guidelines?. *Information Systems Management,* 33(1), pp. 30-41. https://doi.org/10.1080/10580530.2015.1117868

IMF. (2024). *Rising Cyber Threats Pose Serious Concerns for Financial Stability*. Retrieved from https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

ISACA. (2025). *Cybersecurity Trends to Watch in 2025*. Retrieved from https://www.isaca.org/resources/news-and-trends/industry-news/2025/cybersecurity-trends-to-watch-in-2025.

Jacobs, B. A. (2010). "Deterrence and Deterrability". *Criminology,* 48(2), pp. 417-441. https://doi.org/10.1111/j.1745-9125.2010.00191.x

Jaeger, L., Eckhardt, A., and Kroenung, J. (2021). "The role of Deterrability for the Effect of Multi-Level Sanctions on Information Security Policy Compliance: Results of a Multigroup Analysis". *Information and Management*, 58(3), p. 103318. https://doi.org/10.1016/j.im.2020.103318

Jansen, J., and Van Schaik, P. (2018). "Testing a Model of Precautionary Online Behaviour: The Case of Online Banking". *Computers in Human Behavior,* 87, pp. 371-383. https://doi.org/10.1016/j.chb.2018.05.010

Järveläinen, J. (2016). "Integrated Business Continuity Planning and Information Security Policy Development Approach. *International Conference on Information Systems (ICIS)*, Dublin.

Johnston, A. C., and Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly,* 34(3), pp. 549-566. https://doi.org/10.2307/25750691

Kajtazi, M., and Bulgurcu, B. (2013). "Information Security Policy Compliance: An Empirical Study on Escalation of Commitment"|. In *19th Americas Conference on Information Systems*, Chicago, Illinois.

Kam, H. J., Mattson, T., and Kim, D. J. (2021). |The "Right" Recipes for Security Culture: a Competing Values Model Perspective. *Information Technology and People*, 34(5), pp. 1490-1512. https://doi.org/10.1108/ITP-08-2019-0438

Kerner, S. M. (2023). *34 Cybersecurity Statistics to Lose Sleep Over in 2023*. Retrieved from https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020.

Khan, N. F., Yaqoob, A., Khan, M. S., and Ikram, N. (2022). "The Cybersecurity Behavioral Research: A Tertiary Study. *Computers and Security,* 120, p. 102826. https://doi.org/10.1016/j.cose.2022.102826

Leung, L. (2015). "Validity, Reliability, and Generalizability in Qualitative Research. *Journal of Family Medicine and Primary Care*, 4(3), pp. 324-327. https://doi.org/10.4103/2249-4863.161306

Li, L., He, W., Xu, L., Ash, I., Anwar, M., and Yuan, X. (2019). "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior. *International Journal of Information Management*, 45, pp. 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Y. J., and Hoffman, E. (2023). "Designing an Incentive Mechanism for Information Security

Policy Compliance: An Experiment. *Journal of Economic Behavior and Organization*, 212, pp. 138-159. https://doi.org/10.1016/j.jebo.2023.05.033

Liu, C., Wang, N., and Liang, H. (2020). "Motivating Information Security Policy Compliance: The Critical Role of Supervisor-Subordinate Guanxi and Organizational Commitment". *International Journal of Information Management*, 54, p. 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

McLeod, A., and Dolezel, D. (2022). "Information Security Policy Non-Compliance: Can Capitulation Theory Explain User Behaviors?. *Computers and Security*, 112, p. 102526. https://doi.org/10.1016/j.cose.2021.102526

Menard, P., Bott, G. J., and Crossler, R. E. (2017). "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, 34(4), pp. 1203-1230. https://doi.org/10.1080/07421222.2017.1394083

Merhi, M. I., and Ahluwalia, P. (2019). "Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security. *Computers in Human Behavior*, 92, pp. 37-46. https://doi.org/10.1016/j.chb.2018.10.031

Merhi, M. I., and Ahluwalia, P. (2024). "Predicting Compliance of Security Policies: Norms and Sanctions. *Journal of Computer Information Systems*, 64(5), pp. 683-697. https://doi.org/10.1080/08874417.2023.2241413

Michie, S., Van Stralen, M. M., and West, R. (2011). "The Behaviour Change Wheel: a New Method for Characterising and Designing Behaviour Change Interventions. *Implementation Science*, 6(1), p. 42. https://doi.org/10.1186/1748-5908-6-42

Mohammadi, F., Kazempourian, S., and taghva, M. R. (2021). Technology Intelligence in High Tech Organizations. *Science and Technology Policy Letters*, 11(1), pp. 51-68.

