Scientometrics Research Journal

Scientific Bi-Quarterly of Shahed University
Vol. 9, No. 2, Autumn & Winter 2023-24 (Serial 18)

Research Article

DOI: 10.22070/RSCI.2022.14656.1511

Semantic model of Information Security: Extracting Conceptual Network with Analysis Approach of Scientific Publications and Delphi

Adele Ahangar [1]

Fahimeh Babalhavaeji [2*]

Molouk Sadat Hosseini Beheshti [3]

Nadjla Hariri [4]

Maryam Khademi [5]

1. *Ph.D. Student of Knowledge and Information Science, Science and Research Branch, Islamic Azad University, Tehran, Iran.*
Email: adeleahangar@yahoo.com

2. *Associate Professor, Department of Knowledge and Information Science, Science and Research Branch, Islamic Azad University, Tehran, Iran. (Corresponding Author)*
Email: f.babalhavaeji@gmail.com

3. *Associate Prof.of Linguistcs Department, Iranian Research Institute for Information Science and Technology (IRANDOC).*
Email: beheshti@irandoc.ac.ir

4. *Professor, Department of Knowledge and Information Science, Science and Research Branch, Islamic Azad University, Tehran, Iran.*
Email: nadjlahariri@gmail.com

5. *Associate Professor, Department of Applied Mathematics, South of Tehran, Islamic Azad University, Tehran, Iran.*
Email: khademi@azad.ac.ir

Date of Reception: 04/02/2023

Date of Acceptation: 11/07/2023

Abstract

Purpose: Considering the emergence and increasing expansion of various subject domains and the lack of a valid codified thesaurus, the main aim of this study is to provide a semantic model of information security based on a conceptual network for use in domain ontologies, so it is applied research.

Methodology: The research method is a combination of co-word analysis, library, and Delphi methods. In the first stage, the conceptual network was extracted from 7547 scientific documents on "information security" using the co-words analysis method. These documents were indexed in the Scopus databases and WOS from 2013 to 2017. Preprocessing operations on 19648 keywords and tags were done in a completely targeted manner by using five dictionaries in information security, and three dictionaries in computer science. With a minimum co-occurrence of 5 for each word in "VOS Viewer", 207 preferred concepts were selected based on the latest version of the information security dictionary, and its conceptual network was mapped. By "Gephi", betweenness centrality, density, and clustering coefficient indices were checked. Then in the second stage, for extracting a new semantic model, used the library method. So, seven related semantic models: Security ontology, information security ontology, attack ontology, vulnerability ontology, existence - Ontosec mapping, and threat taxonomy as well as the conceptual model of information systems security in libraries. These entities,

Scientometrics Research Journal

Scientific Bi-Quarterly of Shahed University
Vol. 9, No. 2, Autumn & Winter 2023-24 (Serial 18)

Research Article

DOI: 10.22070/RSCI.2022.14656.1511

Adele Ahangar [1]

Fahimeh Babalhavaeji [2*]

Molouk Sadat Hosseini Beheshti [3]

Nadjla Hariri [4]

Maryam Khademi [5]

Date of Reception: 04/02/2023

Date of Acceptation: 11/07/2023

classes, subclasses, relationships between them, concepts, and examples attributed to each class and subclass were studied and examined carefully. Then, 207 conceptual network concepts were adapted to the common components of these models, and a new model was presented. Finally, in third stage, using the fuzzy Delphi technique, the consensus of experts in both fields of Knowledge and Information Science (KIS) and Computer Sciences was examined. Using SPSS and Kendall's non-parametric test, the experts' agreement coefficient about the classes and sub-classes, as well as their associated concepts, were investigated. 5 classes, 6 subclasses and also 71 concepts out of 97 common concepts with an agreement coefficient above 0.7 were obtained. Finally, confirmatory factor analysis and Smart PLS structural modeling were used to check the correctness of the relationships governing the classes and subclasses in the conceptual model.

Findings: The main nodes and strong links in the conceptual network of information security include: "information security," "security," "information system," "privacy," "telecommunication," "information," "intrusion detection system," "cryptography," "cyber security," "authentication," "network," "risk," "threat," and "risk management framework." The extracted semantic model has a goodness of fitting (GOF) of 0.710 and confirms 11 semantic relationships. These relationships include: "Requires level," "Diminish," "Threatens," "Exploited by," "has Source," "Uses of," "Lead to," "Attack," "Vulnerability on," "Implemented by," and "Reduce." Also, it has 5 main classes, including "Information Asset," "Security Attribution," "Threat," "Vulnerability," and "Countermeasure." There are also 6 subclasses, which include "Threat Source," "Access Path (influence way)," "Threat Tools," and "Attack," all related to the Threat class. Additionally, there are Technological countermeasures and Organizational countermeasures, which are related to the Countermeasure class. Also, it was discovered that there are 71 attributive concepts, some of which include: Password, Smart card, User, Integrity, Hacker, Malicious code, Virus, Distributed Denial Of Service (DDOS), Risk management, Backup, Digital signature, Penetration testing, Antivirus, Firewall, and so on.

Conclusion: The conceptual network and semantic model can be inferred in semantic systems and databases. This research can provide a new method for creating high-level ontologies to optimize search engines and reduce false dropping, as well as recover unwanted information.

Keywords: Conceptual Network, Semantic Model, Information Security, Ontology, Search Engine Optimization.

پژوهش‌نامه علم‌سنجی
دوفصلنامه علمی دانشگاه شاهد/ دوره ۹/ شماره ۲/ پاییز و زمستان ۱۴۰۲ (پیاپی ۱۸)

مقاله پژوهشی

DOI: 10.22070/RSCI.2022.14656.1511

مدل معنایی حوزه امنیت اطلاعات: استخراج شبکه مفاهیم با رویکرد تحلیل انتشارات علمی و دلفی

عادله آهنگر [۱]
۱. دانشجوی دکتری علم اطلاعات و دانش‌شناسی، دانشگاه آزاد اسلامی، واحد علوم تحقیقات، تهران. ایران.
Email: adeleahangar@yahoo.com

فهیمه باب‌الحوائجی [۲*]
۲. دکتری علم اطلاعات و دانش‌شناسی، دانشیار، دانشگاه آزاد اسلامی، واحد علوم تحقیقات، تهران. ایران. (نویسنده مسئول)
Email: f.babalhavaeji@gmail.com

ملوک‌السادات حسینی بهشتی [۳]
۳. دکتری زبان‌شناسی، دانشیار، پژوهشگاه علوم و فناوری ایران. (ایرانداک).
Email: beheshti@irandoc.ac.ir

نجلا حریری [۴]
۴. دکتری علم اطلاعات و دانش‌شناسی، استاد؛ دانشگاه آزاد اسلامی، واحد علوم تحقیقات؛ تهران، ایران.
Email: nadjlahariri@gmail.com

مریم خادمی [۵]
۵. دکتری ریاضی کاربردی، دانشیار؛ دانشگاه آزاد اسلامی، واحد تهران جنوب، تهران. ایران.
Email: khademi@azad.ac.ir

صفحه ۲۶۸-۲۴۷
دریافت: ۱۴۰۱/۱۱/۱۵
پذیرش: ۱۴۰۲/۰۴/۲۰

چکیده

هدف: ارائه مدل معنایی حوزه امنیت اطلاعات بر اساس شبکه مفاهیم، برای استفاده در هستی‌نگاری‌های دامنه است.

روش‌شناسی: ترکیبی از روش‌های هم‌رخدادی واژگان، کتابخانه‌ای و دلفی استفاده شد. ابتدا با استفاده از تحلیل هم‌رخدادی واژگان، شبکه مفهومی ۷۵۴۷ مدرک علمی محققان حوزه امنیت اطلاعات، نمایه‌شده در پایگاه‌های اسکوپوس و وبگاه علوم در سال‌های ۲۰۱۳-۲۰۱۷ استخراج؛ سپس مدل معنایی جدید با استفاده از روش کتابخانه‌ای و تطبیق هفت مدل معنایی مرتبط با شبکه مفهومی ارائه، و در انتها با استفاده از تکنیک دلفی فازی میزان اجماع خبرگان دو حوزه علم اطلاعات و دانش‌شناسی و حوزه کامپیوتر مورد بررسی قرار گرفت.

یافته‌ها: یافته‌ها نشان می‌دهد که شبکه مفهومی امنیت اطلاعات مستخرج از «وی.اُ.اس.ویور» [۱]، و «گِفی» [۲]، دارای ۲۰۷ مفهوم مرجع و ۲۷۹۶ پیوند است. همچنین مدل معنایی دانش این حوزهٔ بررسی‌شده توسط تحلیل عاملی تأییدی و مدل‌سازی ساختاری اسمارت پی ال اس دارای برازش کلی ۰.۷۱۰ و ۱۱ رابطه معنایی تأییدشده در ۵ کلاس اصلی، ۶ زیرکلاس، و ۷۱ مفهوم منتسب است.

نتیجه‌گیری: شبکه مفهومی و همچنین مدل معنایی یافته‌شده در حوزه امنیت اطلاعات، قابل استنتاج در سیستم‌های اطلاعاتی و ماشین است و می‌توان با استفاده از این روش، هستی‌نگاری‌های دامنه سطح بالا، جهت بهینه‌سازی موتورهای جستجو ارائه کرد.

واژگان کلیدی: شبکه مفهومی، مدل معنایی، امنیت اطلاعات، هستی‌نگاری، بهینه‌سازی موتورهای جستجو.

1. VOSviewer
2. Gephi

مقدمه و بیان مسئله

با گسترش روزافزون خدمات وب جهان‌گستر ۱.۰، ۲.۰ و ۳.۰ اخیراً نیز ٤.۰ کتابخانه‌ها و مراکز اطلاع‌رسانی همچون دیگر سازمان‌های مدرن اطلاعاتی به‌منظور بقای خود، همراه با جنبش دیجیتالی‌شدن، سرمایه‌گذاری‌های قابل توجهی در ایجاد سامانه‌ها، ارائه خدمات پیوسته به کاربران، ایجاد پایگاه‌های اطلاعاتی پیوسته و OPAC[1]ها انجام دادند (Newby, 2000). تسهیل فرایندهای کاری این مراکز با وجود سیستم‌های اطلاعاتی، ارتباطات و شبکه، تجهیزات کامپیوتری و سامانه‌ها؛ چالش‌هایی چون حفظ حریم خصوصی، امنیت سیستم‌های اطلاعاتی، امنیت شبکه‌های کامپیوتری در مواجهه با انواع تهدیدهای داخلی و خارجی مانند دست‌کاری، سرقت و افشای اطلاعات مُرجّع، آسیب‌زدن و تخریب آنها به‌صورت عمد و غیرعمد را به وجود آورده است (Ismail &Zainab, 2011).

بر اساس تعریف ارائه‌شده از سازمان بین‌المللی استاندارد، ایزو ۲۰۰۲، امنیت اطلاعات عبارت است از حفاظت از محرمانگی،[2] یکپارچگی[3] و دسترس‌پذیری[4] اطلاعات. در این تعریف همچنین با قید اشکال مختلف اطلاعات اعم از چاپی، الکترونیکی، شفاهی و غیره؛ هدف از تأمین امنیت اطلاعات را تضمین تداوم کسب و کارها و به حداقل رساندن آسیب‌های تجاری از طریق محدودکردن تأثیر حملات و رخدادهای امنیتی اعلام می‌کند (Solms & Niekerk, 2013).

