شناسایی و تحلیل چالش‌ها و راه‌کارهای امنیتی در یادگیری الکترونیکی

ابوذر عرب‌سرخی *
دانشجوی دکتری مدیریت سیستم،
دانشکده مدیریت دانشگاه تهران و مؤسسهٔ تحقیقات ارتباطات و فنّاوری اطلاعات (مرکز تحقیقات مخابرات ایران)

امیرمنصور یادگاری
مربی پژوهشی،
پژوهشکده امنیت ارتباطات و فنّاوری اطلاعات؛ مؤسسهٔ تحقیقات ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

فصلنامهٔ علمی پژوهشی
(ویژه‌نامهٔ یادگیری الکترونیکی)
پژوهشگاه علوم و فنّاوری اطلاعات ایران
شاپا(چاپی) ۵۲۰۶-۱۷۳۵
شاپا(الکترونیکی) ۵۵۸۳-۲۰۰۸
نمایه در LISA، SCOPUS و ISC
http://jist.irandoc.ac.ir
دوره ۲۶ | شمارهٔ ۲ | ص ص ۴۴۱ - ۴۶۴

چکیده: یادگیری الکترونیکی، اگرچه امکان دریافت بسیاری از خدمات بریا برون‌خط را برای کاربران شبکه‌های رایانه‌ای فراهم آورده، ولی متناسب با ماهیّت و محیط فعالیّت خود، احتمال روبه‌رویی با انواع گوناگونی از مخاطرات امنیتی را نیز افزایش داده‌است. بنابراین، طبیعی است که موضوع تحلیل و کاهش مخاطرات امنیتی یکی از نگرانی‌های اصلی مدیران چنین حوزه‌ای باشد. مقالهٔ حاضر، با بررسی موردی آسیب‌پذیری‌ها و تهدیدهای امنیتی در سطح فرایندهای یادگیری الکترونیکی در تعدادی از مؤسّسه‌های آموزشی کشور، با روی‌کردی مبتنی بر تحلیل خطرها به ارائهٔ مجموعه راه‌کارهای امنیتی لازم می‌پردازد. مجموعه راه‌کارهای امنیتی ارائه‌شده می‌تواند به عنوان نقشه‌راه پیشرفت امنیت برای گسترش امن فضای مجازی یادگیری الکترونیکی، مورد استفادهٔ مؤسّسه‌های آموزشی کشور قرار گیرد. نقشه‌راه یاد شده، بر اساس نتایج پیمایش متون تخصصی و استانداردها، مطالعات میدانی و تحلیل‌های آماری پیرامون ایده‌ها و نگرش‌های صاحب‌نظران و فعالان حوزهٔ یادگیری الکترونیکی کشور، مورد ارزیابی و تأیید قرار گرفته‌است.

کلیدواژه‌ها: یادگیری الکترونیکی؛ آسیب‌پذیری‌های امنیتی؛ تهدیدهای امنیتی؛ تحلیل مخاطرات امنیتی؛ راه‌کارهای امنیتی.

* پدیدآور رابط: abouzar_arab@itrc.ac.ir

۱. مقدمه

رشد و نفوذ فنّاوری اطّلاعات و ارتباطات (فاوا)[1] در متن زیرساخت‌های اجتماعی، اقتصادی، سیاسی و فنّاورانه موجب تغییر چگونگی فعالیت‌ها در سطح واحدهای اجتماعی، کسب‌وکارها و حتی دولت شده‌است که حاصل آن شکل‌گیری نوع جدیدی از جوامع، با عنوان جوامع اطّلاعاتی است. مشخصهٔ اصلی فضای حاصل از این جوامع، اهمیّت بالای اطّلاعات، دانش و منابع آن‌ها، به عنوان دارایی‌های اصلی و نیازمند به نگهداری است. زیرساخت‌های فراگیر فاوا در جوامع اطّلاعاتی، بستری پایه و تسهیل‌کننده را برای گسترش انواع فضاهای کاربردی الکترونیکی و عرضهٔ طیف گسترده‌ای از سرویس‌های ارزش‌افزودهٔ الکترونیکی به گروه‌های گوناگون جامعهٔ کاربران فراهم می‌آورند. با وجود این، ماهیت این زیرساخت‌ها به‌گونه‌ای است که امکان فعالیت و بروز انواع جدید و تعداد زیادی از تهدیدها و حملات امنیتی را پیرامون سیستم‌ها، کاربری‌ها یا کاربران سرویس‌های الکترونیکی فراهم می‌کنند (Adams and Blandford 2003). ازاین‌رو، نگرانی‌های امنیتی، موضوعی کلیدی در کاربری مطمئن این سرویس‌ها محسوب می‌شود.

دربارهٔ یادگیری الکترونیکی، برخلاف ارائهٔ پیاپی راه‌کارهای گوناگون برای امن‌سازی امور سرویس‌دهی و سرویس‌پذیری در این فضای کاربردی، فراوانی و شدّت مخاطرات و تهدیدهای امنیتی حول آن نیز، همیشه، رو به افزایش است (Hitchings 1995). برخی دلیل این امر را به بی‌توجّهی به عوامل غیرسیستمی، به‌ویژه مسائل انسانی، نسبت می‌دهند. امّا می‌توان ادعا کرد که بی‌توجّهی جامع به تمامی جنبه‌های اثرگذار و اثرپذیر در فرایند عرضه، دریافت و مدیریّت سرویس‌های یادگیری الکترونیکی، زمینه‌ساز رشد و تقویت بیش‌تر مخاطرات و حملات مرتبط با این حوزه است. باتوجّه به اهمیت موضوع امنیّت در حوزهٔ یادگیری الکترونیکی، تاکنون پژوهش‌هایی در این زمینه انجام شده که در ادامه به برخی از شاخص‌ترین آن‌ها اشاره شده‌است.

در برخی از پژوهش‌ها، بر امن‌سازی خدمات شایان عرضه در حوزهٔ یادگیری الکترونیکی تأکید شده‌است. مطالعهٔ انجام شده از طریق «فرنل» و همکارن، یکی از این موارد است که با نگاهی کلّی به فنّاوری‌های این حوزه، چارچوبی مفهومی را برای عرضه امن سرویس‌های یادگیری الکترونیکی پیشنهاد می‌کند (Furnell et al. 1998). نگرش محصول‌گرا یا فنّاورانه به یادگیری الکترونیکی، روی‌کرد دیگری است که بر امن‌سازی سامانه‌های یادگیری الکترونیکی تمرکز دارد. مطالعه «چؤونگ» و «هویی» نمونهٔ مناسبی برای معرفی این روی‌کرد است که در آن، نیازهای امنیتی سامانهٔ یادگیری الکترونیکی از دیدگاه مدیریت هویت بررسی شده‌است (Cheung and Hui 1999). در دستهٔ سوم، پژوهش‌هایی وجود دارند که بر امنیت محتوای یادگیری الکترونیکی تأکید

1. Information and Communication Technology (ICT)

دارند. مطالعهٔ «رمیم» پیرامون چالش‌های امنیتی موجود پیرامون مدیریت محتوا و مواد درسی، نمونه‌ای خوب از این دست پژوهش‌ها محسوب می‌شود (Ramim 2005). با بررسی نمونهٔ پژوهشهای یادآوری شده، می‌توان دریافت که موضوعات امنیّتی پیرامون یادگیری الکترونیکی را می‌توان در چارچوب سه مؤلفهٔ فناوری، محتوا و خدمات بیان کرد (Henry 2001). البته دوباره تأکید می‌شود که کارشناسان این حوزه، بر اساس جهت‌گیری و قلمرو پژوهشی خود به مرور مباحث امنیتی یادگیری الکترونیکی پرداخته‌اند.

رهیافت‌های امن‌سازی، در پنج مجموعهٔ گوناگون قابل افراز هستند که البته هرکدام بر رویکردی خاص در امر امن‌سازی تأکید دارند (Canal 2006): (۱) رهیافت‌های فرایند محور؛ به معنای رسیدن به امنیت مطلوب از طریق طرح‌ریزی و اجرای فرایند های امنیتی، (۲) رهیافت‌های کنترل محور؛ به معنای تحقق امنیت از طریق ایجاد و پیاده‌سازی، یا طراحی و به‌کارگیری مجموعه‌ای از کنترل‌های امنیتی، (۳) رهیافت‌های محصول محور؛ به معنای تمرکز بر روی تولید محصول امنیتی یا به دست آوردن آن برای پوشش ضرورت‌های امنیتی، (۴) رهیافت‌های مبتنی تحلیل مخاطره؛ به معنای طرح‌ریزی برنامه‌ها و اقدامات امنیتی براساس نتایج حاصل از فرایند تحلیل مخاطرات، و (۵) رهیافت‌های مبتنی بر بهترین تتجربه‌ها؛ به معنای امن‌سازی فضای تبادل اطلاعات مبتنی بر روشی که در شرایط مشابه روایی آن تجربه شده‌است. در پژوهش حاضر، از ترکیب رهیافت مبتنی بر تحلیل مخاطره و رهیافت کنترل‌محور استفاده شده‌است، به این طریق که ساختار اصلی انجام‌کار با رهیافت مبتنی بر تحلیل مخاطره و قالب ارائه راه‌کارهای امنیتی با رهیافت کنترل‌محور هم‌خوانی دارد.

