یازدهمین همایش سالانه
بانکداری نوین و
نظام‌های پرداخت

پژوهشکده پولی و بانکی
بانک مرکزی جمهوری اسلامی ایران

بانک مرکزی جمهوری اسلامی ایران

شرکت ملی انفورماتیک

زیست بوم بانکداری هوشمند؛ حکمرانی دیجیتال و نظارت فنّاورانه

تهران، مرکز همایش‌های بین‌المللی برج میلاد ـ ۵ و ۶ آذر ۱۴۰۳ ISC

ارائه چارچوب نوین تعالی فرهنگ امنیت سایبری در بانکداری مدرن

سعید مردانی شهربابک[۱] **علیرضا زالی نژاد**[۲]

چکیده

با توجه به افزایش تهدیدات سایبری در حوزه بانکداری نوین و شرکت‌های فعال در حوزه پرداخت، ارتقای فرهنگ امنیت سایبری به یک ضرورت اساسی تبدیل شده است. این تحقیق به دنبال پاسخگویی به این نیاز، چارچوبی نوین و مبتنی بر ایده‌های جدید را برای ارتقای فرهنگ امنیت سایبری در این صنعت ارائه می‌دهد. علاوه بر این، یک شیوه نوآورانه برای ارزیابی این مدل پیشنهادی نیز طراحی شده است که به‌طور دقیق اثربخشی آن را در سطوح مختلف سازمان مورد بررسی قرار گرفته است.

مزایای این چارچوب شامل نهادینه‌سازی فرهنگ امنیت سایبری در میان تمامی کارکنان و سطوح مختلف سازمان‌های فعال در حوزه بانکداری و پرداخت است. این چارچوب همچنین به بهبود تاب‌آوری در برابر تهدیدات سایبری، افزایش اعتماد مشتریان، و ارتقای کارایی سیستم‌های امنیتی کمک می‌کند.

این تحقیق با ارائه راهکارهای نوآورانه و کاربردی، می‌تواند پایه‌گذار تحولات اساسی در حوزه امنیت سایبری بانکداری نوین و شرکت‌های پرداخت باشد و مسیر جدیدی را برای تحقیقات آتی در این زمینه ایجاد کند.

واژه‌های کلیدی: فرهنگ امنیت سایبری، بانکداری نوین، تهدیدات سایبری، نهادینه‌سازی امنیت، ارزیابی نوآورانه

طبقه‌بندی JEL: G21، G32، L86، M15، O33

[۱] کارشناس عملیات امنیت شرکت شاپرک؛ s.mardani@shaparak.com

[۲] کارشناس عملیات امنیت شرکت شاپرک؛ a.zali@shaparak.com

۱ مقدمه

امروزه در دنیای بانکداری مدرن که به شدت وابسته به فناوری‌های دیجیتال است، تهدیدات سایبری به‌طور مستمر در حال رشد و تحول هستند. حفاظت از دارایی‌های دیجیتال و اطلاعات حساس مشتریان، دیگر تنها به استفاده از ابزارها و فناوری‌های امنیتی محدود نمی‌شود، بلکه نیازمند ایجاد و نهادینه‌سازی یک فرهنگ امنیتی جامع و پایدار در میان کارکنان است (Abraham, 2019). با این حال، چالش اصلی بسیاری از سازمان‌ها و بانک‌ها، فقدان چارچوبی یکپارچه و مؤثر برای توسعه و تقویت فرهنگ امنیت سایبری است.

این مقاله با ارائه یک ایده جدید و کاربردی، برای اولین بار چارچوبی نوین را معرفی می‌کند که بر پایه تحلیل دقیق سیاست‌های امنیتی، تجربیات مدیران امنیت و بررسی حملات سایبری در بانک‌ها طراحی شده است. این مدل نه تنها بر تقویت فرهنگ امنیت سایبری تأکید دارد، بلکه به شکلی ساختاریافته به کاهش ریسک‌ها و تهدیدات سایبری نیز کمک می‌کند. این چارچوب به‌عنوان ابزاری کلیدی برای بانک‌ها و شرکت‌های پرداخت، پایه‌ای علمی و اجرایی برای بهبود فرهنگ امنیت سایبری ارائه می‌دهد و می‌تواند تأثیرات قابل‌توجهی در پایداری و انسجام اقدامات امنیتی داشته باشد.

۲ ضرورت و اهمیت تحقیق

در عصر دیجیتال، بانکداری به یکی از هدف‌های اصلی حملات سایبری تبدیل شده است (Smith, 2020). این حملات، با تهدید دارایی‌های دیجیتال، اطلاعات حساس مشتریان، و اعتماد عمومی به نظام بانکی، ریسک‌های گسترده‌ای را به همراه دارند. بسیاری از سازمان‌ها و بانک‌ها با تکیه بر ابزارهای امنیتی پیشرفته، تلاش کرده‌اند تا از خود در برابر این تهدیدات محافظت کنند(Chaudhary, 2022). اما چالش اصلی همچنان باقی است: نبود یک فرهنگ امنیت سایبری منسجم و پایدار در میان کارکنان. بدون این فرهنگ، حتی بهترین فناوری‌ها و سیاست‌های امنیتی نیز نمی‌توانند به‌طور مؤثر از سازمان‌ها محافظت کنند (Schaik, 2017).

نبود چارچوبی جامع و علمی برای ارتقای فرهنگ امنیت سایبری، اغلب منجر به سستی در رعایت اصول امنیتی، رفتارهای ناهماهنگ و ریسک‌های جدی می‌شود. کارکنانی که نسبت به تهدیدات آگاهی کافی ندارند، به‌راحتی قربانی حملات مهندسی اجتماعی می‌شوند و در مواجهه با موقعیت‌های بحرانی، به‌طور ناخودآگاه ریسک‌های سایبری را افزایش می‌دهند (Alyami, 2023) این عدم توجه به جنبه‌های فرهنگی امنیت، موجب می‌شود که بسیاری از سازمان‌ها علی‌رغم هزینه‌های سنگین برای ابزارها و زیرساخت‌های امنیتی، نتوانند به‌درستی از این سرمایه‌گذاری‌ها بهره‌برداری کنند. چارچوب نوینی که این مقاله ارائه می‌دهد، دقیقاً برای رفع این درد و رنج‌ها طراحی شده است. این مدل به‌صورت ساختاریافته به بانک‌ها و شرکت‌های پرداخت کمک می‌کند تا از طریق تقویت فرهنگ امنیت سایبری، به‌صورت پایدار و مؤثر با تهدیدات سایبری مقابله کنند. (Varakuti, 2020) ضرورت این تحقیق در این است که بدون این چارچوب، سازمان‌ها نه تنها در معرض خطرات جدی سایبری قرار می‌گیرند، بلکه انسجام و کارآمدی تلاش‌های امنیتی خود را نیز از دست خواهند داد.

۳ نوع و روش انجام تحقیق

این تحقیق با هدف ارتقاء فرهنگ امنیت سایبری در حوزه بانکداری و نظام‌های پرداخت انجام شده و به دلیل ارائه مدل جدیدی برای بهبود و پایداری این فرهنگ، از نوع کاربردی ـ توسعه‌ای است. از آنجا که نتایج این پژوهش به‌طور مستقیم در ارتقاء وضعیت امنیت سایبری بانک‌ها و شرکت‌های پرداخت به کار گرفته خواهد شد، این تحقیق بر حل مشکلات واقعی و بهبود عملکرد سازمان‌ها در این زمینه تمرکز دارد.

روش انجام این تحقیق توصیفی ـ تحلیلی است؛ به این صورت که ابتدا به جمع‌آوری و تحلیل داده‌های حاصل از مطالعات اسنادی و نظری پرداخته شده و سپس با بررسی موردی چندین بانک بزرگ و مصاحبه با مدیران امنیت سایبری، اطلاعات لازم برای طراحی چارچوب نوین استخراج گردیده است. این روش به محققان کمک می‌کند تا نه تنها وضعیت فعلی فرهنگ امنیت سایبری را تحلیل کنند (Villanueva, 2020)، بلکه راه‌حل‌های عملی و نوآورانه‌ای را نیز برای بهبود و تعالی آن ارائه دهند.

۴ جامعه آماری و نمونه تحقیق

جامعه آماری این تحقیق شامل گروهی از اساتید، صاحب‌نظران و محققین مراکز دانشگاهی و تحقیقاتی در حوزه بانکداری و امنیت سایبری است. همچنین، مدیران و متخصصان حوزه امنیت سایبری در بانک‌ها و شرکت‌های فعال در زمینه پرداخت الکترونیک نیز بخشی از این جامعه آماری را تشکیل می‌دهند. این افراد به‌عنوان مسئولان اصلی در تدوین و اجرای سیاست‌های امنیت سایبری و ارتقاء فرهنگ امنیت در سازمان‌های خود، نقشی کلیدی در تحقیق دارند.

