مدیریت فناوری اطلاعات
Journal of Information Technology Management
دانشکدهٔ مدیریت دانشگاه تهران
دورهٔ ۸، شمارهٔ ۱
بهـار ۱۳۹۵
ص. ۱۵۴- ۱۴۱

ارائهٔ مدلی مرجع برای تبیین الزامات امنیتی در حوزهٔ یادگیری الکترونیکی از نگاه ذی‌نفعان مختلف

ابوذر عرب‌سرخی میشابی[۱]، محمد موسی‌خانی[۲]، امیر مانیان[۳]

چکیده: توسعهٔ کاربردهـا و خـدمات یـادگیری الکترونیکـی در بسـتر شـبکه‌هـای ارتبـاطی و اطلاعاتی در کنار ارتقای کمّی و کیفی قلمرو فعالیت و نوع خـدمات و دامنـهٔ ارائـهٔ آنهـا، سـبب گسترش روزافزون تهدیدهایی شـده اسـت کـه کمـابیش همـین شـبکه‌هـا و زیرسـاخت‌هـای مخابراتی، محمل بروز آنها هستند. این موضوع پرداخت درست و کارآمد الزامـات امنیتـی را بـه ضرورتی اجتناب‌ناپذیر نزد تصمیم‌سازان امنیتی این حوزه تبدیل کرده است. بر ایـن اسـاس، در مقالهٔ حاضر تلاش شده است با بهره‌مندی از یافته‌های سایر پژوهش‌ها و تجربـه‌هـای مـؤثر در حوزهٔ امنیت یادگیری الکترونیکی و به‌کمک روش فراترکیب، مدلی مرجع برای تبیـین الزامـات امنیتی در حوزهٔ مطالعه‌شده ارائه شود. ساختاری که جایگـاه تعریـف الزامـات امنیتـی یـادگیری الکترونیکی را مشخص می‌کند و می‌تواند به‌عنوان مرجعی برای تبیین الزامات امنیتی این حـوزه به‌کار گرفته شود.

واژه‌های کلیدی: الزامات امنیتی، ذی‌نفعان، مدل مرجع، یادگیری الکترونیکی.

۱. دکتری مدیریت فناوری اطلاعات، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران
۲. دانشیار گروه مدیریت فناوری اطلاعات، دانشکدهٔ مدیریت دانشگاه تهران، تهران، ایران
۳. دانشیار گروه مدیریت فناوری اطلاعات، دانشکدهٔ مدیریت دانشگاه تهران، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹٤/۰٦/۰۹
تاریخ پذیرش نهایی مقاله: ۱۳۹٤/۰۹/۱۲
نویسندهٔ مسئول مقاله: ابوذر عرب‌سرخی میشابی
E-mail: a.arabsorkhi@gmail.com

مقدمه

رشد و نفوذ فناوری اطلاعات و ارتباطات در متن زیرساخت‌های اجتماعی، اقتصادی، سیاسی و فناورانه، موجب تغییر ماهوی فعالیت‌های واحدهای اجتماعی، کسب‌وکارها و حتی دولت شده که حاصل آن شکل‌گیری نوع جدیدی از جوامع با عنوان «جوامع اطلاعاتی» است (زیمبا و ولسزک، ۲۰۱۲). مشخصهٔ اصلی این جوامع، اهمیت زیاد اطلاعات، دانش و منابع آنها، به‌عنوان دارایی‌های اصلی و نیازمند به حفاظت است (عرب‌سرخی، یادگاری و خراط، ۱۳۸۸).

زیرساخت‌های فراگیر فناوری اطلاعات و ارتباطات در جوامع اطلاعاتی، بستر پایه و تسهیل‌کننده‌ای را برای توسعهٔ انواع فضاهای کاربردی الکترونیکی و عرضهٔ گسترده‌ای از سرویس‌های ارزش افزودهٔ الکترونیکی به اقشار مختلف جامعهٔ کاربران فراهم می‌آورد (یونیس، کاتراستیل و سوار، ۲۰۱۳). با وجود این، ماهیت این زیرساخت‌ها به‌گونه‌ای است که امکان فعالیت و بروز انواع جدید و بسیاری از تهدیدها و حمله‌های امنیتی را در سیستم‌ها، کاربری‌ها یا کاربران سرویس‌های الکترونیکی، ازجمله یادگیری الکترونیکی فراهم می‌کند (دفتا، ۲۰۱۱؛ آدامز و بلاندفورد، ۲۰۰۳؛ کاردناس و سانچز، ۲۰۰۵). از این‌رو، نگرانی‌های امنیتی مسئلهٔ اساسی در کاربری مطمئن این سرویس‌ها محسوب می‌شود (ایبل، ۲۰۰۹؛ حیاتی و شینگ، ۲۰۱۰).