Nadelson, S., and Nadelson, L. S. (2014). "Evidence-Based Practice Article Reviews Using CASP Tools: a Method for Teaching EBP. *Worldviews on Evidence-Based Nursing*, 11(5), pp. 344-346. https://doi.org/10.1111/wvn.12059

Nazari, F. (2020). *Factors Affecting Acceptance of Information Security Policy Among Employees of Tejarat Bank*. Master's thesis. Payame Noor University. {In Persian}

Ogbanufe, O. (2021). "Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity". *Computers and Security*, 108, p. 102340. https://doi.org/10.1016/j.cose.2021.102340

Ogbanufe, O. (2023). "Securing Online Accounts and Assets: An Examination of Personal Investments and Protection Motivation. *International Journal of Information Management*, 68, p. 102590. https://doi.org/10.1016/j.ijinfomgt.2022.102590

Ogbanufe, O., Crossler, R. E., and Biros, D. (2023). "The Valued Coexistence of Protection Motivation and Stewardship in Information Security Behaviors. *Computers and Security*, 124, p. 102960. https://doi.org/10.1016/j.cose.2022.102960

Ogbanufe, O., Crossler, R. E., and Biros, D. (2021). "Exploring Stewardship: A Precursor to Voluntary Security Behaviors". *Computers and Security*, 109, p. 102397. https://doi.org/10.1016/j.cose.2021.102397

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... and Moher, D. (2021). The PRISMA 2020 Statement: an Updated Guideline for Reporting Systematic Reviews". *bmj*, 372. https://doi.org/10.1136/bmj.

n71

Petrič, G., and Orehek, Š. (2025). "Expressing Opinions About Information Security in an Organization: the Spiral of Silence Theory Perspective". *Information and Computer Security*, 33(2), pp. 223-241. https://doi.org/10.1108/ICS-04-2024-0083

Phillips, M., and Lu, J. (2018). "A Quick Look at NVivo". *Journal of Electronic Resources Librarianship*, 30(2), pp. 104-106. https://doi.org/10.1080/1941126X.2018.1465535

Posey, C., and Folger, R. (2020). "An Exploratory Examination of Organizational Insiders' Descriptive and Normative Perceptions of Cyber-Relevant Rights and Responsibilities". *Computers and Security*, 99, p. 102038. https://doi.org/10.1016/j.cose.2020.102038

Pourkarimi, J., Abili, K., and Azizi, M. (2025). "Educational Managers' Competencies in Turbulent Environments (A Meta-Synthesis Study)". *Interdisciplinary Journal of Management Studies*, 18(3), pp. 565-581. https://doi.org/10.22059/jipa.2024.372042.3469 {In Persian}

PurpleSec. (2023). *Cyber Security Statistics: The Ultimate List of Stats, Data, and Trends for 2023*. Retrieved from https://purplesec.us/resources/cybersecurity-statistics.

Rajab, M., and Eydgahi, A. (2019). "Evaluating the Explanatory Power of Theoretical Frameworks on Intention to Comply with Information Security Policies in Higher Education". *Computers and Security*, 80, pp. 211-223. https://doi.org/10.1016/j.cose.2018.09.016

Rhee, H. S., Kim, C., and Ryu, Y. U. (2009). "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior". *Computers and Security*, 28(8), pp. 816-826. https://doi.org/10.1016/j.cose.2009.05.008

Rogers, R. W. (1975). "A protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology,* 91(1), pp. 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). "Cognitive and Psychological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation". *Social Psychophysiology: A Sourcebook*, pp. 153-176.

Sandelowski, M., and Barroso, J. (2007). *Handbook for Synthesizing Qualitative Research*. New York, NY: Springer.

Schroeder, P., and Siddiqui, Z. (2023, November 10). *China's Biggest Lender ICBC Hit By Ransomware Attack*. Reuters. Retrieved from https://www.reuters.com/world/china/chinas-largest-bank-icbc-hit-by-ransomware-software-ft-2023-11-09/

Silic, M., Barlow, J. B., and Back, A. (2017). "A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage". *Information and Management*, 54(8), pp. 1023-1037. https://doi.org/10.1016/j.im.2017.02.007

Siponen, M., Mahmood, M. A., and Pahnila, S. (2014). "Employees' Adherence to Information Security Policies: An Exploratory Field Study". *Information and Management*, 51(2), pp. 217-224. https://doi.org/10.1016/j.im.2013.08.006

Straub Jr, D. W. (1990). "Effective IS Security: An Empirical Study. *Information Systems Research*, 1(3), pp. 255-276. https://doi.org/10.1287/isre.1.3.255

Sullivan, P. (2025). *Cyber Attack Statistics to Know in 2025*. Retrieved from https://parachute.cloud/cyber-attack-statistics-data-and-trends.