وجود استانداردهای بین‌المللی فنی و مدیریتی در زمینه امنیت اطلاعات؛ کتابخانه‌ها و مراکز اطلاع‌رسانی را بر آن داشت تا با تدوین خط‌مشی‌ها و سیاست‌گذاری‌های امنیتی حفاظتی به مسئله حفظ حقوق مالکیت فکری و معنوی صاحبان اطلاعات، محافظت از دیتا و متادیتا، سامانه‌ها و غیره بپردازند و در همین راستا مطالعات گوناگونی نیز انجام شده است که عبارت‌اند از: هک‌شدن سرور کتابخانه‌ها (Cheng, 2005)، تجزیه و تحلیل سیستم‌های اطلاعاتی (Fox, 2006)، فرهنگ امنیت اطلاعات (DaVeiga et al., 2007)، امنیت منابع اطلاعاتی (Abubakar & Aduku, 2016)، مدیریت امنیت سامانه‌های دیجیتال (Zhao et al., 2018) در خارج از کشور و امنیت اطلاعات در کتابخانه‌های دیجیتال ایران (حریری و نظری، ۱۳۹۱)، امنیت اطلاعات سامانه‌های تحت وب نهاد کتابخانه‌های عمومی کشور (کوکبی و کوهی، ۱۳۹٤)، میزان رعایت استانداردهای آی ای اس ۲۷۰۰۲ و ۲۷۰۱۹ در حوزه مدیریت امنیت اطلاعات در سازمان اسناد و کتابخانه ملی ایران (آریان‌پور، ۱۳۹۵)، و نظام مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران (حاجی زین‌العابدینی و رفعتی، ۱۳۹٦) در ایران. بررسی‌ها نشان می‌دهد که در موارد فوق‌الذکر، طراحی محیط امن و عوامل مؤثر بر آن با توجه به استانداردها[5] بیشتر مورد توجه نویسندگان بوده است و در هیچ کدام از آنها الگو و چارچوب معنایی حاکم بر حوزه امنیت اطلاعات ارائه نشده است. با توجه به تعریف انجمن

1 . Online Public Access Catalogs
2 . confidentiality
3 . integrity
4 . availability

۵ . مؤلفه‌های استاندارد امنیت اطلاعات ایزو ۲۷۰۰۲ عبارت‌اند از خط‌مشی امنیت، سازمان‌دهی امنیت اطلاعات، مدیریت دارایی‌ها، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی‌ها، تهیه و توسعه و نگهداری سیستم‌های اطلاعاتی، مدیریت حوادث امنیت اطلاعات، مدیریت تداوم کسب و کارها، انطبا؛

هستی‌نگاری، وجود الگوها و چارچوب‌های معنایی در هر حوزه دانشی می‌تواند به عمق و غنای مفاهیم بازیابی‌شده توسط موتورهای جستجو بیفزاید؛ لذا بر این اساس اگر در ساخت هستی‌نگاری‌ها از تاکسونومی‌ها و اصطلاح‌نامه‌ها استفاده شود، هستی‌نگاری‌ها سبک‌وزن و اگر از مدل‌های مفهومی، نظریه‌های منطقی و سایر هستی‌نگاری‌ها استفاده شود هستی‌نگاری سنگین‌وزن محسوب می‌شوند (McGuinness, 2017). ازآنجاکه در این پژوهش اصطلاح‌نامه‌ای در حوزه امنیت اطلاعات یافت نشد، لذا تلاش شد تا با ارائه یک مدل معنایی، هم، آگاهی بخشی مدیران کتابخانه‌ها نسبت به عمق مفهوم امنیت اطلاعات دنبال شود، و هم به‌عنوان روشی جدید در مدل‌سازی‌های معنایی و ساخت هستی‌نگاری‌های سطح بالای دامنه، به بازنمایی مفهوم در ماشین، استنتاج معنایی و استدلال منطقی، و در یک کلام به بهینه‌سازی موتورهای جستجو در بازیابی مفاهیم آن حوزه موضوعی کمک بشود؛ لذا، مسئله اصلی در این پژوهش، ارائه مدل معنایی حوزه امنیت اطلاعات با رویکرد تحلیل انتشارات علمی و دلفی از شبکه مفهومی مستخرج این حوزه از پایگاه‌های اسکوپوس و وبگاه علوم است.

پرسش‌های پژوهش

۱. شبکه مفهومی حوزه «امنیت اطلاعات» بر اساس پایگاه‌های اسکوپوس و وبگاه علوم در سال‌های ۲۰۱۳ تا ۲۰۱۷[1] چگونه است؟

۲. مدل معنایی حوزه «امنیت اطلاعات» بر اساس مدل‌های گذشته و شبکه مفهومی چگونه است؟

۳. میزان توافق خبرگان دو حوزه کامپیوتر و علم اطلاعات و دانش‌شناسی با مفاهیم، کلاس‌ها/زیرکلاس‌های مدل مفهومی به‌دست‌آمده چقدر است؟

چارچوب نظری

از منظر ریاضیات شبکه‌های مفهومی، داده‌های سازمان‌یافته در ساختار شبکه‌ای هستند که با استفاده از شبکه‌ای از گراف‌ها نمایش داده می‌شوند (مازا،۱۳۹۲). گراف‌ها نمایش‌های دیداری از نقاطی به نام گره‌ها یا رأس‌ها هستند که نمونه‌هایی از داده‌ها[2] را به نمایش می‌گذارند. گره‌ها توسط اتصالاتی با نام یال‌ها که دارای جهت، مسیر و مقدار هستند به هم ربط داده شده و روابط بین نمونه‌ها را ارائه می‌دهند. به‌طور خلاصه می‌توان گفت هر شبکه مفهومی، مجموعه‌ای از حداقل ۳ گره و تعدادی یال است که وجود یا عدم وجود ارتباط میان گره‌ها را نشان می‌دهد (احمدی، ۱۳۹٤). در تحلیل شبکه‌های مفهومی شاخص‌های متعددی وجود دارد. به‌عنوان نمونه اندازه شبکه را با تعداد گره، چگالی[3] شبکه را با تعداد رابطه می‌سنجند و شاخص‌های مرکزیت اعم از مرکزیت رتبه،[4] مرکزیت نزدیکی[5] و بینابینی،[6] و مرکزیت بردار ویژه[7] به‌ترتیب به نفوذ و قدرت مفاهیم در شبکه، فاصله یک مفهوم با مفاهیم دیگر شبکه، مقدار نزدیکی یک یک مفهوم به مفاهیم دیگر و قدرت آن مفهوم در میان همسایگانش می‌پردازد (سهیلی و عصاره،۱۳۹۱).

---

۱ . زمان انجام این پژوهش در سال ۲۰۱۸ بوده و لذا با رویکرد گذشته‌نگر ۵ ساله از سال ۲۰۱۳-۲۰۱۷ انتخاب شده است.

۲ . داده‌ها می‌توانند افراد، گروه‌ها، واحدها، سازمان‌ها، مقاله‌ها، استنادها یا مفاهیم یک دامنه موضوعی باشند.

3 . Density
4 . Degree
5 . Closness
6 . Betweenness
7 . Eigenvector centrality

منظور از مدل‌سازی معنایی، مدل‌سازی چارچوب توصیف منبع[1] و موجودیت رابطه پیشرفته[2] است (Daconta et al., 2003, Obrest, 2006) که هر دو مبتنی بر گراف‌اند و جهت ذخیره و بازیابی معنایی قابل پردازش در ماشین، مدل‌هایی سطح بالا از داده ارائه می‌دهند. از این نوع مدل‌های معنایی به‌عنوان ابزار قوی سازمان‌دهی اطلاعات در ساخت هستی‌نگاری‌های سنگین‌وزن استفاده می‌شود (McGuinness, 2017) و شامل نمودارهایی از اشیا و روابط میان آنها هستند (Elmasri & Navathe, 2015) که به توصیف غنی معنایی از مجموعه داده‌های ساختاریافته (مفاهیم) می‌پردازند و موضوع یک هستی‌نگاری را کنترل می‌کنند (Spaccapietra et al., 2008). در این مدل‌ها، مؤلفه‌های معنایی «موجودیت»، «صفت» و «ارتباط» وجود دارد. منظور از موجودیت، مفاهیم خاص و عامی است که در نقش زیرکلاس و یا سوپرکلاس هستند. مفاهیم می‌توانند یک‌کلمه‌ای یا مجموعه‌ای از چند کلمه باشند. در این مدل‌ها، موجودیت Y یک زیرکلاس از موجودیت X است اگر و فقط اگر هر Y لزوماً X باشد. موجودیت زیرکلاس تمام ویژگی‌ها و روابط موجودیت سوپرکلاس خود را به ارث می‌برد. به این ویژگی صفت و ارث رابطه می‌گویند. موجودیت زیرکلاس ممکن است صفات و روابط خاص خود را داشته باشد (همراه با تمام ویژگی‌ها و روابطی که از سوپرکلاس به ارث می‌برد) (Elmasri & Navathe, 2015). منظور از *صفت*، ویژگی‌های خاص هر موجودیت است که می‌تواند ساده یا مرکب، تک‌مقداری یا چندمقداری و غیره باشد. منظور از *ارتباط* بستگی و تعامل بین دو موجودیت یا بیشتر است. به تعبیر دیگر، عملی است که بین انواع موجودیت‌ها جاری بوده، هست یا خواهد بود. هر نوع ارتباط، معنایی مشخص دارد و با یک نام بیان می‌شود (فروزنده، ۱۳۹۰).

پیشینه پژوهش

مطالعات انجام‌شده در زمینه امنیت اطلاعات نشان می‌دهد که محققان رشته‌های مختلف مدیریت، علم اطلاعات و دانش‌شناسی، و کامپیوتر برای شناخت این حوزه، از روش‌های مختلفی استفاده کرده‌اند، در برخی از آنها با شناسایی عوامل مؤثر بر امنیت اطلاعات، به دنبال بررسی نقش و تأثیر مؤلفه‌ها بر یکدیگر بودند که نمونه پژوهش‌ها در ایران عبارت‌اند از پژوهش‌های حریری و نظری (۱۳۹۱) با عنوان امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران؛ خضری پور (۱۳۹۲) تحت عنوان ارائه یک مدل برای بهبود مدیریت امنیت دارایی‌های اطلاعاتی سازمان در سیستم مدیریت امنیت اطلاعات ادارات دولتی شهر کرمان؛ آرین‌پور (۱۳۹۵) با عنوان میزان رعایت استانداردهای ایزو/آی.ای.سی. ۲۰۷۷۲ و ۲۰۷۵۳ در حوزه مدیریت امنیت اطلاعات سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران؛ سیف و نادری (۱۳۹۶) تحت عنوان شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره ایران؛ و شیرواندهی (۱۳۹۷) **با عنوان** سنجش عملکرد مدیریت امنیت اطلاعات در کتابخانه دیجیتال سازمان اسناد کتابخانه ملی ایران. و در خارج از کشور این دست از پژوهش‌ها عبارت‌اند از الشبول و اِسترِف (Alshboul et al., 2015) با عنوان تحلیل مدل امنیت اطلاعات برای سازمان‌های کوچک؛ دَوار (Dawar, 2016) تحت عنوان امنیت اطلاعات دیجیتال در کتابخانه‌های دانشگاهی؛ ژاو و همکاران (Zhao et al., 2018) با عنوان مدیریت امنیت کتابخانه‌های دیجیتالی در دانشگاه‌های نظامی؛ و پژوهش امینی و همکاران (Amini et al., 2021) تحت عنوان عوامل انسانی مؤثر بر امنیت اطلاعات کتابخانه‌ها.

