فصلنامه علمی-پژوهشی مطالعات مدیریت کسب و کار هوشمند- سال هفتم ـ شماره ۲۶ـ زمستان ۱۳۹۷
صفحات ۷۰-۳۷

شناسایی عوامل توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری با رویکرد نظریه داده بنیاد

محمدمهدی قوچانی خراسانی *
داود حسین پور **
ابراهیم محمود زاده ***
سید مهدی الوانی ****

چکیده

تغییر و تحولات سریع در حوزهٔ فناوری، افزایش هزینه‌های نوآوری و رقابت روزافزون در محصولات و خدمات جدید منجر به افزایش نیاز سازمان به تعامل با محیط و ذینفعان خارجی‌شان شده است که این امر منجر به باز شدن مرزهای سازمان و استفاده از پارادایم نوآوری باز در توسعه روندهای داخلی نوآوری و گسترش بازار برای استفاده خارجی از نوآوری شده است؛ از متغیرترین فناوری‌های روز، فناوری‌های مربوط به فضای سایبری و امنیت آن است؛ که حفظ امنیت سایبری از مسائل مهم در امنیت ملی کشور محسوب می‌شود و دستیابی به محصولات بومی امنیت سایبری در کشور از اهمیت بسزایی برخوردار است. این مقاله با هدف شناسایی عوامل توسعه نوآوری باز در نهادهای تحقیقاتی امنیت سایبری، به دنبال شناسایی آن‌ها با توجه به شرایط محیطی ایران و ارائه راه‌حل‌هایی برای توسعه این عوامل در نهادهای تحقیقاتی امنیت سایبری است.در این تحقیق با استفاده از روش نظریه داده بنیاد این عوامل شناسایی‌شده است. بدین منظور ۱۶ مصاحبهٔ نیمه ساختاریافته با خبرگان این موضوع صورت گرفته است. با تحلیل داده‌ها در فرایند کدگذاری باز با کمک نرم‌افزار مکس‌کیودی‌ای ۱۰ منجر به تولید ۱۱ مقولهٔ فرعی در قالب ۳ مقولهٔ اصلی شده است. مدل ارائه شده در این مقاله با رویکرد خود ظهور به دست آمده است و نتایج آن به‌صورت گزاره‌های تئوریک تبیین می‌شود.

واژگان کلیدی: نوآوری باز، نهادهای تحقیقاتی، امنیت سایبری، نظریه داده بنیاد.

---

* دانش‌آموخته دکتری، مدیریت دولتی (سیاست‌گذاری عمومی)، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی. (نویسنده مسئول)؛ ghochany@yahoo.com

** دانشیار، گروه مدیریت دولتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران.

*** دانشیار، دانشگاه صنعتی مالک اشتر، تهران.

**** استاد، گروه مدیریت دولتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران.

تاریخ دریافت:۱۳۹۷/۰٤/۰۵ **تاریخ پذیرش:۱۳۹۷/۱۲/۱٤**

مقدمه

تغییر و تحولات سریع در حوزه فناوری، افزایش هزینه‌های نوآوری و رقابت روزافزون در محصولات و خدمات جدید منجر به افزایش نیاز سازمان به تعامل با محیط و ذینفعان خارجی‌شان شده است که از این طریق سبب باز شدن مرزهای سازمان به‌منظور تبادل ایده‌های نوآورانه است (فلین و زینگر[1]، ۲۰۱۳). امروزه به علت سه عامل، ۱- هزینه‌ی بالای تحقیق و توسعه درون بنگاه‌ها، ۲-کوتاه‌تر شدن چرخه عمر کالاها و فناوری‌های به کار گرفته‌شده در آن‌ها در بازارهای جهانی و نیاز به کسب رضایت مشتریان و ۳- گردش و تمایل نیروی انسانی متخصص به تغییر محیط کاری برای کسب درآمد و مزایای بیشتر، مقوله نوآوری اهمیت روزافزونی در تجارت یافته است (جاکوبیدس و بیلینگر[2]، ۲۰۰۶). این بدان معنی است که شرکت‌ها و بنگاه‌ها در مقایسه دهه‌های گذشته به مقدار زیادتری از منابع جهت توسعه و شکوفایی نوآورانه خود نیازمند هستند، بنابراین باید بتوانند با دسترسی بیشتر به منابع علمی و دانش فنی، ایده‌ها و حق امتیازها در فرایندهای تحقیق و تکمیل نوآوری تسریع ببخشند. قابلیت همکاری شبکه‌ای ارتباطی میان بخش عمومی، خصوصی و غیرانتفاعی تأثیر مهمی در کارکرد فعالیت‌های نوآورانه ایفا می‌کند. در میان فعالیت‌های نوآورانه ابزارهای فناوری اطلاعات و ارتباطات نقش مهمی در زندگی روزمره ما ایفا می‌کند؛ کامپیوترها، تبلت ها، تلفن‌های همراه هوشمند، شبکه جهانی اینترنت، شبکه‌های گسترده اجتماعی همگی زندگی انسان را تحت تأثیر قرار داده‌اند. از سال‌های ابتدایی فراگیر شدن کامپیوترهای شخصی و پس‌ازآن شبکه اینترنت موضوع امنیت شبکه‌ها و اطلاعات کاربران و به بیان کلی‌تر امنیت در فضای سایبر یکی از مباحث مهم بوده است. علاوه بر این حفظ امنیت سایبری در سطح کلان و حاکمیتی آن در پی تأمین امنیت و منافع ملی است و همچنین هدف آن محافظت از زیرساخت‌های حیاتی ملی نظیر ارتباطات، حمل‌ونقل، سوخت، بانکداری و غیره که طی سنوات اخیر در کشور ما بر بستر فضای سایبری قرارگرفته‌اند، است؛ بنابراین دستیابی به محصولاتی که از طریق تحقیق و توسعه بومی طراحی و تولید می‌شوند ازجمله سیاست‌های کلان و از برنامه‌های

1. Felin & Zenger
2. Jacobides & Billinger

توسعه ملی[۱] کشور محسوب می‌گردد. در این مقاله پارادایم نوآوری باز و عوامل توسعهٔ آن به‌عنوان رویکردی جهت استفاده هدفمند از جریان روبه‌داخل و همچنین رو به خارج به‌منظور توسعهٔ روندهای داخلی نوآوری در تحقیقات فضای امنیت تبادل اطلاعات معرفی و بررسی می‌گردد؛ بدین منظور ابتدا مفهوم نوآوری باز و فرایندهای آن در ادبیات موضوع بررسی می‌گردد و در ادامه با استفاده از روش نظریه داده بنیاد، سعی در شناسایی این عوامل در نهادهای تحقیقاتی امنیت سایبری در ایران می‌نماید. همان‌گونه که بیان شد دستیابی به محصولات بومی امنیت سایبری در کشور از اهمیت بسزایی برخوردار است، بنابراین با توجه به اینکه امروزه دستیابی به فناوری‌های این حوزه تنها از طریق نوآوری درون‌سازمانی امکان‌پذیر نیست، بهره‌برداری از پارادایم نوآوری باز می‌تواند در این حوزه راهگشا باشد. این مقاله عوامل توسعهٔ نوآوری باز در ایران را شناسایی نموده و با ارائه گزاره‌های تئوریک حاصل از نظریه داده بنیاد، راهکارهای پیشنهادی در این خصوص ارائه می‌دهد. با توجه به مطالب گفته‌شده، این پژوهش در پی جواب به این سؤال اساسی است که:

عوامل توسعه فرایندهای نوآوری باز در نهادهای تحقیقات امنیت فضای سایبر کدام‌اند؟

از سؤالات فرعی این پژوهش می‌توان به موارد ذیل اشاره نمود:

- عوامل زمینه‌ای مؤثر در توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیتی سایبری در ایران کدام‌اند؟
- نهادهای مؤثر در توسعه فرایندهای نوآوری باز در تحقیقات امنی سایبری کدام‌اند؟

در ادامهٔ مقاله با پاسخگویی به این سؤالات رابطه میان این عوامل با توجه به شرایط محیطی ایران نشان داده می‌شود و در قالب گزاره‌های تئوریک این روابط تبیین می‌گردد.

۱. برنامه توسعه چهارم، پنجم و ششم توسعه کشور

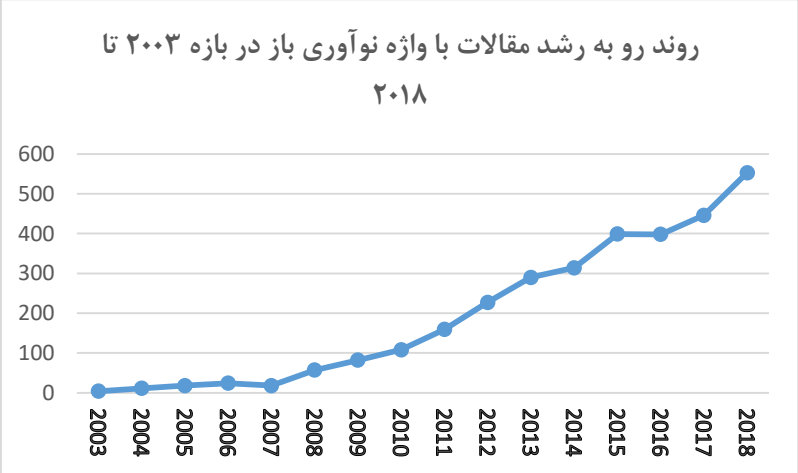
پیشینه پژوهش

نوآوری باز[1]