Sykes, G., and Matza, D. (1957). "Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22(6), pp. 664-670. https://doi.org/10.2307/2089195

Tam, C., de Matos Conceição, C., and Oliveira, T. (2022). "What Influences Employees to Follow Security Policies? *Safety Science*, 147, 105595. https://doi.org/10.1016/j.ssci.2021.105595

Teh, P. L., Ahmed, P. K., and D'Arcy, J. (2015). "What Drives Information Security Policy Violations Among Banking Employees?: Insights from Neutralization and Social Exchange Theory". *Journal of Global Information Management (JGIM)*, 23(1), pp. 44-64. http://doi.org/10.4018/jgim.2015010103

U.S. Department of Justice. (2024, March). *Former Bank Manager Sentenced to 3years in Prison for Theft from Customer Accounts*. Retrieved from https://www.justice.gov/usao-wdwa/pr/former-bank-manager-sentenced-3-years-prison-theft-customer-accounts.

Uchendu, B., Nurse, J. R., Bada, M., and Furnell, S. (2021). "Developing a Cyber Security Culture: Current Practices and Future Needs. *Computers and Security*, 109, p. 102387. https://doi.org/10.1016/j.cose.2021.102387

Van der Kleij, R., Wijn, R., and Hof, T. (2020). "An Application and Empirical Test of the Capability Opportunity Motivation-Behaviour model to Data Leakage Prevention in Financial Organizations". *Computers and Security*, 97, p. 101970. http://dx.doi.org/10.1016/j.cose.2020.101970

Van Slyke, C., and Belanger, F. (2020). "Explaining the Interactions of Humans and Artifacts in Insider Security Behaviors: The Mangle of Practice Perspective. *Computers and Security*, 99, p. 102064. https://doi.org/10.1016/j.cose.2020.102064

Vance, A., Siponen, M., and Pahnila, S. (2012). "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. *Information and management*, 49(3-4), pp. 190-198. https://doi.org/10.1016/j.im.2012.04.002

Vance, A., Siponen, M. T., and Straub, D. W. (2020). "Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures. *Information and Management*, 57(4), p. 103212. https://doi.org/10.1016/j.im.2019.103212

Verizon. (2023). *2023 Data Breach Investigation Report, Verizon*. Retrieved from www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf.

Williams, A. S., Maharaj, M. S., and Ojo, A. I. (2019). "Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks. *International Journal of Computing and Digital Systems*, 8(4). https://doi.org/10.12785/ijcds/080407

Xie, T., and Gorrivan, C. (2024, June26). *Evolve Bank and Trust confirms its data was stolen in cyber attack*. Bloomberg News. Retrieved from https://www.bloomberg.com/news/articles/2024-06-26/evolve-bank-trust-confirms-its-data-was-stolen-in-cyber-attack.

Science and Technology Policy Letters
15, Issue 3, autumn 2025

A Framework of Factors Influencing Employees' Compliance Behavior with Information Security Policies in the Banking Sector

Saeed Kazempourian[1]
Mohammad Reza Taghva[2]
Vajhollah Ghorbanizadeh[3]
Amir Manian[4]

Abstract

Consideringing the critical role of the human factor as a vulnerable link in the information security chain, this study aims to identify, classify, and integrate the factors influencing employee compliance with Information Security Policies (ISPs) in banking sector. The research culminates in the development of a comprehensive conceptual framework for this domain. The study employs a qualitative meta-synthesis methodology. Through a systematic search of academic databases, 67 pertinent articles directly addressing the research topic were selected and subjected to in-depth thematic analysis. The primary theoretical framework for classifying and integrating the extracted factors was the Capability, Opportunity, Motivation-Behavior (COM-B) model, which was synthesized with key concepts from Protection Motivation Theory (PMT), the Theory of Planned Behavior (TPB), Neutralization Theory, and General Deterrence Theory (GDT). The findings reveal that compliant behavior is the product of the interplay of three primary dimensions. The motivation dimension, comprising 13 factors, emerged as the most pivotal dimension, with attitudes and beliefs and cost–benefit evaluations occurring 39 and 24 times, respectively. Within the opportunity dimension, encompassing 11 factors, training and awareness and social norms—with 28 and 21 occurrences respectively—were identified as the most influential environmental factors. In the capability dimension, which consists of 12 factors, self-efficacy, with 18 occurrences, proved more significant than any other factor in that category. This research proposes an integrated, multidimensional framework demonstrating that employee compliance with ISPs in the banking system is not merely a technical requirement but a cognitive and social choice. The framework holds significant practical implications for banking managers, highlighting the necessity of shifting focus from tool-centric strategies to human-centric approaches that emphasize attitude modification, self-efficacy enhancement, and the cultivation of a positive security culture. Furthermore, by providing a comprehensive theoretical foundation, the framework enables future empirical research to examine the relationships among these factors.