در این تحقیق، نمونه‌گیری به صورت هدفمند انجام شده است تا افرادی انتخاب شوند که در زمینه امنیت سایبری، بانکداری، و نظام‌های پرداخت تجربه و تخصص کافی داشته باشند. این شامل مدیران امنیت سایبری در بانک‌ها و شرکت‌های وابسته به آن‌ها، کارشناسان امنیت اطلاعات، و مدیران امنیت در شرکت‌های پرداخت الکترونیکی می‌شود. مصاحبه با این افراد و تحلیل نظرات آنان، به غنای علمی و عملی نتایج این تحقیق کمک شایانی کرده و منجر به طراحی چارچوب نوین تعالی فرهنگ امنیت سایبری شده است. جامعه آماری گسترده و متنوع این تحقیق، امکان تحلیل دقیق‌تر نیازها و چالش‌های واقعی در حوزه امنیت سایبری بانک‌ها و نظام‌های پرداخت را فراهم آورده و نتایج تحقیق را به‌صورت قابل‌اعتمادتری برای به‌کارگیری در این بخش‌ها آماده کرده است.

۵ ابزار و روش جمع‌آوری داده‌ها

در این تحقیق، برای دستیابی به داده‌های مورد نیاز و فراهم‌سازی پایه‌های علمی و عملی چارچوب پیشنهادی، از رویکردهای مختلفی برای جمع‌آوری اطلاعات استفاده شده است. داده‌ها از دو منبع اصلی جمع‌آوری شده‌اند: مطالعات اسنادی و مصاحبه‌های عمیق.

۱.۵ مطالعات و بررسی‌های اسنادی

بخش قابل‌توجهی از داده‌های تحقیق از طریق تحلیل منابع معتبر علمی مانند مقالات پژوهشی، کتب تخصصی، پروژه‌های پیشین و گزارش‌های مرتبط با امنیت سایبری در بانکداری و نظام‌های پرداخت الکترونیک به دست آمده است. این منابع شامل جدیدترین دستاوردهای تحقیقاتی در زمینه فرهنگ امنیت سایبری، مدل‌های تعالی و استانداردهای بین‌المللی مرتبط است. تحلیل این داده‌ها به محقق کمک کرد تا با استفاده از پایه‌های علمی موجود، چارچوب نوینی برای بهبود فرهنگ امنیت سایبری تدوین کند.

۲.۵ مصاحبه‌های عمیق

بخش دیگری از داده‌ها از طریق مصاحبه‌های ساختاریافته و نیمه‌ساختاریافته با اساتید، صاحب‌نظران و محققین دانشگاهی، و همچنین مدیران و فعالان امنیت سایبری در بانک‌ها و شرکت‌های پرداخت الکترونیک گردآوری شده است. این مصاحبه‌ها با هدف شناسایی چالش‌های واقعی، مشکلات اجرایی و نیازهای عملی در حوزه ارتقاء فرهنگ امنیت سایبری انجام شده‌اند. نظرات و تجربیات این افراد، نقشی کلیدی در تدوین و اصلاح چارچوب ارائه‌شده ایفا کرده و به غنای پژوهش افزوده‌اند.

این دو روش جمع‌آوری داده‌ها، با ترکیب رویکردهای نظری و عملی، دیدگاهی جامع و چندلایه از وضعیت موجود و نیازهای آینده فرهنگ امنیت سایبری در بانکداری و نظام‌های پرداخت فراهم کرده و به ارائه مدلی کاربردی و نوین منجر شده است که می‌تواند به‌طور مستقیم در بهبود امنیت سایبری در این حوزه‌ها مورد استفاده قرار گیرد.

۶ فرهنگ امنیت سایبری سازمانی

برای ایجاد یک مدل مناسب از فرهنگ امنیت سایبری، ما سه مفهوم کلیدی را بررسی کردیم: فرهنگ سازمانی، فرهنگ امنیت سایبری و فرهنگ امنیت اطلاعات.

فرهنگ سازمانی به رفتارها، باورها و ارزش‌هایی اشاره دارد که در یک سازمان حاکم است. یک متخصص در این زمینه، سه مؤلفه اصلی برای فرهنگ تعریف می‌کند:

۱) **سیستم‌های باور:** این سیستم‌ها پایه‌گذار رفتارهای جمعی هستند و تعیین می‌کنند که چگونه اعضای سازمان به یکدیگر و به وظایف خود نگاه می‌کنند.

۲) **ارزش‌ها:** ارزش‌ها نمایانگر اولویت‌ها و چیزهایی هستند که کارکنان سازمان آنها را مهم می‌دانند. این ارزش‌ها بر روی تصمیم‌گیری‌ها و رفتارهای روزمره تأثیر می‌گذارند.

۳) **آثار و دست‌ساخته‌ها:** این مؤلفه شامل نمادها، رفتارها و الگوهای اجتماعی است که به‌طور ملموس در سازمان دیده می‌شوند. این شامل هنر، فناوری، زبان و مراسم‌های سازمانی است که همه نمایانگر فرهنگ آن سازمان هستند.

علاوه بر این، مدل ارزش‌های متضاد کوئین چهار نوع فرهنگ سازمانی را معرفی می‌کند:

۱) **گرایش حمایتی:** در این نوع فرهنگ، همکاری و اعتماد بین کارکنان بسیار مهم است و تصمیمات به‌طور غیررسمی اتخاذ می‌شوند.

۲) **گرایش نوآوری:** این فرهنگ به خلاقیت و تمایل به تغییر و جستجوی اطلاعات جدید تأکید دارد.

۳) **گرایش قوانین:** در این فرهنگ، به قوانین و رویه‌های رسمی احترام گذاشته می‌شود و ساختار سازمانی به صورت سلسله‌مراتبی است.

۴) **گرایش هدف:** در اینجا، بر تعیین اهداف واضح و معیارهای سنجش عملکرد تأکید می‌شود که نشان‌دهنده درک کارکنان از مسئولیت‌های خود و اهداف سازمان است.

فرهنگ امنیت اطلاعات به‌عنوان یک زیرمجموعه از فرهنگ سازمانی، شامل نگرش‌ها و رفتارهایی است که کارکنان در تعامل با سیستم‌های اطلاعاتی و رویه‌های امنیتی سازمان به کار می‌برند. این فرهنگ به رفتارهای کارکنان در حفاظت از اطلاعات و سیستم‌ها تأثیر می‌گذارد.

فرهنگ امنیت سایبری از فرهنگ امنیت اطلاعات متمایز است. به‌طور خاص، فرهنگ امنیت سایبری به رفتارهایی اشاره دارد که نه تنها به رعایت سیاست‌های امنیتی مربوط می‌شود، بلکه به مشارکت فعال کارکنان در ایجاد یک محیط امن سایبری نیز اشاره دارد. ما فرهنگ امنیت سایبری سازمانی را به‌عنوان «باورها، ارزش‌ها و نگرش‌هایی که رفتارهای کارکنان را در جهت حفاظت و دفاع از سازمان در برابر حملات سایبری هدایت می‌کند» تعریف می‌کنیم.

۷ مدل فرهنگ امنیت سایبری

هدف اصلی برای مدیران این است که رفتارهای امن سایبری را در سازمان ایجاد کنند. این هدف با شکل‌گیری فرهنگ امنیت سایبری سازمانی (شامل باورها، ارزش‌ها و نگرش‌ها) محقق می‌شود. فرهنگ نیز تحت تأثیر عوامل خارجی و مکانیزم‌های داخلی سازمان قرار دارد که مدیران از آنها استفاده می‌کنند.

مدل معرفی شده شامل چهار مؤلفه اصلی است:

۱) **رفتارهای سایبری:** این رفتارها شامل دو دسته هستند:

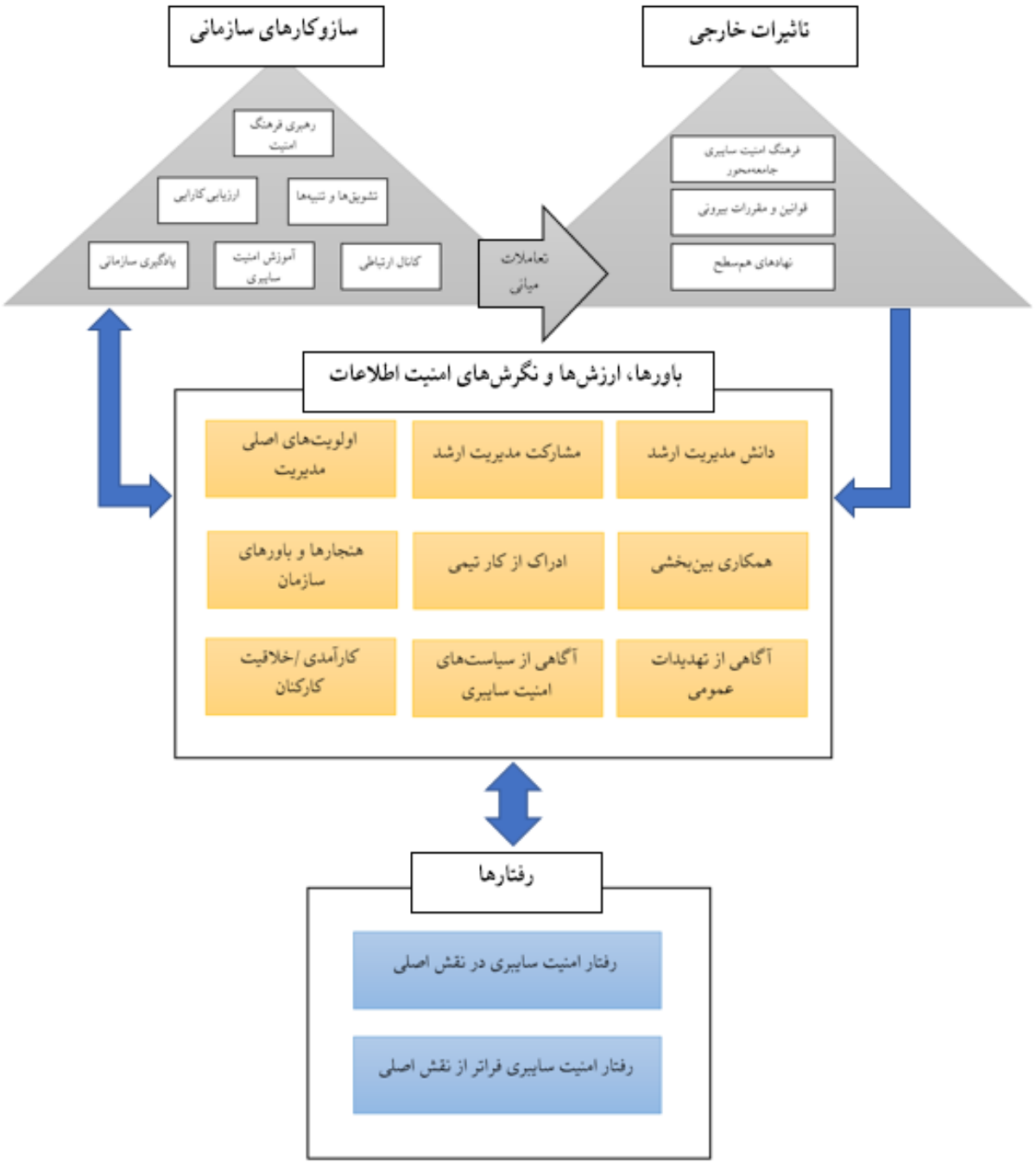
- **رفتارهای درون‌نقش:** اقداماتی که کارکنان در حیطه وظایف رسمی خود انجام می‌دهند، مانند رعایت سیاست‌های امنیتی و کاهش تخلفات.
- **رفتارهای فراتر از نقش:** اقداماتی که کارکنان خارج از وظایف رسمی خود انجام می‌دهند، مانند کمک به دیگران و ابراز نظرات برای بهبود وضعیت امنیت سایبری.

۲) **باورها، ارزش‌ها و نگرش‌ها:** این مؤلفه شامل ارزش‌ها و نگرش‌های غیررسمی است که در رفتارهای کارکنان نمایان می‌شود. هر چه کارکنان به امنیت سایبری بیشتر باور داشته باشند، احتمال بیشتری وجود دارد که رفتارهای امن‌تری از خود نشان دهند.

۳) **مکانیزم‌های سازمانی:** این مکانیزم‌ها شامل اقداماتی است که مدیران برای تقویت فرهنگ امنیت سایبری انجام می‌دهند. به‌عنوان مثال، این می‌تواند شامل آموزش، ارزیابی عملکرد و ایجاد کانال‌های ارتباطی مؤثر باشد.

۴) **تأثیرات خارجی:** این تأثیرات شامل فشارهای اجتماعی و مقررات دولتی هستند که می‌توانند به شکل‌گیری فرهنگ امنیت سایبری در سازمان کمک کنند. برای مثال، رسانه‌ها یا قوانین دولتی می‌توانند آگاهی کارکنان را نسبت به تهدیدات سایبری افزایش دهند.

این مدل به مدیران کمک می‌کند تا بتوانند فرهنگ امنیت سایبری را در سازمان ایجاد کنند، آن را اندازه‌گیری کنند و بر رفتارهای امن تأثیر بگذارند. همچنین در ادامه شیوه‌ای برای ارزیابی این مدل پیشنهادی ارائه شده است.



شکل ۱ . مدل فرهنگ امنیت سایبری سازمانی

این مدل نه تنها بر تقویت فرهنگ امنیت سایبری تأکید دارد، بلکه به شکلی ساختاریافته به کاهش ریسک‌ها و تهدیدات سایبری نیز کمک می‌کند. در ادامه جزییات هر یک از مؤلفه‌های هر بخش این مدل تشریح شده است.

۱.۷ رفتارهای سایبری

رفتارهای سایبری یکی از مؤلفه‌های کلیدی در فرهنگ امنیت سایبری سازمانی است. این رفتارها به دو دسته تقسیم می‌شوند:

۱) رفتارهای درون‌نقش:

- این رفتارها شامل اقداماتی است که کارکنان به‌عنوان بخشی از مسئولیت‌های شغلی خود انجام می‌دهند. این شامل رعایت سیاست‌های امنیتی، کاهش سوءاستفاده از فناوری و پرهیز از نقض قوانین است.
- برای مثال، کارکنان باید از استفاده از رمزهای عبور قوی و عدم به اشتراک‌گذاری اطلاعات حساس اطمینان حاصل کنند.

۲) رفتارهای فراتر از نقش:

- این رفتارها شامل اقداماتی هستند که خارج از وظایف رسمی کارکنان قرار می‌گیرند، مانند کمک به همکاران در مسائل امنیت سایبری یا بیان نظرات و پیشنهادات برای بهبود وضعیت امنیت در سازمان.
- به‌ویژه، رفتارهایی مانند «صدای بلند» و همکاری در شناسایی تهدیدات سایبری می‌تواند تأثیر زیادی بر امنیت کلی سازمان داشته باشد.

۲.۷ باورها، ارزش‌ها و نگرش‌ها

باورها، ارزش‌ها و نگرش‌ها به عنوان هسته فرهنگ امنیت سایبری عمل می‌کنند. این موارد شامل:

- **باورها:** اعتقادات کارکنان درباره اهمیت امنیت سایبری و تأثیر آن بر سازمان.
- **ارزش‌ها:** اولویت‌هایی که کارکنان به امنیت سایبری می‌دهند، مانند همکاری و مسئولیت‌پذیری.
- **نگرش‌ها:** نگرش‌های مثبت یا منفی کارکنان نسبت به سیاست‌های امنیتی و اقدامات حفاظتی.

اگر کارکنان باور داشته باشند که امنیت سایبری مسئولیت همه است، احتمالاً رفتارهایی را انجام خواهند داد که به حفظ امنیت سازمان کمک کند.

۳.۷ مکانیزم‌های سازمانی

مکانیزم‌های سازمانی شامل اقداماتی هستند که مدیران برای تقویت فرهنگ امنیت سایبری انجام می‌دهند. این مکانیزم‌ها می‌توانند شامل موارد زیر باشند:

- **رهبری:** تعیین فردی یا تیمی با مسئولیت رسمی برای ایجاد فرهنگ امنیت سایبری.
- **ارزیابی عملکرد:** گنجاندن معیارهای مربوط به رفتارهای امنیت سایبری در فرآیندهای ارزیابی عملکرد کارکنان.
- **آموزش:** ارائه آموزش‌های مداوم به کارکنان درباره شیوه‌های بهبود امنیت سایبری.
- **کانال‌های ارتباطی:** ایجاد ارتباطات مؤثر برای گزارش‌دهی تهدیدات و اشتراک‌گذاری اطلاعات مربوط به امنیت.

۴.۷ تأثیرات خارجی

تأثیرات خارجی شامل عواملی هستند که به فرهنگ امنیت سایبری در سازمان شکل می‌دهند، از جمله:

- **فرهنگ سایبری جامعه:** ارزش‌ها و باورهای جامعه‌ای که سازمان در آن فعالیت می‌کند.
- **قوانین و مقررات:** قوانین و مقررات دولتی که به سازمان‌ها الزاماتی را برای حفاظت از اطلاعات تحمیل می‌کند.
- **فشار از طرف نهادهای همتایان:** تلاش‌هایی که سازمان‌ها برای پیروی از استانداردهای برتر امنیت سایبری انجام می‌دهند.

۸ الزامات مدل گسترش و ارتقای فرهنگ امنیت سایبری در حوزه بانکداری نوین

با توجه به گسترش بانکداری دیجیتال و افزایش تهدیدات سایبری، نیاز به توسعه فرهنگ امنیت سایبری در بانک‌ها و مؤسسات مالی بیش از گذشته احساس می‌شود. (Smith, 2020) فرهنگ امنیت سایبری نه تنها از طریق قوانین و مقررات قابل پیاده‌سازی است، بلکه نیاز به تغییر نگرش و رفتار کارکنان و مدیران نیز دارد. در این راستا، چندین الزام و عامل کلیدی برای گسترش و ارتقای فرهنگ امنیت سایبری در حوزه بانکداری نوین مطرح می‌شود که در ادامه به تفصیل به آن‌ها پرداخته می‌شود.