نوآوری **به** فرآیند پرورش ایده تا بهره‌برداری و کاربرد عملی آن، اطلاق می‌گردد. نگرش فرآیندی به مقوله نوآوری، شامل بخش‌هایی چون جستجوی ایده‌های نو و فرصت‌های نوآورانه، گزینش آن‌ها، چگونگی تحقق آن‌ها و بهره‌مندی و ارزش‌آفرینی از فرصت‌ها و ایده‌های نوآورانه است (تد و بسنت[2]، ۲۰۰۹). موفقیت سازمان‌ها عمدتاً ریشه در نوآوری دارد و نوآوری، نه‌تنها در سطح بنگاه، بلکه به‌صورت گسترده، به‌عنوان منشأ رشد اقتصاد ملی مطرح گردیده است. مضاف بر اینکه در محیط رقابتی امروز، چنانچه سازمانی نتواند نوآوری‌های بیشتری را عرضه نماید، به‌تدریج مزیت رقابتی خود را ازدست‌داده و در قیاس با رقبا، در معرض عقب‌ماندگی قرار می‌گیرد (تد و بسنت، ۲۰۰۹). نوآوری باز یکی از مهم‌ترین و داغ‌ترین موضوعات مدیریت نوآوری در سال‌های اخیر محسوب می‌شود؛ با یک جستجو در گوگل اسکولار[3] به بیش از ۳,۵ میلیون نتیجه مواجه می‌شوید. نوآوری باز رویکرد جدیدی است که اگرچه از دهه ۸۰ میلادی مطالعات آغازین آن شکل‌گرفته است اما به‌قدری ناچیز است که قابل‌اغماض است. مطالعه در این حوزه با معرفی این مفهوم در سال ۲۰۰۳ میلادی توسط هنری چسبرو به‌سرعت رو به رشد نهاد و از سال ۲۰۰۹ به‌شدت مورد توجه محققان حوزه نوآوری قرار گرفت به‌گونه‌ای که از سال ۲۰۰۳ تا ۲۰۰۹ در این زمینه ۱۸۱ اثر منتشر گردیده است؛ درحالی‌که مقالات منتشره بین سال‌های ۲۰۰۹ تا ۲۰۱۴ به حدوداً ۲۰۰۰ اثر معتبر علمی رسیده است. به‌عنوان نمونه در سایت ساینس‌دایرکت[4] تعداد مقالات یافت شده از جستجوی عبارت «نوآوری باز» حدوداً ۳۰۰۰ مقاله است که با جستجوی این واژه در متن مقالات روند مقالات مرتبط منتشرشده از سال ۲۰۰۳ تا سال ۲۰۱۸ را می‌توان به‌صورت نمودار در شکل ۱ نشان داد؛ که نشانگر روند روبه رشد ادبیات علمی در این حوزه است. اگرچه همه

1. Open Innovation
2. Tidd & Bessant
3. scholar.google.com
4. www.sciencedirect.com

مقالات فوق ازنظر محتوی و تطابق با موضوع تحقیق فعلی دارای ارزش یکسانی نیستند اما روند روبه رشد مقالات نشان‌دهنده اهمیت موضوع است.



شکل ۱. روند تعداد مقالات منتشرشده با کلیدواژه نوآوری باز

رویکرد نوآوری باز در مقابل نوآوری بسته است؛ در نوآوری بسته فرض بر این است که یک شرکت باید بهترین و باهوش‌ترین افراد را بکار گیرد، سود بردن از تلاش‌های نوآورانه مستلزم اکتشاف، توسعه و بازاریابی از سوی خود شرکت است، اول بودن در بازار مستلزم نشئت گرفتن از اکتشافات پژوهشی از درون خود شرکت است و پیشرو بودن در تحقیق و توسعه صرفاً منجر به مطرح‌شدن یا بهترین شدن در محیط رقابتی است. درحالی‌که در نوآوری باز پیش‌فرض‌های مذکور را در دستیابی به نوآوری و کسب موقعیت برتر در بازار را نقض می‌کند. رویکرد نوآوری باز در ابتدا توسط هنری چسبرو (۲۰۰۳)، به‌عنوان مجموعه‌ای از توسعه‌های پیش رو مطرح گردید و پارادایمی تعریف شد که در آن شرکت‌ها اگر می‌خواهند نوآوری خود را پیشرفت دهند می‌توانند و بهتر است ایده‌های خارج سازمان را همچون ایده‌های داخل سازمان به کار گرفته و راه‌های خارجی و داخلی به بازار بیابند (چسبرو[1]، ۲۰۰۳). تغییرات محیط درونی و بیرونی، سازمان را به سمت اتخاذ فرایندهای نوآوری

1. Chesbrough

به‌صورت باز به‌عنوان راهی در خصوص متعادل‌سازی هزینه‌ها و سرمایه‌گذاری‌های بخش تحقیق و توسعه درون‌سازمانی، سوق می‌دهد. بنگاه‌هایی که از رویکرد نوآوری باز پیروی می‌کنند، فعالیت‌های واحد تحقیق و توسعه درون‌سازمانی خود را با شرکا خارج از سازمان و عناصر دیگر محیط خارجی ادغام می‌نمایند (چسبرو، ۲۰۱۴).

مبانی نظری پژوهش

نوآوری باز و فرایندهای آن

همان‌طور که بیان شد، نوآوری باز در ابتدا توسط هنری چسبرو، در کتاب نوآوری باز به‌عنوان مجموعه‌ای از توسعه‌های پیش رو مطرح گردید و پارادایمی تعریف شد که در آن شرکت‌ها اگر می‌خواهند نوآوری خود را پیشرفت دهند بهتر است ایده‌های خارج سازمان را همچون ایده‌های داخل سازمان به کار گرفته و راه‌های خارجی و داخلی به بازار بیابند؛ هنری چسبرو نوآوری باز را چنین تعریف می‌کند:"استفاده هدفمند از جریانات دانشی، به‌صورت ایده، علم و یا فناوری، چه به سمت درون سازمان و چه به سمت بیرون آن، به ترتیب برای شتاب بخشیدن به فرایند نوآوری در داخل سازمان و یا گسترش بازار برای استفاده بیرونی از نوآوری‌های سازمان"(چسبرو ۲۰۰۳) طبق تعریف نوآوری باز می‌تواند برای افراد مختلف معانی متفاوتی ممکن است داشته باشد و ازآنجاکه حوزه‌های زیادی تحت‌الشعاع این مفهوم قرار می‌گیرند، برحسب اینکه از چه دریچه‌ای به گشودگی در فرآیندهای یادگیری و نوآوری یک سازمان نگاه شود، تقسیم‌بندی‌های مختلفی از این فرآیندها می‌توان ارائه داد.

قبل از توضیح در مورد فرآیندها، لازم به ذکر است همه‌ی آن‌ها برای شرکت‌های مختلف اهمیت یکسانی ندارند. درواقع هر شرکت یک فرآیند اصلی را انتخاب و فرآیندهای دیگر را با دیگران یکپارچه می‌کند. تعریف گسترده چسبرو به انتقال مؤثر دانش در هر دو جهت (درونی[1] و بیرونی[2]) اشاره دارد. نوآوری باز رو به بیرون به انتقال فناوری به خارج از سازمان اشاره می‌کند و پیشنهاد می‌دهد که شرکت‌ها می‌توانند به دنبال سازمان‌های دیگر با مدل‌های

1. Inward
2. Outward

کسب‌وکاری مناسب برای تجاری‌سازی فناوری خود باشند. وجه دیگر این تعریف بردن فناوری‌ها داخلی به خارج از شرکت است که ارائه دانش داخلی برای بازیگران خارجی محیط کسب‌وکاری است. نوع سومی از فرآیند نیز با نام ترکیبی است که به معنای به‌کارگیری هردو رویکرد در اکتساب نوآوری است (زمایتس[1]، ۲۰۱۴). با توجه به اینکه این تحقیق به دنبال شناسایی عوامل مؤثر در توسعهٔ فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری است، بنابراین با مطالعه مدل‌های مختلف باید بتوان یک رویکرد مناسب برای توسعهٔ این فرایندها در نهادهای تحقیقاتی امنیت سایبری احصاء نمود؛ در جدول ۱ انواع فرایندهای نوآوری باز از جنبه‌های مختلف نشان داده‌شده است:

جدول ۱. بررسی تطبیقی انواع فرایندهای نوآوری باز

نام نویسنده	سال	تمرکز مدل	فرایندهای نوآوری باز							مراجع
چسبرو، گاسمن و انکل	۲۰۰۳ و ۲۰۰٤	فرایندهای درونی و بیرونی	فرآیند بیرون به درون	فرآیند درون به بیرون	فرآیند ترکیبی					(چسبرو، ۲۰۰۳)؛ (گاسمن و انکل[2]، ۲۰۰٤)
فتروچف	(۲۰۰٦)	کسب نوآوری خارجی	جستجوی فرصت	ارزیابی پتانسیل بازاری و سرمایه‌گذاری	گرفتن شرکای توسعه‌ای بالقوه	ایجاد ارزش از طرق تجاری سازی	گسترش نوآوری های ارائه‌شده			فتروچف و ولکل[3]، ۲۰۰٦)
هرستد	(۲۰۰۸)	بهبود عملکرد نوآورانه	همکاری	جستجو	حفاظت از مالکیت فکری	نوآوری خارجی				هرستد و همکاران[4]، ۲۰۰۸)

1. Zemaitis
2. Gassmann & Enkel
3. Fetterhoff & Voelkel
4. Herstad et al.

نام نویسنده	سال	تمرکز مدل	فرایندهای نوآوری باز								مراجع
جروئن	(۲۰۰۸)	سیاست گذاری	شبکه سازی	همکاری	کارآفرینی شرکتی	مدیریت مالکیت معنوی	تحقیق و توسعه				دی جانگ و همکاران[1]، (۲۰۰۸)
والین و کرو	(۲۰۱۰)	یکپارچگی دانش مدیریتی	تعریف فرآیند نوآوری	تشخیص دانش نوآورانه مرتبط	انتخاب مکانیسم یکپارچه‌سازی مناسب	ایجاد مکانیسم حکمرانی مناسب	تعادل میان مشوق‌ها و کنترل‌ها				والین و کرگ[2]، (۲۰۱۰)
هافکسبرینک	(۲۰۱۰)	آماده‌سازی سازمان	آمادگی سازمانی	توانمندی های مشارکتی	ظرفیت جذب						هافکسبرینک و اسکرول[3]، (۲۰۱۰)
چیارونی و	(۲۰۱۱)	تغییر سازمانی	سازمان دهی داخلی	توسعهٔ شبکه‌ها	فرایندهای ارزیابی	نظام‌های مدیریت دانش	انباشت عظیم از دانش‌پایه	نیروی کار آموزش دیده و پویا	دسترسی خوب به اعتبار		چیارونی و همکاران[4]، (۲۰۱۱)
منطقی و همکاران	۲۰۱۲	عوامل مؤثر در موفقیت	شبکه‌سازی خارجی	واسطه‌های نوآوری	هوشمندی فناوری	ظرفیت جذب نوآوری	مدل کسب‌و کار	عوامل انسانی			صفدری و همکاران، (۱۳۹۳)

1. de Jong et al.
2. Wallin & Krogh
3. Hafkesbrink & Schroll
4. Chiaroni et al.