1 . Resource Description Framework/Schedule (RDF/S)
2 . Enhanced Entity–Relationship (EER) model (or Extended Entity–Relationship model)

در برخی از پژوهش‌های مرتبط با این حوزه با استفاده از شبکه‌های مفهومی، تولیدات علمی محققان را ارزیابی کردند و مهم‌ترین مفاهیم این حوزه را استخراج و با استفاده از ترسیم شبکه مفهومی روابط پنهان معنایی واژگان در بافت متون را کشف کردند که در اینجا به علت فضای محدود مقاله صرفاً نمونه‌هایی از شبکه‌های مفهومی و مدل‌های معنایی این حوزه بیان شده است:

ونگ (Wang, 2013) در پژوهشی تحت عنوان شبکه‌ای نامرئی از دانش امنیت و حریم خصوصی سلامت، با تجزیه و تحلیل ۱۰۲۱۸ استناد از ۳۴۹ مقاله منتشرشده در مجلات حوزه امنیت و حفظ حریم سلامت، از سال ۲۰۰۳ تا ۲۰۱۲، ساختار فکری امنیت و حریم خصوصی مطالعات بهداشتی را ترسیم می‌کند .با تجزیه و تحلیل کلمات کلیدی و ابربرچسب‌ها، مفاهیم «فناوری»، «سوابق»، «محرمانه»، «اینترنت»، «ارتباط» و «کنترل دسترسی» به‌عنوان مفاهیم در حال ظهور در حوزه امنیت و حریم خصوصی شناسایی شدند. اولیجنیک(Olijnyk, 2015) در پژوهش خود به «بررسی کمّی ساختار فکری امنیت اطلاعات از سال‌های ۱۹۶۵ تا ۲۰۱۵» پرداخت نتایج پژوهش نشان داد چین و آمریکا در این حوزه بیشترین تأثیر را داشتند و حتی چین از آمریکا پیشی گرفت. مضامین علمی متعددی مانند «رمزنگاری»، «مدیریت و مدیریت امنیت اطلاعات» در طول دهه‌ها ظهور یافت؛ مفاهیم ویژه‌تر مثل«تشخیص نفوذ»، «امنیت داده‌های پزشکی»، «پاتوگرافی»، «امنیت بی‌سیم» نیز رشد پیدا کرد. انور و همکاران (Anwar et al., 2018) در پژوهشی تحت عنوان ترسیم نقشه دانش امنیت ملّی در سدهٔ ۲۱ به بررسی ساختار فکری، توسعه و تکامل پژوهش‌های امنیت ملی از طریق تجزیه و تحلیل کتاب‌شناختی مقالات پژوهشی این حوزه از سال‌های ۲۰۰۰ تا ۲۰۱۷ پرداخته‌اند. از بررسی ۵۴۵۷۲ سند که توسط ۵۸۲۷ نویسنده در ۸۱۷ مجله منتشرشده، مهم‌ترین کلمات کلیدی عبارت‌اند از «امنیت ملی»، «امنیت»، «سیاست»، «امنیت غذایی»، «ایالات متحده»،«جنگ»، «تغییرات آب و هوا» و «چین». همچنین نتایج نشان می‌دهد که مجلات «علوم سیاسی آمریکا»، «علوم»، «امنیت بین‌المللی»، «مجله امور خارجه و سازمان بین‌المللی» به‌عنوان مجلات برتر، و پنج نویسنده پراستناد از «ایالات متحده آمریکا»، «انگلیس»، «استرالیا»، «کانادا»و «آلمان» هستند. پروین و همکاران (Parvin et al., 2019) در پژوهشی تحت عنوان رویکرد علم‌سنجی به امنیت اطلاعات، هدف پژوهش خود را، بررسی روند تولیدات علمی حوزه امنیت اطلاعات در خاورمیانه و جهان از دیدگاه علم‌سنجی بیان کردند و نتایج حاصل از پژوهش آنها نشان داد که بیشتر نشریات علمی در زمینه امنیت اطلاعات در ایالات متحده آمریکا و چین تولید شده‌اند. در میان کشورهای خاورمیانه، ایران از نظر انتشارات علمی در حوزه امنیت اطلاعات، اوّل و در بین کشورهای جهان در رده ۲۳ام قرار دارد دونیکووا و همکاران (Doynikova et al.,2020) در مقاله‌ای تحت عنوان مدل معنایی برای ارزیابی امنیت سیستم‌های اطلاعاتی به توسعه و کاربرد یک مدل معنایی برای هستی‌نگاری ارزیابی امنیت پرداخته‌اند. معیارها در مدل پیشنهادی بر اساس روابط بین موجودیت‌های مربوط به امنیت، ویژگی‌های اصلی و اهداف ارزیابی امنیت است. این معیارها، نمودار سلسله‌مراتبی بر اساس ویژگی‌های داده و اهداف ارزیابی امنیت ترسیم می‌کند.

همچنین در برخی از تحقیقات تلاش شده است تا با استفاده از مدل‌سازی‌های معنایی و ساخت پایگاه‌های اطلاعاتی در این زمینه، این حوزه موضوعی را به رایانه و ماشین بشناسانند مانند پژوهش یانگ و همکاران (Yang et al., 2012) نشان می‌دهد که سیستم‌های اطلاعاتی مبتنی بر استنتاج و درک معنا، با استفاده از فنون کامپیوتری و به‌کارگیری آمار، ارتباط میان مؤلفه‌ها و نمونه‌ها را با استفاده از تشابه در الگوها (هم‌بستگی) و متغیرهای پنهان (تحلیل عاملی) به‌طور خلاصه نشان می‌دهند و بدین ترتیب تصویرسازی یا نگاشت معنایی امکان‌پذیرتر می‌شود.

ازآنجاکه سوابق پژوهشی در مورد شبکه‌های مفهومی و مدل‌های معنایی امنیت اطلاعات در داخل کشور یافت نشد در این تحقیق تلاش شده است تا با توجه به اهمیت موضوع این خلأ پژوهشی پر شود.

روش‌شناسی پژوهش

این پژوهش از نظر هدف کاربردی است. از نظر روش آمیخته‌ای از روش‌های هم‌رخدادی واژگان، مطالعات کتابخانه‌ای و تکنیک دلفی است که در سه مرحله انجام شده است، در مرحله نخسن با هدف کشف ساختار شبکه مفهومی این حوزه از روش هم‌رخدادی واژگان به‌عنوان یکی از روش‌های علم‌سنجی استفاده شده است. در این مرحله کلیه تولیدات علمی پژوهشگران در حوزه «امنیت اطلاعات» در عرصه بین‌المللی و از پایگاه‌های استنادی اسکوپوس و وبگاه علوم طی سال‌های ۲۰۱۳ الی ۲۰۱۷ استخراج و به نرم‌افزار اندنوت[1] منتقل شدند. پس از پالایش متون، ۷۵٤۷ مدرک علمی جهت بررسی **فیلد** کلیدواژه‌ها و ابربرچسب‌ها به نرم‌افزار زوترو[2] منتقل و عملیات پیش‌پردازش روی ۱۹٦٤۸ کلیدواژه‌ها و ابربرچسب‌ها با استفاده از پنج واژه‌نامه در حوزه امنیت اطلاعات (Slade, 2006; Calder & Steve, 2007; Manoilov & Radichkova, 2007; Kissel, 2011; Gattiker, 2004) و سه واژه‌نامه در حوزه علوم کامپیوتر(Henderson, 2009; IBM, 2010; Rigdon, 2016) به‌صورت کاملاً هدفمند انجام شد. در انتها با احتساب حداقل هم‌رخدادی ۵ برای هر واژه در نرم‌افزار «وی.اُ.اس.ویور» نسخه ۱.٦.۱۰، ۲۰۷واژه مرجّح و مستند بر اساس آخرین نسخه از واژه‌نامه امنیت اطلاعات (Kissel, 2011) انتخاب[3] و شبکه مفهومی آن ترسیم شد. به کمک نرم‌افزار «گِفی» نسخه ۰.۹.۲، شاخص‌های مرکزیت بینابینی، چگالی، ضریب خوشه‌بندی بررسی شدند.[4] لذا در این مرحله از نرم‌افزارهای اندنوت، زوترو، وی.اُ.اس.ویور، گفی و اکسل استفاده شده است.

در مرحله دوم برای ارائه مدل معنایی قابل درک برای ماشین، مطالعات کتابخانه‌ای انجام و مشخص شد که مدل‌های مفهومی داده‌ای چون مدل‌های موجودیت رابطه پیشرفته، چارچوب توصیف منبع که در توسعه هستان‌نگاری ها استفاده می‌شوند، ابزارهای قوی سازمان‌دهی اطلاعات هستند که تفکر ماشینی را امکان‌پذیر می‌کنند[5] (Deconta et al., 2003; Obrest, 2006; McGuinness, 2017). این مدل‌ها پایه و اساس ارائه گزاره‌های منطقی قرار می‌گیرند که از زبان‌های OWL ، UML، DAML+OIL در منطق توصیفی مرتبه اول و مودال جهت تعاملات معنایی استفاده می‌کنند. در این مدل‌ها موجودیت، نهاد، کلاس و زیرکلاس، مفاهیم، روابط موجود در هر حوزه دانشی توسط گراف‌های جهت‌دار نشان داده می‌شوند. لذا مدل‌های مختلف هستی‌نگاری امنیت (Ekelhart & Fenz, 2009) هستی‌نگاری امنیت اطلاعات (Herzog et al., 2007) هستی‌نگاری حمله (Razzaq et al., 2014)، هستی‌نگاری آسیب‌پذیری(Brandão, 2006)، هستی‌نگاری[6] (Martimiano & dos Santos Moreira, 2006) و تاکسونومی تهدید (Jouini et al., 2014) و همچنین مدل مفهومی امنیت سیستم‌های اطلاعاتی در کتابخانه‌ها (Ismail &

1 . End Not
2 . Zotero
۳ . برای هرگونه انتخاب محقق نیازمند یک منبع استاندارد و موثق است که در این پژوهش مفاهیم مرجّح از واژه‌نامه امنیت اطلاعات (کیسِل، ۲۰۱۱) انتخاب شدند.
۴ . لازم به توضیح است که برای استفاده خوانندگان داخلی (**بومی‌سازی**) و مستندسازی مفاهیم، لغات بیان‌شده در این پژوهش با *واژه‌نامه و فرهنگ امنیت فضای تولید و تبادل اطلاعات (افتا)* (گروه واژه‌گزینی انجمن رمز ایران، ۱۳۹۴) ترجمه شدند.
۵ . توضیحات بیشتر در متن پایان‌نامه ذکر شده است.
6 . Ontosec

اِسووگِل کتابخانه‌های آنتولوژی به زبان اُ دبلیو ال جهت بررسی، اصلاح و توسعه (Noy et al., 2001) استخراج و تمامی موجودیت‌ها، کلاس‌ها، زیرکلاسها، روابط میان آنها، مفاهیم و نمونه‌های منتسب به هر کلاس و زیرکلاس، با دقت بررسی شدند (جدول ۱ و ۲). سپس۲۰۷ مفهوم شبکه مفهومی (استخراج‌شده در مرحله نخست) با اجزای مشترک این مدل‌ها تطبیق داده شدند و مدل جدیدی ارائه شد. در این مرحله علاوه‌بر پایگاه‌های اطلاعاتی و موتورهای جستجوی فوق‌الذکر از نرم‌افزار اکسل برای تطبیق استفاده شد.