۱.۸ آموزش مستمر و آگاهی‌سازی کارکنان

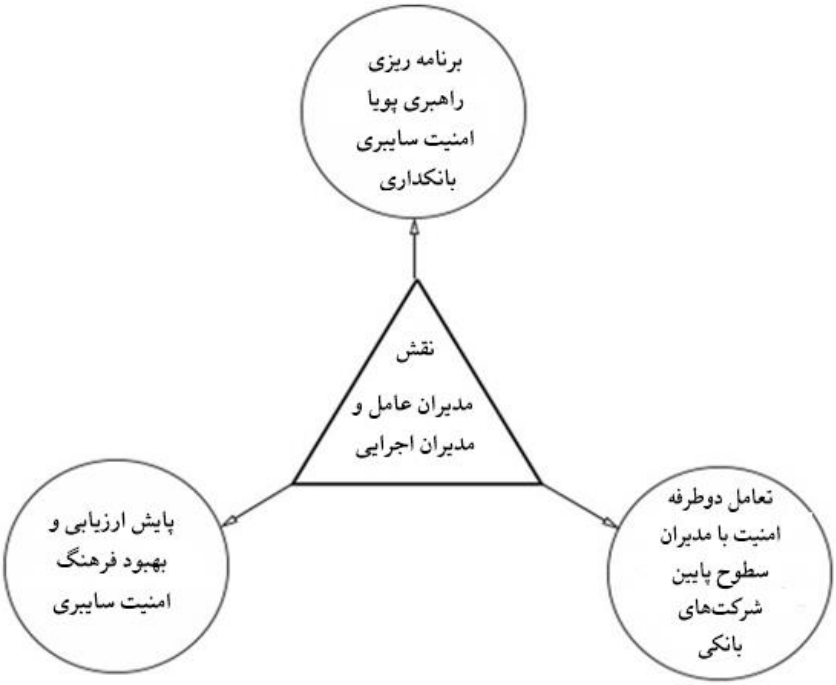
یکی از اصلی‌ترین الزامات ارتقای فرهنگ امنیت سایبری در بانکداری نوین، آموزش مداوم و افزایش آگاهی کارکنان است. (Chaudhary, 2020) به دلیل تغییرات سریع در تکنولوژی و ظهور تهدیدات جدید، آموزش امنیت سایبری باید همواره به‌روز باشد. برنامه‌های آموزشی شامل آموزش‌های تئوریک و عملی برای تمامی سطوح سازمان، از مدیران ارشد تا کارکنان معمولی، باید به‌طور منظم برگزار شود. بانک‌ها باید از ابزارهای متنوعی مانند کارگاه‌های آموزشی، ویدئوهای تعاملی و شبیه‌سازی حملات سایبری برای افزایش آگاهی کارکنان خود استفاده کنند. آموزش امنیت سایبری همچنین باید به‌گونه‌ای طراحی شود که به کارکنان کمک کند تا رفتارهای صحیح امنیتی را در کارهای روزمره خود پیاده‌سازی کنند.

۲.۸ پیاده‌سازی سیستم‌های انگیزشی برای بهبود امنیت

فرهنگ امنیت سایبری قوی زمانی محقق می‌شود که سیستم‌های انگیزشی مناسبی برای کارکنان وجود داشته باشد. این سیستم‌ها باید شامل پاداش‌های ملموس و معنوی برای افرادی باشد که در بهبود امنیت سایبری سازمان مشارکت دارند. (Yerby, 2018) برای مثال، می‌توان برنامه‌هایی را برای تشویق گزارش‌دهی رفتارهای مشکوک یا حملات احتمالی سایبری راه‌اندازی کرد. این پاداش‌ها می‌تواند شامل ارتقای شغلی، جوایز مالی یا تقدیر رسمی از کارکنان باشد.

۳.۸ ارزیابی مداوم ریسک‌ها و به‌روزرسانی سیاست‌ها

یکی از الزامات مهم برای ارتقای فرهنگ امنیت سایبری، ارزیابی مداوم ریسک‌ها و تهدیدات جدید است. با توجه به تغییرات سریع در محیط سایبری، سیاست‌ها و پروتکل‌های امنیتی نیز باید به‌طور مرتب مورد بازبینی و به‌روزرسانی قرار گیرند. بانک‌ها باید از ابزارهای ارزیابی ریسک‌های امنیت سایبری برای شناسایی نقاط ضعف خود استفاده کنند و به سرعت پاسخ دهند.

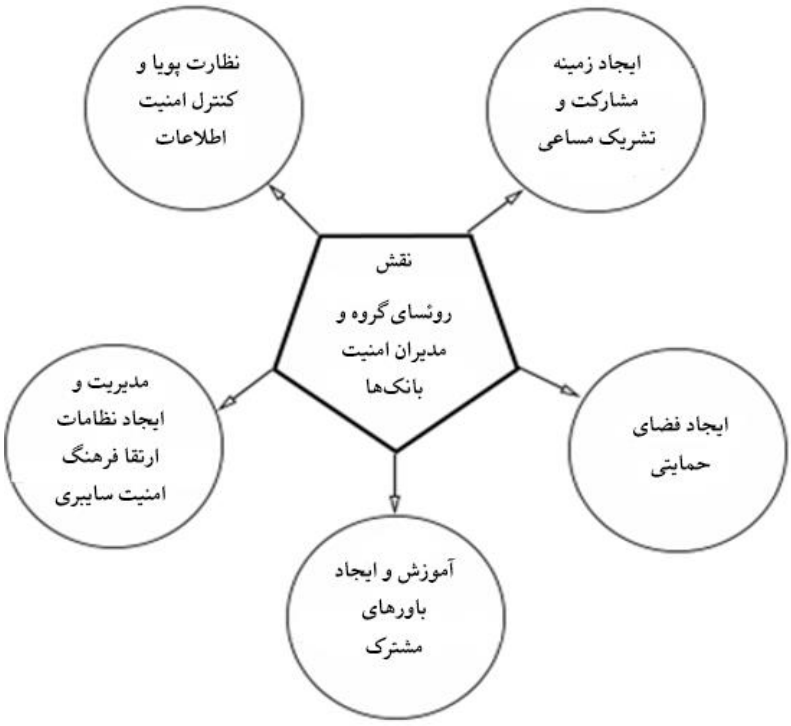


شکل ۲ . نقش مدیریت عامل و مدیران اجرایی در ارتقاء فرهنگ امنیت سایبری در بانک‌ها

در شکل ۲ ، نقش مدیریت عامل و مدیران اجرایی در ارتقاء فرهنگ امنیت سایبری در بانک‌ها توضیح داده شده است. مدیران ارشد باید نقش فعال در تدوین و اجرای سیاست‌های امنیتی ایفا کنند و از تطابق آن‌ها با استانداردهای بین‌المللی اطمینان حاصل کنند.

۴.۸ تعامل فعال بین واحدهای فنی و کسب‌وکار

یکی از چالش‌های مهم در ایجاد فرهنگ امنیت سایبری در بانک‌ها، فاصله بین تیم‌های فنی و کسب‌وکار است. برای پیاده‌سازی موفق امنیت سایبری، نیاز است که این دو بخش به‌طور مداوم با یکدیگر همکاری کنند. تیم‌های امنیت سایبری باید به‌طور مداوم با تیم‌های کسب‌وکار در تعامل باشند تا مطمئن شوند که تمامی جنبه‌های امنیتی در فرآیندهای تجاری مدنظر قرار گرفته است.



شکل ۳. نقش رفتار رؤسای گروه و مدیران امنیت بانک‌ها در ارتقاء فرهنگ امنیت بانکداری

در شکل ۳، نقش رفتار رؤسای گروه و مدیران امنیت بانک‌ها در ارتقاء فرهنگ امنیت بانکداری به‌طور شماتیک نشان داده شده است. این تعامل باید به شکلی باشد که بخش‌های کسب‌وکار اهمیت امنیت سایبری را درک کنند و از آن به عنوان یک عامل کلیدی در موفقیت تجاری خود استفاده کنند.

۵.۸ نهادینه‌سازی امنیت در فرهنگ سازمانی

یکی از الزامات اساسی برای ایجاد و ارتقای فرهنگ امنیت سایبری، نهادینه‌سازی امنیت به‌عنوان یک ارزش سازمانی است. به این معنا که امنیت سایبری نباید تنها به عنوان یک وظیفه اضافی یا یک الزام قانونی دیده شود، بلکه باید به‌عنوان یک جزء اساسی از هویت سازمان و یک اولویت استراتژیک در نظر گرفته شود. این امر مستلزم ایجاد یک فرهنگ امنیتی جامع است که در آن تمامی سطوح سازمان به امنیت سایبری اهمیت بدهند.

برای نهادینه کردن این فرهنگ، لازم است که مدیران ارشد به‌طور مداوم به اهمیت امنیت سایبری تأکید کنند و به کارکنان نشان دهند که امنیت سایبری یک ضرورت استراتژیک است. شکل ۲ به‌خوبی نقش مدیران در نهادینه کردن این ارزش سازمانی را نشان می‌دهد.