الگوی مفهومی پژوهش

با توجه به هدف تحقیق و بررسی ادبیات پژوهش، تلاش شد، مطالعات نسبتاً جامعی از عوامل مؤثر در فرایندهای نوآوری باز انجام شود. بر اساس مطالعهٔ انجام‌شده و با توجه به جمع‌بندی صورت گرفته، عوامل آمادگی درون‌سازمانی و آمادگی بیرون سازمانی ازجمله عوامل توسعه فرایندهای نوآوری باز محسوب می‌شود که می‌توان مدل‌های دیگر را در این قالب تقسیم‌بندی نمود. در کنار آن برای بررسی این عوامل در نهادهای تحقیقاتی امنیت سایبر در ایران باید عوامل زمینه‌ای مؤثر در آن را نیز احصا نمود. بدین منظور جهت شکل‌گیری چارچوب تحقیق از الگوی تحلیل محیطی[1] (عوامل سیاسی، اقتصادی، اجتماعی و فناورانه) بهره‌مند شده است که در شکل ۲ قابل‌مشاهده است:

1. PEST analysis (political, economic, social and technological)

شکل ۲. چارچوب نظری تحقیق

روش پژوهش

در این پژوهش با توجه به موضوع و سؤالات تحقیق از روش کیفی استفاده‌شده است و از بین استراتژی‌های مختلف از نظریه داده بنیاد بهره‌مند شده است. سه مرحلهٔ اساسی در این روش که شامل، کدگذاری باز، کدگذاری محوری و کدگذاری انتخابی در این پژوهش تشریح می‌گردد (دانایی‌فرد و امامی، ۱۳۸۶). در پژوهش حاضر به‌منظور ثبت داده‌ها، پس از اخذ

مجوزهای لازم تمامی مصاحبه‌ها به شکل صوتی ضبط شد، در مرحلهٔ بعد مصاحبه‌ها به‌طور کامل پیاده و در قالب نرم‌افزار ورد[1] فایل‌ها وارد نرم‌افزار مکس‌کیودی‌ای ۱۰[2] گردید.

انتخاب مصاحبه‌شوندگان به‌صورت هدفمند (نمونه‌گیری جهت‌دار یا نظری) و یا به‌صورت گلوله برفی بوده است. در این مقاله در هر مرحله، فرایند جمع‌آوری داده‌ها تا جایی ادامه پیدا می‌کند که به اشباع نظری رسیده شود و مطلب جدیدی به مدل اضافه نگردد. در این تحقیق با مصاحبه با ۱۶ نفر[3] ترکیبی از متخصصین (اعضاء هیئت‌علمی دانشگاه و محققین و ...)، مدیران ارشد (بخش حاکمیتی و خصوصی) از نهادهای امنیت سایبری که تجربه‌های موفقی در تحقیقات این حوزه داشتند به اشباع و کفایت نظری دست‌یافته شده است.

با توجه به رویکرد تحقیق از استراتژی‌های جدول ۴ برای تأمین اعتمادپذیری استفاده شده است.

جدول ۲. روش‌های تأمین اعتمادپذیری در پژوهش حاضر(دانایی‌فرد، ۱۳۸۹)

معیار	زیرمعیارها		استراتژی تأمین	اقدام صورت گرفته
قابل‌قبول بودن	روایی ورودی‌های پژوهش	روایی داده‌های ورودی پژوهش	نمونه‌گیری گلوله برفی	معرفی مصاحبه‌شوندگان بعدی توسط مصاحبه‌شوندگان قبلی
			نمونه‌گیری بر مبنای اعتبار	انتخاب مصاحبه‌شوندگان بر اساس توصیه متخصصان
	روایی تحلیل‌های انجام‌شده در پژوهش	روایی توصیفی	بازخور مشارکت‌کننده	ارائه بازخورد توصیفی مصاحبه به مصاحبه‌شونده و دریافت نظرات اصلاحی
		روایی تفسیری	استفاده از توصیف گرهای با حداقل مداخله	بهره‌گیری از عبارات توصیفی مانند نقل‌قول در تفسیرها
	انتقال‌پذیری		استفاده از روش نمونه‌گیری بر مبنای اعتبار	انتخاب مصاحبه‌شوندگان از بین افراد معتبری مدیران ارشد نظامی و دولتی و خصوصی در تحقیقات امنیت سایبری

1. Microsoft Word
2. MAXQDA10

۳. اطلاعات مصاحبه‌شوندگان نزد محققین محفوظ است.

معیار	زیرمعیارها	استراتژی تأمین	اقدام صورت گرفته
		وصف تفصیلی همه جزئیات	ارائه یک تصویر مفصل از زمینه‌ای که پژوهش در آن انجام‌شده
	قابلیت اطمینان	ممیزی قابلیت اطمینان	در اختیار گذاشتن داده‌ها، روش‌ها و تصمیمات باهدف بازبینی و موشکافی تحقیق توسط دیگر پژوهشگران
	تأیید پذیری	ارائه جزئیات روش‌ها و داده‌های پژوهش	ارائه گزیده مصاحبه‌ها و نیز توضیح روند تحلیل داده‌ها تا دستیابی به نتایج تحقیق

تجزیه‌وتحلیل یافته‌ها

کدگذاری باز

در نظریه داده بنیاد، فرایند تحلیل داده‌ها با کدگذاری باز آغاز می‌شود. کدگذاری باز فرایندی تحلیلی است که طی آن مفاهیم شناسایی‌شده و ویژگی‌ها و ابعاد مربوط به هر مفهوم کشف می‌شود. در کدگذاری باز وقایع مشاهده‌شده در داده‌ها نام‌گذاری می‌شوند. در این مرحله، دو فعالیت کلیدی شامل مفهوم‌سازی و مقوله‌بندی وجود دارد.

مفهوم‌سازی

شکل‌گیری یک نظریه با مفهوم‌سازی آغاز شود. مفهوم‌سازی به کوشش محقق برای کاوش عمیق در یک مشاهده، جمله، پاراگراف یا یک صفحه و برگزیدن یک نام برای هر رویداد یا اتفاق اطلاق می‌شود. محقق کمک می‌کند تا وقایع، ایده‌ها یا رویدادهای مشابه را تحت عنوانی واحد یا در قالب دسته‌ای واحد گروه‌بندی کند. پدیده‌هایی که برای آن‌ها اسمی انتخاب می‌شود را اصطلاحاً مفهوم می‌نامند. مفاهیم زیربنای نظریه به‌حساب می‌آیند.

مقوله‌بندی

هنگامی‌که داده‌ها باز شد و مفاهیم از درون آن‌ها سر برآورد، محقق به دنبال مصداق‌هایی می‌گردد که بتواند با کمک آن‌ها، مفاهیم را در قالب مقوله‌هایی دسته‌بندی کند. طبق دیدگاه استراوس و کوربین (۱۹۹۸) برخی مفاهیم را می‌توان در قالب مقوله‌ای که از انتزاع بالاتری نسبت به آن مفاهیم برخوردار است، دسته‌بندی نمود (استراوس و کوربین[1]، ۱۹۹۸). به کمک مقوله‌ها می‌توان چیزهای در حال وقوع را توصیف کرد. در جدول ۳ نحوهٔ شکل‌گیری یکی از مقوله‌های اصلی قابل‌مشاهده است:

جدول ۳. نمونه‌ای از نحوهٔ شکل‌گیری مقولهٔ توسعه فرایندهای نوآوری باز

مقوله اصلی	مقوله‌های فرعی	کدگذاری باز	گزاره کلامی
توسعهٔ فرایندهای نوآوری باز	آمادگی درون‌سازمانی	شبکه‌سازی	در این شبکه هر گره یا نود هم می‌تواند فعالیت مختص خود را انجام دهد و هم‌قسمتی از فعالیت مربوط به نود قبلی و بعدی خود را پوشش دهد
			مراکز آپا در کشور که درواقع کل ظرفیت امنیت سایبری کشور را می‌تواند پوشش دهد، این مراکز در کل گستره جغرافیایی ایران هستند و ظرفیت بالقوه مناسبی دارند
		بهره‌مندی از نخبگان در امنیت سایبری	پیشنهاد می‌شود نسل اول انقلاب که تجربه خوبی دارند باید در قالب شرکت‌هایی باشند که بتوانند در اتاق فکری آن‌ها را حفظ کرد البته در سطح راهبردی بتوانند فعالیت کنند.
	آمادگی بیرون سازمانی	شناسایی نهادهای مختلف امنیت سایبری	مرکز ملی فضای مجازی از نهادهای مختلف رصد می‌کند و بر اساس آن در صحن کمیسیون می‌آورد.
		شناسایی و	در کشور یکسری افراد و اشخاص در امنیت سایبری

1. Strauss & Corbin

مقوله اصلی	مقوله‌های فرعی	کدگذاری باز	گزاره کلامی
		استفاده از نخبگان	صاحب‌نظر هستند که در قالب گروه یا نهادی نیستند و در قالب شخص حقیقی کمک خوبی انجام می‌دهند
		ایجاد شرایط رقابتی	مرکز باید با ایجاد شرایط رقابتی کاری کند که همه بتوانند کار کنند و شرایط برای همه مهیا شود.