مقالهٔ حاضر، ابتدا و برای شفاف‌سازی و طراحی مسأله، چارچوبی مرجع را برای یادگیری الکترونیکی گزینش می‌کند و مبتنی بر آن، فرایندهای یادگیری الکترونیکی و مشخصه‌های امنیتی را تعیین می‌نماید. سپس، به تحلیل و دسته‌بندی نظام‌مند انواع راه‌کارهای فنی، رویه‌ای و قانونی لازم برای امن‌سازی فضای کاربردی یادگیری الکترونیکی می‌پردازد و در پایان، پیشنهاداتی را برای استفادهٔ مؤسسه‌های آموزشی کشور جمع‌بندی می‌کند. متناسب با مطالعات کتابخانه‌ای، میدانی یا موردی انجام‌شده، تحلیل محتوایی یا آماری پشتیبان برای سنجش اهمیت و روایی نتایج صورت گرفته‌است.

۲. شفاف‌سازی و طراحی مسأله

۲-۱. گزینش چارچوب مرجع

نخستین مرحلهٔ انجام مطالعه، گزینش چارچوبی مرجع برای تعریف یادگیری الکترونیکی و درنتیجه تعیین سرمایه‌ها و منابع اطلاعاتی این حوزهاست. امکان نگاشتن چارچوب مرجع به دو

صورت وجود دارد: (۱) مبتنی بر فرایندهای اصلی یادگیری الکترونیکی و (۲) مبتنی بر مؤلّفه‌های سیستمی اصلی یادگیری الکترونیکی. در پژوهش حاضر، روش نخست برای رسم کردن ساختار یادگیری الکترونیکی گزینش شده‌است. نگاشتن ساختار فرایند محور بر مبنای ارزیابی پیشنهادهای خبرگانی انجام شده‌است که در زمینهٔ یادگیری الکترونیک دارای پیشینهٔ تألیف مقاله یا کتاب هستند. در این راستا، ۶۴ پژوهش‌گرو صاحب‌نظر شناسایی شدند و برای آن‌ها پرسش‌نامه‌ای متشکل از هفت گویه (فرایند مرجع) ارسال شده‌است. فرایندهای مرجع هفت‌گانه، بر اساس متون تخصصی حوزهٔ یادگیری‌الکترونکی، عبارتند از فرایندهای (ارائه محتوا، طراحی دروس، سفارشی‌سازی، همکاری آموزشی، مدیریت منابع، مدیریت تجربه‌های یادگیری و ارزیابی آموزشی) که در جدول ۱ گردآوری شده‌اند (Gregg 2007)، (Khan 2005) و (Gunasekaran, McNeil, and Shaul 2002).

از جامعهٔ خبرگان برگزیده، تعداد ۵۸ نفر پاسخ‌گو بودند که پیشنهادهای خود را پیرامون درستی یا نادرستی فرایندهای مرجع یادگیری الکترونیکی در قالب طیف لیکرت عرضه داشته‌اند که نتایج تحلیل پیشنهادات یادشده در جدول یک نشان داده شده‌است. آن‌طور که در این جدول مشخص شده، برای ارزیابی دیدگاه‌های خبرگان از آزمون میانگین (t) استفاده شده‌است. نگاهی گذرا به نتایج ارائه‌شده در این جدول، بیانگر تأیید و توانایی اتکای تمامی فرایندهای مرجع خارج شده از متون تخصصی حوزهٔ یادگیری الکترونیکی است. گفتنی است که هر کدام از فرایندهای مرجع به عنوان سرمایه‌های ارزشمند نیازمند به نگهداری در حوزهٔ یادگیری الکترونیکی محسوب می‌شوند و این سرمایه‌ها، مبنایی برای تحلیل مخاطرات امنیتی در مراحل بعدی پژوهش حاضر خواهند بود.

جدول ۱. نتایج آزمون میانگین دیدگاه‌های خبرگان پیرامون فرایندهای مرجع یادگیری الکترونیکی

فرایندهای مرجع یادگیری الکترونیکی	مقدار آزمون = ۳							
	میانگین	انحراف معیار	tمقدار	درجه آزادی	سطح معناداری	اختلاف میانگین	برآورد فاصله‌ای	
							حد پایین	حد بالا
ارائه محتوا	۴.۴۷	۰.۵۹۹	۱۸.۶۴۲	۵۷	۰.۰۰۰	۱.۴۶۶	۱.۳۱	۱.۶۲
طراحی دروس	۳.۵۷	۰.۷۲۸	۵.۹۵۱	۵۷	۰.۰۰۰	۰.۵۶۹	۰.۳۸	۰.۷۶
سفارشی‌سازی	۳.۳۱	۰.۵۹۸	۳.۹۴۹	۵۷	۰.۰۰۰	۰.۳۱۰	۰.۱۵	۰.۴۷
همکاری آموزشی	۳.۵۵	۰.۸۲۰	۵.۱۲۳	۵۷	۰.۰۰۰	۰.۵۵۲	۰.۳۴	۰.۷۷
مدیریت منابع	۳.۳۱	۰.۵۰۳	۴.۷۰۰	۵۷	۰.۰۰۰	۰.۳۱۰	۰.۱۸	۰.۴۴
مدیریت تجارب یادگیری	۳.۳۱	۰.۶۵۴	۳.۶۱۱	۵۷	۰.۰۰۱	۰.۳۱۰	۰.۱۴	۰.۴۸
ارزیابی آموزشی	۳.۹۵	۰.۶۸۶	۱۰.۵۲۳	۵۷	۰.۰۰۰	۰.۹۴۸	۰.۷۷	۱.۱۳

همچنین مبتنی بر بررسی ادبیات موضوعی فرایندهای اساسی یادگیری الکترونیکی، بر عوامل و نقش‌آفرینان اصلی این حوزه نیز تمرکز شده که نمایه‌ای فشرده از نتایج به‌دست آمده در جدول ۲ بیان شده‌است. به عبارت دیگر، سه عامل (استاد، فراگیر و گسترش‌دهندهٔ محتوا)، نقش‌آفرینان اصلی در طراحی و عرضهٔ خدمات یادگیری الکترونیکی محسوب می‌شوند (Gregg 2007). سلول‌های جدول ۲، کارکردهای زیر فرایندهای یادگیری الکترونیکی و چگونگی نقش‌آفرینی هر کدام از عامل‌ها را در مراحل گوناگون سرویس‌دهی مشخص می‌کند. شایان ذکر است که در هرکدام از سلول‌های جدول ۲ تنها یکی از کارکردها، به عنوان مثال، ارائه شده‌است.

جدول۲. ساختار مرجع یادگیری الکترونیکی (نگاه فرایندی)

نقش‌آفرین فرایند	استاد	فراگیر	گسترش‌دهنده محتوا
ارائه محتوا	–	–	گزینش مفاد درسی
طراحی دروس	تعیین توالی عناوین درسی	–	تعیین منابع و زمان‌بندی آموزشی
سفارشی‌سازی	–	گزینش مفاد یادگیری و بهبود زمان‌بندی	–
همکاری آموزشی	ایجاد انجمن	اجتماعی‌سازی	–
مدیریت منابع	جای‌گیری و استفاده از منابع درسی	امکان جستجوی انواع اطلاعات	جای‌گیری و طبقه‌بندی مواد درسی جدید
مدیریت تجارب یادگیری	بهبود موارد و محتوای درسی	ارزیابی شخصی و انعکاس به استاد	–
ارزیابی آموزشی	پیشرفت کیفی دوره	اصلاح برنامه‌ریزی درسی	پیشرفت کیفی دوره

۲-۲. تعیین مشخصه‌های امنیتی

۲-۲-۱. آسیب‌پذیری‌های امنیتی

با معیّن شدن چارچوب مرجع برای یادگیری الکترونیکی، نیاز است که آسیب‌پذیری‌های امنیتی رایج در سطح فرایندها یا منابع تشکیل‌دهندهٔ چارچوب یاد شده شناسایی شوند. آسیب‌پذیری به نقطه‌ضعفی در یک یا گروهی از فرایندها گفته می‌شود که ممکن است از طریق یک یا چند تهدید، برای آسیب‌رسانی، مورد سوءاستفاده قرار گیرد (ISO/IEC 13335-1 2005). بررسی مطالعات انجام‌شده پیرامون چالش‌های امنیتی یادگیری الکترونیکی ما را به مجموعه‌ای از

آسیب‌پذیری‌های امنیتی متداول این حوزه راهنمایی می‌کند. برای مثال، آگاهی‌رسانی ضعیف (Furnell et al. 1998)، سیاست‌گذاری امنیتی نامناسب (Cheung and Hui 1999)، ضعف در طرّاحی سیستم (Yau et al. 2003)، ناکارآمدی آموزش‌های امنیتی (Furnell et al. 1998)، سازوکار ضعیف نظارت بر فرایندهای آموزشی (Ramim 2005) و سازوکار ناکارآمد مدیریت هویت و دسترسی (Cheung and Hui 1999) نمونه‌هایی شاخص از آسیب‌پذیری‌های امنیتی مستند شده در این حوزه هستند.