به‌موازات افزایش ارزش خدمات یادگیری الکترونیکی و حجم سرمایه‌گذاری‌ها در این حوزه، موضوع تضمین صحت و استمرار خدمات از یک‌سو و صیانت از محرمانگی داده‌ها به‌خصوص ارزیابی‌های آموزشی از سوی دیگر، به دغدغهٔ اصلی توسعه‌دهندگان فناوری‌ها و عرضه‌کنندگان خدمات یادگیری الکترونیکی مبدل شده است (فرنل، ۱۹۹۹)؛ زیرا کم‌توجهی به مقولهٔ امنیت می‌تواند استفاده از سرویس یا کاربرد یادگیری الکترونیکی را به‌شدت تحت تأثیر قرار دهد (آدامز و بلاندفورد، ۲۰۰۳؛ ایبل، ۲۰۰۹؛ حیاتی و شینگ، ۲۰۱۰). با این تفاسیر هنوز هم به موضوعات امنیتی در حوزهٔ تئوری و عملی توجه کافی نمی‌شود (رامیم و لوی، ۲۰۰۶). این نکته به‌روشنی مبیّن ضرورت فعالیت‌های پژوهشی و توسعه‌ای در حوزهٔ امنیت سرویس یادگیری الکترونیکی است. در این راستا و به‌رغم ارائهٔ مستمر راه‌کارهای متنوع برای امن‌سازی امور توسعهٔ کاربردها، سرویس‌دهی و سرویس‌پذیری در حوزهٔ یادگیری الکترونیکی، فراوانی و شدت خطرها و تهدیدهای امنیتی حول آن دائماً، رو به افزایش است (ایبل، ۲۰۰۸؛ کاردناس و سانچز، ۲۰۰۵؛ هیتچینگس، ۱۹۹۵). برخی دلیل این امر را به بی‌توجهی به عوامل غیرسیستمی، به‌ویژه مسائل انسانی، نسبت می‌دهند (عرب‌سرخی و یادگاری، ۱۳۸۹). اما می‌توان ادعا کرد که نداشتن توجه جامع و کامل به تمام جوانب اثرگذار و اثرپذیر در فرایند توسعه، مدیریت عرضه و دریافت سرویس‌های یادگیری الکترونیکی، زمینه‌ساز رشد و تقویت اغلب خطرها و حمله‌های مرتبط با

این حوزه است (زوو، ۲۰۱۲). از این‌رو برخورداری از مدل مرجعی برای تبیین الزامات امنیتی، به امری اجتناب‌ناپذیر در حوزهٔ یادگیری الکترونیکی تبدیل شده است.

در راستای دستیابی به وضعیت امن در فضای توسعهٔ فناوری‌ها، سرویس‌دهی و سرویس‌پذیری در حوزهٔ یادگیری الکترونیکی، دو نیاز اصلی احساس می‌شود که اولی، مواجههٔ نظام‌مند با تهدیدهای امنیتی و چالش‌های این حوزه است (عرب‌سرخی و یادگاری، ۱۳۸۹؛ حیاتی و شینگ، ۲۰۱۰) و دومی، برخورداری از نگرشی جامع و فراگیر برای شناسایی و پوشش تمام حوزه‌های چالش‌انگیز از لحاظ امنیتی است. این دو نیاز با ارائهٔ مدلی مرجع برای مهندسی الزامات امنیتی (ملادو، بلانکو، سانچز و فرناندزمدینا، ۲۰۱۰) در حوزهٔ یادگیری الکترونیکی پاسخ داده می‌شود که مقالهٔ حاضر در راستای توسعهٔ مدل مرجع برای تبیین الزامات امنیتی از نگاه تمام ذی‌نفعان در حوزهٔ یادگیری الکترونیکی تدوین شده است.

پیشینهٔ پژوهش

نگاهی گذرا به پژوهش‌های اجراشده در حوزهٔ یادگیری الکترونیکی بیان‌کنندهٔ این نکته است که موضوعات مختلفی در حوزهٔ امنیت یادگیری الکترونیکی از لحاظ مفهومی، مدیریتی و فنی مد نظر بوده است. نتایج به‌دست‌آمده از پژوهش‌های مرتبط پیشین در قالب جدول ۱ ارائه شده است.

جدول ۱. خلاصهٔ بررسی پژوهش‌های مرتبط

ملاحظه / موضوع	مؤلف و سال پژوهش	نوع ملاحظات امنیتی	صورت‌بندی/ دسته‌بندی ملاحظات	دیدگاه تبیین ملاحظات
ارائهٔ راه‌کارها و الزامات امنیتی در یادگیری الکترونیکی	عرب‌سرخی، یادگاری و خراط (۱۳۸۸)	الزامات امنیتی استاندارد	مدیریتی، فنی و رویه‌ای	تمرکز بر خدمات
شناسایی و تحلیل چالش‌ها و راه‌کارهای امنیتی در یادگیری الکترونیکی	عرب‌سرخی و یادگاری (۱۳۸۹)	الزامات امنیتی استاندارد	مدیریتی، فنی و رویه‌ای	متولیان عرضهٔ خدمات
به‌سوی کاربردهای یادگیری الکترونیکی امن: یک پلات‌فرم چندعامله	وبر، لیما، کاسا و ریبیرو (۲۰۰۷)	الزامات امنیتی فنی	ندارد	فناوری و کاربرد
یادگیری الکترونیکی و مدیریت امنیت اطلاعات	حیاتی (۲۰۱۰)	ملاحظات امنیتی عمومی	ندارد ولی بر وجود آن تأکید دارد	عرضهٔ خدمات
درک تبعات اخلاقی حملات امنیتی یادگیری الکترونیکی از طرف دانشجویان	رامیم و لوی (۲۰۱۰)	الزامات امنیتی عمومی	ندارد ولی بر وجود آن تأکید دارد	دریافت‌کنندهٔ خدمت