در مرحله سوم، مدل مفهومی جدید با پنج کلاس، شش زیرکلاس و یازده رابطه معنایی توسط تکنیک دلفی فازی، به اجماع خبرگان دو حوزه کامپیوتر و حوزه علم اطلاعات و دانش‌شناسی رسید. با استفاده از پرسشنامه الکترونیکی محقق‌ساخته دلفی، در دو راند از ١٤ نفر خبرگان دو حوزه کامپیوتر و علم اطلاعات و دانش‌شناسی خواسته شد، میزان توافق خود را در مورد کلاس‌ها، زیرکلاس‌ها اعلام بفرمایند و ۹۷ مفهوم مشترک در شبکه مفهومی را با توجه به ماهیت معنایی به یکی از کلاس‌ها و یا زیرکلاس‌ها نسبت دهند. با استفاده از اس پی اس اس ۲۲ و آزمون ناپارامتریک کندال، ضریب توافق کلیه کلاس‌ها و زیرکلاس‌ها و همچنین ۹۷ مفهوم مشترک مورد بررسی قرار گرفتند؛ به دلیل عدم اطمینان در تصمیم‌گیری خبرگان محترم در مورد کلاس‌ها، زیرکلاس‌ها و انتساب مفاهیم به آنها از روش دلفی فازی از نوع فازی مثلثی سو و یانگ استفاده شده است. بر اساس روش دلفی فازی میانگین حسابی کران پایین، وسط و بالا برای هر یک از اعضای مجموعه محاسبه می‌شود. در مرحله بعد میانگین‌های فازی به‌دست‌آمده، به اعداد قطعی تبدیل می‌شوند یعنی فازی‌زدایی[1] انجام می‌شود و ضریب کندال آن محاسبه می‌شود که بین صفر تا یک متغیر است، صفر نشان‌دهنده عدم هم‌رأیی و یک نمایانگر هم‌رأیی کامل است. ضریب کندال ۰.۷ یا بیشتر، توافق رضایت‌بخش و حد آستانه مورد قبول در این پژوهش است. ۵ کلاس، ٦ زیرکلاس و همچنین ۷۱ مفهوم از میان ۹۷ مفهوم مشترک با ضریب توافق، بالای ۰.۷ پذیرفته شدند. درنهایت، برای بررسی درستی روابط حاکم بر کلاس‌ها، زیرکلاس‌ها در مدل مفهومی، از تحلیل عاملی تأییدی و مدل‌سازی ساختاری در دو بعد اندازه‌گیری و ساختاری اسمارت پی ال اس استفاده شد.

جدول ۱. موجودیت‌های (کلاس‌ها و زیرکلاس‌ها) مشترک در مدل‌ها

ردیف	کلاس‌های اصلی	زیرکلاس‌ها	نام مدل هستان‌نگاری/نام تاکسونومی/ نام مدل مفهومی	نام هستان‌نگار
۱	دارایی‌های اطلاعاتی[2]	–	آنتولوژی امنیت	فنز و اکلهارت
			آنتولوژی حمله	رزاق و دیگران
			آنتولوژِی Ontose	مارتیمیانو و موریرا
			آنتولوژی امنیت اطلاعات	هرزوگ، شاه‌مهری و دوما
۲	ویژگی‌های امنیتی[3]	–	آنتولوژی امنیت	فنز و اکلهارت

1 . DFuzzy
2 . Informaiton Asset
3 . Security Atribution

ادامه جدول ۱. موجودیت‌های (کلاس‌ها و زیرکلاس‌ها) مشترک در مدل‌ها

ردیف	کلاس‌های اصلی	زیرکلاس‌ها	نام مدل هستان‌نگاری/نام تاکسونومی/ نام مدل مفهومی	نام هستان‌نگار
۳	تهدیدات[1]	منبع و عامل تهدید[2]	تاکسونومی تهدید	جونیا، بن‌ارفع ربیع و بن‌عایسب
			آنتولوژی امنیت	فنز و اکلهارت
			آنتولوژی حمله	رزاق و دیگران
			آنتولوژِی Ontose	مارتیمیانو و موریرا
		راه‌های نفوذ[3]	آنتولوژی حمله	رزاق و دیگران
			آنتولوژِیOntosec	مارتیمیانو و موریرا
		ابزارهای نفوذ[4]	آنتولوژی حمله	رزاق و دیگران
			آنتولوژِی Ontose	مارتیمیانو و موریرا
		حمله[5]	آنتولوژی حمله	رزاق و دیگران
			آنتولوژِی Ontose	مارتیمیانو و موریرا
			آنتولوژی امنیت اطلاعات	هرزوگ، شاه‌مهری و دوما
٤	آسیب‌پذیری و پیامد[6]	–	آنتولوژی امنیت	فنز و اکلهارت
			آنتولوژی آسیب‌پذیری	برندوا
			آنتولوژِی Ontosec	مارتیمیانو و موریرا
			آنتولوژی حمله	رزاق و دیگران
			آنتولوژی امنیت اطلاعات	هرزوگ، شاه‌مهری و دوما
۵	اقدامات کنترلی[7]	اقدامات فناورانه[8]	مـدل امـنیت سیستم‌های اطلاعاتی در کتابخانه‌ها	اسماعیل و زینب
		اقدامات سازمانی[9] سازمانی[9]		اسماعیل و زینب
			آنتولوژی امنیت	فنز و اکلهارت
			آنتولوژی امنیت اطلاعات	هرزوگ، شاه‌مهری و دوما

1 . Threat
2 . Threat Source
3 . Access Path
4 . Threat Tools
5 . Attack
6 . Vulnerability
7 . Countermeasure
8 . Thechnological countermeasure
9 . Organizational countermeasure

جدول ۲. روابط معنایی مشترک میان موجودیت‌ها (کلاس‌ها و زیرکلاس‌ها)

ردیف	نام کلاس/ زیرکلاس	نام رابطه معنایی	نام کلاس/زیرکلاس
۱	دارایی‌های اطلاعاتی	نیاز دارد به سطحی از[1]	ویژگی‌های امنیتی
۲	ویژگی‌های امنیتی	–	–
۳	تهدیدات	تضعیف می‌کند[2]	ویژگی‌های امنیتی
٤	تهدیدات	تهدید می‌کند[3]	دارایی‌های اطلاعاتی
٥	تهدیدات	منجر می‌شود به[4]	آسیب‌ها و پیامدها
٦	تهدیدات	منبع دارد[5]	منبع و عامل تهدید
۷	تهدیدات	استفاده می‌کند از[6]	ابزار نفوذ
۸	تهدیدات	استفاده می‌کند از	راه نفوذ
۹	تهدیدات	حمله رخ می‌دهد[7]	حمله
۱۰	منبع و عامل	استفاده می‌کند از	ابزار نفوذ
۱۱	منبع و عامل	استفاده می‌کند از	راه نفوذ
۱۲	منبع و عامل	حمله می‌کند[8]	حمله
۱۳	آسیب‌پذیری و پیامد	آسیب می‌زند به[9]	دارایی‌های اطلاعاتی
١٤	اقدامات کنترلی	اعمال می‌شود بر[10]	دارایی‌های اطلاعاتی
۱۵	اقدامات کنترلی	کاهش می‌دهد[11]	آسیب‌پذیری و پیامد
١٦	اقدامات کنترلی	کاهش می‌دهد	تهدیدات
۱۷	اقدامات کنترلی	نوع دارد[12]	اقدامات سازمانی
۱۸	اقدامات کنترلی	نوع دارد	اقدامات فناورانه

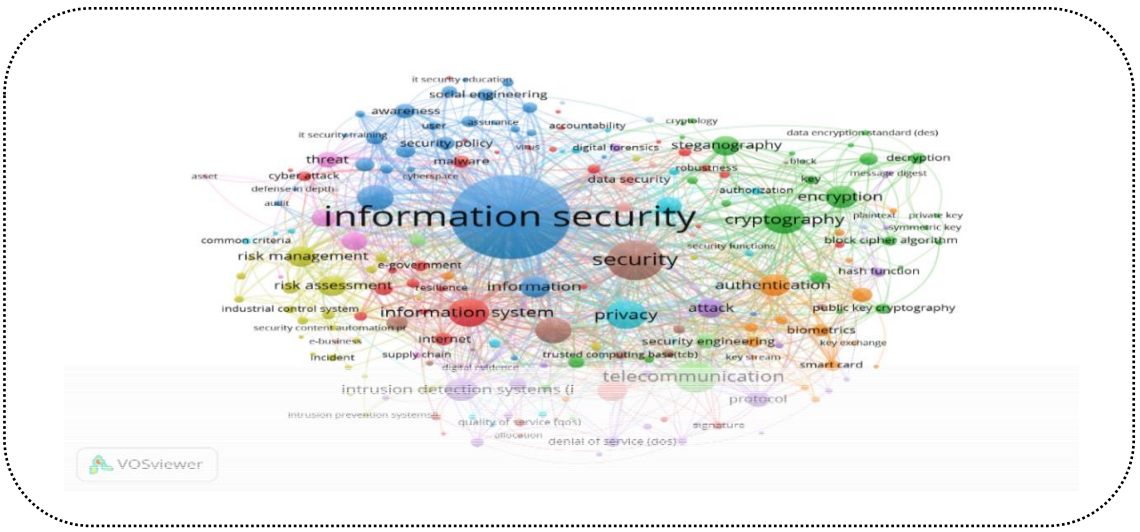
1 . Requires level
2 . Diminish
3 . Threatens
4 . Exploited by
5 . has Source
6 . Uses of
7 . Lead to
8 . Attack
9 . Vulnerability on
10 . Implemented by
11 . Reduce
12 . has Type

یافته‌های پژوهش

پاسخ به پرسش نخست پژوهش. شبکه مفهومی حوزه امنیت اطلاعات بر اساس پایگاه‌های اسکوپوس و وبگاه علوم در بیـن سال‌های ۲۰۱۳ تا ۲۰۱۷چگونه است؟

در مرحله نخست، پس از پیش‌پردازش کلیدواژه‌ها و ابربرچسب‌ها در «زوتـرو» بـا تهیـه خروجـی «آر.آی.اس»[1] و انتقال آن به نرم‌افزار «وی.اُ.اس.ویور»، نقشه هم‌رخدادی، مطـابق شـکل ۱ ترسـیم شـد. بزرگـی و کـوچکی دایـره‌هـا نشان‌دهنده میزان دانش موجود در مورد هر مفهوم است. همان‌طور که در شکل نشان داده شـده، متـون مـورد مطالعـه به‌ترتیب بـر روی موضوعـات «امـنیت اطلاعـات»، «امـنیت»، «حریـم خـصوصـی»، «سیستـم‌هـای اطلاعـاتی»، «رمـزگذاری»، «رمزگشایی» متمرکزند و کم‌تکرارتـرین‌هـا «قـوانین مالکیـت معنـوی»، «مرجـع صـدور گـواهی‌نامـه و نرم‌افزار»، «طیف گسترده» هستند که به معنی فقر مقالات علمی در این حوزه است.