Keywords: Meta Synthesis, Information Security, Bank, Compliance, Protection Motivation Theory, General Deterrence Theory, Theory of Planned Behavior

---

1.Ph.D. Candidate in Information Technology Management, Faculty of Management and Accounting, Allameh Tabataba'i University , Tehran, Iran. saeed.kazem.313@gmail.com

2. Professor, Department of Information Technology Management, Faculty of Management and Accounting, Allameh Tabataba'i University, Tehran, Iran.

3.Professor, Department of Public Administration, Faculty of Management and Accounting, Allameh Tabataba'i University, Tehran, Iran.

4. Professor, Department of Information Technology Management, College of Management, University of Tehran, Tehran, Iran.

نقش‌نامه و فرم تعارض منافع

الف) نقش نامه

پدیدآورنده	سعید کاظم‌پوریان	محمدرضا تقوا	وجه‌الله قربانی‌زاده	امیر مانیان
نقش	نویسندهٔ مسئول	نویسنده	نویسنده	نویسنده
نگارش متن	نگارش متن اصلی	بازنگری و مرور متن	بازنگری و مرور متن	بازنگری و مرور متن
ویرایش متن و ...	ویرایش متن	یادداشت‌گذاری روی متن نهایی	یادداشت‌گذاری روی متن نهایی	یادداشت‌گذاری روی متن نهایی
طراحی/ مفهوم‌پردازی	طراحی چهارچوب کلی	ویرایش چهارچوب	-	ویرایش چهارچوب
گردآوری داده	گردآوری داده‌ها به روش PRISMA	-	-	-
تحلیل/ تفسیر داده	تحلیل یافته‌ها به روش تحلیل مضمون	اعلام نظر روی چهارچوب	اعلام نظر روی چهارچوب	اعلام نظر روی چهارچوب
سایر نقش‌ها	-	نظارت بر رساله (استاد راهنما)	نظارت بر رساله (استاد مشاور)	نظارت بر رساله (استاد مشاور)

ب) اعلام تعارض منافع

در جریان انتشار مقالات علمی تعارض منافع به این معنی است که نویسنده یا نویسندگان، داوران و یا حتی سردبیران مجلات دارای ارتباطات شخصی و یا اقتصادی می‌باشند که ممکن است به طور ناعادلانه‌ای بر تصمیم‌گیری آن‌ها در چاپ یک مقاله تأثیرگذار باشد. تعارض منافع به خودی خود مشکلی ندارد بلکه عدم اظهار آن است که مسئله‌ساز می‌شود.

بدین وسیله نویسندگان اعلام می‌کنند که رابطه مالی یا غیرمالی با سازمان، نهاد یا اشخاصی که موضوع یا مفاد این تحقیق هستند ندارند، اعم از رابطه و انتساب رسمی یا غیررسمی. منظور از رابطه و انتفاع مالی از جمله عبارت است از دریافت پژوهانه، گرنت آموزشی، ایراد سخنرانی، عضویت سازمانی، افتخاری یا غیررسمی، اشتغال، مالکیت سهام، و دریافت حق اختراع، و البته محدود به این موارد نیست. منظور از رابطه و انتفاع غیرمالی عبارت است از روابط شخصی، خانوادگی یا حرفه‌ای، اندیشه‌ای یا باورمندانه، و غیره.

چنانچه هر یک از نویسندگان تعارض منافعی داشته باشد (و یا نداشته باشد) در فرم زیر تصریح و اعلام خواهد کرد:

مثال: نویسندهٔ الف هیچ‌گونه تعارض منافعی ندارد. نویسندهٔ ب از شرکت فلان که موضوع تحقیق بوده است گرنت دریافت کرده است. نویسندگان ج و د در سازمان فلان که موضوع تحقیق بوده است سخنرانی افتخاری داشته‌اند و در شرکت فلان که موضوع تحقیق بوده است سهام‌دارند.

اظهار (عدم) تعارض منافع: با سلام و احترام؛ به استحضار می‌رساند نویسندگان مقاله هیچ‌گونه تعارض منافعی ندارد.

نویسندهٔ مسئول: سعید کاظم‌پوریان

تاریخ: ۱۴۰۴/۰۸/۲۲