ادامهٔ جدول ۱

ملاحظه / موضوع	مؤلف و سال پژوهش	نوع ملاحظات امنیتی	صورت‌بندی/ دسته‌بندی ملاحظات	دیدگاه تبیین ملاحظات
رهیافت زیرساخت کلید عمومی برای توسعهٔ محیط‌های پیشرفتهٔ امن توزیع‌شده یادگیری الکترونیکی و یادگیری سیال	کامبوراکیس، کونتونی، روسکس و گریتزالیس (۲۰۰۷)	الزامات امنیتی فنی	الزامات مبتنی بر مدل اعتماد	زیرساخت ارائهٔ خدمت
دغدغه‌های حریم خصوصی در حوزهٔ یادگیری الکترونیکی	می و سباستین (۲۰۱۱)	الزامات امنیتی عمومی	الزامات مبتنی بر حریم خصوصی	دریافت‌کنندهٔ خدمت
امنیت اطلاعات در پلات‌فرم‌های یادگیری الکترونیکی	دفتا (۲۰۱۱)	الزامات امنیتی فنی و عمومی	رویه‌ای و فنی	نرم‌افزار ارائهٔ خدمت
یک متدولوژی امنیت مهندسی وب برای سیستم‌های یادگیری الکترونیکی	الجوارنه (۲۰۱۱)	ملاحظات توسعهٔ امن خدمات	الزامات فنی	عرضهٔ خدمات

در بررسی پژوهش‌های مرتبط که عمدتاً شامل پژوهش‌های نظری می‌شوند، چند موضوع رخ می‌نماید. اولین موضوع، نگرش‌های بخشی و فنی و نه کلان به موضوع ایمن‌سازی در حوزهٔ یادگیری الکترونیکی است. موضوع دیگر، درنظرنگرفتن هم‌زمان الزامات امنیتی از دید تمام ذی‌نفعان حوزهٔ یادگیری الکترونیکی است. درنهایت نگرش جامعی نسبت به موضوع مدیریت و مهندسی الزامات امنیتی در حوزهٔ یادگیری الکترونیکی وجود ندارد که در بسیاری از مقاله‌های جدید (زوو، ۲۰۱۲؛ حیاتی و شینگ، ۲۰۱۰) هم به این موضوع اشاره شده است. بر این اساس محقق در پژوهش حاضر، توسعهٔ مدلی مرجع و نظام‌مندی برای الزامات امنیتی حوزهٔ یادگیری الکترونیکی را ملاک عمل قرار داده است.

روش‌شناسی پژوهش

در بخش پیشینهٔ پژوهش، مطالعاتی که به‌طور عمده کیفی بودند و با موضوع این پژوهش کاملاً ارتباط داشتند، بررسی شدند، اما هیچ‌یک از آنها مدل جامعی برای صورت‌بندی ملاحظات امنیتی حوزهٔ یادگیری الکترونیکی ارائه نکردند. بر این اساس، پژوهشگر از روش فراترکیب برای صورت‌بندی بهتر یافته‌های به‌دست‌آمدهٔ قبلی در قالب مدل مرجع استفاده کرده است. فراترکیب که بسیاری به‌اشتباه از آن با عنوان فراارزیابی یا مطالعهٔ سیستماتیک یاد می‌کنند، به فرایند تجمیع نتایج کیفی پژوهش‌های منفرد در سطحی انتزاعی‌تر اشاره دارد که از طریق تفسیر و

ترکیب، شناسایی نتایج، فرضیه‌سازی و بررسی قیاسی الگوها در سطحی بالا، محقق می‌شود (زیمر، ۲۰۰۶). قابلیت‌های این روش در ساماندهی و ارتقای پژوهش‌های کیفی سبب شده است استفاده از آن به‌عنوان روش پرکاربرد علمی، روند روبه‌رشدی داشته باشد. با توجه به این موضوع، پژوهشگر با بهره‌مندی از روش فراترکیب سعی کرد یافته‌های مرتبط با صورت‌بندی ملاحظات امنیتی یادگیری الکترونیکی را در قالب مدلی مرجع، تجمیع، تفسیر، ترکیب و ساماندهی کند.

شایان ذکر است که برای اولین‌بار به‌منظور ساخت مدل مرجع تبیین الزامات امنیتی در حوزهٔ یادگیری الکترونیکی روش فراترکیب به‌کار گرفته می‌شود و تا کنون نمونه‌ای برای آن در حوزهٔ مطالعه‌شده، مشاهده نشده است.

یافته‌های پژوهش

در بخش اول، سؤال پژوهش مطرح می‌شود. در این راستا و برای دستیابی به هدف مد نظر با استفاده از روش فراترکیب، سؤال زیر تدوین شده است.

سؤال پژوهش: مدل مرجعی که بتوان بر مبنای آن الزامات امنیتی حوزهٔ یادگیری الکترونیکی را از نگاه ذی‌نفعان مختلف طرح، تبیین و ساماندهی کرد، چیست و چه ابعادی دارد؟

برای صورت‌بندی مدل مرجع، تبیین و ساماندهی الزامات امنیتی حوزهٔ یادگیری الکترونیکی، مطالعات پیشین در دو محور زیر تحلیل و بررسی شدند:

- پژوهش‌های ناب حوزهٔ امنیت یادگیری الکترونیکی؛
- پژوهش‌های ناب حوزهٔ یادگیری الکترونیکی.

در بررسی پژوهش‌های حوزهٔ امنیت یادگیری، هدف شناسایی ملاحظات امنیتی است که به‌صورت خاص برای صورت‌بندی و ترسیم یادگیری الکترونیکی از آن بهره‌برداری می‌شود. حال آنکه در بررسی پژوهش‌های حوزهٔ یادگیری الکترونیکی، هدف شناسایی ملاحظات کلیدی و عناصر تشکیل‌دهنده‌ای است که به‌صورت مستقیم برای صورت‌بندی سرویس یادگیری الکترونیکی مد نظر قرار می‌گیرد. در انتهای این فعالیت، پژوهشگر به‌دنبال ترسیم مدل مرجعی است که برپایهٔ آن بتواند تمام ملاحظات و موضوعات امنیتی یادگیری الکترونیکی را صورت‌بندی و تبیین کند.