بر اساس شاخص مرکزیت بینابینی، مفـاهیمی چون «امنیت اطلاعات»، «امنیت»، «سیسـتم‌هـای اطلاعـاتی»، «حـریم خصوصی»، «ارتباطات از راه دور»، «اطلاعات»، «سیستم‌های تشخیص نفوذ»، «رمـزنگـاری»، «احـراز هویـت»، «امنیـت سایبری»، «شبکه»، «ریسک»، «مدیریت ریسک و چارچوب های آن» و «تهدید»، از لحاظ مکـانی در مرکـز شـبکه قـرار گرفته‌اند، یعنی مرکزیت بالاتری هستند و مفاهیـمی چون «حـمله تشعشعات مخاطره‌آمیز»، «تحلیـل ترافیـک شبکـه»، «امنیت لایه نقل و انتـقال»، «قابـلیت اعتـماد»، «دسترسـی غیرمجاز»، «اعـتبارسنجی»، «ماشـین مجـازی»، «شـبکه‌هـای مجازی خصوصی»، «ارزیابی آسیب‌پذیری»، «کرم‌ها» که در پیرامون شبـکه هـستند، از مرکزیـت کمتـر و در نتیجـه از میزان رؤیت‌پذیری کمتری برخوردارند.



شکل ۱. نقشه هم‌رخدادی واژگان حوزه امنیت اطلاعات بر اساس سنجه مرکزیت رتبه

شبکه هم‌رخدادی مفاهیم حوزه امنیت اطلاعات از ۲۰۷ گره و ۲۷۹۶ پیوند تشکیل شده است، ازآنجاکه تعـداد پیونـدها نسبت به گره‌ها بیشتر است، بنابراین شبکه پیوسته است. متوسط ضریب خوشه‌بندی ۰.۳۰۱ است که می‌توان گفـت حـدوداً ۳ مفهوم در اطراف هر گره وجود دارد. شکل ۲ نمای کلی از چگالی شبکه را نشانی می‌دهد که اندازه آن **۰.٤٥٣** است.[2]

1 . RIS (Research Information Systems)

۲ . متوسط ضریب خوشه‌بندی و میزان چگالی شبکه توسط نرم‌افزار گفی محاسبه شده است.

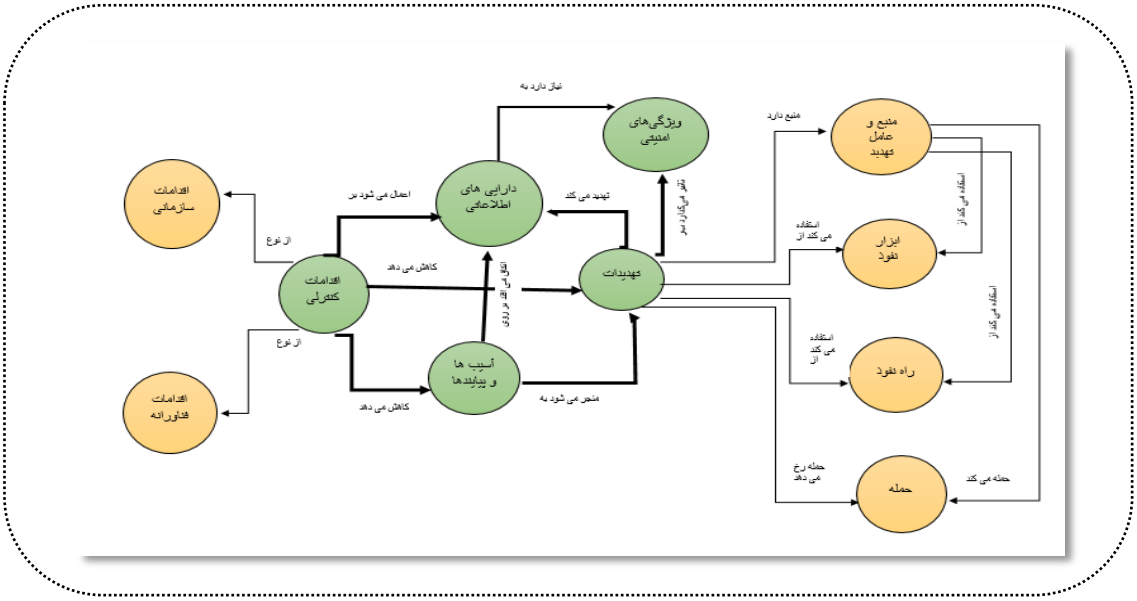
شکل ۲. چگالی شبکه مفهومی امنیت اطلاعات بر اساس نرم‌افزار VOS viewer

پاسخ به پرسش دوم پژوهش. مدل معنایی حوزه «امنیت اطلاعات» بر اساس مدل‌های گذشته و شبکه مفهومی چگونه است؟

در مرحله دوم پژوهش حاضر، با توجه به مطالعات کتابخانه‌ای (جداول ۱ و ۲)، مدل مفهومی جدیدی ارائه شد که دارای ۵ کلاس اصلی«دارایی‌های اطلاعاتی»، «ویژگی‌های امنیتی»، «تهدیدات»، «آسیب‌پذیری‌ها و پیامدها» و «اقدامات کنترلی» است؛ کلاس تهدیدات دارای ٤ زیرکلاس «منبع و عامل تهدید»، «ابزار نفوذ»، «مسیر نفوذ» و «حمله» و کلاس اقدامات کنترلی دارای ۲ زیرکلاس «اقدامات فناورانه»و «اقدامات سازمانی» است (شکل ۳) و ۱۱ رابطه معنایی دارد که به‌صورت فرضیه در این مدل در نظر گرفته شده است (جدول ۳).

جدول ۳. روابط معنایی حاکم بر مدل معنایی امنیت اطلاعات

ردیف	فرضیه
۱	اقدامات کنترلی بر دارایی‌های اطلاعاتی تأثیر معنادار مثبت دارند.
۲	اقدامات کنترلی بر تهدیدات تأثیر معنادار منفی دارند.
۳	آسیب‌ها و پیامدها بر دارایی‌های اطلاعاتی تأثیر معنادار منفی دارند.
٤	آسیب‌ها و پیامدها بر اقدامات کنترلی تأثیر معنادار منفی دارند.
۵	تهدیدات بر دارایی‌های اطلاعاتی تأثیر معنادار منفی دارند.
٦	تهدیدات بر ویژگی‌های امنیتی تأثیر معنادار منفی دارند.
۷	تهدیدات بر آسیب‌ها و پیامدها تأثیر معنادار مثبت دارند.
۸	دارایی‌های اطلاعاتی بر ویژگی‌های امنیتی تأثیر معنادار مثبت دارند.
۹	منبع و عامل تهدیدات بر ابزار نفوذ تأثیر معنادار مثبت دارند.
۱۰	منبع و عامل تهدیدات بر راه نفوذ تأثیر معنادار مثبت دارند.
۱۱	منبع و عامل تهدیدات بر حمله تأثیر معنادار مثبت دارند.



شکل ۳. مدل مفهومی امنیت اطلاعات بر اساس توسعه و اصلاح مدل‌های قبلی و شبکه مفهومی

پاسخ به پرسش سوم پژوهش. میزان توافق خبرگان دو حوزه کامپیوتر و علم اطلاعات و دانش‌شناسی با مدل معنایی چقدراست؟

برای بررسی میزان توافق خبرگان با مدل معنایی، بر اساس روش تحقیق ارائه‌شده در مرحله سوم، ضریب کندال ۹ موجودیت (کلاس و زیرکلاس) به همراه نمره کندال ۷۱ مفهوم مورد پذیرش محاسبه شده است.

در بررسی درستی روابط میان موجودیت‌ها و مفاهیم، در مدل‌سازی مبتنی بر معادلات ساختاری باید به برازش مناسب در هر دو نوع مدل اندازه‌گیری و ساختاری توجه کرد. مدل اندازه‌گیری، قسمت‌هایی از مدل کلی (شکل ۳) است که ارتباط بین مفاهیم و موجودیت‌ها (کلاس‌ها و زیرکلاس‌ها) را نشان می‌دهند. در بررسی برازش مدل اندازه‌گیری، محاسبه بارهای عاملی و اعداد معنادار T ضروری است. با توجه به اینکه ضرایب بارعاملی برای ۷۱ مفهوم بیش از ۰.٤ و اعداد معنادار T نیز بیش از ۱.۹٦ است می‌توان ادعا کرد واریانس بین موجودیت‌ها و مفاهیم توصیف‌کننده آن از واریانس خطای اندازه‌گیری آن سازه بیشتر و در نتیجه پایایی مدل اندازه‌گیری قابل قبول است. مقادیر ضریب توافق کندال، بار عاملی و اعداد معنادار T برای هر یک از موجودیت‌های مدل و نیز کلیه مفاهیم منتسب به آنها در جدول ٤ آمده است.

جدول ٤. مقادیر ضریب توافق کندال، بارهای عاملی و آماره T برای موجودیت‌های مدل و مفاهیم وابسته به آنها

کلاس/زیرکلاس	ضریب توافق کندال (W)	بار عاملی	مفاهیم منتسب	نمره کندال	بار عاملی	آماره T
دارایی‌های اطلاعاتی	۰.۹۱	۰.۹۱٦	شبکه‌های موقت	۰.۷۵۰	۰.۸٦٦	٦.۱۱۸
			نرم‌افزار کاربردی	۰.۷۹	۰.۸۰۷	٤.٤۲۹
			زیست‌سنجی	۰.۸۸	۰.۷۳٦	۷.۳۵۹
			فضای سایبری	۰.۹	۰.٦٦۲	۱۰.۰٤٤
			داده	۰.۷۷	۰.۸۹۷	۵.٦۲۳

ادامه جدول ٤. مقادیر ضریب توافق کندال، بارهای عاملی و آماره T برای موجودیت‌های مدل و مفاهیم وابسته به آنها

کلاس/زیرکلاس	ضریب توافق کندال (W)	بار عاملی	مفاهیم منتسب	نمره کندال	بار عاملی	آماره T
دارایی‌های اطلاعاتی	۰.۹۱	۰.۹۱٦	دامنه	۰.۷٤	۰.۹۵۲	٦.۱۳۲
			اطلاعات	۰.۷٦	۰.۹۱٦	۷.۹۳۵
			مالکیت معنوی	۰.۷٦	۰.۸٤۸	۷.۰۱۵
			اینترنت	۰.۷	۰.۹۰۸	۸.۳۱۹
			تکنولوژی‌های اطلاعاتی	۰.۷۸	۰.٤٤۸	۵.۱٤۲
			شبکه	۰.۷	۰.۸۸۹	۵.۳۵۵
			سیستم عامل	۰.۷٤	۰.٤٦۲	۷.۰٦۳
			کلمه رمز	۰.۸	۰.۹۱۷	۵.٦۸۲
			حریم خصوصی	۰.۷۲	۰.۹٤۲	٦.۷٤۰
			رکورد	۰.۷۳	۰.۹۰۵	۹.۷۷۸
			کارت هوشمند	۰.۷۹	۰.۵۹۷	٦.٤۸۱
			نرم‌افزار	۰.۷۹	۰.۹۳٤	۲.٤۲۹
			کاربر	۰.۷۵	۰.۸٦۸	٤.۹۲۷
			شبکه‌های خصوصی مجازی	۰.۸	۰.۸۷۷	۵.٦۱۵
ویژگی‌های امنیتی	۰.۹٤	۰.۸۰۸	احراز هویت	۰.۷۳	۰.٤٦٤	۳.۱۱٦
			دسترس‌پذیری	۰.۷۷	۰.۹۱۹	٤.٦٦٤
			یکپارچگی	۰.۷۱	۰٦۸۷	۳.٤۹۲
منبع و عامل تهدید	۰.۸۹	۰.۹٦۳	هکر	۰.۷	۰.۸۱٤	۲.۷۵۰
			کد مخرب	۰.۷٦	۰.۹۱٦	٤.۲٦۱
			بدافزار	۰.۸٦	۰.۷۸۲	٦.۸۵۷
			هرزنامه	۰.۸	۰.۵۱۹	۸.۳۷۷
			اسب تروجان	۰.۷۷	۰.٦۱٦	۷.۸٤۵
			ویروس	۰.۸	۰.۹۱۸	۱۳.٤٦۳
			کرم	۰.۸۱	۰.۹۵۳	٦.۰۰۷
ابزار تهدید	۰.۸۵	۰.۷٦۹	پروتکل اینترنت	۰.۷۸	۰.۹۰٦	۳.٦٦۰
راه نفوذ	۰.۸٦	۰.۸۱۰	در مخفی	۰.۷	۰.۸۲٦	٦.۸۸۲
حمله	۰.۸۸	۰.٦٦۷	حمله شبکه‌های کامپیوتری	۰.۷۹	۰.۸۹۳	٤.٦۵۹
			حمله سایبری	۰.۷	۰.۹۰۳	٦.۰۱۰
			انکار خدمات توزیع‌شده	۰.۷۹	۰.۹۱۸	۵.۵٦۲
			خودداری از سرویس	۰.۷٤	۰.٦۹۲	۵.۷۹٦
			حمله مرد میانی	۰.۷۷	۰.۵۰۱	۵.۷۹۱