در پژوهش حاضر در مرحلهٔ کدگذاری باز از مجموع ۱۶ مصاحبه، ۴۸۸ کد توصیفی استخراج شد که به روش نظام‌مندی که در شرح بالا ذکر شد، مورد تجزیه‌وتحلیل قرار گرفتند و در قالب ۶۵ مضمون توصیفی بدون تکرار نمایان شدند. در جدول ۴ نحوهٔ شکل‌دهی مقوله‌های فرعی و شکل‌دهی آن‌ها به مقوله‌های اصلی نشان داده‌شده است.

جدول ٤. ساخت مقولات اصلی و مقولات فرعی

ردیف	مقوله‌های اصلی	مقوله‌های فرعی	میزان فراوانی کدهای باز
۲	عوامل مؤثر در توسعه فرایندهای نوآوری باز	آمادگی درون‌سازمانی	۸۹
		آمادگی بیرون سازمانی	۵۲
۲	شرایط زمینه‌ای مؤثر در توسعهٔ نوآوری باز در نهادهای تحقیقاتی امنیت سایبری	شرایط فناورانه	۱۷
		شرایط مالی و اقتصادی	۳٤
		شرایط سیاسی و قانونی	٤۰
		شرایط اجتماعی و فرهنگی	۵۳
۳	نهادهای مؤثر توسعه فرایندهای نوآوری باز در تحقیقات امنیت سایبری	نهادهای بین‌المللی امنیت سایبری	۱٤
		نهادهای سیاست‌گذار	۲۷
		نهادهای تحقیقاتی حاکمیتی	۱۱۷
		نهادهای تحقیقاتی خصوصی	۳٦
		نهادهای بهره‌بردار امنیت سایبری	۹

عوامل مؤثر در توسعه فرایندهای نوآوری باز

توضیحات مصاحبه‌شوندگان در پاسخ به سؤالات مربوط به عوامل توسعه فرآیندهای نوآوری باز در نهادهای تحقیقات امنیت فضای سایبر منجر به شناسایی کدهای باز جدول زیر شده است؛ لازم به ذکر است اعداد داخل جدول خروجی نرم‌افزار مکس‌کیودی‌ای ۱۰ و نشان‌دهندهٔ میزان فراوانی کدهای ذکرشده از سوی مصاحبه‌شوندگان است. در راستای پاسخ به این سؤال ۱۴۱ نکته کلیدی در قالب ۲۹ مفهوم و ۲ مقولهٔ فرعی به شرح جدول ۵ شکل گرفت:

جدول ۵. مقوله‌های اصلی و فرعی

عنوان مقولهٔ اصلی	عنوان مقوله‌های فرعی	تعداد مفاهیم زیرمجموعه
عوامل مؤثر در توسعه فرایندهای نوآوری باز	آمادگی درون‌سازمانی	۱۸
	آمادگی بیرون سازمانی	۱۱

مطابق با یادداشت نظری گردآوری‌شده در روش نظریه داده بنیاد علاوه بر جدول فوق که برآمده از رویکرد استقرایی روش تحقیق مذکور است در جدول دیگری عناصر آمادگی درون‌سازمانی و آمادگی بیرون سازمانی برای توسعهٔ فرایندهای نوآوری باز به شرح جدول ۶ تهیه شده است.

جدول ٦. کدگذاری باز مربوط به عوامل مؤثر در توسعه فرایندهای نوآوری باز

ردیف	کدگذاری اولیه	مقوله‌های فرعی
۱	شبکه‌سازی[7] (دی جانگ و همکاران[1]، ۲۰۰۸)	آمادگی درون‌سازمانی[89]
۲	بهره‌مندی از نخبگان در امنیت سایبری[5]	
۳	اصلاح فرایندهای تحقیقاتی[5]	
۴	اعتمادسازی در بخش خصوصی[7]	
۵	ایجاد فرایند ارزیابی محصولات امنیتی[4]	
۶	دغدغه تحقیقات و تولید داخلی [5]	
۷	درک مدیریتی از تحقیقات[13]	

1. de Jong, et al.

ردیف	کدگذاری اولیه	مقوله‌های فرعی
۸	تهیه منشور اخلاقی[2]	
۹	ایجاد توانمندی درون شبکه[2]	
۱۰	توانمندسازی نیرو انسانی در مقابل تهدیدات سایبری[8]	
۱۱	پرورش نیروی انسانی در امنیت سایبری[6]	
۱۲	اعتماد در بخش حاکمیتی[4]	
۳	توانمند نمودن افراد در مقابل تهدیدات سایبری[4]	
۱۴	انتخاب افراد توانمند در امنیت سایبری[2]	
۱۵	ایجاد فرایند ارزیابی و ارائه تأییدیه‌های امنیتی[6]	
۱۶	آموزش مرتبط با امنیت سایبری به نیروی انسانی [4]	
۱۷	شناختن صحیح نیاز تحقیقاتی[3]	
۱۸	نگاه صحیح به بخش خصوصی[2]	
۱۹	شناسایی نهادهای مختلف امنیت سایبری [1]	آمادگی بیرون سازمانی[52]
۲۰	شناسایی و استفاده از نخبگان[16]	
۲۱	ایجاد شرایط رقابتی [5]	
۲۲	استفاده از تمام ظرفیت‌های کشور[11]	
۲۳	مالکیت معنوی[8] (هرستاد و همکاران[1]، ۲۰۰۸)	
۲۴	شناسایی فرصت‌های خارجی[2]	
۲۵	شناسایی شرکت‌های نوپا[1]	
۲۶	امنیت سایبری ایران در خارج از کشور[2]	
۲۷	حفظ نخبگان[2]	
۲۸	محققان و نخبگان نظامی[1]	
۲۹	شایسته‌سالاری[3]	

1. Herstad, et al.

مقولهٔ شرایط زمینه‌ای مؤثر در توسعهٔ نوآوری باز در نهادهای تحقیقاتی امنیت سایبری

توضیحات مصاحبه‌شوندگان در پاسخ به سؤالات مربوط به شرایط زمینه‌ای مؤثر در توسعهٔ نوآوری باز در نهادهای تحقیقاتی امنیت سایبری، منجر به شناسایی کدهای باز طبق جدول ۷ شده است؛ همان‌طور که ملاحظه می‌شود، ۱۴۵ کد باز مربوط به شرایط زمینه‌ای است که از نرم‌افزار مکس کیودی‌ای استخراج‌شده است.

جدول ۷. کدگذاری باز مربوط به شرایط زمینه‌ای مؤثر در توسعهٔ نوآوری باز در نهادهای تحقیقاتی امنیت سایبری

ردیف	کدگذاری اولیه	مقوله‌های فرعی
۱	سرعت تغییرات فناوری در امنیت سایبری [5]	شرایط فناورانه[17]
۲	اهمیت فناوری‌های بومی در امنیت سایبری [11]	
۳	سطح فنّاوری در امنیت سایبری[1]	
٤	حمایت از نهادهای تحقیقاتی [14]	شرایط مالی و اقتصادی[34]
٥	اعتبارات در امنیت سایبری [12]	
٦	فعال کردن بازار امنیت سایبری[5]	
۷	بازار امنیت سایبری[3]	
۸	امکانات و ظرفیت بالای امنیت سایبری در کشور[1]	
۹	الزامات نانوشته [4]	شرایط سیاسی و قانونی[40]
۱۰	الزامات قانونی و رسمی [22]	
۱۱	قاطعیت در حاکمیت[2]	
۱۲	سیاست زدگی در سیاست‌گذاری[5]	
۳	خط‌مشی‌های برخورد با بخش خصوصی[1]	
١٤	نظام‌های قراردادی صحیح[3]	
١٥	تغییرات مدیریتی در بخش دولتی[2]	
١٦	مشروعیت به نهادهای خصوصی[1]	
۱۷	ایجاد دغدغه و فرهنگ امنیت در کشور[16]	شرایط اجتماعی و فرهنگی[53]
۱۸	فرهنگ تحقیقات و تولید[9]	

ردیف	کدگذاری اولیه	مقوله‌های فرعی
۱۹	تغییر فضای اجتماعی[4]	
۲۰	فضای مجازی و امنیت آن در جامعه شهروندی[4]	
۲۱	فرهنگ شهروندی در فضای مجازی[3]	
۲۲	روند رو به رشد استفاده از شبکه‌های اجتماعی[3]	
۲۳	عوامل فرهنگی مؤثر در امنیت سایبری[3]	
۲٤	اصلاح فرهنگ بخش دولتی[5]	
۲۵	مهندسی اجتماعی[6]	

مقولهٔ نهادهای مؤثر توسعه فرایندهای نوآوری باز در تحقیقات امنیت سایبری

توضیحات مصاحبه‌شوندگان در پاسخ به سؤالات مربوط به نهادهای مؤثر در توسعه فرایندهای نوآوری باز در تحقیقات امنیت سایبری، منجر به شناسایی کدهای باز جدول ۸ شده است؛ همان‌طور که ملاحظه می‌شود، ۱۵۷ کد باز مربوط به این نهادها است که از خروجی نرم‌افزار مکس‌کیودی‌ای استخراج‌شده است.

در تقسیم‌بندی نهادهای مؤثر در تحقیقات امنیت سایبری، با توجه به مصاحبه‌های صورت گرفته، نهادهای سیاست‌گذار، نهادهای بهره‌بردار، نهادهای تحقیقاتی حاکمیتی، نهادهای تحقیقاتی خصوصی و نهادهای بین‌المللی مطرح هستند. دانشگاه‌ها و مراکز تحقیقاتی هم که به‌عنوان نهادهای غیرانتفاعی در ادبیات ذکرشده‌اند به دلیل اینکه متأثر از سیاست‌های حاکمیت است می‌توان در زمرهٔ نهادهای تحقیقاتی حاکمیتی و نهادهای سیاست‌گذار تقسیم‌بندی نمود. همان‌طور که ذکر شد منظور از حاکمیت نهادی است که متأثر از سیاست‌های نظام است حال دولتی می‌تواند باشد یا نظامی.