اگرچه مبنای طرح همهٔ آسیب‌پذیری‌های امنیتی یاد شده مراجع و متون علمی معتبر هستند، ولی در راستای هدف‌گذاری ارائه راه‌کارهای امن‌سازی برای حوزهٔ یادگیری الکترونیکی مؤسسه‌های آموزش عالی کشور، پردازش و شاید، اصلاح یا محلی‌سازی هرکدام از انواع آسیب‌پذیری‌های مستند شده، ناگزیر و مهم بیان می‌شود. از این‌رو، نسبت به سنجش نگرش صاحب‌نظران پیرامون آسیب‌پذیری‌های امنیتی رایج یادگیری الکترونیکی اقدام شده‌است. در این راستا، افراد و موقعیت‌های شغلی مرتبط با فرایندهای یادگیری الکترونیکی (جدول ۲) در سطح دانشگاه‌های فعال در این حوزه، شناسایی شدند و پیرامون وجود یا نبود چنین آسیب‌پذیری‌هایی در حوزهٔ تخصصّی فعالیت آن‌ها، مورد پرسش قرار گرفته‌اند. بررسی نخستین هشت دانشگاه فعال دولتی و خصوصی کشور در حوزهٔ یادگیری الکترونیک مبنای تعیین ۵۴ بهره‌ور آگاه در این موضوع است که نمایه‌ای از این جامعه در جدول سه نشان داده شده‌است.

برای ارزیابی پیشنهادهای خبرگان پیرامون آسیب‌پذیری‌های رایج امنیتی حوزهٔ یادگیری الکترونیکی از آزمون میانگین (t) استفاده شده‌است. این مرحله از جمع‌آوری اطلاعات از طریق تدوین و پراکندن پرسش‌نامه انجام شده است. نتایج حاصل از تحلیل پیشنهادهای این بهره‌وران در جدول چهار وجود دارد. نگاهی گذرا به نتایج ارائه شده در جدول چهار بیانگر تأیید بومی همهٔ آسیب‌پذیری‌های امنیتی متعارف مستند شده از طریق مراجع علمی حوزهٔ یادگیری الکترونیکی است.

جدول پنج، آسیب‌پذیری‌های امنیتی را براساس نوع، ماهیت و حوزهٔ اثر، به فرایندهای اصلی یادگیری الکترونیکی بیان می‌کند. راه‌برد مناسب برای تحلیل آسیب‌پذیری‌های امنیتی در سطح فرایندهای مرجع یادگیری الکترونیک، مطالعهٔ موردی، موردپژوهی یا قضیه‌کاوی است (Dul and Hak 2008). دلیل این گزینش را می‌توان به نیاز برای بررسی تفصیلی فرایندهای یادگیری الکترونیکی از دیدگاه آسیب‌پذیری‌ها و تهدیدات امنیتی در محیطی واقعی نسبت داد (Zucker 2001). در این راستا، از روش تحلیل محتوا برای کشف حقیقت از درون توصیف عینی، منظّم و کمی محتوای اطلاعات به‌دست‌آمده از بهره‌وران یادگیری الکترونیکی استفاده شده‌است. جدول پنج، در واقع نتایج حاصل از مستندسازی مشاهدات صاحب‌نظران یادگیری الکترونیکی را از دیدگاه آسیب‌پذیری‌های امنیتی ارائه می‌دهد.

جدول۳. شناس‌نامهٔ جامعهٔ خبرگان مورد مطالعه برای شناسائی آسیب‌پذیری‌های امنیتی رایج یادگیری الکترونیکی

بهره‌مندان سیستم یادگیری‌الکترونیک	تعداد برگزیده‌شده	چگونگی گزینش	تعداد پاسخ‌گو
معاونت فنّاوری اطلاعات دانشگاه	۸	سرشماری	۴
مدیر شبکه	۴	سرشماری	۳
مدیر پورتال	۳	سرشماری	۲
کارشناس فنّاوری اطلاعات	۸	نمونه‌گیری خوشه‌ای	۴
گسترش‌دهندهٔ سیستم	۲	سرشماری	۲
معمار سیستم	۱	سرشماری	۱
تحلیل‌گر سیستم	۳	سرشماری	۲
مدیر پایگاه داده سیستم	۲	سرشماری	۱
تکنسین تعمیر و نگهداری سیستم	۳	سرشماری	۲
تولیدکننده محتوای الکترونیکی	۲	سرشماری	۲
ممیز سیستم	۲	سرشماری	۲
استاد	۸	نمونه‌گیری خوشه‌ای	۴
دانشجوی مجازی	۸	نمونه‌گیری خوشه‌ای	۴

جدول٤. نتایج آزمون میانگین دیدگاه‌های خبرگان پیرامون آسیب‌پذیری‌های امنیتی رایج یادگیری الکترونیکی

آسیب‌پذیری‌های امنیتی رایج یادگیری الکترونیکی	مقدار آزمون = ۳							
	میانگین	انحراف معیار	مقدار t	درجه آزادی	سطح معناداری	اختلاف میانگین	برآورد فاصله‌ای	
							حد پایین	حد بالا
آگاهی‌رسانی ضعیف	۴.۱۲	۰.۶۵۰	۹.۹۱۱	۳۲	۰.۰۰۰	۱.۱۲۱	۰.۸۹	۱.۳۵
سیاست امنیتی ضعیف	۳.۴۸	۰.۷۵۵	۳.۶۸۹	۳۲	۰.۰۰۱	۰.۴۸۵	۰.۲۲	۰.۷۵
ضعف در طراحی سیستم	۳.۵۸	۰.۷۹۲	۴.۱۷۷	۳۲	۰.۰۰۰	۰.۵۷۶	۰.۳۰	۰.۸۶
آموزش امنیتی ناکارآمد	۳.۷۳	۰.۷۶۱	۵.۴۸۸	۳۲	۰.۰۰۰	۰.۷۲۷	۰.۴۶	۱.۰۰
نظارت ضعیف بر فرایندهای آموزشی	۳.۳۶	۰.۶۰۳	۳.۴۶۴	۳۲	۰.۰۰۲	۰.۳۶۴	۰.۱۵	۰.۵۸
مدیریت هویت ناکارآمد	۳.۳۳	۰.۵۹۵	۳.۲۱۸	۳۲	۰.۰۰۳	۰.۳۳۳	۰.۱۲	۰.۵۴

بررسی اطلاعات به‌دست‌آمده از آسیب‌پذیری‌های تجربه شده از طریق ۳۳ صاحب‌نظر حاضر در هشت دانشگاه فعال حوزهٔ یادگیری الکترونیکی ما را به نتایج اصلی زیر نزدیک می‌کند:

- جمع‌بندی مشاهدات صاحب‌نظران بیانگر تأییدی بودن نتایج حاصل از به‌کار بستن روش تحلیل محتوا است. به این معنا که پاسخ‌های خبرگان به تأیید آسیب‌پذیری‌های شناسایی‌شده در مراجع علمی پرداخته، آسیب‌پذیری جدیدی به موارد پیشین اضافه نشده‌است؛ یعنی تحلیل محتوا جنبهٔ اکتشافی در پی نداشته‌است (Zucker 2001).

جدول۵. نتایج تحلیل محتوای پیشنهادهای خبرگان پیرامون آسیب‌پذیری‌های امنیتی مشاهده‌شده در حوزهٔ یادگیری الکترونیکی

آسیب‌پذیری / فرایند	آگاهی رسانی ضعیف	سیاست امنیتی ضعیف	ضعف در طراحی سیستم	آموزش امنیتی ناکارآمد	نظارت ضعیف بر فرایندهای آموزشی	مدیریت هویت ناکارآمد	مجموع مشاهدات
ارائه محتوا	۰	۱۱	۵	۰	۰	۳	۱۹
طراحی دروس	۰	۹	۱۴	۳	۴	۰	۳۰
سفارشی‌سازی	۲	۰	۷	۰	۲	۱	۱۲
همکاری آموزشی	۵	۱۳	۸	۷	۰	۵	۳۸
مدیریت منابع	۰	۶	۴	۶	۲	۰	۱۸
مدیریت‌تجارب یادگیری	۳	۰	۰	۰	۰	۱	۴
ارزیابی آموزشی	۰	۳	۴	۲	۴	۳	۱۶
مجموع مشاهدات	۱۰	۴۲	۴۲	۱۸	۱۲	۱۳	–

- چنانچه براساس روش‌شناسی مطالعهٔ موردی، فرایندهای مرجع یادگیری الکترونیکی را به‌عنوان مورد[1]های مستقل و آسیب‌پذیری‌های امنیتی رایج در سطح آن‌ها را به‌عنوان مقوله[2]های منحصربه‌فرد لحاظ نماییم، دو نوع تحلیل مستقل پیرامون داده‌های به دست‌آمده، اجرایی خواهد بود (Larsson 1993):

۲-۲-۱-۱. تجزیه و تحلیل میان‌موردی[3]: در این نوع تحلیل، یافته‌های پیرامون آسیب‌پذیری امنیتی در سطح فرایندهای گوناگون یادگیری الکترونیکی مورد ملاحظه قرار می‌گیرد.

1. Case 2. theme 3. cross-case analysis

۲-۲-۱-۲. تجزیه و تحلیل درون‌موردی[1] : در این نوع تحلیل، یافته‌های پیرامون آسیب‌پذیری‌های امنیتی گوناگون در سطح فرایند یادگیری الکترونیکی مورد ملاحظه قرار می‌گیرند.