۶.۸ استفاده از ابزارها و فناوری‌های نوین

برای ارتقای فرهنگ امنیت سایبری، بانک‌ها باید از فناوری‌های نوین در زمینه امنیت سایبری بهره ببرند. استفاده از ابزارهای پیشرفته مانند هوش مصنوعی، یادگیری ماشین، و تحلیل داده‌های بزرگ برای شناسایی و مقابله با تهدیدات

سایبری امری ضروری است. این فناوری‌ها به بانک‌ها کمک می‌کند تا تهدیدات بالقوه را پیش‌بینی کنند و به‌طور پیشگیرانه از وقوع حملات جلوگیری کنند.

علاوه بر این، استفاده از فناوری‌های خودکار برای نظارت بر رفتارهای مشکوک و تحلیل لاگ‌های سیستم می‌تواند به بهبود سرعت واکنش به تهدیدات کمک کند.

۷.۸ مدیریت تغییرات و انطباق با استانداردها

در دنیای امروز، استانداردها و مقررات مربوط به امنیت سایبری به‌طور مداوم در حال تغییر هستند؛ بنابراین، یکی از الزامات مهم برای ارتقای فرهنگ امنیت سایبری در بانکداری نوین، مدیریت تغییرات و تطابق با استانداردهای جدید است. بانک‌ها باید خود را با استانداردهای بین‌المللی مانند ISO 27001 و NIST منطبق کنند و از رعایت آن‌ها در تمامی بخش‌های سازمان اطمینان حاصل کنند.

۸.۸ ایجاد شفافیت و ارتباطات مؤثر در سازمان

برای تقویت فرهنگ امنیت سایبری، شفافیت و ارتباطات مؤثر در سازمان ضروری است (Pramod,2014).بانک‌ها باید از طریق ایجاد فرآیندهای شفاف در ارتباط با امنیت سایبری، کارکنان را در جریان تغییرات و خطرات احتمالی قرار دهند. ارتباطات منظم بین واحدهای مختلف سازمان می‌تواند به کاهش سوءتفاهم‌ها و تقویت همکاری‌های داخلی کمک کند.

در نهایت، این الزامات به ایجاد و ارتقای یک فرهنگ امنیت سایبری قوی در بانکداری نوین منجر می‌شود که نه‌تنها امنیت اطلاعات و سیستم‌ها را تضمین می‌کند، بلکه باعث افزایش اعتماد مشتریان و بهبود عملکرد کلی بانک می‌شود.

۹ مؤلفه‌های خط سیر ارتقا فرهنگ امنیت سایبری در حوزه بانکداری نوین

در ادامه، روندی برای نشان دادن مراحل خط سیر این ارتقا فرهنگ امنیت با استفاده از چارچوب و مدل معرفی شده برای ارتقای فرهنگ امنیت سایبری در حوزه بانکداری نوین طراحی شده است که در قالب یک جدول در ذیل آورده شده است. این جدول شامل عناوین کلیدی هر مرحله از این خط سیر است و رویکردی جدید و کاربردی برای پیاده‌سازی فرهنگ امنیت سایبری ارائه می‌دهد.

جدول ۱

تشریح مؤلفه‌های خط سیر ارتقا فرهنگ امنیت سایبری در بانکداری نوین

مرحله	عنوان مرحله	توضیحات کلیدی
مرحله ۱	تحلیل و شناسایی ریسک‌های فرهنگی و سازمانی	شناسایی نقاط ضعف فرهنگی سازمان در زمینه امنیت سایبری
مرحله ۲	طراحی برنامه آموزشی جامع و هدفمند	طراحی دوره‌های آموزشی برای تمامی سطوح سازمان بر اساس نیازهای خاص بانک
مرحله ۳	ایجاد انگیزه‌های سایبری برای کارکنان	توسعه سیستم‌های پاداش و تشویق برای رفتارهای امنیت‌محور
مرحله ۴	پیاده‌سازی سیستم‌های خودارزیابی فرهنگی	راه‌اندازی ابزارهای خودارزیابی رفتارهای امنیتی توسط کارکنان و مدیران
مرحله ۵	تقویت ارتباطات بین واحدهای فنی و تجاری	تقویت همکاری‌های میان تیم‌های امنیت سایبری و بخش‌های کسب‌وکار
مرحله ۶	نهادینه‌سازی ارزش امنیت در اهداف استراتژیک	نهادینه‌کردن امنیت سایبری به عنوان بخشی از مأموریت و اهداف سازمان
مرحله ۷	ارزیابی و به‌روزرسانی مستمر سیاست‌های امنیتی	ارزیابی دوره‌ای و به‌روزرسانی سیاست‌ها و رویه‌ها برای مقابله با تهدیدات جدید
مرحله ۸	پیاده‌سازی فناوری‌های نوین و پیشرفته	استفاده از ابزارهای پیشرفته مانند هوش مصنوعی و تحلیل داده‌ها برای بهبود امنیت
مرحله ۹	ایجاد محیط کار با فرهنگ سایبری مثبت	ایجاد فضای کاری که رفتارهای امنیتی را تقویت و حمایت کند
مرحله ۱۰	سنجش مداوم تأثیرات و موفقیت برنامه	ارزیابی مداوم تأثیرات و تغییرات در فرهنگ امنیت
مرحله ۱۱	بهبود مستمر و توسعه مداوم فرهنگ امنیتی	بازبینی و بهبود مستمر فرآیندها و استراتژی‌های امنیت سایبری بر اساس بازخوردها
مرحله ۱۲	مدیریت ریسک در خطسیر ارتقای فرهنگ امنیت سایبری	شناسایی و کاهش ریسک‌های انسانی و سازمانی برای بهبود فرهنگ امنیت.

این خط سیر جدید با تأکید بر نوآوری در هر مرحله، به بانک‌ها کمک می‌کند تا فرهنگ امنیت سایبری خود را به سطحی بالاتر ارتقا دهند در ادامه جزییات هر کدام از این مراحل شرح داده شده است.

ایده و مدل نوین برای ارتقای فرهنگ امنیت سایبری در حوزه بانکداری نوین بر اساس یک رویکرد چندمرحله‌ای طراحی شده است که هر مرحله به شکلی تخصصی و کاربردی اجرا می‌شود. در ادامه، هر یک از مراحل این مدل با جزئیات شرح داده شده است:

۱.۹ تحلیل و شناسایی ریسک‌های فرهنگی و سازمانی

این مرحله شامل بررسی وضعیت موجود سازمان از لحاظ فرهنگ امنیت سایبری است. در این گام باید نقاط ضعف فرهنگی که ممکن است منجر به ریسک‌های امنیتی شود، شناسایی گردد. روش‌های شناسایی ریسک شامل مصاحبه با کارکنان، ارزیابی فرهنگ سازمانی فعلی و تحلیل رفتارهای امنیتی موجود است.

- **ابزارها:** استفاده از ابزارهای سنجش فرهنگ سازمانی و ابزارهای تحلیل رفتارهای امنیتی.
- **نتیجه:** شناسایی نقاط ضعف و ریسک‌های فرهنگی در حوزه امنیت سایبری که مانع از ایجاد فرهنگ امنیتی مؤثر در سازمان می‌شود.

۲.۹ طراحی برنامه آموزشی جامع و هدفمند

در این مرحله، برنامه‌های آموزشی ویژه‌ای برای تمامی سطوح سازمان، از مدیران ارشد تا کارکنان اجرایی، طراحی می‌شود. این برنامه‌ها باید بر اساس نیازهای واقعی بانک و تحلیل ریسک‌های فرهنگی توسعه یابد. موضوعات کلیدی شامل امنیت اطلاعات، شناخت تهدیدات سایبری، و بهترین شیوه‌های مدیریت امنیت سایبری است.

- **ابزارها:** برنامه‌های آموزش الکترونیک (E-learning)، جلسات حضوری و آموزش‌های تعاملی.
- **نتیجه:** افزایش آگاهی کارکنان از تهدیدات امنیتی و آماده‌سازی آنها برای مقابله با چالش‌های امنیت سایبری.

۳.۹ ایجاد انگیزه‌های سایبری برای کارکنان

ایجاد سیستم‌های انگیزشی که به کارکنان در تقویت رفتارهای امنیت‌محور انگیزه دهد. پاداش‌های مالی و غیرمالی مانند ارتقا شغلی، تشویق‌های عمومی و امکانات رفاهی، می‌تواند مؤثر باشد. این مرحله شامل تشویق رفتارهای مثبت مرتبط با امنیت سایبری و تقویت فرهنگ مسئولیت‌پذیری است.

- **ابزارها:** سیستم‌های پاداش و برنامه‌های تشویقی، برنامه‌های شناسایی دستاوردهای امنیتی.
- **نتیجه:** افزایش انگیزه کارکنان برای رعایت الزامات امنیتی و ترویج رفتارهای مسئولانه در قبال امنیت سایبری.

۴.۹ پیاده‌سازی سیستم‌های خودارزیابی فرهنگی

توسعه ابزارهایی که کارکنان و مدیران بتوانند خودشان را از نظر فرهنگ و رفتارهای امنیتی ارزیابی کنند. این سیستم‌ها باید امکان شناسایی ضعف‌ها و فرصت‌های بهبود را فراهم کنند و به کاربران کمک کنند تا خودشان درک بهتری از موقعیت امنیتی‌شان پیدا کنند.