جدول ۸.کدگذاری باز مربوط به نهادهای مؤثر توسعه فرایندهای نوآوری باز در تحقیقات امنیت سایبری

ردیف	کدگذاری اولیه	مقوله‌های فرعی
۱	وضعیت بین‌المللی امنیت سایبری [6]	نهادهای بین‌المللی امنیت سایبری[14]
۲	استفاده از نهادهای بین‌المللی در امنیت سایبری[8]	
۳	نظام‌های مختلف مؤثر در امنیت سایبری [6]	نهادهای سیاست‌گذار[27]
٤	نهاد سیاست‌گذار در امنیت سایبری [12]	
٥	نقش وزارت علوم در امنیت سایبری [9]	
٦	نقش دانشگاه‌ها در امنیت سایبری [28]	نهادهای تحقیقاتی حاکمیتی[117]
۷	بازیگران تحقیقاتی در امنیت سایبری [45]	
۸	نهادهای تحقیقاتی امنیت سایبری [20]	
۹	نقش نهادهای تحقیقاتی دولتی[24]	
۱۰	نهادهای خصوصی تحقیقاتی در امنیت سایبری [36]	نهادهای تحقیقاتی خصوصی[36]
۱۱	نهادهای بهره‌بردار امنیت سایبری [8]	نهادهای بهره‌بردار امنیت سایبری[8]

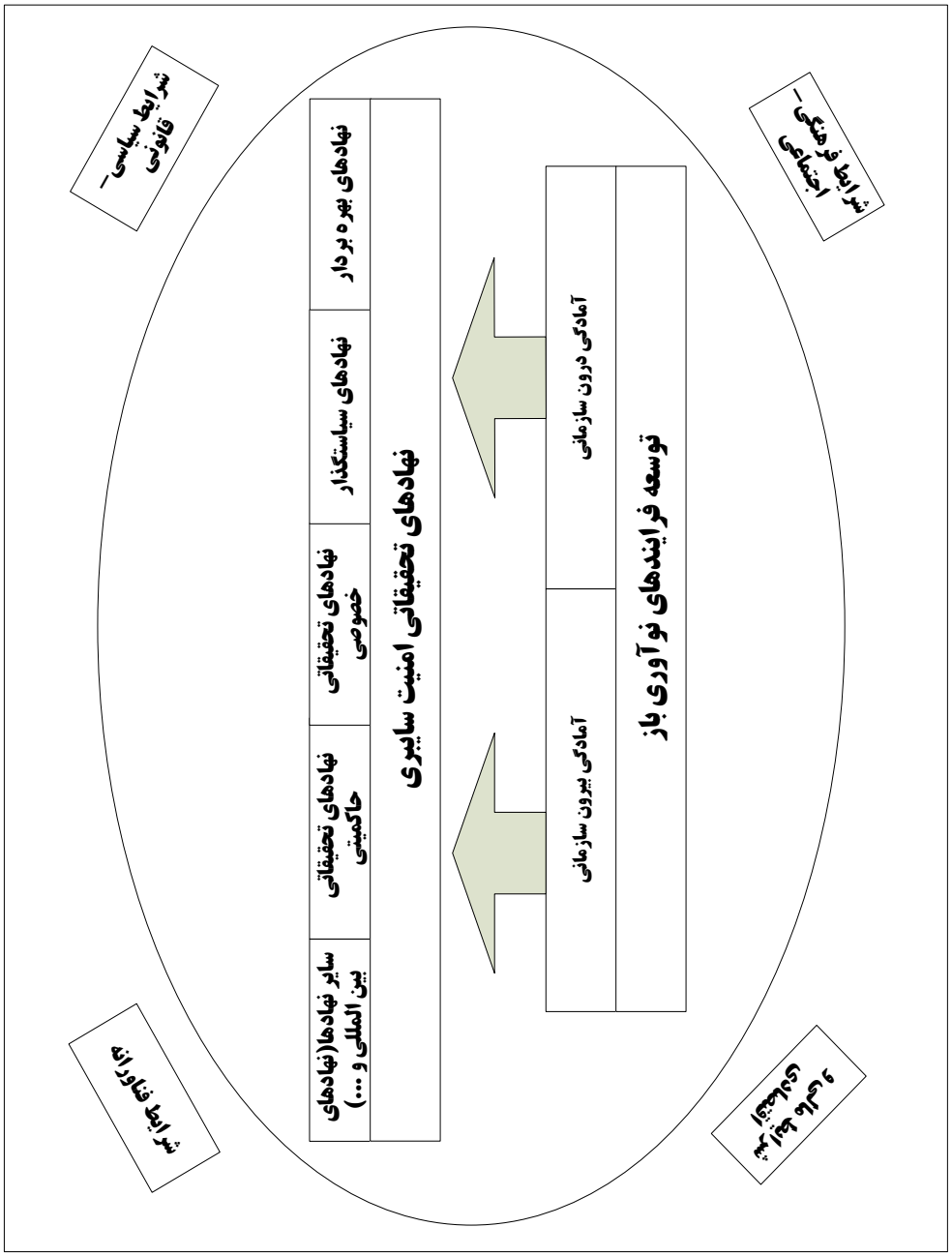
کدگذاری محوری: نظریه‌پردازی

کدگذاری محوری مرحله‌ی دوم تجزیه‌وتحلیل در نظریه داده بنیاد است. هدف از این مرحله برقراری ارتباط بین مقوله‌های تولیدشده در مرحله‌ی کدگذاری باز است. این تحقیق از رویکرد خود ظهور نظریه داده بنیاد (مدل گلاسر وکوربین) و بر اساس داده‌های جمع‌آوری‌شده در مصاحبه‌های عمیق میان بازیگران مهم نهادهای تحقیقاتی امنیت سایبری در کشور استفاده نموده است. در مدل گلاسر بر اهمیت ظهور یک نظریه از دل داده‌ها به‌جای استفاده از طبقه‌بندی معین از قبل تعیین‌شده نظیر آنچه در پارادایم کدگذاری محوری (شرایط علی، محتوا، شرایط مداخله‌گر، استراتژی‌ها و پیامدها) تأکید می‌کند؛ بنابراین همان‌طور که در شکل زیر مشاهده می‌شود؛ خروجی کدگذاری محوری روابط میان طبقه‌ها را بدون مراجعه به یک نمودار یا تصویر است. در این روش، تجزیه‌وتحلیل داده‌ها در دو سطح اصلی انجام

می‌شود: سطح متنی و سطح مفهومی. سطح متنی شامل بخش‌بندی و سازمان‌دهی فایل‌های داده، کدگذاری داده‌ها و نگارش یادداشت‌ها است که در بخش قبلی اشاره شد و در سطح مفهومی بر ساخت مدل شامل مرتبط کردن کدها و شکل دادن شبکه‌ها تأکید دارد. خروجی این رویکرد به دنبال شناسایی عوامل توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری است؛ اساس فرایند ارتباط دهی در کدگذاری محوری بر بسط و گسترش یکی از مقوله‌ها قرار دارد که در شکل زیر قابل‌مشاهده است. لازم به توجه است که در رویکرد مورداستفاده در این تحقیق (خود ظهور) داده‌ها بر اساس چهار معیار (تناسب، عملی بودن، مناسب بودن و اصلاح‌پذیری) در درون طبقه‌ها قرارگرفته است؛ بنابراین از فرایندهای کدگذاری روش داده بنیاد موارد ذیل حاصل می‌شود:

۱. ساخت مقولات اصلی با توجه به مقولات فرعی و ایجاد ارتباط بین آن‌ها؛ در این بخش ابتدا نتایج مربوط به این کارکرد مرحلهٔ کدگذاری محوری ارائه‌شده است به‌گونه‌ای که ۱۱ مقولهٔ فرعی ظهور یافته در جریان تحقیق در قالب دسته‌های انتزاعی‌تر طبقه‌بندی و ارتباط میان آن‌ها تبیین می‌شود.

۲. ایجاد شبکهٔ ارتباطی میان کل مقولات در قالب چندطبقه: کلیه مقولات (اعم از فرعی و اصلی) در قالب "کدگذاری محوری " حول یک مقولهٔ محوری سامان می‌یابند.



شکل ۳. عوامل توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری با رویکرد خود ظهور

کدگذاری انتخابی: استخراج گزاره‌های تئوریک

نظریه‌پردازان داده بنیاد، نظریه‌ها را در سه قالب ممکن ارائه می‌دهند: ۱- الگوی کدگذاری بصری ۲- مجموعه‌ای از قضایا (فرضیه‌ها) و ۳- داستانی به شکل روایی نگاشته می‌شود. ابتدا نظریه تحقیق در قالب گزاره‌های حکمی و یا قضایای تئوریک که طی فرایند کدگذاری انتخابی به‌دست‌آمده‌اند و بیان می‌شوند. در ادامه با استناد به اظهارات مصاحبه‌شوندگان به تشریح قضایا و نیز زیر قضیه‌های تئوریک فوق پرداخته می‌شود. دراین‌باره به توجه سه نکتهٔ زیر حائز اهمیت است:

۱- قضایای تئوریک حاصل از کدگذاری انتخابی روش داده بنیاد است و تلاش پژوهشگر در خلق و دسته‌بندی آن‌ها مبتنی بر تحلیل نظری از مهم‌ترین نکات مستخرج از مقولات حاصل از دو مرحله کدگذاری باز و محوری است.

۲- در تشریح هرکدام از قضایا و زیر قضایای تئوریک از نکات مهم اظهارات مصاحبه‌شوندگان استفاده‌شده است.