- تحلیل درون‌موردی اطلاعات به‌دست‌آمده بیانگر این واقعیت است که بیش‌ترین آسیب‌پذیری‌های امنیتی گزارش‌شده در حوزه همکاری‌های آموزشی است. این امر بیانگر وجود اشکال‌های مشهود یا فزاینده‌تر در حوزهٔ ارتباطات، تبادل اطلاعات و نیز تعاملات حوزهٔ یادگیری الکترونیکی است که زیرساخت‌ها و ارکان این فرایند را تشکیل می‌دهند.
- تحلیل میان‌موردی به‌دست‌آمده بیانگر این واقعیت است که بیش‌ترین ضعف‌های امنیتی گزارش‌شده حول سیاست‌های تدوین‌شده و طراحی سیستم یادگیری الکترونیکی است.

برای تقویت و تأیید یافته‌های به‌دست‌آمده از طریق تحلیل محتوا از روش آماری آنتروپی شانون برای اولویت‌بندی و تفسیر بهتر آسیب‌پذیری‌های امنیتی حوزهٔ یادگیری الکترونیکی استفاده شده‌است. این روش امکان تعیین میزان اهمیت و پشتیبانی دیدگاه‌های خبرگان از موارد مورد بررسی را فراهم می‌سازد (دانایی‌فرد، الوانی، و آذر ۱۳۸۳). در روش یادشده، محتوای پیام‌ها به‌صورت نظام‌مند و کمی توصیف می‌شوند و از این‌رو، این روش را می‌توان روش تبدیل داده‌های کیفی به داده‌های کمی نامید. برای استفاده از روش آماری آنتروپی شانون، ابتدا باید پیام را برحسب مقوله‌ها در قالب فراوانی شمارش نمود. سپس با استفاده از فرمول ۱ مقدار عدم اطمینان حاصل از هر مقوله (E_j) محاسبه شود:

$$E_j = -K \sum_{i=1}^{m} [P_{ij} \cdot \ln P_{ij}], \quad (j = 1, 2, \dots, n) \quad \text{(فرمول ۱)}$$

که در آن (m) تعداد موردها، (n) تعداد کل مقوله‌ها، (P_{ij}) بیانگر مقدار نرمال فراوانی هر مقوله و (K) ضریبی ثابت معادل با ($1/\ln(m)$) است. سپس باید با استفاده از بار اطلاعاتی مقوله‌ها ($j = 1,2,\dots,n$)، ضریب اهمیت هرکدام از مقوله‌ها را برآورد کرد که این امر از طریق فرمول ۲ امکان‌پذیر است.

$$W_j = E_j / \sum_{j=1}^{n} E_j \quad \text{(فرمول ۲)}$$

ضریب اهمیت هر مقوله نیز بیانگر رتبهٔ آن مقوله است. مبتنی بر روش بیان شده، نتایج اولویت‌بندی آسیب‌پذیری‌های امنیتی مطرح برای یادگیری الکترونیکی در قالب جدول ۶ ارائه شده‌است.

1. within-case analysis

جدول ٦. تعیین ضریب اهمیت هرکدام از آسیب‌پذیری‌های امنیتی یادگیری الکترونیکی

فرایند	جمع فراوانی	عدم اطمینان (Ej)	ضریب اهمیت (Wj)	رتبه
آگاهی‌رسانی ضعیف	۱۰	۰.۵۲۹۱	۰.۱۲۴۵	۶
سیاست امنیتی ضعیف	۴۲	۰.۷۷۶۲	۰.۱۸۲۷	۲
ضعف در طراحی سیستم	۴۲	۰.۸۶۴۳	۰.۲۰۳۴	۱
آموزش امنیتی ناکارآمد	۱۸	۰.۶۵۵۹	۰.۱۵۴۴	۵
نظارت ضعیف بر فرایند های آموزشی	۱۲	۰.۶۸۳۳	۰.۱۶۰۸	۴
مدیریت هویت ناکارآمد	۱۳	۰.۷۳۹۴	۰.۱۷۴۰	۳

همان‌طورکه در جدول ششم نشان داده شده‌است، بیش‌ترین تأکید صاحب‌نظران حوزهٔ یادگیری الکترونیکی بر وجود ضعف در حوزهٔ سیاست‌گذاری و طراحی سیستم‌های این حوزه قرار دارد. در ادامه، به موضوع کیفیت سوءاستفاده از آسیب‌پذیری‌ها از طریق نوع‌شناسی تهدیدهای امنیتی مرتبط با آن‌ها پرداخته خواهد شد.

۲-۲-۲. تهدیدهای امنیتی

خدمات یادگیری الکترونیکی همواره با انواع تهدیدات امنیتی روبه‌رو هستند. این تهدیدات، عوامل بالقوهٔ ایجاد رویدادهای امنیتی نامطلوبی هستند که می‌توانند موجب وارد آمدن خسارت در سطح خدمات یادگیری الکترونیکی شود. البته باید توجه داشت که تبدیل تهدیدی به حمله یا حادثه نیازمند وجود آسیب‌پذیری‌هایی است که در بخش پیش به آن‌ها اشاره شد. نتایج حاصل از بررسی مقاله‌ها و متون تخصصی مرتبط با موضوع تهدیدات امنیتی رایج در سطح خدمات یادگیری الکترونیکی در قالب جدول هفت ارائه شده‌است. بنابر جدول هفت، تهدیدات امنیتی یادگیری الکترونیکی را می‌توان در سرفصل‌هایی بیان کرد که هک، ویروس ترجان، انسداد سرویس‌دهی، جعل هویت، دسترسی غیرمجاز، تصرف مجوز دسترسی، اخبار نادرست، مسؤولیت‌ناپذیری، نیافتن اطلاعات و نادرستی سیستم از این موارد هستند. البته تأکید می‌شود که این تهدیدات در منابع گوناگون ، به شکل‌های متفاوتی توجّه شدند و جمع‌بندی آن‌ها در جدول هفت خلاصه شده‌است.

برای تعیین میزان اهمیّت و پشتیبانی مراجع علمی و استانداردهای امنیتی از هرکدام از تهدیدات بالا، همانند بخش پیشین، از روش تحلیل محتوای آنتروپی شانون استفاده شده که نتیجه در قالب جدول هشت ارائه شده است. همان‌طورکه در جدول هشت نشان داده شده‌است، بیش‌ترین تأکید مراجع امنیتی بر وجود امکان انتشار اخبار نادرست در سطح سیستم‌های یادگیری

الکترونیکی قرار دارد. شاید بتوان دلیل این امر را به مشاهدهٔ تحقق این نوع تهدید در سطح بیش‌تر فرایند های مرجع یادگیری الکترونیکی نسبت داد. نگاهی گذرا به یافته‌های ارائه‌شده در جدول ۹ نیز این موضوع را تأیید می‌کند.

جدول ۷. تهدیدات امنیتی شناسایی‌شده یادگیری الکترونیکی

مرجع بررسی‌کننده / عامل تهدید / تهدید	(Yau et al. 2003)	(Pinder 2002)	(Rudasill and Moyer 2004)	(Rosado et al. 2006)	(Adams and Blandford 2003)	(Ramim 2005)	شناسه تهدیدها
هک			*		*		H
ویروس/ ترجان			*		*		V
انسداد سرویس‌دهی	*		*	*			DoS
جعل هویت		*			*		I.F
دسترسی غیرمجاز		*		*		*	U.A
تصرف مجوز دسترسی		*	*		*		C.T
اخبار نادرست	*	*		*	*	*	D.N
مسؤولیت ناپذیری	*	*				*	N.A
بازنیافتن اطلاعات	*	*		*			N.R
نادرستی سیستم	*	*					N.I

جدول ۸. تعیین ضریب اهمیت هرکدام از تهدیدهای امنیتی یادگیری الکترونیکی

فرایند	جمع فرآوانی	عدم اطمینان	ضریب اهمیت	رتبه
هک	۲	۰.۳۸۶۸	۰.۰۷۰۲	۳
ویروس/ ترجان	۲	۰.۳۸۶۸	۰.۰۷۰۲	۳
انسداد سرویس‌دهی	۳	۰.۶۱۳۱	۰.۱۱۱۲	۲
جعل هویت	۲	۰.۳۸۶۸	۰.۰۷۰۲	۳
دسترسی غیرمجاز	۳	۰.۶۱۳۱	۰.۱۱۱۲	۲
تصرف مجوز دسترسی	۳	۰.۶۱۳۱	۰.۱۱۱۲	۲
اخبار نادرست	۵	۰.۸۹۸۲	۰.۱۶۳۰	۱
مسؤولیت ناپذیری	۳	۰.۶۱۳۱	۰.۱۱۱۲	۲
بازنیافتن اطلاعات	۳	۰.۶۱۳۱	۰.۱۱۱۲	۲
نادرستی سیستم	۲	۰.۳۸.۶۸	۰.۰۷۰۲	۳

جدول ۹. نگاشت تهدیدات بالقوه به آسیب‌پذیری‌های شناسایی‌شده در سطح فرایندهای یادگیری الکترونیکی

آسیب‌پذیری / فرایند	آگاهی‌رسانی ضعیف	سیاست امنیتی ضعیف	ضعف در طراحی سیستم	آموزش امنیتی ناکارآمد	نظارت ضعیف بر فرایندهای آموزشی	مدیریت هویت ناکارآمد
ارائه محتوا		D.N	DoS			U.A
طراحی دروس		N.A	N.I	D.N	U.A	
سفارشی‌سازی	D.N		N.I		N.R	N.A
همکاری آموزشی	C.T	I.F	N.R	U.A		H
مدیریت منابع		V	N.I	DoS	N.A	
مدیریت‌تجارب‌یادگیری	D.N					U.A
ارزیابی آموزشی		D.N	N.R	U.A	N.A	U.A

نظر به توجّه و تأکید مراجع علمی بر مجموعه تهدیدهای نوشته شده در جدول هفت، جدول ۹ نوشتاری از تهدیدهای امنیتی را به آسیب‌پذیری‌ها در سطح چارچوب مرجع یادگیری الکترونیکی ارائه می‌دهد. این نوشتار با دو هدف انجام شده‌است:

- امکان‌سنجی بروز تهدیدهای امنیتی گوناگون در سطح فرایندهای یادگیری الکترونیکی؛
- بررسی امکان بهره‌برداری از آسیب‌پذیری‌های شناسایی‌شده در سطح فرایندهای یادگیری الکترونیک از طریق عوامل تهدید.