ادامه جدول ٤. مقادیر ضریب توافق کندال، بارهای عاملی و آماره T برای موجودیت‌های مدل و مفاهیم وابسته به آنها

کلاس/زیرکلاس	ضریب توافق کندال (W)	بار عاملی	مفاهیم منتسب	نمره کندال	بار عاملی	آماره T
حمله	۰.۸۸	۰.٦٦٧	حمله شکستن کلمه رمز	۰.۸۳	۰.۷۸۰	۵.۳٦۰
			حمله فیشینگ	۰.۸٤	۰.۷۷۷	۳.۵٦۵
			مهندسی اجتماعی	۰.۷۷	۰.٦۸٤	۲.۱۷۳
			حمله اسپوفینگ	۰.۷٦	۰.۷۵۰	۳.۵۸۹
			حمله جاسوسی با تشعشعات مخاطره‌آمیز	۰.۷٤	۰.۸۹۰	۳.۸۷۱
آسیب‌ها و پیامدها	۰.۸۹	۰.۵٤۰	ارزیابی آسیب‌پذیری	۰.۷۵	۰.۸٦۰	۲.۲۳۰
اقدامات کنترلی سازمانی	۰.۹۳	۰.٤٦۲	آموزش	۰.۷	۰.٦۹۹	۲.۹۰۹
			تحلیل ریسک	۰.۷۹	۰.۷۹۳	۳.۵۰۹
			مدیریت ریسک	۰.۸۲	۰.۹۸٦	۳.۱۹۸
اقدامات کنترلی فناورانه	۰.۹۱	۰.۹۸۱	کنترل دسترسی	۰.۸۵	۰.۷۸۰	۳.۳۵۱
			استاندارد رمزنگاری پیشرفته	۰.۸۱	۰.۷۰۳	۲.۷۰۷
			نرم‌افزار آنتی‌ویروس	۰.۸۷	۰.۸٦۰	٤.۳٦۲
			تهیه پشتیبان	۰.۷٦	۰.۵۹۹	٤.۷٦۱
			الگوریتم رمزنگاری قالبی	۰.۸۳	۰.٦۰۵	۵.۷٤۹
			رمزنگاری	۰.۷۱	۰.۷۸۳	۸.۱۵۳
			رمزگشایی	۰.۷٤	۰.۸۰۵	۳.۸۱۹
			دفاع در عمق	۰.۷	۰.۸۱۲	۵.۷۱۳
			امضای دیجیتال	۰.۷۱	۰.۷۰۵	۱۰.۰۵۰
			رمزگذاری	۰.۷۷	۰.٦٦۳	۱۱.۱٦۵
			فایروال	۰.۸۲	۰.۷۰٦	۱۱.۳۱۰
			تابع هش	۰.۷۸	۰.۷۱۲	۱۱.۷۲۳
			هانی پات	۰.۷۹	۰.۷٦۳	۱۲.۹٦۸
			سیستم‌های تشخیص نفوذ	۰.۷۵	۰.۷۹۵	۵.۸۵۱
			سیستم‌های پیشگیری از نفوذ	۰.۸۱	۰.۷٦۰	٦.۲۲٦
			تبادل کلید	۰.۸	۰.۷۵۹	٦.۱۱٦
			کد تأیید پیام	۰.۷٤	۰.٦۸۸	۱۱.۲۸۳
			خلاصه پیام	۰.۷۲	۰.۷۰۲	۸.۰٦۹
			تست نفوذ	۰.۷٤	۰.٦۵۵	۹.۲۹۵
			پروتکل	۰.۷۹	۰.۸۰٤	٦.۰۱۰
			کلید عمومی	۰.۷۳	۰.۸۱۳	۵.۵٦۲

ادامه جدول ٤. مقادیر ضریب توافق کندال، بارهای عاملی و آماره T برای موجودیت‌های مدل و مفاهیم وابسته به آنها

کلاس/زیرکلاس	ضریب توافق کندال (W)	بار عاملی	مفاهیم منتسب	نمره کندال	بار عاملی	آماره T
اقدامات کنترلی فناورانه	۰.۹۱	۰.۹۸۱	کنترل دسترسی نقش‌محور	۰.۸٦	۰.۸۲۹	۹.۵۷۱
			زبان علامت‌گذاری امنیتی (سامل)	۰.۷۷	۰.۸٦۵	٤.۷۷۷
			الگوریتم هش ایمن	۰.۷۹	۰.۷٤٦	۵.٤٤۵
			لایه سوکت امن	۰.۷۲	۰.۷۳۳	٦.۹۷۸
			پنهان نگاری	۰.۷۵	۰.۷۵۵	۷.۱۵۹
			الگوریتم رمزنگاری مشترک	۰.۷۳	۰.۸٦٦	٦.۷٤۰
			کلید مشترک	۰.۸٤	۰.۸۰۷	۸.۸۷۵

در گام بعدی ضریب آلفای کرونباخ، پایایی و روایی هم‌گرا (با شاخص میانگین واریانس استخراج‌شده) به‌عنوان معیارهای دیگری برای سنجش برازش مدل اندازه‌گیری محاسبه شدند. حد بحرانی برای پذیرش آلفای کرونباخ، پایایی ترکیبی و روایی هم‌گرا به‌ترتیب ۰.۷، ۰.۷و ۰.۵ گزارش شده است (داوری و رضازاده ،۱۳۹۵)، بر همین اساس همان‌طور که از جدول ۵ مشخص است این مقادیر برای همه سازه‌های مدل بالاتر از حد بحرانی قرار دارند.

جدول ۵. مقادیر مربوط به پایایی ترکیبی، آلفای کرونباخ، روایی هم‌گرا، Q^2 و R^2 در موجودیت‌های مدل

موجودیت‌های مدل	پایایی ترکیبی	آلفای کرونباخ	AVE	Q^2	R^2
دارایی‌های اطلاعاتی	۰.۹۷۵	۰.۹۷۱	۰.٦۸۳	۰.٤۰٤	۰.۹۱٦
ویژگی‌های امنیتی	۰.۸۰۳	۰.۷۸۹	۰.۵۲۷	۰.٤۰۹	۰.۸۰۸
تهدیدات (منبع و عامل)	۰.۸۸۸	۰.۷۲۷	۰.٦٦۷	۰.۳٦٤	۰.۹٦۲
تهدیدات (ابزار تهدید)			۰.٦۸۲	۰.۲۹٦	۰.۷٦۹
تهدیدات (راه نفوذ)			۰.۷۹۷	۰.۲۲۵	۰.۸۰۹
تهدیدات (حمله)			۰.٦۰۲	۰.۳۰۷	۰.٦٦۷
آسیب‌ها و پیامدها			۰.۷۳۹	۰.٤۱٤	۰.۵٤۰
اقدامات کنترلی سازمانی	۰.۸٤۲	۰.۷٦۵	۰.۷۳۹	۰.٤۱٤	۰.۵٤۰
اقدامات کنترلی فناورانه	۰.۸۳۲	۰.۸۱۰	۰.٦۹٦	۰.۲۲۳	۰.٤٦۲

معیار نهایی برای بررسی برازش مدل اندازه‌گیری، بررسی روایی و واگرایی است که در این پژوهش با هر دو روش بارهای عاملی متقابل و معیار فورنل ولارکر تأیید شد. پس از بررسی برازش مدل اندازه‌گیری پژوهش و اطمینان از توصیف درست موجودیت‌های مدل توسط مفاهیم، معیارهای مربوط به برازش مدل ساختاری یعنی چگونگی ارتباط میان کلاس‌ها و زیرکلاس‌ها مورد بررسی قرار گرفت. اولین و اساسی‌ترین معیار برای بررسی برازش مدل ساختاری، سنجش اعداد معنادار T است. برای معناداربودن ارتباط بین دو متغیر در سطح اطمینان ۰.۹۵ باید قدر مطلق عدد معناداری T بزرگ‌تر از ۱.۹٦ باشد. همان‌طور که جدول ٦ نشان می‌دهد تمامی اعداد معناداری T بین موجودیت‌های این مدل بزرگ‌تر از ۱.۹٦ است که نشان از معناداربودن روابط این پژوهش است. همچنین این جدول، مقدار ضریب تأثیر و نتایج فرضیه‌ها را نیز بیان می‌کند.

جدول ٦. مقادیر ضریب تأثیر و T-Value برای هر یک از روابط میان موجودیت‌ها در مدل معنایی

روابط بین موجودیت‌های مدل معنایی	ضریب تأثیر	T-Value	نتیجه رابطه
تأثیر اقدامات کنترلی بر دارایی‌های اطلاعاتی	۰.۲۵۹	۲.۷٦۰	تأیید رابطه
تأثیر اقدامات کنترلی بر تهدیدات	-۰.۲٤۰	۳.۱۱٤	تأیید رابطه
تأثیر آسیب‌ها و پیامدها بر دارایی‌های اطلاعاتی	-۰.۳۰۱	۲.۰۲٦	تأیید رابطه
تأثیر اقدامات کنترلی بر آسیب‌ها و پیامدها	-۰.۳۸۱	۲.۳۲۰	تأیید رابطه
تأثیر تهدیدات بر دارایی‌های اطلاعاتی	-۰.۹۷۰	۱٦.۲۸٦	تأیید رابطه
تأثیر تهدیدات بر ویژگی‌های امنیتی	-۰.۲۳۸	٤.٤۱٤	تأیید رابطه
تأثیر تهدیدات بر آسیب‌ها و پیامدها	۰.۲۳٤	۳.۲۸۹	تأیید رابطه
تأثیر دارایی‌های اطلاعاتی بر ویژگی‌های امنیتی	۰.۹۳۵	۵.٦۹۰	تأیید رابطه
تأثیر عامل منبع و عامل تهدیدات بر عامل ابزار نفوذ تهدیدات	۰.۵۱٤	۲.۲٤٤	تأیید رابطه
تأثیر عامل منبع و عامل تهدیدات بر عامل راه نفوذ تهدیدات	۰.۵۳٦	۲.۲۲۳	تأیید رابطه
تأثیر عامل منبع و عامل تهدیدات بر عامل حمله تهدیدات	۰.۹۲۲	۳.٤۷۵	تأیید رابطه

یکی دیگر از معیارهای برازش مدل ساختاری بررسی مقادیر R^2 برای متغیرهای وابسته مدل است. این معیار در پژوهش‌ها نشان از تأثیری دارد که یک متغیر مستقل بر یک متغیر وابسته می‌گذارد. با توجه به مقادیر ۰.۱۹، ۰.۳۳ و ۰.٦۷ به‌عنوان ملاک برای مقادیر ضعیف، متوسط و قوی (داوری، رضازاده، ۱۳۹۵) می‌توان گفت تمامی متغیرهای وابسته در مدل از سطح R^2 قابل قبولی برخوردارند و در مورد ۵ موجودیت «دارایی‌های اطلاعاتی»، «ویژگی‌های امنیتی»، «منبع و عامل تهدید»، «ابزار تهدید» و «راه نفوذ» با توجه به اینکه از مقدار ۰.٦۵ بیشتر هستند، از وابستگی بیشتری برخوردارند. علاوه‌براین معیار Q^2 شاخصی برای قدرت پیش‌بینی مدل است. توجه به مقادیر مربوط به معیار Q^2 مطابق جدول ۵ و با توجه به اندازه مقادیر بحرانی سه مقدار ۰.۰۲، ۰.۱۵ و ۰.۳۵ به‌ترتیب نشان از قدرت پیش‌بینی کم، متوسط و زیاد متغیرهای مستقل مدل گزارش شده‌اند (Henseleret al., 2009)؛ می‌توان گفت دارایی‌های اطلاعاتی، ویژگی‌های امنیتی، منبع و عامل تهدید، آسیب‌ها و پیامدها، اقدامات کنترلی سازمانی، قدرت پیش‌بینی زیادتری دارند[1].