۳- این قضایا درواقع چکیده‌ای پرمغز از محتوای مفاهیم کدگذاری شده در پژوهش است و مبین شماری از مهم‌ترین عوامل مؤثر توسعهٔ نوآوری باز است و به کمک این قضایا می‌توان مسائل مهم در نهادهای تحقیقاتی امنیت سایبری در کشور را واکاوی و حل نمود. به‌بیان‌دیگر می‌توان گفت هرکدام از مفاهیم و مقولات ایجادشده در فرایندهای کدگذاری قبلی به‌تدریج منجر به ایجاد قضایای تئوریک در این بخش شده است.

قضایای تئوریک و تشریح آن

قضیه – توسعه فعالیت‌های تحقیقاتی بومی امنیت سایبری در کشور نیازمند آماده‌سازی درونی و بیرونی نهادهای تحقیقاتی امنیت سایبری است.

از مهم‌ترین مسائل در حفظ امنیت سایبری کشور، استقلال و خودکفایی در تولیدات محصولات امنیت سایبر است؛ چون محصولات وارداتی اعم از نرم‌افزار، سخت‌افزار و محصولات شبکه، شکاف‌های امنیتی نهفته و آشکاری دارند؛ بنابراین توسعه فعالیت‌های

تحقیقاتی بومی امنیت سایبری در کشور نیازمند توسعه نهادهای تحقیقاتی است. با افزایش هزینه‌های نوآوری و رقابت روزافزون در محصولات و خدمات جدید منجر به افزایش نیاز سازمان‌ها به تعامل با محیط و ذینفعان خارجی‌شان شده است که از این طریق سبب باز شدن مرزهای سازمان به‌منظور تبادل ایده‌های نوآورانه است؛ ازاین‌رو توسعه نوآوری در نهادهای تحقیقاتی، این نهادها هم نیازمند آماده نمودن شرایط داخلی و هم خارجی خود در کسب نوآوری (با توجه به تعریف نوآوری باز) می‌باشند. با مصاحبه‌های صورت گرفته در این زمینه عوامل درونی و بیرونی توسعه نوآوری در نهادهای تحقیقاتی امنیت سایبری به‌منظور فعال‌سازی این نهادها در جدول ۸ اشاره شد. اکنون با تشریح زیرقضیه‌های ذیل این مقوله تبیین می‌گردد:

زیرقضیه ۱- فعال کردن نهادهای تحقیقات امنیت سایبری در کشور نیازمند سیاست‌گذاری بخشی نهادها در بهره‌مندی از منابع انسانی نخبه و توانمند (گرفتن شرکای توسعه‌ای بالقوه) است.

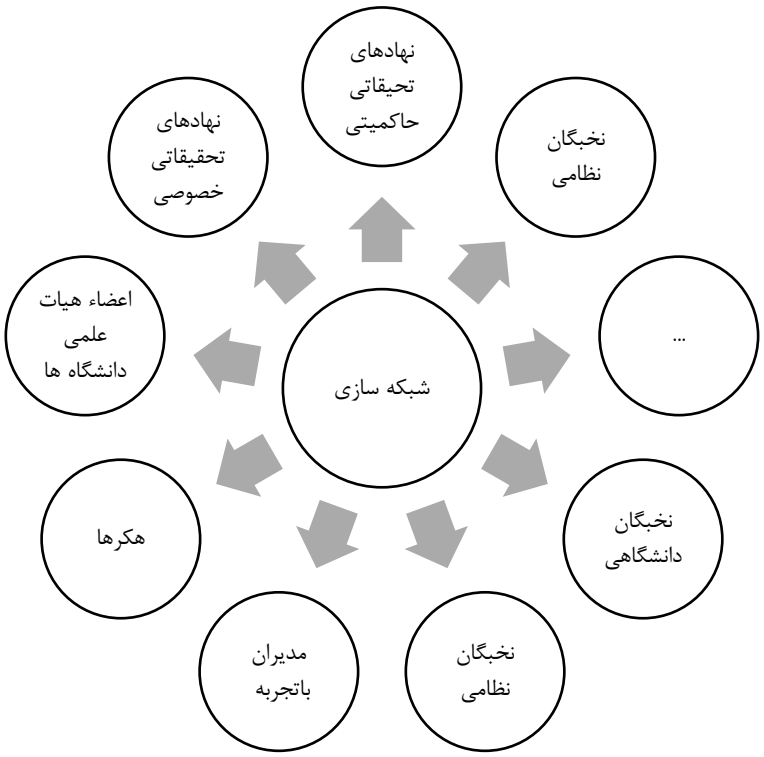
در کنار سیاست‌گذاری کلان در حوزهٔ امنیت سایبری در کشور، هر بخش و هر نهاد نیازمند سیاست‌گذاری بخشی ذیل سیاست‌های کلان حاکمیتی است؛ این سیاست‌های بخشی درواقع برخاسته از همان قوانین و مقررات کلی وضع‌شده در حوزهٔ امنیت سایبری کشور است که برحسب نیاز راهبردی، عملیاتی و یا فنی آن نهاد بازنویسی و بومی‌شده است. برای نمونه بهره‌مندی از نخبگان امنیت سایبر در کشور به‌عنوان یک اصل برای بهره‌مندی از ظرفیت امنیت سایبری کشور است اما اینکه نهادهای مختلف هرکدام چگونه از این منابع انسانی بهره‌مند شوند نیازمند سیاست‌گذاری بخشی مختص خود دارد. مثلاً وزارت علوم می‌تواند با تدوین دستورالعمل‌های لازم از ظرفیت آموزشی و پژوهشی در این حوزه بهره‌مند شود؛ هم‌اکنون فرایندهای تحقیقاتی مناسبی برای بهره‌مندی از این ظرفیت در دانشگاه‌ها موجود نیست، فعالیت‌های تحقیقاتی دانشگاه‌ها در حوزهٔ امنیت سایبری بیشتر سلیقه‌ای و برحسب علاقه‌مندی است و مکانیسم مشخصی برای فعال کردن این ظرفیت در کشور وجود ندارد،

پیشنهادی که ارائه می‌گردد، قطب‌بندی دانشگاه‌های کشور در حوزه‌های مختلف علوم و فناوری‌های نوین است و متناسب با این قطب‌بندی می‌توان پژوهانه‌های پژوهشی و یا حمایت‌های مالی در قالب‌های مختلف از طرح‌های مرتبط با امنیت سایبر در کشور اعطا نمود؛ نمونهٔ دیگر نیروهای مسلح می‌باشند. البته این نیروها به دلیل بهره‌مندی از قانون کسر یا جایگزین خدمت برای دانشجویان تحصیلات تکمیلی فرایند مؤثری برای استفاده از این ظرفیت در خدمت صنعت امنیت سایبری کشور برخوردار است. البته نیروهای مسلح در کنار بهره‌مندی از نخبگان و دانشجویان تحصیلات تکمیلی، می‌تواند از نخبگان نظامی و همچنین مدیران نخبهٔ نظامی که درصحنه‌های عملیاتی و راهبردی تجربه‌های خوبی دارند نیز بهره‌مند گردد. ازجمله سیاست‌های بخشی در خصوص نخبگان نظامی شاغل می‌توان به ایجاد فرایندهای بهره‌مندی از این نخبگان مانند فعالیت در انجمن‌های علمی و ... و در خصوص مدیران نخبه بازنشسته می‌توان تسهیلاتی در خصوصی ایجاد شرکت‌هایی در حوزه امنیت سایبری در سطوح راهبردی، عملیاتی و فنی نمود. نکتهٔ قابل‌توجه در این زیر قضیه این است که این باید متمرکز بر ایجاد ظرفیت باشد. برای نمونه با تقویت مراکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری) در کشور با توجه قطب‌بندی که تشریح شد می‌تواند کل ظرفیت امنیت سایبری در کشور را فعال نمود.

زیرقضیه ۲- توسعه فعالیت‌های تحقیقاتی امنیت سایبری نیازمند شبکه‌سازی، شناخت صحیح نیازهای تحقیقاتی، اصلاح فرایندهای تحقیقاتی (شبکه‌سازی در تحقیق و توسعه) با تأکید بر ایجاد اعتماد میان نهادهای مختلف است.

همان‌طور که ذکر گردید؛ توسعه فعالیت‌های تحقیقاتی بومی امنیت سایبری در کشور نیازمند توسعه نهادهای تحقیقاتی است. شبکه‌سازی نهادهای تحقیقاتی امنیت سایبر در کشور بر اساس مصاحبه‌های صورت گرفته مشارکت کل نهادها در سطوح راهبردی، عملیاتی و فنی امنیت سایبری است. البته این مشارکت بر اساس تائیدیه‌هایی است که نهادهای سیاست‌گذار به این مجموعه شرکت‌ها داده می‌شود. این شبکه‌سازی بر اساس قطب‌بندی است که نهاد

سیاست‌گذار می‌تواند برای مجموعه شرکت‌های تحقیقاتی در حوزهٔ امنیت سایبری ایجاد نماید و این شرکت‌ها بر اساس توانمندی خود در این قطب‌ها فعالیت کنند. البته ایجاد نظام‌مهندسی امنیت سایبری می‌تواند به این حوزه کمک نماید؛ بنابراین ازجمله افراد یا نهادهایی که می‌توان در این شبکه‌ها استفاده نمود می‌توان به نخبگان دانشگاهی، نخبگان نظامی، مدیران باتجربه، هکرها، نهادهای تحقیقاتی دولتی و غیردولتی نام برد.



شکل ٤. شبکه‌سازی عناصر تحقیقاتی امنیت سایبری در کشور

از موارد دیگر می‌توان به شناخت صحیح نیاز تحقیقاتی از نهادهای بهره‌بردار و کارفرما در این حوزه اشاره نمود. نهادهای بهره‌بردار بعضاً با عدم شناخت صحیح نیاز تحقیقاتی باعث ایجاد هزینه‌های اضافه به بخش خصوصی شده و یا با تعریف ناصحیح مسئله از نهادهای دانشگاهی استفاده صحیحی نمی‌شود. از موارد دیگر اصلاح فرایندهای تحقیقاتی در حوزهٔ امنیت سایبری در کشور است که شامل ارائه صلاحیت‌های تولید محصولات امنیتی به شرکت‌های تحقیقاتی است که آن‌ها بتوانند با اخذ این صلاحیت‌ها به تحقیق و تولید اقدام نمایند؛ با ارائه تعریف صحیحی از تحقیق می‌تواند فرایندهای حمایتی صحیحی از آن نیز داشت؛ این حمایت باعث ایجاد بازار باثبات و مطمئن از آن‌هاست و این باعث ایجاد اعتماد بین بخش خصوصی و دولتی می‌گردد.