باید توجه داشت که هر تهدید ممکن است از یک یا چند آسیب‌پذیری برای خدشه‌دار کردن خدمات یادگیری الکترونیکی بهره‌برداری کند. همچنین، هر آسیب‌پذیری ممکن است هدف یک یا چند تهدید امنیتی قرار بگیرد.

پردازش وتحلیل مجموعه تهدیدهای امنیتی به دو صورت امکان‌پذیر است: نخست اینکه، منابع و مراجع مرتبط در قالب مطالعهٔ کتابخانه‌ای مطالعه و نتایج منعکس شود و دوم آنکه، مشاهدات گزارش‌شده در هشت دانشگاه مورد مطالعه، بازنمایی شوند. باتوجه به بومی‌سازی فرایندهای یادگیری الکترونیکی و آسیب‌پذیری‌های امنیتی در مراحل پیشین و نظر به پیروی نکردن تحقّق تهدیدها در رخدادهای امنیتی از الگویی ویژه، پژوهش حاضر مبتنی بر روش دوم به ارائهٔ نتایج پرداخته‌است. به این ترتیب تنها آن دسته از تهدیدهای امنیتی که در فضای یادگیری الکترونیکی مؤسّسه‌های آموزش عالی کشور به فعلیت رسیده و سبب ایجاد رویدادی امنیتی با

پیامدهای نامطلوب شده‌اند، بررسی شدند. به عبارت دیگر، تحلیل‌های مربوط به تهدیدهای امنیتی در پژوهش حاضر، بر اساس مشاهدات ۳۳ بهره‌ور دانشگاهی در دنیای واقعی پایه‌گذاری شده‌است.

باتوجه به اینکه اطلاعات به‌دست‌آمده پیرامون آسیب‌پذیری‌ها و تهدیدهای امنیتی رایج در سطح فرایند های مرجع یادگیری الکترونیکی از طریق پرسش‌نامه‌ای واحد حاصل شده‌است، تهدیدها تنها در دامنهٔ آسیب‌پذیری‌ها، بازنمایی شده‌اند. این امر بیانگر هم‌گرایی پیشنهادها و ایده‌های بهره‌وران دانشگاهی پیرامون آسیب‌پذیری‌ها و تهدیدهای امنیتی مرتبط با این حوزه است. مبتنی بر مجموعه تهدیدهای شناسایی‌شده، اطلاعات گوناگونی حاصل شده که نمایه‌ای از تحلیل‌های انجام‌شده بر روی آن‌ها در قالب جدول ۱۰ ارائه شده‌است. بخشی از این تحلیل‌ها مربوط به اهمیتی است که جامعهٔ مخاطب برای هرکدام از تهدیدهای امنیتی فرض کرده‌است که در ستون‌های دوم و سوم جدول نشان داده شده‌است. در بخش دوم (ستون‌های چهارم و پنجم)، موضوع فراوانی رویدادهای امنیتی ناشی از هرکدام از تهدیدها منعکس شده که مبنای برآورد مخاطرهٔ مرتبط با هر تهدید قرار داده شده‌است.

جدول ۱۰. تحلیل داده‌های تهدیدات امنیتی گزارش‌شده در سطح آسیب‌پذیری‌های و فرایندهای یادگیری الکترونیکی

تهدیدهای امنیتی	تحلیل اجمالی				تحلیل درون موردی		تحلیل میان‌موردی	
	میانگین اهمیت از نظر مخاطب	ضریب اهمیت	فراوانی گزارش‌شده	احتمال وقوع نسبی در قیاس با دیگر تهدیدها	تعداد فرایندهای اثرپذیر	میزان خطرپذیری فرایند	تعداد آسیب‌پذیری‌های اثرپذیر	توان تهدید کنندگی
هک	۴.۷	دوم	۲	٪۱	۱	پنجم	۱	سوم
ویروس/ ترجان	۴.۱	ششم	۱۹	٪۸	۱	پنجم	۱	سوم
انسداد سرویس‌دهی	۴.۸	اول	۴۳	٪۱۸	۲	چهارم	۲	دوم
جعل هویت	۴.۷	دوم	۳	٪۱	۱	پنجم	۱	سوم
دسترسی غیرمجاز	۴.۵	چهارم	۲۷	٪۱۱	۵	اول	۳	اول
تصرف مجوز دسترسی	۴.۶	سوم	۲	٪۱	۱	پنجم	۱	سوم

ادامه جدول ۱۰. تحلیل داده‌های تهدیدات امنیتی گزارش‌شده در سطح آسیب‌پذیری‌های و فرایندهای یادگیری الکترونیکی

تهدیدهای امنیتی	تحلیل اجمالی				تحلیل درون موردی		تحلیل میان‌موردی	
	میانگین اهمیت از نظر مخاطب	ضریب اهمیت	فراوانی گزارش‌شده	احتمال وقوع نسبی در قیاس با دیگر تهدیدها	تعداد فرایندهای اثرپذیر	میزان خطرپذیری فرایند	تعداد آسیب‌پذیری‌های اثرپذیر	توان تهدید کنندگی
اخبار نادرست	۴.۳	پنجم	۵۷	٪۲۳	۵	اول	۳	اول
مسؤولیت ناپذیری	۴.۱	ششم	۲۶	٪۱۱	۴	دوم	۳	اول
باز نیافتن اطلاعات	۴.۷	دوم	۴۶	٪۱۹	۳	سوم	۲	دوم
نادرستی سیستم	۴.۷	دوم	۱۸	٪۷	۴	دوم	۱	سوم

شایان ذکر است که همانند بخش پیشین امکان پیش‌برد دو نوع تحلیل درون‌موردی (در سطح هر فرایند یادگیری الکترونیکی) و میان‌موردی (در سطح آسیب‌پذیری‌های امنیتی رایج یادگیری الکترونیکی) وجود داشته که در قالب جدول ۱۰ ارائه شده است. نگاهی گذرا به این نتایج امکان ارائهٔ تفسیرهای گوناگونی را پیرامون تهدیدهای امنیتی این حوزه امکان‌پذیر می‌کند. برای مثال، دسترسی غیرمجاز و اخبار نادرست از معدود تهدیدهایی هستند که سبب بروز رویدادهای نامطلوب امنیتی در سطح پنج فرایند گوناگون هستند (ستون‌های ششم و هفتم). از این رو، می‌توان بالاترین ضریب مخاطره‌آفرینی در این حوزه را به این نوع تهدیدها اختصاص داد.

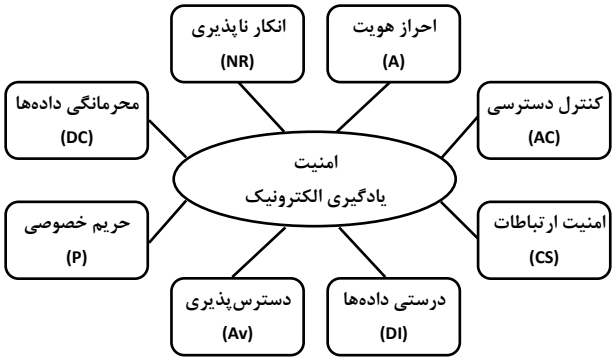
به علاوه، می‌توان الگوهای حمله یا نفوذ عامل‌های تهدیدکننده را در اطّلاعات درج شده در ستون‌های هشتم و نهم جستجو کرد. اطلاعات نوشته شده در ستون‌های اخیر، مطابق با اطلاعات مربوط به حوزه‌های نفوذ یا همان آسیب‌پذیری‌های قابل سوءاستفاده برای هر عامل تهدیدکننده در جدول ۹، تنظیم و تحلیل شده‌اند. با مرور این نتایج می‌توان دریافت که دسترسی غیرمجاز، اخبار نادرست و مسؤولیت‌ناپذیری از جمله تهدیدهایی محسوب می‌شوند که بیش‌ترین امکان تحقق حملات و رویدادهای نامطلوب امنیتی را فراهم می‌آورند. دلیل این امر را می‌توان به امکان‌های نفوذ یا آسیب‌پذیری‌هایی نسبت داد که مورد سوءاستفادهٔ این تهدیدها قرار می‌گیرند. نکتهٔ شایان توجه آن‌که نتایج تحلیل محتوای پیشنهادهای بهره‌وران دانشگاهی پیرامون اهمیت و اولویت

تهدیدهای امنیتی با نتایج به‌دست‌آمده پیرامون مراجع علمی (جدول ۸) تا حدود شایان توجهی هم‌خوانی دارد که این خود بیانگر تأیید اعتبار متقابل داده‌های پژوهش است.