در ادامهٔ پژوهش، بر اساس واژگان کلیدی تعریف‌شده، پژوهشگر از انواع موتورهای جست‌وجو برای فعالیت پژوهشی استفاده کرد. این امکان وجود داشت که در روند استفاده از هر موتور جست‌وجو، یک یا مجموعه‌ای از گروه‌ها و مراجع تخصصی، ارزیابی و تحلیل شده باشند. در کنار موتورهای جست‌وجو، پایگاه‌های علمی تخصصی قرار دارند که مبنای سرشماری بسیاری

از مقاله‌ها و منابع معتبر علمی و دربرگیرندهٔ تعداد زیادی از نشریه‌های علمی تخصصی معتبرند. برای سرشماری مقاله‌های مرتبط با موضوع یادگیری الکترونیکی و امنیت یادگیری الکترونیکی، مجموعهٔ مشخصی از این پایگاه‌های داده و نشریه‌های معتبر فهرست‌شده در آنها، مطالعه شدند.

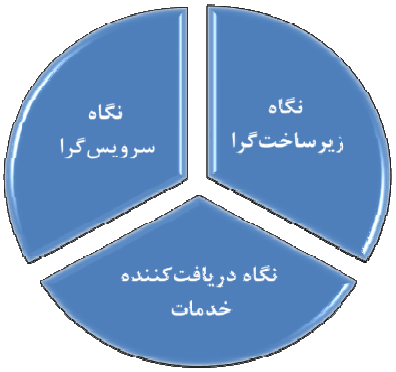
در مرحلهٔ بعد، بررسی و انتخاب مقاله‌های مناسب براساس مجموعه‌ای از شاخص‌ها در دستور کار پژوهشگر قرار گرفت. بر اساس شاخص‌های مد نظر گزینش مقاله، طی روند جست‌وجو مقاله‌های نهایی برای پیشبرد فعالیت فراترکیب انتخاب شدند. در این میان ۴۷ مقاله در زمینهٔ امنیت یادگیری الکترونیکی و ۲۴ مقاله دربارهٔ حوزهٔ یادگیری الکترونیکی به‌طور جداگانه مبتنی بر روش CASP ارزیابی شدند که درنهایت ۲۹ مقاله با موضوع امنیت یادگیری الکترونیکی و ۱۷ مقاله با موضوع یادگیری الکترونیکی حداقل امتیاز برای اجرای تحلیل کیفی محتوا را کسب کردند.

در سراسر فرایند فراترکیب، پژوهشگر پیوسته مقاله‌های منتخب و نهایی‌شده را به‌منظور دستیابی به یافته‌های مرتبط با تبیین ملاحظات امنیتی یادگیری الکترونیکی مطالعه کرد. در بخش تحلیل و ترکیب یافته‌های کیفی پژوهش، محقق موضوعات یا تم‌هایی را جست‌وجو می‌کند که در مطالعات منتخب در فراترکیب پدیدار شده‌اند و به‌نوعی با موضوعات کلیدی یادگیری الکترونیکی و امنیت یادگیری الکترونیکی ارتباط دارند یا می‌توانند برای تبیین ملاحظات این حوزه استفاده شوند. با مرور چندبارهٔ مطالعات و یافته‌ها، موضوعات شناسایی و مشخص شدند و سپس پژوهشگر موضوعات را طبقه‌بندی کرد. در ادامه، طبقه‌بندی‌های مشابه در محوری قرار گرفتند که ملاحظات یادگیری الکترونیکی و امنیت یادگیری الکترونیکی را به بهترین شکل ممکن توصیف می‌کردند. این نوع تحلیل، در قالب جدولی مجزا صورت‌بندی و تدوین می‌شود.

آخرین موضوع روش فراترکیب برای مدل مرجع مهندسی الزامات امنیتی، کنترل کیفی یافته‌هاست. در این مرحله پژوهشگر رویکردها و نگرش‌های مستقر را برای تلفیق مطالعات اصلی در پژوهش کیفی استفاده می‌کند. حال آنکه برای انتخاب کیفی مقالات نیز پژوهشگر مجموعه‌ای از معیارهای استاندارد را در فرایند فراترکیب در قالب روش CASP به‌کار گرفته است. علاوه بر این، پژوهشگر هر دو راه‌کار جست‌وجوی الکترونیکی و دستی را به‌کار برد تا مقالات را به‌شکلی جامع جست‌وجو کند.

براساس مجموعهٔ مراحل یادشده، پژوهشگر با بهره‌مندی از روش فراترکیب و تحلیل چارچوب‌ها، مدل‌های نظریِ حوزهٔ یادگیری الکترونیکی و امنیت اطلاعات، درصدد برآمد مدلی مرجع برای تبیین الزامات امنیتی در حوزهٔ یادگیری الکترونیکی ارائه کند. مدلی که با مقاصد مختلفی همچون شناسایی حوزه‌های طراحی، توسعه، مدیریت، عرضه و کاربری کاربردها و

خدمات یادگیری الکترونیکی؛ شناسایی دیدگاه‌های مرجع برای طرح موضوعات کلیدی امنیتی و غیرامنیتی در حوزهٔ یادگیری الکترونیکی؛ شناسایی موضوعات کلیدی رایج و متغیرهای تصمیم اصلی یادگیری الکترونیکی در هر یک از حوزه‌های یادشده و شناسایی دامنه‌های تعریف امنیت یا اهداف کنترلی یادگیری الکترونیکی در هر یک از حوزه‌های یادشده، ارائه شده است. مدلی سه‌بعدی برای تبیین ملاحظات و الزامات امنیتی یادگیری الکترونیکی که سه بعد آن عبارت است از: نگاه زیرساخت‌گرا[1]؛ نگاه سرویس‌گرا[2] و نگاه دریافت‌کنندهٔ خدمات[3].