- **ابزارها:** پرسشنامه‌های خودارزیابی، نرم‌افزارهای مانیتورینگ رفتار امنیتی.
- **نتیجه:** شناسایی خودکار ضعف‌های امنیتی فردی و تیمی و تلاش برای بهبود مستمر.

۵.۹ تقویت ارتباطات بین واحدهای فنی و تجاری

در این مرحله باید همکاری نزدیک‌تری بین تیم‌های فنی مانند تیم‌های IT و امنیت سایبری و واحدهای تجاری بانک برقرار شود تا درک مشترکی از اهمیت امنیت سایبری شکل بگیرد. ارتباطات قوی‌تر باعث تسهیل در حل مسائل امنیتی و اتخاذ تصمیمات امنیتی بهتر می‌شود.

- **ابزارها:** جلسات مشترک، گروه‌های کاری چندرشته‌ای، سیستم‌های همکاری دیجیتال.
- **نتیجه:** تقویت همکاری بین واحدهای فنی و تجاری و افزایش هماهنگی در پیاده‌سازی امنیت سایبری.

۶.۹ نهادینه‌سازی ارزش امنیت در اهداف استراتژیک

امنیت سایبری باید به عنوان بخشی از اهداف استراتژیک سازمان تعریف شود. این مرحله شامل گنجاندن امنیت در چشم‌انداز سازمان، خط‌مشی‌ها و استراتژی‌های بلندمدت بانک است. مدیران باید امنیت سایبری را به عنوان یک اولویت مهم در تصمیم‌گیری‌ها و سرمایه‌گذاری‌ها لحاظ کنند.

- **ابزارها:** تدوین خط‌مشی‌های امنیتی و ادغام آنها در اهداف کلان سازمانی.

- **نتیجه:** نهادینه‌سازی امنیت سایبری به عنوان یک عنصر اساسی در استراتژی و عملکرد سازمان.

۷.۹ ارزیابی و به‌روزرسانی مستمر سیاست‌های امنیتی

سیاست‌های امنیتی باید به طور منظم مورد ارزیابی و به‌روزرسانی قرار گیرند تا با تغییرات فناوری و تهدیدات جدید هماهنگ باشند. این مرحله شامل ارزیابی دوره‌ای سیاست‌ها، رویه‌ها و اقدامات امنیتی و به‌روزرسانی آنها بر اساس نتایج ارزیابی‌ها است.

- **ابزارها:** بررسی‌های دوره‌ای، تحلیل‌های امنیتی و استفاده از استانداردهای جدید امنیت سایبری.
- **نتیجه:** سیاست‌های امنیتی به‌روز و کارآمد که با تغییرات فناوری و تهدیدات سایبری همگام هستند.

۸.۹ پیاده‌سازی فناوری‌های نوین و پیشرفته

استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی (AI)، یادگیری ماشین (ML)، تحلیل کلان داده‌ها و اتوماسیون برای بهبود امنیت سایبری. این فناوری‌ها می‌توانند به شناسایی تهدیدات، تحلیل رفتارها و جلوگیری از حملات کمک کنند.

- **ابزارها:** سیستم‌های تحلیل داده‌ها، نرم‌افزارهای مدیریت ریسک، ابزارهای هوش مصنوعی.
- **نتیجه:** استفاده از فناوری‌های پیشرفته برای بهبود پیش‌بینی تهدیدات و واکنش سریع‌تر به آنها.

۹.۹ ایجاد محیط کار با فرهنگ سایبری مثبت

ایجاد محیط کاری که رفتارهای امنیتی و سایبری را تقویت کند و کارکنان را به رعایت اصول امنیتی تشویق نماید. محیط کار باید تعاملات سالم و مسئولانه را ترویج دهد و به کارکنان امکان دهد تا به راحتی مسائل امنیتی را گزارش دهند.

- **ابزارها:** سیستم‌های مدیریت رفتار سازمانی، برنامه‌های توسعه فرهنگی و امنیتی.
- **نتیجه:** ایجاد یک فرهنگ کاری مثبت که امنیت سایبری را تقویت و ترویج می‌کند.

۱۰.۹ سنجش مداوم تأثیرات و موفقیت برنامه

در این مرحله، تأثیرات برنامه ارتقا فرهنگ امنیت سایبری سنجیده می‌شود. این سنجش شامل ارزیابی میزان تغییرات در رفتارهای امنیتی کارکنان و تأثیر کلی آن بر امنیت سازمان است.

- **ابزارها:** تحلیل داده‌ها و گزارش‌های دوره‌ای، ابزارهای سنجش موفقیت برنامه.
- **نتیجه:** شناسایی نقاط قوت و ضعف برنامه ارتقا و اعمال تغییرات لازم برای بهبود بیشتر.

۱۱.۹ بهبود مستمر و توسعه مداوم فرهنگ امنیتی

این مرحله بر بهبود مستمر و توسعه مداوم فرهنگ امنیتی متمرکز است. برنامه‌های امنیت سایبری باید با بازخوردهای داخلی و تهدیدات جدید به‌روز شوند و استراتژی‌های جدیدی برای تقویت فرهنگ امنیتی ایجاد شود.

- **ابزارها:** بازخوردهای منظم کارکنان، جلسات دوره‌ای بهبود و توسعه فرهنگ امنیتی.

- **نتیجه:** بهبود مستمر و پیشرفت در فرهنگ امنیت سایبری بانک و بهبود واکنش به تهدیدات جدید.

این مراحل به صورت یکپارچه و مستمر اجرا می‌شوند تا فرهنگ امنیت سایبری در سازمان بهبود یافته و بانک بتواند با تهدیدات سایبری نوین مقابله کند

۱۲.۹ مدیریت ریسک در خطسیر ارتقای فرهنگ امنیت سایبری

مدیریت ریسک به‌عنوان یکی از مؤلفه‌های اصلی در ارتقای فرهنگ امنیت سایبری، تمرکز خود را بر شناسایی، ارزیابی، کنترل، و نظارت بر ریسک‌های مرتبط با عوامل انسانی، فرآیندهای سازمانی، و فناوری‌های نوین قرار می‌دهد. این مؤلفه شامل اقدامات زیر است:

۱.۱۲.۹ تحلیل ریسک‌های فرهنگی

تحلیل دقیق ریسک‌هایی که مستقیماً بر فرهنگ امنیت سایبری تأثیر می‌گذارند، با استفاده از چارچوب‌هایی مانند OCTAVE یا FAIR انجام می‌شود. این تحلیل به ارزیابی شکاف‌های رفتاری در سازمان، مانند سطح پایین آگاهی امنیتی یا عدم پایبندی به رویه‌های امنیتی، کمک می‌کند.

۲.۱۲.۹ اولویت‌بندی ریسک‌های بحرانی در رفتارهای امنیتی

ریسک‌های مرتبط با رفتار کارکنان مانند فیشینگ، افشای اطلاعات محرمانه، یا تنظیمات نادرست سیستم‌ها بر اساس شدت و احتمال وقوع اولویت‌بندی می‌شوند. این فرآیند با استفاده از متریک‌هایی نظیر تعداد رخدادهای امنیتی انسانی و میزان خسارت احتمالی انجام می‌شود.

۳.۱۲.۹ ادغام مدیریت ریسک در آموزش و آگاهی‌سازی

برای کاهش ریسک‌های شناسایی‌شده، برنامه‌های آموزشی و شبیه‌سازی حملات سایبری طراحی می‌شوند. این برنامه‌ها بر رفتارهای پرریسک شناسایی‌شده تمرکز داشته و با استفاده از داده‌های ریسک به‌روزرسانی می‌شوند. برای مثال، آموزش مقابله با حملات فیشینگ می‌تواند با استفاده از کمپین‌های آزمایشی و تحلیل میزان شکست کارکنان در این آزمون‌ها اجرا شود.

۴.۱۲.۹ طراحی سیاست‌های سازمانی مبتنی بر ریسک

سیاست‌های امنیتی باید متناسب با ریسک‌های رفتاری و فرآیندی سازمان طراحی شوند. برای نمونه، تنظیم سیاست‌های حداقل‌سازی دسترسی (Least Privilege) یا الزام به احراز هویت چندعاملی (MFA) در واکنش به رفتارهای پرخطر کارکنان از ریسک‌های غیرضروری جلوگیری می‌کند.

۵.۱۲.۹ ارزیابی مستمر اثربخشی اقدامات کاهش ریسک

شاخص‌های کلیدی عملکرد (KPIs) برای ارزیابی اثربخشی اقدامات کاهش ریسک تعریف می‌شوند. این شاخص‌ها شامل کاهش نرخ وقوع رخدادهای انسانی، افزایش تعداد گزارشات امنیتی از سوی کارکنان، و بهبود امتیازهای ارزیابی امنیتی داخلی است.