۳. تحلیل و ارائهٔ راه‌کار

۳-۱. چارچوب دسته‌بندی راه‌کارهای امنیتی

راه‌کارهای امنیتی، در واقع روش‌های حفاظتی ویژه‌ای هستند که با پوشش آسیب‌پذیری‌های موجود در سرمایه‌ها، احتمال اثرگذاری نامطلوب تهدیدها بر سرمایه‌ها را تا حد مطلوبی کاهش می‌دهند. با پیمایش استانداردها و مستندات مرجع امنیتی درمی‌یابیم که دسته‌بندی‌های گوناگونی برای راه‌کارهای امنیتی وجود دارد که بیش‌تر آن‌ها با عنوان ابعاد یا مجموعه اقدامات امنیتی یاد می‌شود. برای مثال، کنترل دسترسی (AC[1])، احراز هویت (A[2])، انکارناپذیری (NR[3])، محرمانگی داده‌ها (DC[4])، امنیت ارتباطات (CS[5])، درستی داده‌ها (DI[6])، دسترسی‌پذیری (Av[7]) و حریم خصوصی (P[8]) یکی از دسته‌بندی‌های استاندارد شده برای ابعاد امنیتی هستند؛ (Khan 2005) و (ISO/IEC 18028-2 2006). ابعاد امنیتی هشت‌گانهٔ یاد شده، مبنای طرح‌ریزی چارچوبی برای دسته‌بندی راه‌کارهای امنیتی هستند که در شکل ۱، بر اساس (Rosado et al. 2006)، نمایش داده شده‌است.



شکل ۱. چارچوب دسته‌بندی راه‌کارهای امنیتی

برای تعیین ابعاد امنیتی مؤثر در برابر تهدیدهای امنیتی در سطح فرایندهای پایه یادگیری الکترونیکی دو روش وجود دارد: (۱) روش استانداردمحور و (۲) روش مبتنی بر تحلیل موقعیتی. در روش استانداردمحور، الگوهای ارائه شده در قالب برخی استانداردهای مرجع، به شفاف‌سازی

1. accessibility
2. authentication
3. non-repudiation
4. aata confidency
5. security communication
6. data integrity
7. availibilty
8. privacy

ابعاد امنیتی مؤثر در برابر تهدیدها می‌پردازند. حال آن‌که در روبه‌رویی عینی با سیستم و خدمات یادگیری الکترونیکی و یا تحلیل پیشنهادهای بهره‌وران این حوزه، می‌توان به شناسایی و آشکارسازی ابعاد امنیتی اثرگذار در برابر تهدیدات امنیتی پرداخت. در پژوهش حاضر، علاوه بر روش نخست، با بررسی موردی فرایندهای یادگیری الکترونیکی و همچنین گرفتن پیشنهادهای خبرگان این حوزه (جامعهٔ آماری معرفی‌شده در جدول سه منهای جامعهٔ برگزیدهٔ استادان و دانش‌جویان)، نسبت به تعیین ابعاد امنیتی اثرگذار در برابر تهدیدات اقدام شده‌است. نمایه‌ای از نتایج حاصل از این کار در قالب جدول ۱۱ ارائه شده است. با بررسی تحلیل‌های انجام‌شده در قالب جدول ۱۱ دو نتیجهٔ عمومی حاصل می‌شود. نخست اینکه، هر تهدیدی دارای حوزه‌های اثر خاص خود است. دوم آن‌که، ابعاد امنیتی اثرگذار در برابر هر کدام از تهدیدات، از فرایندی به فرایند دیگر تغییر می‌کند.

جدول ۱۱. اثرگذاری تهدیدها بر ابعاد امنیتی در سطح فرایندهای یادگیری الکترونیکی

تهدید امنیتی / فرایند	هک	ویروس/ ترجان	انسداد سرویس‌دهی	جعل هویت	دسترسی غیرمجاز	تصرف مجوز دسترسی	اخبار نادرست	مسؤولیت ناپذیری	باز نیافتن اطلاعات	نادرستی سیستم
ارائه محتوا			Av CS AC		A DC P		DI P Av			
طراحی دروس					A AC DC		DI Av	A AC NR		Av DI A AC NR
سفارشی‌سازی							DI P	A NR	DI Av	DI DC P A
همکاری آموزشی	A AC DC DI P			A AC NR	A DC P AC NR	A AC NR Av			Av DI CS	
مدیریت منابع		AC Av DI	Av CS AC NR					A AC NR		Av A AC DC NR
مدیریت تجارب یادگیری					A P DC		DI P DC			
ارزیابی آموزشی					A Ac P DC		DI P DC Av NR	A AC NR DI	Av DI	DI DC P NR A

۳-۲. راه‌کارهای امنیتی

راه‌کارهای امنیتی علاوه بر توانایی دسته‌بندی در چارچوب شکل یک، دارای ماهیت فنی، رویه‌ای یا قانونی هستند. ازاین‌رو، تعداد ۳(×۸)دسته راه‌کار امنیتی، به عنوان نقشه‌راه پیشرفت امنیت، برای یادگیری الکترونیکی قابل ارائه است (Rudasill and Moyer 2004)، (Pinder 2002) و (Rosado et al. 2006). راه‌کارهای امنیتی جمع‌بندی شده برای یادگیری الکترونیکی، با هدف پوشش تهدیدها و کاهش مخاطرات برآورد شده‌اند. این راه‌کارها علاوه بر پیمایش متون تخصصی، از طریق مطالعهٔ میدانی و شمردن پیشنهادهای بهره‌وران امنیتی این حوزه تدوین شده‌اند که در ادامه و بر اساس چارچوب راه‌کارهای امنیتی شکل یک به طور مختصر معرفی می‌شوند.

- کنترل دسترسی به مجموعه‌ای از عملیات اشاره دارد که برای نگهداری از دسترسی موجودیت‌های اثرگذار به موجودیت‌های اثرپذیر انجام می‌شود. مجموعه‌ای از راه‌کارهای امنیتی شناسایی‌شده این حوزه در قالب جدول ۱۲ ارائه شده‌است.
- آشکار کردن هویت به فرایندی اشاره دارد که طی آن هویت ادعایی موجودیت، ارزیابی و تأیید می‌شود. مجموعه‌ای از راه‌کارهای امنیتی شناسایی‌شده این حوزه در قالب جدول ۱۳ ارائه شده‌است.
- انکارناپذیری از اقدامات جامع و رایج امنیتی است. این الزام به سازوکاری اشاره دارد که امکان نقض مسؤولیت از طریق موجودیت فعال را در خصوص رفتار و اقداماتش می‌گیرد. مجموعه‌ای از راه‌کارهای امنیتی شناسایی شدهٔ این حوزه در قالب جدول ۱۴ ارائه شده‌است.
- محرمانگی داده‌ها به سازوکاری اشاره دارد که امکان دسترسی افراد یا پردازه‌های غیرمجاز به داده‌ها را می‌گیرد. مجموعه‌ای از راه‌کارهای امنیتی شناسایی‌شده این حوزه در قالب جدول ۱۵ ارائه شده است.
- امنیت ارتباطات بر نگهداری از ارتباطات و داده‌های در حال تبادل تأکید دارد. مجموعه‌ای از راه‌کارهای امنیتی شناسایی‌شدهٔ این حوزه در قالب جدول ۱۶ ارائه شده‌است.
- درستی داده به سازوکاری اشاره دارد که اطمینان دهد که داده‌ها تبه‌طورتصادفی یا عمدی دچار تغییر، تخریب یا کمبود نمی‌شوند. مجموعه‌ای از راه‌کارهای امنیتی شناسایی شدهٔ این حوزه در قالب جدول ۱۷ ارائه شده‌است.
- دسترس‌پذیری، بر دایر بودن، قابل استفاده بودن و سرویس‌دهی مناسب و مورد انتظار سیستم تأکید دارد. مجموعه‌ای از راه‌کارهای امنیتی شناسایی شدهٔ این حوزه در قالب جدول ۱۸ ارائه شده‌است.
- حریم خصوصی، به حقّی برای فردی اشاره دارد که براساس آن بتواند بر نوع اطلاعاتی که در مورد وی گردآوری و نگهداری می‌شود و نیز اینکه این اطلاعات در اختیار چه فرد

یا افرادی قرار می‌گیرد، نظارت کرده و تأثیرگذار باشد. مجموعه‌ای از راه‌کارهـای امنیتـی شناسایی‌شده این حوزه در قالب جدول ۱۹ ارائه شده‌است.