شکل ۱. مدل مرجع تبیین الزامات امنیتی یادگیری الکترونیکی از نگاه ذی‌نفعان

نگاه زیرساخت‌گرا یا نگاه توسعه‌دهندهٔ فناوری به حوزهٔ توسعه (باشا و دهاواچلوان، ۲۰۱۰) یا انتقال فناوری‌ها (رافه، ۲۰۰۲؛ ونتلینگ، ویقت، گالاهر، لافلور، وانگ و کانفر، ۲۰۰۰)، کاربردها و راهکارهای فنی کاربردپذیر (بارلو، ۲۰۰۷؛ باشا و دهاواچلوان، ۲۰۱۰؛ نورمین‌شاه، ۲۰۱۲) در حوزهٔ یادگیری الکترونیکی اشاره دارد. بعدی که فروشندگان سیستم‌های یادگیری الکترونیکی با بهره‌مندی از توان بومی و محلی یا استفاده از فرصت‌های انتقال فناوری به عرضهٔ محصولات (بارلو، ۲۰۰۷؛ باشا و دهاواچلوان، ۲۰۱۰)، تدارک زیرساخت (اسمیت و راپ، ۲۰۰۴؛ چین و کن، ۲۰۰۳) و نیز پشتیبانی از عرضهٔ خدمات (بارلو، ۲۰۰۷؛ مور، دیکسون‌دین و گلین، ۲۰۱۱؛ نورمین‌شاه، ۲۰۱۲) یادگیری الکترونیکی به متقاضیان می‌پردازند. چگونگی صورت‌بندی آنچه بیان شد در شکل ۲ به‌تصویر کشیده شده است.

---

1. Infrastructure Oriented Point of View
2. Service Oriented Point of View
3. Recipient Oriented Point of View

شکل ۲. چارچوب صورت‌بندی ملاحظات نگاه زیرساخت‌گرا

در چنین فضایی، توسعهٔ امن فناوری‌های یادگیری الکترونیکی (باشا و دهاواچلوان، ۲۰۱۰؛ الجوارنه، ۲۰۱۱؛ وبر، لیما، کاسا و ریبیرو، ۲۰۰۷؛ گلبرد، ۲۰۰۳)، ایجاد بسترهای لازم برای مدیریت و عرضهٔ خدمات (یاو، هویی، چونگ و یو، ۲۰۰۳؛ یانگ، ۲۰۱۱؛ کاردناس و سانچز، ۲۰۰۵؛ جلال، زب و پشاوار، ۲۰۰۸؛ لیم و جین، ۲۰۰۶؛ وبر، لیما، کاسا و ریبیرو، ۲۰۰۷) و ارائه و دریافت خدمات امنیتی (آدامز و بلاندفورد، ۲۰۰۳؛ بارلو، ۲۰۰۷؛ بالاساندارم، ۲۰۱۱) برای ارتقای استانداردهای ایمن‌سازی، از متغیرهای اصلی تصمیم توسعه‌دهندگان و متولیان زیرساخت است.

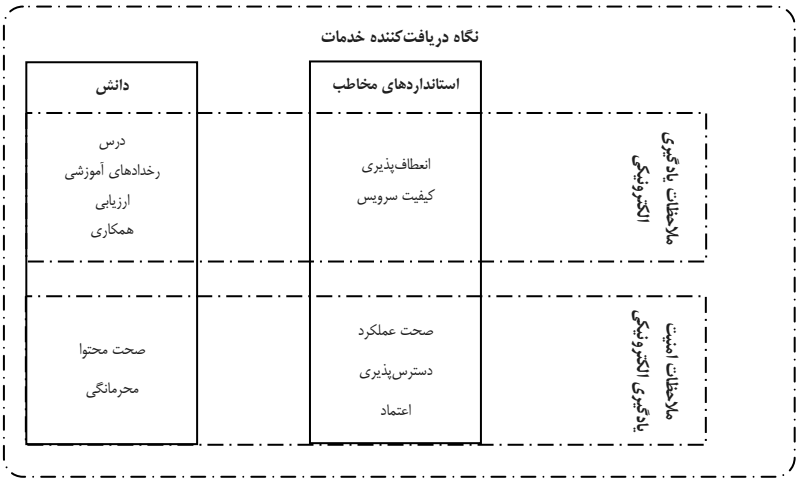
نگاه سرویس‌گرا یا نگاه عرضه‌کنندهٔ خدمات، به حوزهٔ مدیریت، پیکربندی و عرضهٔ (مور و همکاران، ۲۰۱۱؛ اسمیت و راپ، ۲۰۰۴؛ اندرسون، ۲۰۰۹؛ حمید، ۲۰۰۲؛ کاسه و بالونیوا، ۲۰۱۳) خدمات یادگیری الکترونیکی اشاره دارد. در این بعد دانشگاه‌ها، کتابخانه‌های دیجیتالی و حتی شرکت‌های خصوصی، بسته به مأموریت کاری، نیازهای حوزهٔ فعالیت و نیز درخواست‌های آموزشی واصله، نسبت به استفادهٔ موردی یا کامل (وانگ، ۲۰۰۷؛ جترو، گریس و توماس، ۲۰۱۲؛ چین و کن، ۲۰۰۳؛ نورمین‌شاه، ۲۰۱۲؛ خدابنده، افشاری و مانیان، ۲۰۱۰) از انواع کاربردها و خدمات یادگیری الکترونیکی (بلیمان، ۲۰۰۴؛ کاسه و بالونیوا، ۲۰۱۳؛ مور و همکاران، ۲۰۱۱) اقدام می‌کنند.