۶.۱۲.۹ تطبیق مستمر با تغییرات ریسک‌زا

در حوزه بانکداری نوین، ماهیت ریسک‌ها به دلیل تغییرات سریع فناوری و روش‌های حمله متغیر است. استفاده از ابزارهای تحلیل ریسک تطبیقی (Adaptive Risk Assessment) و ادغام با سامانه‌های مدیریت اطلاعات و رویدادهای امنیتی (SIEM) برای نظارت بر رفتارهای غیرعادی، مدیریت ریسک را با فرهنگ امنیتی همسو می‌سازد.

این بخش تخصصی، نشان‌دهنده ضرورت مدیریت دقیق و سیستماتیک ریسک‌های مرتبط با رفتار کارکنان و سیاست‌های سازمانی در ایجاد و نگهداری فرهنگ امنیت سایبری در بانکداری نوین است.

۱۰ شیوه ارزیابی چارچوب پیشنهادی

در راستای ارتقاء فرهنگ امنیت سایبری در حوزه بانکداری نوین و شرکت‌های پرداخت، چارچوب‌های مختلفی برای پیاده‌سازی و بهبود فرهنگ امنیتی طراحی شده‌اند. با این حال، یکی از چالش‌های کلیدی در این حوزه، ارزیابی دقیق و مستمر عملکرد این چارچوب‌ها و میزان تأثیرگذاری آن‌هاست. مدل ارائه‌شده در اینجا بر اساس یک رویکرد نوین، به‌عنوان بخشی از چارچوب اصلی طراحی شده است که به‌طور خاص برای ارزیابی مستمر و کارآمد میزان پیشرفت و تأثیر فرهنگ امنیت سایبری در سازمان‌های بانکی و پرداختی کاربرد دارد.

این بخش از چارچوب به سازمان‌ها این امکان را می‌دهد تا با استفاده از معیارهای کمی و کیفی و ابزارهای پیشرفته ارزیابی، وضعیت فرهنگ امنیت سایبری خود را به‌صورت منظم پایش کنند. این مدل نه‌تنها به ارزیابی موفقیت برنامه‌های ارتقای امنیت سایبری می‌پردازد، بلکه با فراهم کردن دیدی جامع و دقیق از نقاط قوت و ضعف، به بهبود مستمر و هدفمند این فرهنگ کمک می‌کند.

در این روش، مراحل ارزیابی به گونه‌ای طراحی شده‌اند که با نیازهای خاص بانکداری نوین و شرکت‌های پرداخت سازگار باشند. به عبارت دیگر، این مدل بخشی از یک چارچوب جامع‌تر است که سازمان‌ها را قادر می‌سازد تا در مسیر بهبود امنیت سایبری، گام‌های مؤثری بردارند.

در ادامه، جدول ارزیابی این بخش از چارچوب ارائه شده است که به‌طور خلاصه مراحل کلیدی برای ارزیابی و پایش مداوم فرهنگ امنیت سایبری در این سازمان‌ها را نشان می‌دهد. جدول زیر نشان‌دهنده مراحل کلیدی ارزیابی چارچوب نوین ارتقاء فرهنگ امنیت سایبری است که به‌طور خاص برای حوزه بانکداری نوین و شرکت‌های فعال در صنعت پرداخت طراحی شده است. هر مرحله به‌طور کامل بر موضوعات اصلی امنیت سایبری در این حوزه‌ها متمرکز بوده و از ابزارها و معیارهای مشخص برای ارزیابی وضعیت فعلی و بهبود مستمر استفاده می‌کند.

جدول ۲

ارزیابی چارچوب نوین ارتقاء فرهنگ امنیت سایبری در حوزه بانکداری نوین و شرکت‌های پرداخت

مرحله ارزیابی	شرح و ابزارها	معیارهای ارزیابی
۱ـ ارزیابی کیفی و کمی فرهنگ امنیت	استفاده از پرسشنامه‌ها و مصاحبه‌ها برای سنجش فرهنگ امنیت سایبری در بانکداری نوین و شرکت‌های پرداخت	تغییرات در درک کارکنان نسبت به تهدیدات امنیتی کاهش حوادث مرتبط با رفتار انسانی
۲ـ شاخص‌های کلیدی عملکرد (KPIs)	تحلیل عملکرد برنامه‌های آموزشی و امنیتی از طریق شاخص‌های کلیدی مانند کاهش حوادث سایبری و افزایش آگاهی	میزان مشارکت کارکنان در آموزش‌ها کاهش رخدادهای امنیتی
۳ـ تجزیه‌وتحلیل داده‌های رفتاری	استفاده از ابزارهای مانیتورینگ و تحلیل لاگ‌ها برای رصد رفتار کارکنان در سیستم‌های بانکی و پرداختی	تعداد اقدامات پیشگیرانه شناسایی رفتارهای مشکوک و غیرعادی
۴ـ اثربخشی برنامه‌های آموزشی	سنجش تأثیر آموزش‌ها از طریق آزمون‌ها، نظرسنجی‌ها و میزان موفقیت کارکنان در اجرای پروتکل‌های امنیتی	میزان موفقیت در آزمون‌ها رضایت کارکنان از آموزش‌ها و مشوق‌ها
۵ـ ارزیابی سیستم‌های خودارزیابی	استفاده از نرم‌افزارهای خودارزیابی امنیتی برای تحلیل رفتارهای امنیتی کارکنان و بهبود رفتارها از طریق بازخوردهای مؤثر	تعداد کاربران فعال در سیستم‌های خودارزیابی بهبود رفتارهای امنیتی
۶ـ تطبیق با استانداردهای بین‌المللی	ارزیابی میزان تطابق چارچوب با استانداردهای بین‌المللی مانند ISO 27001.	میزان تطابق با استانداردها شناسایی نقاط بهبود بر اساس شیوه‌های بین‌المللی
۷ـ تأثیر بر عملکرد سازمانی	بررسی تأثیر چارچوب بر کاهش هزینه‌های امنیتی و بهبود بهره‌وری کارکنان و اعتماد مشتریان به امنیت بانک‌ها و شرکت‌های پرداخت	کاهش هزینه‌های حوادث سایبری افزایش رضایت و اعتماد مشتریان
۸ـ بازخوردهای مستمر	جمع‌آوری و تحلیل بازخوردهای منظم از کارکنان و مدیران	تعداد و کیفیت بازخوردهای دریافتی بهبود مستمر فرایندها بر اساس بازخوردها

جدول ارزیابی فوق یک رویکرد جدید و نوآورانه برای ارتقاء فرهنگ امنیت سایبری در حوزه بانکداری نوین و شرکت‌های پرداخت ارائه می‌دهد. این روش با ترکیب ارزیابی‌های کیفی و کمی، شاخص‌های کلیدی عملکرد (KPIs) و ابزارهای تحلیل داده، به شکل منسجم و سیستماتیک عمل می‌کند تا بهبود مستمر فرهنگ امنیت سایبری را تضمین کند.

نوآوری این چارچوب در تمرکز بر ارزیابی مستمر و پویا، تلفیق آموزش‌های هدفمند و بازخوردهای کارکنان، و استفاده از استانداردهای بین‌المللی برای انطباق بیشتر با نیازهای صنعت بانکی است. از آنجا که تهدیدات سایبری به سرعت تغییر می‌کنند، این مدل با تاکید بر به‌روزرسانی‌های منظم و تحلیل رفتار کاربران، به مدیران و تیم‌های امنیتی

کمک می‌کند تا با چالش‌های جدید بهتر مقابله کنند. در نتیجه، این روش یک راهکار جامع برای افزایش امنیت و اعتماد مشتریان و کاهش رخدادهای سایبری در بانکداری و شرکت‌های پرداخت محسوب می‌شود.

چارچوب نوین ارزیابی فرهنگ امنیت سایبری در حوزه بانکداری نوین و شرکت‌های پرداخت، با ارائه رویکردی چندبعدی و منسجم، به طور مؤثری قادر است فرهنگ امنیتی را در این حوزه‌ها به سطح بالاتری ارتقا دهد. استفاده از شاخص‌های کلیدی عملکرد (KPIs)، ابزارهای تحلیل داده‌های رفتاری، و سیستم‌های خودارزیابی، به مدیران این امکان را می‌دهد که وضعیت کنونی فرهنگ امنیت سایبری را به طور مستمر پایش و تحلیل کنند. این روش‌ها نه‌تنها در شناسایی نقاط ضعف و فرصت‌های بهبود مؤثر هستند، بلکه به توسعه یک محیط کاری ایمن‌تر و هوشمندتر منجر می‌شوند. با ارزیابی دقیق تأثیر آموزش‌های امنیتی و تحلیل رفتارهای کاربران در مواجهه با تهدیدات سایبری، این چارچوب می‌تواند به بهینه‌سازی فرآیندهای امنیتی و کاهش وقوع رخدادهای سایبری کمک کند. همچنین تطابق با استانداردهای بین‌المللی مانند ISO 27001 و به‌کارگیری بهترین شیوه‌های امنیت سایبری، تضمینی برای بهبود مستمر و ارتقاء کیفیت امنیت اطلاعات خواهد بود. این امر به‌ویژه در بخش بانکداری و پرداخت اهمیت دارد، جایی که حفظ اعتماد مشتریان و کاهش هزینه‌های ناشی از حملات سایبری از اولویت‌های اصلی محسوب می‌شود. بازخوردهای منظم از کارکنان و مدیران نیز نقش کلیدی در بهبود مستمر فرآیندهای امنیتی ایفا می‌کند. این بازخوردها باعث شناسایی چالش‌های جدید و فرصت‌های بهبود در برنامه‌های امنیتی می‌شود، که به نوبه خود به انعطاف‌پذیری بیشتر چارچوب و افزایش اثربخشی آن کمک می‌کند.