زیرقضیه ۳- توسعه فعالیت‌های تحقیقاتی امنیت سایبری مبتنی بر نوآوری باز نیازمند استفاده از تمام ظرفیت‌های داخل و خارج ایران با ایجاد شرایط رقابتی برابر و حفظ حقوق مالکیت معنوی آن‌ها است.

همان‌طور که در مرور بر ادبیات اشاره گردید، با افزایش نیاز سازمان‌ها به تعامل با محیط و ذینفعان خارجی به‌منظور تبادل ایده‌های نوآورانه باید شرایط داخلی و هم خارجی در کسب نوآوری آماده گردد. در مصاحبه‌های صورت گرفته عوامل متعددی به‌عنوان عوامل داخلی و بیرونی اشاره گردید. ازجمله این عوامل که در این زیر قضیه به دلیل اهمیت آن به‌طور جداگانه تبیین می‌گردد؛ ایجاد شرایط رقابتی برابر و حفظ حقوق مالکیت معنوی آن‌هاست. حمایت از حقوق مالکیت فکری جهت حفظ حقوق معنوی ایده پردازان، مخترعان جهت توسعهٔ نوآوری می‌تواند کمک مؤثری در تولید نوآوری ایفا نماید. جهت حمایت از پژوهشگران در امور تحقیقاتی برای حفظ حقوق مالکیت فکری آن‌ها می‌توان به موارد ذیل توجه نمود:

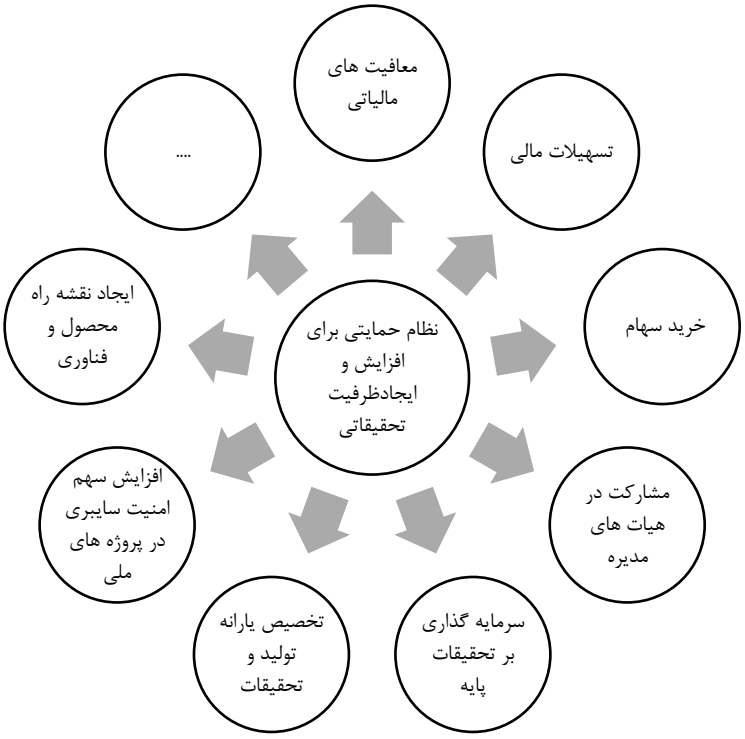
- رفع دغدغه خطرپذیری مالی در انجام مراحل پژوهشی و امور نوآورانه و حمایت از تجاری‌سازی دستاوردهای آنان و تقویت ابعاد معنوی، بصیرت افزایی، خودباوری و تعلق ملی
- حمایت مالی از ایجاد و توسعه بورس ایده و بازار فناوری به‌منظور استفاده از ظرفیت‌های علمی در جهت پاسخگویی به نیاز بخش‌های صنعت،
- اقدامات به‌منظور گسترش حمایت‌های هدفمند مادی و معنوی از نخبگان و نوآوران علمی و فناوری
- تأمین و پرداخت بخشی از هزینه‌های ثبت جواز امتیاز علمی[1] در سطح ملی و بین‌المللی و ایجاد تمهیدات و تسهیلات لازم برای انتشار آثار مفید علمی آنان

متأسفانه به حقوق مالکیت معنوی بخش خصوصی توجه نمی‌گردد. این حقوق هم بین بخش خصوصی و حاکمیتی مهم است و هم درون بخش‌های حاکمیتی مطرح هست. بعضاً محقق‌های این نهادهای حاکمیتی به دلیل عدم رعایت این حقوق از ارائه ایده‌های نوآورانه خود خودداری نموده‌اند.

همان‌گونه که اشاره گردید؛ به‌جای ایجاد نهادهای مختلف دولتی در این حوزه که بر سربار دولت افزوده می‌شود و بعضاً نتایج قابل‌توجهی هم در امور تحقیقاتی ندارند، می‌توان از ظرفیت‌های موجود در بخش خصوصی و مردم استفاده نمود. متأسفانه دولتمردان در واگذاری به بخش خصوصی انحصاری عمل نموده و حتی شرکت‌های خانوادگی ایجاد می‌نمایند. با توجه به توانمندی بخش خصوصی به اعتراف بسیاری از مدیران ارشد حاکمیتی تقویت این نهادها باید در اولویت امر قرار گیرد. به نقل‌قول مصاحبه‌شوندگان به شرکت‌های دانش‌بنیان، نخبگان خارج از کشور، هکرها، شرکت‌های خصوصی فعال، مدیران بازنشسته حوزهٔ امنیت سایبری و مراکز آپا در سطح کشور همه ظرفیت‌هایی هستند که می‌توان با استفاده از ایجاد شرایط رقابتی و حفظ حقوق مالکیت معنوی از آن‌ها بهره‌مند گردید؛ بنابراین پیشنهاد می‌گردد برای حفظ و تأمین حقوق مالکیت معنوی که یکی از عناصر توسعه دانش و نوآوری

1. patent

در نهادهای تحقیقاتی محسوب می‌شود؛ نظام‌نامه‌ای در نهادهای سیاست‌گذار همراه با الزامات قانونی قوی تهیه و اجرایی شود. از مهم‌ترین دغدغه‌های بخش غیردولتی حمایت نهادهای حاکمیتی از آن‌ها از دو جنبه است. اول حمایت از آن‌ها جهت رشد و توسعه و دوم ایجاد بازار باثبات. بنا بر گفتهٔ مصاحبه‌شوندگان ظرفیت تحقیقات امنیت سایبر در کشور مناسب است اما مدیریت آن نیازمند بازنگری دارد؛ حاکمیت می‌تواند با جهت‌دهی نهادهای تحقیقاتی در راستای نیازها و تهدیدات کشور در این حوزه به افزایش مشارکت و شکوفا شدن ظرفیت‌های تحقیقاتی کمک نماید. این نظام حاکمیتی می‌تواند حول محصولات راهبردی موردنیاز امنیت سایبری در کشور شکل بگیرد؛ بنابراین نظام حمایتی می‌تواند با ایجاد بازار امنیت سایبری در حوزه‌های راهبردی کشور شکل بگیرد. نهادهای حاکمیتی علاوه بر ایجاد بازار به طرق مختلف می‌تواند، ظرفیت‌های تحقیقاتی را در کشور در این حوزه فعال نماید. ازجمله می‌توان به معافیت‌های مالی و مالیاتی، تسهیلات در ضمانت‌های مالی، وارد نکردن هزینه‌های اضافی به آن‌ها، ایجاد نقشه راه امنیت سایبری و حمایت از طریق خرید سهام آن‌ها یا عضویت در هیئت‌مدیره بخش‌های خصوصی اشاره نمود. در شکل زیر عناصر این نظام حمایتی را می‌توان مشاهده نمود:



شکل ۵. عناصر نظام حمایتی امنیت سایبری برای نهادهای غیردولتی

زیرقضیه ۴- ایجاد ظرفیت تحقیقاتی امنیت سایبری مستلزم شناخت و آموزش مبانی امنیت سایبری، شبکه‌های مجازی و فناوری‌های مهندسی اجتماعی در جوامع سازمانی و غیرسازمانی کشور است.

از مباحث مهمی که در مصاحبه‌های صورت گرفته اشاره گردید، استفاده از ظرفیت تحقیقاتی امنیت سایبری در کشور است. البته بعضی از مصاحبه‌شوندگان بر این باور بودند که ظرفیت بالایی در کشور موجود است. نکته‌ای که باید به آن توجه نمود، ضعف فرهنگ امنیت در کشور در لایه‌های مختلف از راهبردی و عملیاتی گرفته تا سطح تکنیک و حتی شهروندان وجود دارد. ممکن است اخبار پراکنده‌ای از سرقت اطلاعات در محیط مجازی چه به‌صورت

یک حمله سایبری، ویروس و یا هک صفحات خصوصی شنیده شود؛ اما اهمیت این موضوع هنوز در لایه‌های مختلف دولت و مردم در ایران محرز نشده است که این مستلزم ایجاد برنامه‌های آموزشی مناسب در کشور است. با احراز اهمیت امنیت سایبری در کشور و اهمیت بومی بودن محصولات امنیت سایبری توجه به تحقیقات و ایجاد ظرفیت‌های تحقیقاتی نیز خودبه‌خود موردتوجه قرار می‌گیرد؛ بنابراین تهیه برنامه‌های آموزشی امنیت سایبری در کشور در سیاست‌گذاری‌های کلان کشور باید توجه شود. لازم است سرفصلی در سیاست‌گذاری کلان به‌عنوان آموزش امنیت سایبری در کشور اضافه شود.