در چنین فضایی، امن‌سازی کاربرد و خدمات یادگیری الکترونیکی (باشا و دهاواچلوان، ۲۰۱۰؛ دفتا، ۲۰۱۱؛ وبر، لیما، کاسا و ریبیرو، ۲۰۰۷) و محمل آن (چنگ، چن، وو و چاو، ۲۰۱۲؛ دانگ،

لی، چن و ژنگ، ۲۰۰۲؛ کامبوراکیس، دی.پی.ان، روسکس و گریتزالیس، ۲۰۰۷؛ لیم و جین، ۲۰۰۶؛ یاو و همکاران، ۲۰۰۳)، ارتقای ضرایب و کیفیت عرضهٔ امن خدمات (یانگ، ۲۰۱۱؛ پراکویک و رمنار، ۲۰۱۰) و نیز امن‌سازی مؤلفه‌های سیستم یا کارکردهای آموزشی (دفتا، ۲۰۱۱؛ لامبرینوداکیس، گریتزالیس، دریدی و پرنول، ۲۰۰۳؛ زیسیس، لکاس و اسپیرو، ۲۰۰۷)، از متغیرهای اصلی تصمیم عرضه‌کنندگان خدمات یادگیری الکترونیکی محسوب می‌شود. چگونگی صورت‌بندی این ملاحظات در شکل ۳ به‌تصویر کشیده شده است.

شکل ۳. چارچوب صورت‌بندی ملاحظات نگاه سرویس‌گرا

نگاه دریافت‌کنندهٔ خدمات، به کارکنان سازمان‌ها یا دانشجویانی اشاره دارد که برای دریافت مدرک تحصیلی (چن، ۲۰۱۱؛ ونتلینگ و همکاران، ۲۰۰۰؛ وانگ، ۲۰۰۷؛ اسمیت و راپ، ۲۰۰۴) و گذراندن دوره‌های ضمن خدمت و ارتقای شغلی (وانگ، ۲۰۰۷؛ جترو و همکاران، ۲۰۱۲؛ خدابنده و همکاران، ۲۰۱۰؛ رافه، ۲۰۰۲)، متقاضی دریافت خدمات حوزهٔ یادگیری الکترونیکی هستند. چگونگی صورت‌بندی این ملاحظات در شکل ۴ مشاهده می‌شود.



شکل ٤. چارچوب صورت‌بندی ملاحظات نگاه دریافت‌کنندهٔ خدمات

در چنین فضایی، صحت (باشا و دهاواچلوان، ۲۰۱۰؛ آدامز و بلاندفورد، ۲۰۰۳؛ حیاتی و شینگ، ۲۰۱۰) و محرمانگی (آسفا و سولمس، ۲۰۰۹؛ کاردناس و سانچز، ۲۰۰۵؛ ال‌خطیب، کبرا، خو و یی، ۲۰۰۳؛ فرنل و کارونی، ۲۰۰۱) داده‌های آموزشی و نیز سطح اعتماد (متلا، ۲۰۱۱؛ گلبرد، ۲۰۰۳؛ کامبوراکیس و همکاران، ۲۰۰۷) و الزامات امنیتی و کیفی خدمات یادگیری الکترونیکی (دفتا، ۲۰۱۱؛ آسفا و سولمس، ۲۰۰۹؛ فرنل، ۱۹۹۸؛ فرنل و کارونی، ۲۰۰۱؛ لامبرینوداکیس و همکاران، ۲۰۰۳؛ پراکویک و رمنار، ۲۰۱۰)، از متغیرهای اصلی تصمیم دریافت‌کنندگان خدمات محسوب می‌شود.

در هر یک از نگاه‌ها و نگرش‌های یادشده، برخی موضوعات کلیدی مطرح می‌شود که متغیرهای تصمیم آن حوزه شناخته می‌شوند. هریک از این موضوعات دربرگیرندهٔ شاخص‌های معرفی هستند که در تصمیم‌گیری، توسعه و برنامه‌ریزی در آن موضوع مشخص، کاربرد دارند. بنابراین به‌کمک روش فراترکیب پژوهشگر توانست مدل مرجعی مبتنی بر ابعاد یادشده، ارائه کند.