در نهایت، این شیوه ارزیابی با ایجاد فرهنگ امنیت سایبری قوی‌تر و نهادینه کردن آن در سازمان‌های بانکی و پرداخت، می‌تواند به بهبود بهره‌وری کارکنان، افزایش اعتماد مشتریان، و کاهش هزینه‌های مرتبط با رخدادهای امنیتی منجر شود. این چارچوب نوین، یک ابزار مؤثر و جامع برای سازمان‌ها است تا در محیط پیچیده و پرچالش امروزی، امنیت اطلاعات خود را به نحو مؤثری مدیریت و ارتقا دهند.

۱۱ نتیجه‌گیری و جمع‌بندی

تحقیق نشان می‌دهد که برای ایجاد یک فرهنگ امنیت سایبری مؤثر، سازمان‌ها باید به‌طور همزمان بر روی ابعاد مختلف فرهنگ کار کنند. این فرهنگ نه‌تنها به استفاده از فناوری‌های پیشرفته نیاز دارد، بلکه به رفتارهای انسان‌محور نیز وابسته است. مدیران باید باورها، ارزش‌ها و نگرش‌های کارکنان را با اهداف امنیتی سازمان هماهنگ کنند تا بتوانند به یک فرهنگ سایبری قوی دست یابند. همچنین چارچوبی نوین برای ارتقای فرهنگ امنیت سایبری در حوزه بانکداری نوین ارائه شد که با تمرکز بر آموزش مستمر، تقویت همکاری‌های سازمانی، و استفاده از فناوری‌های پیشرفته، به دنبال ایجاد فرهنگ امنیتی پایدار و مؤثر است. یافته‌ها نشان می‌دهند که رویکردهای سنتی برای مقابله با تهدیدات سایبری دیگر کافی نیستند و نیاز به تغییرات بنیادی در سطح فرهنگ سازمانی وجود دارد. این چارچوب با در نظر گرفتن نیازهای خاص بانک‌ها و شرکت‌های پرداخت، تلاش می‌کند تا امنیت را نه‌تنها در سطح فناوری بلکه در بطن فرهنگ و رفتار کارکنان نهادینه کند.

از جمله اقدامات کلیدی این مدل، برنامه‌های آموزشی مداوم، نظام‌های تشویقی برای ارتقای مشارکت کارکنان، و ارزیابی مستمر برنامه‌های امنیتی است که نقش مهمی در افزایش آگاهی و تعهد کارکنان به امنیت سایبری دارد. همچنین، استفاده از ابزارهای نوین سیستم‌های ارزیابی پیشرفته می‌تواند به شناسایی زودهنگام تهدیدات و تقویت امنیت سازمان‌ها کمک کند.

نتایج این تحقیق نشان می‌دهد که ایجاد یک فرهنگ امنیتی جامع و پایدار، نقش مهمی در کاهش آسیب‌پذیری‌های سایبری و افزایش اعتماد مشتریان به سیستم‌های بانکی دارد. این مدل می‌تواند به عنوان یک چارچوب قابل پیاده‌سازی برای دیگر سازمان‌های مالی و پرداخت نیز مورد استفاده قرار گیرد و پایه‌گذار تحولات بزرگ در ارتقای امنیت سایبری در این صنعت باشد.

این مقاله به‌طور خاص به مدیران کمک می‌کند تا بفهمند که چگونه می‌توانند از طریق رهبری مؤثر، آموزش و ارتباطات قوی، رفتارهای امن سایبری را در سازمان تقویت کنند. در نهایت، این تحقیق بر اهمیت فرهنگ امنیت سایبری به‌عنوان یک عنصر کلیدی در کاهش ریسک‌های امنیتی تأکید دارد و به مدیران این امکان را می‌دهد که به‌طور سیستماتیک به ساخت و تقویت این فرهنگ در سازمان‌های خود بپردازند.

۱۲ پیشنهادات کاربردی

در این تحقیق، پیشنهاد می‌شود که برای تقویت فرهنگ امنیت سایبری در بانکداری نوین، برنامه‌های آموزشی منظم و هدفمند برای کارکنان طراحی و اجرا شود. این برنامه‌ها باید بر شناسایی تهدیدات و ارتقاء آگاهی امنیتی تمرکز داشته باشند. همچنین، برقراری جلسات دوره‌ای میان واحدهای مختلف سازمان می‌تواند به بهبود همکاری و افزایش شفافیت در موضوعات امنیتی کمک کند. ایجاد نظام‌های تشویقی برای ترغیب کارکنان به مشارکت فعال در امنیت سایبری و بهره‌گیری از فناوری‌های نوین مانند هوش مصنوعی برای شناسایی تهدیدات، از دیگر اقدامات ضروری به شمار می‌روند. نهایتاً، باید یک نظام ارزیابی مستمر برای نظارت بر اثربخشی برنامه‌های امنیتی و فرهنگ سایبری پیاده‌سازی شود.

برای تحقیقات آتی، پیشنهاد می‌شود که تأثیر فرهنگ امنیت سایبری بر اعتماد مشتریان و کارایی آموزش‌های آنلاین در این زمینه بررسی شود. همچنین، مقایسه فرهنگ امنیت در کشورهای مختلف و تحلیل نقش فناوری‌های نوین، نظیر بلاک‌چین، در بهبود فرهنگ امنیت سایبری می‌تواند موضوعات مهمی برای پژوهش‌های آینده باشد.

فهرست منابع

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. Computers & Security, 87, 101586

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2023). The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model. Information Technology & People, 36(8), 94-125.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. Journal of Cybersecurity, 8(1), 006.

Corradini, I. (2020). Building a cybersecurity culture. Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology, 63-86.

Yerby, J. & Floyd, K. (2018). Faculty and Staff Information Security Awareness and Behavior. Journal of The Colloquium for Information System Security Education (CISSE) 6. 138-160.

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. International Journal of Applied Engineering Research, 9(23), 19133-19144.

Filippos, Georgios Kambourakis, Andreas Papasalouros, and Stefanos Gritzalis. Security Education and Awareness for K-6 Going Mobile. International Journal of Interactive Mobile Technology 10, no. 2 (2016): 41–48

Li, X., & Chen, J. (2022). Cybersecurity Threats and Risk Mitigation in Payment Systems (Working Paper No. 312). New York: IMF. 15-38.

Varakuti, D., & Shwethashri, K. (2023). Cybersecurity Awareness in Online Education: A Case Study Analysis. International Research Journal of Modernization in Engineering Technology and Science, 5(7), 1785.

Schultz, E. E., & Kauffman, A. (2021). Building a Cybersecurity Culture: The Role of Leadership and Employee Engagement. International Journal of Information Management, 56, 102265

Pérez, G., & Green, M. (2021). Building Resilience in Financial Institutions through Cybersecurity Awareness (Working Paper No. 415). Washington, DC: World Bank. 23.

Prasad, R., & Rohokale, V. (2020). Cyber security: The lifeline of information and communication technology. Switzerland: Springer.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior, 75, 547-559

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information technology Security techniques Information security management systems. ISO.

Chakraborty, S. (2019). Malware attack and malware analysis: A research. International Journal of Scientific Research in Computer Science, 5(3), 268-272

Villanueva, J. A., Lacatan, L. L., Vinluan, A. A. (2020). Information technology security infrastructure malware detector system. International Journal of Advanced Trends in Computer Science and Engineering, 9(2), 1583–1587

Presenting a Novel Framework for Enhancing Cybersecurity Culture in Modern Banking

Saeed Mardani Shahrbabak[1] **Alireza Zalinejad**[2]

Abstract

Given the increasing cyber threats in modern banking and payment processing companies, enhancing cybersecurity culture has become a fundamental necessity. This research addresses this need by presenting a novel framework based on innovative ideas to elevate the cybersecurity culture within this industry. Additionally, an innovative evaluation method has been designed to assess the proposed model, thoroughly examining its effectiveness across various organizational levels.

The advantages of this framework include embedding cybersecurity culture among all employees and across different levels of banking and payment organizations. It also contributes to improving resilience against cyber threats, boosting customer trust, and enhancing the efficiency of security systems.

By offering practical and innovative solutions, this research can pave the way for significant advancements in modern banking cybersecurity and payment companies, while also opening up new avenues for future research in this field.

Keywords: Cybersecurity Culture, Modern Banking, Cyber Threats, Security Embedding, Innovative Evaluation

JEL Classification: G21, G32, L86, M15, O33

[1] Security Operations Specialist at Shaparak Company; S.mardani@Shahparak.com

[2] Security Operations Specialist at Shaparak Company; A.zali@Shaparak.com