درنهایت برای سنجش برازش کلی مدل، از معیار GOF استفاده می‌شود (Tenenhaus et al., 2004). با جایگذاری دو پارامتر $\overline{Communalities}$ (میانگین مقادیر اشتراکی کلیه موجودیت‌ها) و $\overline{R^2}$ (میانگین مقادیر R^2 مربوط به تمامی موجودیت‌ها) در فرمول زیر معیار GOF برای مدل کلی این پژوهش به شرح زیر محاسبه می‌شود:

$$GOF=\sqrt{\overline{R^2}} \times \sqrt{\overline{\text{communalities}}} = \sqrt{0.768} = 0.710 = \sqrt{0.658}$$

۱. ازآنجاکه مدل معنایی حوزه امنیت اطلاعات فرایندمحور است و برخی موجودیت‌ها در روابط موجود در این چرخه گاهی نقش متغیر مستقل و گاهی نقش متغیر وابسته را دارند، به همین دلیل برخی از موجودیت‌ها در Q^2 و R^2 تکراری هستند.

با توجه به اینکه مقادیر ۰.۰۲ ، ۰.۱۵و ۰.۳۶ را به‌ترتیب به‌عنوان مقادیر ضعیف، متوسط و قوی برای GOF معرفی شده‌اند (Wetzels et al., 2009) به‌دست‌آوردن مقدار ۰.۷۱۰ برای معیار GOF بیانگر برازش قوی مدل کلی این پژوهش است.

بحث و نتیجه‌گیری

بر اساس تحلیل یافته‌های حاصل از پژوهش اهم نتایج عبارت‌اند از:

مهم‌ترین مفاهیم حوزه امنیت اطلاعات شامل«امنیت اطلاعاتم، «امنیت»، «سیستم‌های اطلاعاتی»، «حریم خصوصی»، «ارتباطات از راه دور»، «اطلاعات»، «سیستم‌های تشخیص نفوذ»، «رمزنگاری»، «احراز هویت»، «امنیت سایبری»، «شبکه»، «ریسک»، «مدیریت ریسک و چارچوب‌های آن» و «تهدید» هستند که در پژوهش‌های ونگ (Wang, 2013)، اولیجنیک (Olijnyk, 2015) و انور (Anwar et al., 2018) نیز برخی از آنها یافت شده است و در این پژوهش با استخراج سایر مفاهیم همچون حریم خصوصی، سیستم‌های اطلاعات، قوانین مالکیت معنوی، سیستم‌های تشخیص نفوذ، احراز هویت، تهدید و امنیت سایبری پژوهش‌های گذشتگان را تکمیل کرده است.

همان‌گونه که اِلماسری و نواثه (Elmasri & Navathe, 2015) و دوینیکوف و همکاران (Doynikova et al., 2020) در پژوهش‌های خود مدل‌های معنایی بر اساس معیارهای سلسله‌مراتبی ویژگی‌های داده ارائه دادند، در این پژوهش نیز مدل معنایی سطح بالایی که حاصل بررسی هفت مدل معنایی حوزه امنیت اطلاعات بوده است، برای استفاده در سیستم‌های سنجش معنا ارائه شده که دارای ساختار سلسله‌مراتبی و گراف‌هایی با یال‌های جهت‌دار است و نحوه ارتباط میان موجودیت‌ها اعم از کلاس و زیرکلاس را نشان می‌دهد.

مدل معنایی ساخته‌شده در این پژوهش دارای پنج کلاس اصلی دارایی‌های اطلاعاتی، ویژگی‌های امنیتی، تهدیدات، آسیب‌ها و پیامدها، اقدامات کنترلی و شش زیرکلاس منبع و عامل تهدید، ابزار نفوذ، راه نفوذ و حمله از کلاس اصلی «تهدید» و دو زیرکلاس اقدامات سازمانی و اقدامات فناورانه از کلاس اصلی «اقدامات کنترلی»، ۱۱ رابطه معنایی و ۸۶ مفهوم است. همان‌گونه که یانگ و همکاران (Yang et al., 2012) در پژوهش خود استفاده از فنون کامپیوتری و به‌کارگیری آمار؛ تشابه در الگوها (هم‌بستگی) و متغیرهای پنهان (تحلیل عاملی) را در تصویرسازی یا نگاشت معنایی امکان‌پذیر می‌دانند، در این پژوهش نیز ابتدا با استفاده از تکنیک دلفی، اجزای مدل اعم از کلاس‌ها، زیرکلاس‌ها و مفاهیم منتسب به هر کدام مورد تأیید خبرگان دو حوزه علم اطلاعات و دانش‌شناسی و حوزه کامپیوتر قرار گرفت؛ سپس از طریق معادلات ساختاری، روابط حاکم بر مدل به تأیید ماشین رسید و به این ترتیب مدل حاصل‌شده به‌منظور نگاشت در سیستم‌های مبتنی بر هستی‌شناسی‌ها ارائه شد.

پیشنهادهای اجرایی پژوهش

این پژوهش با توجه به رویکرد متخصصان علم اطلاعات و دانش‌شناسی انجام شده است؛ لذا با توجه به ماهیت موضوع پیشنهاد می‌شود:

- از روش این پژوهش، برای مدل‌سازی و ساخت هستی‌نگاری‌های دامنه در هر حوزه موضوعی استفاده شود تا در جستجوهای معنایی موتورهای جستجو کمتر شاهد ریزش کاذب و بازیابی اطلاعات ناخواسته باشیم؛
- با استفاده از اعمال الگوریتم‌های بازیابی متن روی مدل می‌توان آن را در یکی از سیستم‌های ذخیره و بازیابی اطلاعات حوزه امنیت اطلاعات پیاده‌سازی کرد.

پیشنهاد برای پژوهش‌های آتی

با توجه به بررسی‌های انجام‌شده در این پژوهش، برای مطالعات بعدی موارد زیر پیشنهاد می‌شود:

- هستی‌نگاری حوزهٔ امنیت اطلاعات و اشتراک‌گذاری اطلاعات با استفاده از معیارهای استخراج‌شده نگاشته شود؛
- مدل معنایی امنیت اطلاعات توسط مهندسان کامپیوتر و امنیت اطلاعات و به روش استفاده تمام متن از تولیدات علمی این حوزه به زبان فارسی و انگلیسی و از طریق الگوریتم‌های داده‌های عظیم ارائه شود.

تقدیر و تشکر

این پژوهش برگرفته از رسالهٔ دکتری رشتهٔ علم اطلاعات و دانش‌شناسی بوده که در دانشگاه آزاد علوم و تحقیقات دفاع شده است.

فهرست منابع

احمدی، ح. (۱۳۹٤). ترسیم و تحلیل شبکه مفهومی و هستی‌شناسی ساختار دانش حوزه علم‌سنجی ایران بر اساس رویکرد تحلیل حوزه [رساله دکتری منتشر نشده]. دانشگاه شهید چمران اهواز.

آرین‌پور، م. (۱۳۹۵). میزان رعایت استانداردهای آی ای اس ۲۷۰۰۲ و ۲۷۰۱۹ در حوزه مدیریت امنیت اطلاعات در سازمان اسناد و کتابخانه ملی ایران [پایان‌نامه کارشناسی ارشد منتشر نشده]. دانشگاه الزهرا.

حاجی زین‌العابدینی، م.، و رفعتی، م. (۱۳۹٦). بررسی نظام مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران، *پژوهش‌های نظری و کاربردی در علم اطلاعات و دانش‌شناسی*، ۷ (۱)، ۲۵۷-۲۷۹. https://doi.org/10.22067/RIIS.V7I1.55215

حریری، ن.، و نظری، ز. (۱۳۹۱). امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران، *کتابداری و اطلاع‌رسانی*، ۱٦ (۲)، ٦۱-۹۰. https://lis.aqr-libjournal.ir/article_43010.html

خضری‌پور، ف. (۱۳۹۲). ارائه یک مدل برای بهبود مدیریت امنیت دارایی‌های اطلاعاتی سازمان در سیستم مدیریت امنیت اطلاعات ادارات دولتی شهر کرمان [پایان‌نامه کارشناسی ارشد منتشر نشده]. دانشگاه پیام نور.

داوری، ع.، و رضازاده، آ. (۱۳۹۳). *مدل‌سازی معادلات ساختاری با نرم‌افزار pls*. تهران: جهاد دانشگاهی.

سهیلی، ف.، و عصاره، ف. (۱۳۹۱). مفاهیم مرکزیت و تراکم در شبکه‌های علمی و اجتماعی، *فصلنامه مطالعات ملی کتابداری و سازمان‌دهی اطلاعات*، ۲٤ (۳)، ۹۲-۱۰۸. https://nastinfo.nlai.ir/?_action=article&kw=500&_kw

سیف، ی.، و نادری بنی، ن. (۱۳۹٦). شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره ایران، *مدیریت فناوری اطلاعات*، ۹ (٤)، ۸۵۱-۸۷۰. https://www.sid.ir/paper/140422/fa

شیرواندهی، ش. (۱۳۹۷). *سنجش عملکرد مدیریت امنیت اطلاعات در کتابخانه دیجیتال سازمان اسناد کتابخانه ملی ایران*، [پایان‌نامه کارشناسی ارشد منتشر نشده]. دانشگاه آزاد اسلامی علوم تحقیقات تهران.

فروزنده، ح. (۱۳۹۰). *مدیریت پایگاه داده*. تهران: عابد.

کوکبی، م.، و کوهی رستمی، م. (۱۳۹٤). امنیت اطلاعات سامانه‌های تحت وب نهاد کتابخانه‌های عمومی کشور، *تحقیقات اطلاع‌رسانی و کتابخانه‌های عمومی*، ۲۱ (۸۰)، ۸۹-۱۰۷.
https://doi.org/20.1001.1.26455730.1394.21.1.5.9

مازا، ر. (۱۳۹۳). *مقدمه‌ای بر دیداری‌سازی اطلاعات*. ترجمهٔ فریده عصاره، مازیار نصیری، سپیده قلمباز و حمید احمدی. همدان: نشر سپهر.