جدول ۱۲. راه‌کارهای کنترل‌دسترسی یادگیری‌الکترونیکی

راه‌کارهای امنیتی کنترل دسترسی	دسته‌بندی
سامانهٔ کشف نفوذ (IDS)	فنی
دیواره آتش	
سامانهٔ رمزگذاری	
زیرساخت کلید عمومی (PKI)	
امنیت پروتکل اینترنت (IPSec)	
سامانه تبادل الکترونیکی امن (SET/SSL)	
راه‌بردهای مقابله با ویروس	رویه‌ای
رویهٔ دسترسی (دسترسی کاربر باید تنها به آن خدمات یادگیری الکترونیکی امکان‌پذیر باشد که برای پشتیبانی از موارد درخواستی لازم هستند)	
مدیریت دسترسی (تملک و صدور حقوق دسترسی کاربر باید همیشه زیر کنترل مدیریت سیستم باشد)	
مدیریت اعتبارات (برای مدیریت سیستم باید امکان فسخ حقوق دسترسی کاربر بدون حضور یا دخالت کاربر وجود داشته باشد)	
صدور گواهی دیجیتال (برای اخذ مدارک و تایید فعالیت‌های آموزشی)	قانونی
سیاست‌ها و بیانیه‌های سازمانی (برای اجتماعی‌سازی و تعیین حقوق دسترسی)	

جدول ۱۳. راه‌کارهای آشکار کردن هویت یادگیری‌الکترونیکی

راه‌کارهای امنیتی آشکار سازی هویت	دسته‌بندی
سازوکار صدور گواهی دیجیتال	فنی
سازوکار کیفیت نگهداری (QoP)	
سازوکار مدیریت امنیت مبتنی بر نقش	
سامانهٔ فیلترینگ داده	
سامانهٔ رمزگذاری	
سازوکار اتصال منفرد به سیستم (SSO)	
سیستم بازرسی نقطه‌ای	

ادامه جدول ۱۳. راه‌کارهای آشکار کردن هویت یادگیری‌الکترونیکی

امکان دسترسی به خدمات یادگیری الکترونیکی باید تنها برای کاربران مجاز فراهم گردد.	رویه‌ای
ارائهٔ امکان دسترسی کاربر به خدمات یادگیری الکترونیکی باید حداقل الزام برای برآوردن نیازهای مؤسّسهٔ آموزشی برای آن خدمت یا کارکرد مدیریتی را داشته باشد.	
دسترسی کاربر به خدمات یادگیری الکترونیکی نیازمند ارائهٔ اعتبارنامه‌های آشکار شدن هویت و اطلاعات پشتیبان برای شناسایی فرد خواستار دسترسی است.	
تصویب قانون امضای دیجیتال در مجلس	قانونی
ایجاد و بهره‌برداری از مراکز صدور گواهی دیجیتالی در کشور	
پیش‌بینی و تصویب قوانین مربوط به جرائم رایانه‌ای در کشور	

جدول ١٤. راه‌کارهای انکارناپذیری یادگیری الکترونیکی

راه‌کارهای امنیتی انکارناپذیری	دسته‌بندی
امضای دیجیتالی	فنی
حسابرسی ممیزی امنیت	
ناظرین امنیت شبکه	
خدمات یادگیری الکترونیکی باید مدرکی ایجاد کنند که تراکنش دریافتی از کاربر مجاز به‌طور واقعی از کاربری که مسؤولیت تراکنش را رد نمی‌کند، ایجاد شده‌است.	رویه‌ای
خدمات یادگیری الکترونیکی باید مدرکی ارائه دهند که اطلاعات دریافتی از کاربر به‌طور واقعی از سوی وی ارائه‌شده و خدمات آشکار شدن هویت اطلاعات را رد نمی‌کند.	
خدمات یادگیری الکترونیکی باید مدرکی ایجاد کنند که خدمت به‌طور واقعیً از سوی مراجع آموزشی مرکزی یا محلی ارائه شده‌است.	
قانون ارتباطات الکترونیکی (این قانون الزامات امضای الکترونیکی و هم‌ارزیشان با امضاءهای سنتی را مشخص می‌کند)	قانونی

جدول ۱۵. راه‌کارهای محرمانگی دادهٔ یادگیری الکترونیکی

راه‌کارهای امنیتی محرمانگی داده‌ها	دسته‌بندی
رمزگذاری تراکنش‌های عملیاتی و آموزشی کاربران	فنی
استفاده از سازوکارهای امنیت لایه‌ای (لایه‌بندی امنیت)	
سازوکار کیفیت نگهداری	

ادامه جدول ۱۵. راه‌کارهای محرمانگی دادهٔ یادگیری الکترونیکی

خدمات یادگیری الکترونیکی باید حفاظت کافی از اطلاعات فردی و خصوصی در مقابل مشاهده یا آشکارسازی، هنگام گذر در بخش‌های آسیب‌پذیر شبکه، را به‌عمل آورند.	**رویه‌ای**
مطابق با قانون حفاظت داده، خدمات یادگیری الکترونیکی باید اطلاعات شخصی و خصوصی را در مقابل سوءاستفاده، هنگام ذخیره و پردازش‌شدن، در قلمرو اجرای خدمات یادگیری الکترونیکی، حفظ نمایند.	
قانون حفاظت داده یا DPA (الزامات مدیریت و حفاظت از اطلاعات فردی موجود در سیستم‌های پردازش اطلاعات را مشخص می‌کند)	**قانونی**

جدول ۱۶. راه‌کارهای امنیت ارتباطات یادگیری الکترونیکی

راه‌کارهای امنیتی ارتباطات امن	دسته‌بندی
کارگزاران امنیت شبکه	**فنی**
سیستم‌های رخدادنگاری	
سازوکارهای رمزنگاری ارتباطات و تراکنش‌ها	
رویه‌های امن‌سازی موجودیت‌های رایانه‌ای زیر شبکه (برنامه‌کاربردی خدمات یادگیری الکترونیکی و زیرساخت شبکه آن باید در مقابل حملات خارجی که ارائهٔ پیاپی خدمات را مختل می‌کنند، نگهداری شوند)	**رویه‌ای**
قانون نگهداری داده	**قانونی**
قانون بیمهٔ فضای سایبر	

جدول ۱۷. راه‌کارهای درستی دادهٔ یادگیری الکترونیکی

راه‌کارهای امنیتی درستی داده‌ها	دسته‌بندی
دیواره آتش	**فنی**
سازوکارهای امنیت لایه‌ای (لایه‌بندی امنیت)	
فیلتر داده‌ها (محتوا)	
خدمات یادگیری الکترونیکی باید اطلاعات انتقال‌یافته در شبکه‌های عمومی را از سوءاستفاده در مقابل تغییرات، حذف یا پاسخ تصادفی/عمدی غیرمجاز نگهداری کند.	**رویه‌ای**
خدمات یادگیری الکترونیکی باید اطلاعات و خدمات ذخیره‌شده در قلمرو کاربران تأیید شده را در مقابل سوءاستفاده از طریق تغییرات تصادفی/عمدی، نگهداری کنند.	
خدمات یادگیری الکترونیکی باید اطلاعات ذخیره شده در اجرای خدمات یادگیری الکترونیکی را در مقابل تغییرات عمدی یا تخریب مهاجمان خارجی نگهداری کند.	
خدمات یادگیری الکترونیکی باید اطلاعات ذخیره‌شده یا انتقال‌یافته در حوزه اجرای خدمات را از گم شدن یا تحریف تصادفی نگهداری کنند.	

ادامه جدول ۱۷. راه‌کارهای درستی دادهٔ یادگیری الکترونیکی

قانونی	قانون نگهداری داده
	انتشار بیانیه‌های امنیتی در حوزه کاربری از خدمات یادگیری الکترونیکی

جدول ۱۸. راه‌کارهای دسترس پذیری یادگیری الکترونیکی

دسته‌بندی	راه‌کارهای امنیتی دسترس‌پذیری
فنی	استفاده از سیستم‌های پشتیبان‌گیری
	استفاده از لینک‌های افزونه (برای سرویس‌دهنده‌ها)
	استفاده از سایت‌های سرد
رویه‌ای	خدمات یادگیری الکترونیکی باید در مقابل حملات خارجی که به‌نظر می‌رسد قصد خرابی یا انحراف سرویس‌دهی به کاربران مجاز را دارند، نگهداری شوند.
	خدمات یادگیری الکترونیکی باید در مقابل نارسایی تجهیزات داخلی که ممکن است به ارائه مستمر خدمات آسیب رسانده یا از آن ممانعت کنند، نگهداری شوند.
	خدمات یادگیری الکترونیکی باید در مقابل گم‌شدن داده‌ها، تجهیزات یا دیگر وقایع ناسازگار خارجی، نگهداری شوند.
	خدمات یادگیری الکترونیکی باید امکان بازیابی داده‌های مهم یا فردی را که تخریب شده‌اند، فراهم آورند.
	خدمات یادگیری الکترونیکی باید امکان بازیابی اطلاعات حفاظت‌شده را چنان‌چه مشتری یا دیگر کاربران قادر به تأمین اعتبارنامه دسترسی نیستند، فراهم آورند.
قانونی	گسترش رسمی طرح‌های بازیابی در مقابل بلایا در سطح مؤسسه‌های آموزشی
	قانون نگهداری داده

جدول ۱۹. راه‌کارهای حریم خصوصی یادگیری الکترونیکی

دسته‌بندی	راه‌کارهای امنیتی حریم خصوصی
فنی	سازوکار رمزگذاری داده‌ها، فعالیت‌ها و تراکنش‌ها در سطح فعالیت‌های آموزشی
	سازوکار امنیت لایه‌ای
	سازوکار کیفیت نگهداری
رویه‌ای	خدمات یادگیری الکترونیکی باید نگهداری را کافی از اطلاعات فردی و خصوصی در مقابل مشاهده یا آشکارسازی هنگام گذر در بخش‌های آسیب‌پذیر شبکه انجام دهد.
	مطابق با قانون حفاظت داده، خدمات یادگیری الکترونیکی باید اطلاعات شخصی و خصوصی را در مقابل سوءاستفاده هنگام ذخیره و پردازش‌شدن در قلمرو اجرای خدمات یادگیری الکترونیکی، نگهداری کنند.