نتیجه‌گیری و پیشنهادها

پژوهشگر در پژوهش حاضر با بهره‌گیری از روش فراترکیب نسبت به ارائهٔ مدلی مرجع برای تبیین ملاحظات امنیتی در حوزهٔ یادگیری الکترونیکی اقدام کرده است، مدل پشتیبانی که می‌توان برای مهندسی الزامات امنیتی به‌کار برد. این مدل از چند جهت به پشتیبانی از مهندسی الزامات امنیتی در حوزهٔ یادگیری الکترونیکی می‌پردازد. اول اینکه، مدل مرجع پیشنهادشده با

معرفی سه دیدگاه و حوزهٔ کاری مختلف یادگیری الکترونیکی، معرف خوبی برای اهداف کنترلی و ملاحظات امنیتی متمایزی است که هریک مجموعه‌ای خاص از الزامات امنیتی رادربردارند و باید در چارچوب مهندسی الزامات امنیتی، معماری شوند. از این‌رو، نوعی غربالگری الزامات در پرتو استفاده از مدل پیشنهادی محقق می‌شود. دوم اینکه، هر یک از دیدگاه‌های یادشده و قلمروی هریک، اهداف کنترلی و نیازهای امنیتی خاصی دارند و جدا از این، بسته به نوع اهمیت در حوزهٔ یادگیری الکترونیکی، الزامات و روندهای امنیتی متفاوتی را پی‌گیری می‌کنند. از این‌رو در توجیه وجودداشتن یا نداشتن فرایند اصلی یا کارکرد پشتیبان مهندسی الزامات امنیتی، می‌توانند همچون سنگ محک عمل کنند. از این‌رو نوعی غربالگری فرایندی و رویه‌ای نیز در پرتو استفاده از مدل مرجع ارائه‌شده، محقق می‌شود. درنهایت هر حوزه ذی‌نفعان و کارگزاران امنیتی خاص خود را دارد که به‌نوعی در فعالیت‌های مهندسی الزامات امنیتی اثربخش‌اند. بدیهی است که ذی‌نفعان امنیتی هر حوزه و نوع تأثیر آنها در حوزهٔ مهندسی الزامات امنیتی، از ذی‌نفعان امنیتی و نقش‌آفرینی آنها در سایر بخش‌ها متفاوت است. از این‌رو نوعی غربالگری عملکردی نیز در پرتو استفاده از مدل مرجع ارائه‌شده محقق می‌شود. بر این اساس، مدل مرجع پیشنهادی به ارائهٔ پشتیبانی همه‌جانبه از مهندسی الزامات امنیتی در حوزهٔ یادگیری الکترونیکی می‌پردازد.

References

Adams, A. & Blandford, A. (2003). *Security and Online Learning: To Protect or Prohibit.* Idea Group Inc. UK: IDEA Publishing.

Aljawarneh, S. (2011). A web engineering security methodology for e-learning systems. *Network Security,* 3: 12-15.

Anderson, J. (2009). The Work-Role Transition of Expert Clinician to Novice Academic Educator. *Journal of Nursing Education,* 48(4): 203-208.

Arabsorkhi, A. & Yadegari, A. (2011). Identifying and Analysis of Security Challenges and Solutions in e-Learning Environments. *Journal of Information Processing and Management,* 26(2): 441-464. (*in Persian*)

Arabsorkhi, A., Yadegari, M. & Kharrat, M. (2009). Some tactics and their requirements for assuring security in e-learning enviroment. *International Conference on E-Learning & Teching.* Iran University of Science & Technology. (*in Persian*)

Assefa, S. & Solms, V. (2009). *An InformationSecurity Reference Framework for e-Learning Management Systems (ISRFe-LMS).* Proceedings of 9th WCCE. https://ujdigispace.uj.ac.za/handle/10210/3901.

Balasundaram, S. (2011). Securing tests in E-learning environment. *In Proceedings of the 2011 International Conference on Communication.* Computing & Security (ICCCS '11), pp. 624-627.

Barlow, R. (2007). *A study of security in learning management systems.* An essay submitted in partial fulfillment of the requirements for the degree of master of science in information systems. Athabasca, Alberta.

Bleimann, U. (2004). Atlantis University: a new pedagogical approach beyond e-learning. *Campus-wide Information Systems*. 24(5): 191-195.

Cardenas, R. & Sanchez, E. (2005). Security Challenges of Distributed e-Learning Systems. *Fifth IEEE Int. Symp. And School on Advanced Distributed Systems (ISSADS)* (pp. 538-544). Berlin: Springer.

Chen, J. (2011). The effects of education compatibility and technological expectancy on e-learning acceptance. *Computers & Education* 57(2): 1501–1511.

Chin, K. & Kon, P. (2003). Key factors for a fully online e-learning mode: A Delphi study. *Proceedings of the 20th Annual Conference of the Australasian Society for Computers in Learning in Tertiary Education.*

Chuang, U., Chen, C., Wu, T. & Chao, H. (2012). Establish a Secure and Trustworthy ICT Environment for Educational Systems: A Case Study. *Journal of Intelligent Manufacturing,* 23(4): 965-975.

Defta, L. (2011). Security Issues in E-learning Platforms. *World Journal on Educational Technology,* 3(3): 153-167.

Dong, Y., Li, M., Chen, M. & Zheng, S. (2002). Research on intellectual property right problems of peer-to-peer networks. The Electronic Library*,* 20(2): 143-150.

Eibl, C.J.: Risk Analysis towards Secure E-Learning. In: Wheeler, S.; Kassam, A.; Brown, D. (eds.): LYICT 2008. Proc. on CD-ROM, July 2008.

Eibl, C. (2009). Privacy and Confidentiality in E-Learning Systems. *Fourth International Conference on Internet and Web Applications and Services (ICIW 2009).* IEEE Computer Society Press. doi:978-0-7695-3613-2

El-Khatib, K., Kobra, L., Xu, Y. & Yee, G. (2003). Privacy and Security in E-Learning. *Journal of Distance Education,* 1(4): 1-19.

Furnell, S. (1999). Security Considerations in Online Distance Learning. *Proceedings of Euromedia*, 99: 131-5.