Abubakar, F., & Aduku, B. S. (2016). Approaches to security of information resources in academic libraries in Niger State, Nigeria. *Samaru Journal of Information Studies*, *16*(1), 12-24. https://www.ajol.info/index.php/sjis/article/view/174811

Ahmadi, H, (2016). *Mapping and Analysis of Iranian Conceptual Network of the Structure of Scientometrics* [Unpublished doctoral dissertation], Shahid Chamran university of Ahvaz [In Persian].

Alshboul, Y., & Streff, K.(2015). Analyzing Information Security Model for Small-Medium Sized Businesses. Proceeding of Americas Conference on Information Systems (AMCIS) in Information systems security, Assurance and privacy (SIGSEC), June 26, Corpus ID: 41307801.
https://www.researchgate.net/publication/281079574_Analyzing_Information_Security_Model_for_Small-Medium_Sized_Businesses

Amini, M., Vakilimofrad, H., & Saberi, M. K. (2021). Human factors affecting information security in libraries. *The Bottom Line*, *34* (1), 45-67. https:/doi.org/10.1108/BL-04-2020-0029

Anwar, M.A., Rongting, Z., Dong, W., Asmi, F., & Meissner, R. (2018). Mapping the knowledge of national security in 21st century a bibliometric study. *Cogent Social Sciences*, *4*(1). https:/doi.org/10.1080/23311886.2018.1542944

Arianpour, M. (2017). Examining compliance with IES 27002 and 27019 standards in information security management in the National Library and Documents Organization of Iran [Unpublished master dissertation], Alzahra university [In Persian].

Brandão, A. J. S. (2006). *Using Ontologies to Classify Vulnerabilities on Security Systems* [Unpublished master dissertation], ICMC-USP. São Carlos-SP-Brazil.
https://protege.stanford.edu/conference/2005/submissions/posters/poster-martimiano.pdf

Calder, A., & Steve, W. G. (2007). *A Dictionary of Information Security Terms, Abbreviation and Acronyms*, IT Governance publishing, United Kingdom.

Cheng, K. (2005). Surviving hacker attacks proves that every cloud has a silver lining. *computers in libraries*, *25*(3), 52-56.
https://www.researchgate.net/publication/234576575_Surviving_Hacker_Attacks_Proves_That_Every_Cloud_Has_a_Silver_Lining

Da Veiga, A., Martins, N., & Eloff, J. H. (2007). Information security culture-validation of an assessment instrument. *Southern African business Review*, *11*(1), 147-166.
https://www.researchgate.net/publication/235526018_Information_security_culture_-_Validation_of_an_assessment_instrument

Daconta, M.C., Obrst, L.J., & Smith, K.T. (2003). *The Semantic Web: A Guide to the Future of XML, Web Services, and Knowledge Management*, Wiley. Publisher: WileyISBN: 978-0-471-43257-9

Davari, A., & Rezazadeh, A. (2015), *Structural equation modeling with pls software*. Tehran: Jahad Daneshgahi [In Persian].

Dawar, V. (2016). DIGITAL INFORMATION SECURITY FOR ACADEMIC LIBRARIES, *Proceedings of TIFR-BOSLA National Conference on Future Librarianship: Innovation for Excellence*, (April), 22-23, Mumbai, India. https://www.researchgate.net/publication/335389774_DIGITAL_INFORMATION_SECURITY_FOR_ACADEMIC_LIBRARIES

Dictionary of IBM & computing technology (2010). New York: IBM.

Doynikova, E., Fedorchenko, A., & Kotenko, I. (2020). A Semantic Model for Security Evaluation of Information Systems, *Journal of Cyber Security and Mobility*, 9(2). https://doi.org/10.13052/jcsm2245-1439.925

Ekelhart, A., & Fenz, S. (2009, March). Ontology-Based Decision Support for Information Security Risk Management. *Proceedings of 4th International Conference on Systems* (ICONS), 1-6, Gosier, France. https://doi.org/10.1109/ICONS.2009.8.

Elmasri, R., & Navathe, S. B. (2015). *Fundamentals of database systems* (7th ed.). Pearson. https://amirsmvt.github.io/Database/Static_files/Fundamental_of_Database_Systems.pdf

Faruzandeh, H. (2019). *Database management*. Tehran: Abed. [In Persian].

Fox, R. (2006). Digital libraries: the systems analysis perspective, vandals at the gate, *OCLC systems & services*, *22*(4), 249-255. https://doi.org/10.1108/DLP-022016-0006

Gattiker, U. E. (2004). THE INFORMATION SECURITY DICTIONARY Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology, KLUWER ACADEMIC PUBLISHERS, NEW YORK.

Hariri, N., & Nazari, Z. (2012). Information security in Iran's digital libraries, *library and information Science*,*15*(2), No 58. https://lis.aqr-libjournal.ir/article_43010.html [In Persian].

Henderson, H. (2009). *Encyclopedia of computer science and technology*, Facts on File, New York.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In *New challenges to international marketing*, Vol. 20, pp. 277-319). Emerald Group Publishing Limited. https:/doi.org/10.1108/S1474-7979(2009)0000020014

Herzog, A., Shahmehri, N., & Duma, C. (2007) An Ontology of Information Security, *International Journal of Information Security and Privacy. 1*(4), 1-23. https:/doi.org/10.4018/jisp.2007100101

Ismail, R., & Zainab, A. N.(2011). Information systems security in special and public libraries: an assessment of status, *Malaysian Journal of Library & Information Science*, *1*(2), 45-62. https://www.researchgate.net/publication/234813293_Information_systems_security_in_special_and_public_libraries_An_assessment_of_status

Jouini, M., Ben Arfa Rabai, L., & Ben Aissab, A. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496. https://doi.org/10.1016/j.procs.2014.05.452

Khezripour, F (2014). Model for improving the security management of the organization's information assets in the information security management system of Kerman government departments [Unpublished master dissertation], Payame Noor University. [In Persian].

Kissel, R. (Ed.). (2011). *Glossary of key information security terms*. Diane Publishing.

Kokabi, M., & Kohi Rostami, M. (2015). Information security of Web-based systems in Iran Institution of public libraries. *Research on Information Science and Public Libraries,* 21 (1), 89-107. https:/doi.org/ 20.1001.1.26455730.1394.21.1.5.9 [In Persian].

Manoilov, G., & Radichkova, B. (2007). *Elsevier's Dictionary of Information Security*. Elsevier.

Martimiano, L.A.F., & dos Santos Moreira, E. (2006). The evaluation process of a computer security incident ontology. *Proceedings of 2nd Workshop on Ontologies and their applications (WONTO06)*, October 23-27, Brazil: Corpus ID: 6735571. https://www.researchgate.net/publication/221336544_The_Evaluation_Process_of_a_Computer_Security_Incident_Ontology

Mazza, R. (2013). *An introduction to information visualization*. Translated by Osareh, F. et al. Hamedan: Sepehr Publishing. [In Persian].

McGuinness, D. L. (2017). *Ontologies for the Modern Age*, Slide share, Slide 4.

Newby, G. B.(*May* 2000). Information security for libraries, *Proceeding* of *Information Resources Management Association International conference An Charge*, 21-24, Alaska,USA: 558-563. https://www.researchgate.net/publication/221412122_Information_security_for_libraries

Noy, N. F., & McGuinness, D. L. (2001). Ontology Development 101: A Guide to Creating Your First Ontology, *Stanford Knowledge Systems Laboratory Technical Report KSL-01-05and Stanford Medical Informatics Technical Report SMI-2001-0880*. Available from http://protege.stanford.edu/publications/ontology_ development/ontology101-noy-mcguinness.html

Obrest, L. (2006). *The Ontology Spectrum & Semantic Models*, MITRE Pwerpoint, slid 9. https://slideplayer.com/slide/12792399/77/images/1/The+Ontology+Spectrum+%26+Semantic+Models.jpg

Olijnyk, N. (2015). A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015, *Scientometrics*, *105*, 883–904. https://link.springer.com/article/10.1007/s11192-015-1708-1

Parvin, S., Sadoughi, F., Karimi,A., Mohammadi, M., & Aminpour, F.(2019). Information Security from a Scientometric Perspective, *Webology,* 16(1), 196- 209. https://www.webology.org/data-cms/articles/20200515032131pma187.pdf

Razzaq, A., Anvar, Z., Farooq Ahmad, H., Latif, K., & Munir, F.(2014). Ontology for attack detection: An intelligent approach to web application security. *Computers & Security, 45*, 124- 146. https://doi.org/10.1016/j.cose.2014.05.005

Rigdon, J. C. (2016). *Dictionary of computer and internet terms*, Eastern Digital Resources, Cartersville.

Seif, Y. & Nadery Bany, N. (2018). Identifying the effective components on information security management in the information technology of Iranian continental shelf oil company, *Management Information Technology*, 9(4), 851-870. https://doi.org/10.22059/JITM.2017.239211.2127 [In Persian].

Shirvandehi, S. (2017). Measuring the performance of information security management in the digital library of the National Library of Iran [Unpublished master dissertation], Islamic Azad University of Research Sciences, Tehran branch. [In Persian].

Slade, R. (2006). *Dictionary of Information Security*, Syngress, Rockland.

Soheili, F., & Osareh , F. (2014). Concepts of Centrality and Density in Scientific and Social Networks, *Library studies and information organization*, 24(3). https://nastinfo.nlai.ir/?_action=article&kw=500 [In Persian].

Solms , R., & Nikert, J. (2013). From information security to cyber security. *Computer & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Spaccapietra, S., Parent, C., Vangenot, C., & Cullot, N. (2004). On Using Conceptual Modeling for Ontologies. In: Bussler, C., *et al.* Web Information Systems – WISE 2004 Workshops. WISE 2004. Lecture Notes in Computer Science, vol 3307. Springer, Berlin: Heidelberg. https://doi.org/10.1007/978-3-540-30481-43

Tenenhaus, M., Amato, S., & Esposito Vinzi, V. (2004). A global goodness of fit index for PLS Structural equation modeling. *In Proceedings of the XLII SIS Scientific Meeting*, *1*(2), 739-742. https://www.researchgate.net/publication/284462849_A_global_goodness-of-fit_index_for_PLS_structural_equation_modelling

Wang, C. K. (2013). An Invisible Network of Knowledge of Security and Privacy of Health. *International Journal of Engineering and Technology*, *5*(3), 357-360. http://www.ijetch.org/papers/575-ST0024.pdf

Wetzels, M., Odekerken-Schröder, G., & Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS quarterly*, 177-195. https://doi.org/10.2307/20650284

Yang, Y., Wu, M., & Cui, L. (2012). Integration of three visualization methods based on co-word analysis. *Scientometrics*, *90*(2), 659-673. https://doi.org/10.1007/s11192-011-0541-4

Zeinolabedini, M., & Rafati, M. (2018). Survey of Information Security Management System in the Central Library of the Universities in Tehran, *Theoretical and applied researches in information science and epistemology*, 7(1). https://doi.org/10.22067/RIIS.V7I1.55215 [In Persian].

Zhao, L., Zhang, L., & Wang, D. (2018, July). Security Management and Operation Mechanism of Digital Libraries in Military Academies. In *3rd International Conference on Contemporary Education, Social Sciences and Humanities (ICCESSH 2018)*, 019-1022, Atlantis Press. https:/doi.org/ 10.2991/iccessh-18.2018.231