ادامه جدول ۱۹. راه‌کارهای حریم خصوصی یادگیری الکترونیکی

قانون حقوق انسانی (حقوق هر فرد را در حریم خصوصی‌اش تنظیم می‌کند)	**قانونی**
قانون نگهداری داده	
قانون حریم خصوصی	

مجموعه راه‌کارهای جمع‌بندی‌شده در جدول‌های ۱۲ تا ۱۹، برای گسترش‌دهندگان حوزهٔ یادگیری الکترونیکی این امکان را فراهم می‌آورد تا با دانشی کاربردی و بینشی صحیح به راه‌بری پروژه‌های یادگیری الکترونیکی بپردازند.

٤. جمع‌بندی و پیشنهادات

نظر به اهمیت چالش‌های امنیتی در حوزهٔ یادگیری الکترونیکی و لزوم پرداخت به این موضوع، در این مقاله کوشش شد تا نسبت به ارائهٔ مجموعه‌ای فراگیر از راه‌کارهای امنیتی برای این حوزهٔ کاربردی اقدام شود. در این راستا و برای خارج کردن راه‌کارها، از رهیافت مبتنی بر تحلیل مخاطره استفاده گردید. ابتدا و با بررسی ادبیات موضوعی، فرایندهای مرجع یادگیری الکترونیکی نگارش و بومی شد. سپس، آسیب‌پذیری‌های امنیتی رایج در سطح فرایندها آشکار شد که روش انجام این کار، ترکیبی از روش مرور ادبیات موضوع و روش پیش‌برد هشت مطالعهٔ موردی و سنجش پیشنهادهای صاحب‌نظران امنیتی بوده‌است. سپس تهدیدها و ابعاد امنیتی مرتبط با خدمات یادگیری الکترونیکی، هم ازطریق پیمایش متون تخصصی و هم مبتنی بر تحلیل‌های محتوای مشاهده‌های گزارش‌شده از طریق صاحب‌نظران، برآورد شد. در پایان و برای روبه‌رویی با تهدیدها و تعدیل اثرهای مربوطه، مجموعه‌ای نظام‌مند از راه‌کارهای امنیتی برای فضای کاربردی یادگیری الکترونیکی پیشنهاد شد که به نظر می‌رسد به عنوان نقشه‌راه پیشرفت امنیت، از طریق مؤسّسه‌های آموزش عالی داخل کشور قابل استفاده باشد.

به عبارت دیگر، نظر به این‌که طرح اولیه پژوهش حاضر با درخواست تعدادی از دانشگاه‌های فعال در عرصهٔ یادگیری الکترونیکی همراه بوده‌است، در تمامی مراحل پژوهش تلاش شد تا با توجه به یافته‌های علمی مرتبط با موضوع، نسبت به بررسی و تحلیل شواهد و ابعاد عینی گزارش‌شده حول محورهای مورد بررسی اقدام شود. این امر در قالب روش‌شناسی‌های ویژه مطالعه موردی و تحلیل محتوا مورد توجه پژوهش‌گر قرار گرفته که نتایج مربوطه در بخش‌های گوناگون این مقاله نشان داده شده‌است. باتوجه به مطالعات انجام‌شده در سطح دامنهٔ پژوهش برای شناسایی و ارائهٔ پیشنهادهای کاربردپذیر برای به‌کارگیری راه‌کارهای امنیتی، موارد زیر به عنوان جمع‌بندی پیشنهاد می‌شود:

- در صورت تصمیم مؤسّسهٔ آموزشی برای گسترش سیستم یادگیری الکترونیکی، بهتر است ملاک گزینش سیستم، پوشش‌دهی راه‌کارهای پیشنهاد شده باشد.
- در صورت تمایل مؤسّسهٔ آموزشی برای به‌سازی امنیتی سیستم یادگیری الکترونیکی موجود، بهتر است که راه‌کارهای امنیتی براساس دسته‌بندی ارائه‌شده مورد توجه قرار گیرند.

در پایان، این نکته شایان ذکر است که توجه به مجموعهٔ راه‌کارهای ارائه‌شده در این مقاله پذیرفتار آشکار نشدن حادثهٔ امنیتی در سطح سیستم یادگیری الکترونیکی نیست و مجموعهٔ تدوین‌شده، تنها امکان راه‌بری امنیتی بهتر را در این حوزه فراهم می‌کند.

فهرست منابع

دانایی‌فرد، حسن، مهدی الوانی ، و عادل آذر. ۱۳۸۳. *روش‌شناسی پژوهش کمی در مدیریت، روی‌کردی جامع*. تهران: انتشارات صفار – اشراقی.

Adams, Anne, and Ann Blandford. 2003. Claude Ghaoui: Usability evaluation of online learning programs in Security and online learning: to protect or prohibit, 331–359. UK: IDEA Group Publishing.

Canal, Vicente Aceituno. 2006. ISM3: Information Security Management Maturity Model. Version 1.2. Creative Commons.

Cheung, Bruce, and Lucas C.K. Hui. 1999. Student authentication for web-based distance learning system in Proceedings of 5th International Conference on Information Systems Analysis and Synthesis, 441-446. Florida: ISAS.

Dul, Jan, and Tony Hak. 2008. Case study methodology in business research. London: Elsevier.

Furnell, S.M., P.D. Onions, M. Knahl, P.W. Sanders, U. Bleimann, U. Gojny, and H.F. Röder. 1998. A Security Framework for online distance learning and training. Internet Research: Electronic Networking Applications and Policy 8(3): 236-242.

Gregg, Dawn G. 2007. E-learning agents. Emerald: The Learning Organization 14(4): 300-312.

Gunasekaran, A., R. D. McNeil, and D. Shaul. 2002. e-Learning: research and applications. Emerald: Industrial and Commercial Training 34(2): 44-53.

Henry, Paul. 2001. E-learning: technology, content and services. MCB University Press: Education + Training 43(4): 249-255.

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

ISO/IEC TR 13335-1. 2005. IT - Security techniques - Management of ICT security - part 1: Concepts and models for ICT security management. Geneva: ISO Publisher.

ISO/IEC 18028-2. 2006. Security techniques - IT network security - Part 2: Network security architecture. Geneva:ISO Publisher.

Khan, Badrul Huda. 2005. Managing e-learning strategies: design, delivery, implementation and evaluation. Hershey: Information Science Publication.

Larsson, Rickard. 1993. Case survey methodology: quantitative analysis of patterns across case studies. Academy of Management Journal 36(6): 1515–1546.

Pinder, Andrew. 2002. Security: e-Government strategy framework policy and guidelines. http://webarchive.nationalarchives.gov.uk/20061004085342/http:/govtalk.gov.uk/documents/security_v4.pdf (accessed March 12, 2011).

Ramim, Michelle M. 2005. Towards an understanding and definition of academic misconduct in online learning environments in Proceedings of the IEEE SoutheastCon 2005, 641- 650. Florida: IEEE Publication.

Rosado, D. G., C. Gutie´rrez, E. Fernandez-Medina, and M. Piattini. 2006. Security patterns and requirements for internet-based applications. Internet Research 16(5): 519-536.

Rudasill, Lynne, and Jessica Moyer. 2004. Cyber-security, cyber-attack, and the development of governmental response: the librarian's view. New Library World 105(1202/1203): 248-255.

Yau, Joe C. K., Lucas C. K. Hui, Bruce Cheung, and S. M.Yui. 2003. eCX: A secure infrastructure for e-course delivery. Internet Research: Electronic Networking Applications and Policy 13(2): 116-125.

Zucker, Donna M. 2001. Using case study methodology in nursing research. The Qualitative Report 6(2). http://www.nova.edu/ssss/QR/QR6-2/zucker.html (accessed March 12, 2011).

Identifying and Analysis of Security Challenges and Solutions in e-Learning Environments

Abouzar Arabsorkhi*
Management Department - Tehran University
and Iran Telecommunication Research Center

Amirmansour Yadegari
Member of Scientific Board
Iran Telecommunication Research Center

Information Sciences & Technology

Iranian Research Institute
For Science and Technology
ISSN 1735-5206
eISSN 2008-5583
Indexed in LISA, SCOPUS & ISC
Vol.26 | No.2 | pp: 441-464
Winter 2011

Abstract: E-learning, despite providing the possibility of delivering several online and off-line services for users of computer networks, due to its nature and environment for activity, increases the possibility of a variety of security risks. Therefore, analysis and identifying the lessening of security risks is naturally a major concern for managers in such area. This paper, reviewing the security vulnerabilities and threats at the level of e-learning processes in some educational institutions, presents the required security tactics based on a security risk analysis approach. The presented set of security tactics can be applied by educational institutions as a security roadmap. The mentioned security roadmap is verified based on field studies, research findings and statistical analyses through the selected communities of e-learning experts and activists.

Keywords: E-Learning, Security Vulnerabilities, Security Threats, Security Risk Analysis, Security Tactics

* Corresponding Author: abouzar_arab@itrc.ac.ir