زیرقضیه ۵- ایجاد نظام‌های قراردادی صحیح میان نهادهای تحقیقاتی (حاکمیتی و خصوصی) با حفظ حقوق مالکیت معنوی، بسترساز استفادهٔ حداکثری از توانمندی‌های شبکه‌های تحقیقاتی امنیت سایبر است.

ازجمله عوامل فعال شدن این شبکه‌های تحقیقاتی امنیت سایبری، حفظ حقوق مالکیت معنوی آن‌هاست؛ ایجاد بستر حفظ این حقوق با ایجاد نظام‌های قراردادی رسمی میان اعضای این شبکه‌ها امکان دارد. از مهم‌ترین زیرساخت‌های لازم برای گسترش ظرفیت‌های شبکه‌های فناوری زیرساخت‌های مالی و معاملاتی در تعامل با شبکهٔ همکاران و گلوگاه‌های موجود در این زمینه است (انصاری، ۱۳۹۱). روشن بودن این قوانین باعث ایجاد و توسعهٔ اعتماد متقابل میان شبکه‌ها، گسترش همکاری و ارتباطات متقابل، ارتقای قابلیت و خواست طرفین برای تسهیم منافع و ریسک‌های همکاری و درنهایت توسعهٔ تعهد متقابل میان آن‌ها می‌شود. با این اوصاف ارتقای قابلیت‌های قانونی و حقوقی از طریق قوانین مالی و معاملاتی از گام‌های مهم در ایجاد بستر استفاده از نهادهای تحقیقاتی امنیت سایبری محسوب می‌شود، درواقع زیرساخت قانونی درزمینهٔ مالی و معاملاتی سازگار و تسهیل‌کننده جریان همکاری با شبکه است (فرتوک زاده و همکاران، ۱۳۹۱).

نتیجه‌گیری

همان‌گونه که در مقدمه بیان گردید؛ با تغییر و تحولات سریع در حوزه فناوری به‌خصوص فناوری اطلاعات و امنیت سایبری و اهمیت دستیابی به محصولات بومی در این حوزه، استفاده از پارادایم نوآوری باز در کسب فناوری‌ها و نوآوری‌ها از اهمیت بسزایی برخوردار است. در این مقاله باهدف شناسایی عوامل توسعه نوآوری باز در نهادهای تحقیقاتی امنیت سایبری، ابتدا فرایندهای نوآوری باز در ادبیات تحقیق موردبررسی قرار گرفت. این عوامل به دو بعد عوامل آمادگی درون‌سازمانی و آمادگی بیرون سازمانی تقسیم گردید. با کمک روش نظریه داده بنیاد و مصاحبه‌های اکتشافی نیمه ساختاریافته توانست عوامل این مدل را در نهادهای تحقیقاتی امنیت سایبر ایران شناسایی و با توجه به شرایط محیطی و زمینه‌ای در ایران تبیین نماید. از مهم‌ترین نتایج این مقاله می‌توان به قضایای تئوریکی اشاره نمود که حاصل کدگذاری انتخابی روش داده بنیاد است. با توجه به نتایج به‌دست‌آمده در این پژوهش نهادهای مختلفی و متنوعی در کشور در حوزهٔ امنیت فضای سایبر فعالیت می‌کنند نیازمند آمادگی درون‌سازمانی و بیرون سازمانی از قبیل؛ تدوین سیاست‌های بخشی در بهره‌مندی از نخبگان توانمند، شبکه‌سازی مناسب میان نهادهای تحقیقاتی، شناخت صحیح نیازها و فرایندهای تحقیقاتی، استفاده از تمام ظرفیت‌های داخل و خارج با ایجاد شرایط رقابتی و آموزش مبانی امنیت سایبری است. ازجمله نتایج دیگر این تحقیق توجه به الزامات قانونی به‌عنوان رکن حکمرانی مؤثر در نهادهای تحقیقاتی امنیت سایبری است. تدوین نظام‌های قراردادی صحیح میان نهادهای تحقیقاتی (حاکمیتی و خصوصی) با حفظ حقوق مالکیت معنوی، بسترساز استفادهٔ حداکثری از توانمندی‌های شبکه‌های تحقیقاتی امنیت سایبر است و در کنار آن تربیت مدیرانی توانمند با قاطعیت اجرایی که خود را متعهد به بخش خصوصی دانسته و به‌دوراز سیاست زدگی و برخوردهای سلیقه‌ای بتوانند از این ظرفیت در تولید محصول بومی امنیت سایبری در کشور بهره‌مند شوند. ازجمله مواردی که می‌توان در تحقیقات آتی در این حوزه به آن اشاره نمود، تبیین و تشریح هرکدام از قضایای ارائه‌شده در

این تحقیق و ارائه راهکارهای اجرایی مؤثر برای مدیران ارشد سیاست‌گذار در نهادهای تحقیقاتی امنیت سایبری در کشور است.

از محدودیت‌های تحقیقات کیفی ازجمله این تحقیق جمع‌آوری اطلاعات، مصاحبه‌های اکتشافی با مدیران و سوگیری محقق در ارائه اطلاعات است که در این تحقیق با توجه به روایی و پایایی ارائه‌شده در روش تحقیق سعی شده است که محدودیت‌های مذکور درنتیجه تحقیق تأثیری نداشته باشد. البته همانند اغلب مطالعات مبتنی بر نظریه داده بنیاد، یافته‌های تحقیق با اتکا به دیدگاه‌ها و تجربیات افراد نسبتاً محدودی حاصل‌شده است که با در نظر گرفتن طیف گسترده‌ای از خبرگان از نهادهای مختلف امنیت سایبری در کشور سعی بر غلبه بر این محدودیت شده است. ازجمله محدودیت‌های دیگر می‌توان به راهبردی بودن موضوع این تحقیق اشاره نمود، مدیران تحقیقاتی بعضاً با ادبیات نوآوری باز آشنا نبوده و مدیران سیاست‌گذار در این حوزه با ادبیات تولید محصولات بومی امنیت سایبری آشنا نبودند؛ که با انتخاب افرادی که در این دو حوزه تجربه داشتند سعی در برطرف نمودن این محدودیت شده است.

منابع

انصاری، باقر .(۱۳۸۷) .تدوین قراردادهای نمونه و اطلاع‌رسانی دربارهٔ شیوهٔ استفادهٔ آن‌ها . در *سازوکارهای حقوقی حمایت از تولید علم* (ص ۳۷۸) .تهران: سمت.

چسبرو، هنری .(۱۳۹۰) .*نوآوری باز؛ پارادایم نوین آفرینش و تجاری‌سازی فناوری* .موسسه خدمات فرهنگی رسا.

دانایی‌فرد، حسن. (۱۳۸۹). *استراتژی‌های نظریه‌پردازی*. تهران: سمت.

صفدری، مصطفی. منطقی، منوچهر؛ و توکلی، غلامرضا. (۱۳۹۳). نوآوری باز؛ نگاهی جامع بر مفاهیم، رویکردها، روندها و عوامل کلیدی موفقیت. *رشد فناوری*، ۴۰, ۱۰-۱۷.

فرتوک زاده، حمیدرضا. دره شیری، محمدرضا؛ و محبی، محمد .(۱۳۹۱) .بررسی گلوگاه‌های قوانین مالی و معاملاتی صنایع دفاعی در تعامل با شبکهٔ همکاران .*مدیریت بهبود*، ۱۳، ۶۴-۸۴.

Cheng, C. C. & Huizingh, E. K. (2014). when is open innovation beneficial? the role of strategic orientation. *Product Development & Management Association*.

Chesbrough, H. (2003). *Open Innovation: The new imperative for creating and profiting from technology.* Harvard Business School Press.

Chesbrough, H. Vanhaverbeke, W. & West, J. (2006). *Open innovation Researching a New Paradigm.* New York: Oxford University Press.

Chiaroni, D. Chiesa, V. & Frat, F. (2011). The Open Innovation Journey: How firms dynamically implement the emerging innovation management paradigm. *Technovation*, 31, 34-43.

de Jong, J. P. Vanhaverbeke, W. Kalvet, T. & Chesbrough, H. (2008). *Policies for Open Innovation: Theory, Framework and cases*`. Vision EraNet.

Felin, T. & Zenger, T. (2013). Closed or open innovation? Problem solving and the governance choice. *Research Policy*.

Fetterhoff, T. & Voelkel, D. (2006). Managing Open innovation In Biotechnology. *Research–Technology Management*, 3, 49(3),14–18.

Gassmann, O. & Enkel, E. (2004). Towards a Theory of Open Innovation: Three Core Process Archetypes. *R&D Management Conferece*.

Hafkesbrink, J. & Schroll, M. (2010). Organizational Competences for Open Innovation in Small and Medium Sized Enterprises of the Digital Economy. In J. Hafkesbrink, H. Hoppe, & J. Schlichter, Competences Management for Open Innovation. Tools and IT- support to unlock the innovation potential beyond company boundaries (pp. 21-52). Lohmar.

Herstad, S. Bloch, C. Ebersberger, B. & Velde, E. (2008). *Open innovation and globalisation: Theory, evidence and implications.* Vision EraNet project report.

Jacobides, M. & Billinger, S. (2006). Designing the boundaries of the firm: From "make, buy, or ally" to the dynamic benefits of vertical architecture. *Organization Science*, 17(2), 249-261.

Strauss, A. & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory.* SAGE Publications.

Tidd, J. & Bessant, J. (2009). *Managing Innovation: Integrating Technological, Market and Organizational change* (4th ed.).

twining, j. (2000). *a naturalistic journey into the collaboratory: in search - Hrast.* Texas: Texas womans university.

Wallin, M. & Krogh, G. (2010). Organizing for Open Innovation: Focus on the Integration of Knowledge. *Organizational Dynamics*, 39(2), 145–154.

Zemaitis, E. (2014). Knowledge management in open innovation paradigm context: high-tech sector perspective. *Procedia - Social and Behavioral Sciences*, 164-173.