Furnell, S. & Karweni, T. (2001). Security issues in Online Distance Learning. *VINE,* 31(2): 28-35.

Furnell, S., Onions, P., Knahl, M., Sanders, P., Bleimann, U., Gojny, U. & Roder, H. (1998). A security framework for online distance learning and training. Internet Research, 8(3): 236-242.

Gelbord, B. (2003). On the use of PKI technologies for secure and private e-Iearning environments. *4th International Conference Conference on Computer Systems and Technologies: e-Learning*, pp. 568-572.

Hamid, A. (2002). E-learning Is it the "e" or the Learning that matters? *The Internet and Higher Education*, 4(3-4): 311-316.

Hayaati, N. & Ip-Shing, F. (2010). E-learning and Information Security Management. *International Journal of Digital Society*, 1(2): 148-156.

Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Proceedings of Computers & Security,* 14(5): 377-383.

Jalal, A., Zeb, M. & Peshawar, P. (2008). Security enhancement for e-learning portal. *International Journal of Computer Science and Network Security,* 2(4): 236.

Jethro, O., Grace, A. & Thomas, A. (2012). E-Learning and its effects on teaching and learning in a global age. *Indian Journal of Education and Information Management,* 1(2): 73-78.

Kambourakis, G., D-P.N, K., Rouskas, A. & Gritzalis, S. (2007). A PKI approach for deploying modern secure distributed e-learning and m-learning environments. *Computers & Education*, 48(1): 1-16.

Kasse, P. & Balunywa, W. (2013). An assessment of e-learning utilization by a section of Ugandan universities: challenges, success factors and way forward. *Conference Papers – International Conference on ICT for Africa.*

Khodabandeh, A., Afshari, H. & Manian, A. (2010). Critical factors affecting e-learner's satisfaction an empirical study. *Presented at World Conference on Educational Multimedia, Hypermedia and Telecommunications 2010,* Chesapeake, VA.

Lambrinoudakis, C., Gritzalis, S., Dridi, F. & Pernul, G. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications,* 26(16): 1873-1883.

Lim, C., & Jin, J. (2006). A study on applying software security to information systems: e-learning portals. *International Journal of Computer Science and Network Security*, 6 (3B): 162-166.

May, M. & Sébastien, G. (2011). Privacy Concerns in E-learning: Is Using Tracking System a Thread? *International Journal of Information and Education Technology,* 1(1): 1-8.

Mellado, D., Blanco, C., Sánchez, L. & Fernández-Medina, E. (2010). A systematic review of security requirements engineering. *Computer Standards & Interfaces,* 32(4): 153-165.

Moore, J., Dickson-Deane, C. & Galyen, K. (2011). e-Learning, online learning, and distance learning environments: Are they the same? *The Internet and Higher Education,* 14(2): 129–135.

Mutula, S. (2011). Ethics and trust in digital scholarship. *The Electronic Library,* 29(2): 261-267.

Noorminshah, A. (2012). The impact of e-learning on students performance in tertiary institutions. *International Journal of Computer Networks and Wireless Communications,* 2(2): 121-130.

Perakovic, D. & Remenar, V. (2010). *Security audit and mechanism of protecting e-Learning system at the Faculty of Transport and Traffic Sciences,* Fakultet prometnih znanosti, Vukeliceva 4, 10000.

Ramim, M. & Levy, Y. (2006). Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University. *Journal of Cases on Information Technology,* 8(4): 24-34.

Roffe, I. (2002). E-learning: engagement, enhancement and execution. *Quality Assurance in Education,* 10(1): 40-50.

Saleem Basha, M.S. & Dhavachelvan, P. (2010). Web Service Based Secure E-Learning Management System – EweMS. *Journal of Convergence Information Technology,* 5(7): 57-69.

Smith, A., & Rupp, W. (2004). Managerial implications of computer-based online/face-to-face business education: a case study. *Online Information Review,* 28(2): 100- 109.

Webber, C., Lima, M., Casa, M., Ribeiro, A. (2007). Towards Secure E-Learning Applications: a Multiagent Platform. *Journal of Software,* 2(1): 60-69.

Wentling, T., Waight, C., Gallaher, J., La-Fleur, J., Wang, C. & Kanfer, A. (2000). *E-learning-A review of literature.* University of Illinois.

Wong, D. (2007). A critical literature review on e-learning limitations. *Journal for the Advancement of Science and Arts*, 2(1): 55-62.Yau, J., Hui, L., Cheung, B. & Yiu, S. (2003). eCX: a secure infrastructure for e-course delivery. *Internet Research,* 13(2): 116- 125.

Yong, J. (2011). Security and privacy preservation for mobile e-learning via digital identity attributes. *Journal of Universal Computer Science,* 17(2): 296-310.

Younis, A., Cater-Steel, A. & Soar, J. (2013). IT infrastructure services as a requirement for e-learning system success. *Computers & Education,* 69(3): 431-451.

Ziemba, E. & Olszak, C. (2012). Building a regional structure of an information society on the basis of e-administration. *Issues in Informing Science and Information Technology*, 9: 129-150.

Zimmer, L. (2006). Qualitative meta-synthesis: A question of dialoguing with texts. *Journal of Advanced Nursing,* 53(3): 311-318.

Zisis, D., Lekkas, D. & Spyrou, T. (2007). Security services in e-School and their role in the evaluation of educational processes. *International Conference on Institutional Evaluation Techniques in Education, ICIETE07.*

Zuev, V. (2012). E-learning Security Models. *Management Information Systems,* 7(2): 024-028.