دراسة مفاهيمية وعملية لأنظمة الأمن لمكافحة الهجمات الإلكترونية في مجال التعليم والإدارة والتربية

فاطمة مرادي (الكاتب المسؤول)
المستوى الثالث التربية الإسلامية، جامعة الزهراء، قم، إيران
moradiaf1394@gmail.com
فاطمه قنبري
أستاذة في الحوزة العلمية وفي السطوح العالية في جامعة الزهراء سلام الله عليها، عضو اللجنة العلمية في جامعة الزهراء، عضو اللجنة في المستوى الرابع في مؤسسة معصومية التعليمية والمستوى الثالث في الحوزات النسائية في قم، إيران
f.ghanbari.313@gmail.com
مريم كاظمي مجد
بكالوريوس برمجيات، جامعة الزهراء، قم، إيران
Maryam135123@gmail.com

Conceptual and practical study of security systems to combat cyber attacks in the field of education, management and training

Fatemeh Moradi (Responsible Writer)
Level 3 Islamic Education, Al-Zahra University, Qom, Iran
Fatemeh Qanbari
Professor in the seminary and a teacher in the higher levels at Al-Zahra University , a member of the scientific committee at Al-Zahra University , a member of the committee at the fourth level at Masoumiyeh Educational Foundation and the third level in women's seminaries in Qom , Iran
Maryam Kazemi Majd
Bachelor of Software, Zahra University, Qom, Iran

الملخص:-

يعد الأمن السيبراني محل اهتمام للمؤسسات الإدارية والتعليمية والتربوية. لقد أدى ارتفاع الهجمات الإلكترونية الهادفة ضد البنية التحتية للبيانات والمعلومات إلى مضاعفة أهمية الإلمام بأنظمة الأمن. تتعرض المؤسسات التعليمية من خلال استخدام التقنيات الحديثة وأنظمة الاتصالات لمخاطر مثل الكشف عن المعلومات وتعطيل العمليات التنفيذية. الهدف من البحث هو مراجعة شاملة لأنظمة الأمن ومكافحة الهجمات السيبرانية في المجالات الإدارية والتربوية و التعليمية و محاولة تحديد التحديات الأمنية لتحسين أمن المعلومات في المؤسسات. يستخدم البحث المنهج المكتبي والوصفي التحليلي و يقوم بتحليل نقاط الضعف في أنظمة الأمن الموجودة من خلال تحليل النتائج العلمية، حيث تلعب نتائج مثل تشفير البيانات والمصادقة متعددة الخطوات والتحديثات المستمرة للبرامج وتدريب المستخدمين على الأمن السيبراني واستخدام أنظمة كشف ومنع الاختراق (IDS/IPS) دورًا فعالًا في زيادة مستوى الأمن في المجالات التعليمية والإدارية والتربوية.

الكلمات المفتاحية: المفاهيم، تطبيق أنظمة الأمن السيبراني، الهجمات السيبرانية، الإدارة، التعليم والتدريب.

Abstract:-

Cybersecurity is a concern for management, education and training institutions. The increase in targeted cyber attacks against data and information infrastructures has doubled the importance of familiarity with security systems. Concept; Educational institutions, through the use of modern technologies and communication systems, are exposed to risks such as information disclosure and disruption of executive operations. The aim is to comprehensively examine security systems and combat cyber attacks in the management-education and training fields and to try to identify security challenges in order to improve information security in institutions. The research used a library and descriptive-analytical method and analyzed the weaknesses of existing security systems by analyzing scientific findings. Results such as data encryption, multi-step authentication, continuous software updates, cybersecurity training for users, and the use of intrusion detection and prevention systems (IDS/IPS) play an effective role in increasing the level of security in educational, management, and training environments.

Key words: Conceptualization, Application of Cybersecurity Systems, Cyberattacks, Management, Education, and Training.

المقدمة:ـ

لقد أصبح الأمن السيبراني قضية رئيسية للمنظمات الإدارية والتربوية والتعليمية. كما أن إلى جانب الفرص التي وفرتها التقنيات الجديدة مثل شبكات التواصل الاجتماعي وإنترنت الأشياء والذكاء الاصطناعي للتعليم، فقد خلقت أيضًا العديد من التحديات. ولهذه التحديات أهمية خاصة في المؤسسات التعليمية المسؤولة عن تثقيف وتوجيه الجيل القادم. ومن بين التحديات الرئيسية زيادة التعرض للهجمات الإلكترونية والتهديدات الأمنية، مما قد يؤدي إلى انتهاك الخصوصية والتلاعب غير القانوني بالمعلومات وتغييرها وإضعاف عمليات الإدارة. وتعكس هذه الظروف أهمية الحاجة إلى إيلاء المزيد من الاهتمام لقضايا الأمن السيبراني في المؤسسات التعليمية وتؤكد على أهمية وضع التدابير المناسبة لحماية المعلومات والبيانات الحساسة. (قائمي نيا، ١٤٠٠، ص ٥٠). في العصر الرقمي، أحدث الاعتماد المتزايد على التقنيات الحديثة تغييرات عميقة في مجالات الإدارة والتعليم. و لم تؤدي هذه التبعيات الرقمية إلى تحويل المناهج التعليمية فحسب، بل سلطت الضوء أيضًا على الحاجة إلى الاهتمام بالأمن السيبراني و ضرورة اتخاذ تدابير حماية الجديدة. في مواجهة هذه التغييرات، لا بد من مراجعة أساليب الإدارة والتعليم وتكييفها مع متطلبات العصر الرقمي، بما يسمح بالتعامل بفعالية أكبر مع التحديات المستقبلية. (دريفوس، ١٣٨٩، ص ١١٠-١٢٠) ويمكن أن يؤدي الوصول السطحي و السريع إلى المعلومات في الفضاء الإلكتروني إلى انخفاض في عمق المعرفة و يزيد من حدة التحديات الإدارية والتعليمية في المؤسسات التعليمية. (لينش، ١٣٩٨، ص ٣٧-٣٨) وتشمل التحديات الإلكترونية في المؤسسات التعليمية: تسرب المعلومات والكشف عن الخصوصية وانتشار الأخبار الكاذبة وتغير أنماط السلوك. وتثير هذه التهديدات القلق بشكل خاص في المؤسسات التعليمية التي تلعب دوراً أساسياً في تشكيل شخصية الجيل القادم. (الطارمي، ١٣٨٧، ص ٣٥)؛ يهدف هذا البحث إلى تحليل أنظمة الأمن الفعالة لمكافحة الهجمات الإلكترونية في المؤسسات الإدارية التربوية. تحاول هذه الدراسة دراسة مفهوم الأمن السيبراني و تحديد التهديدات السيبرانية في هذه المؤسسات وتقديم حلول عملية لتعزيز الأمن. في هذه المقالة، يتم أولاً تقديم مفهوم الأمن السيبراني ثم يتم تحليل التهديدات الرئيسية و بالأخير يتم اقتراح حلول

فعالة للحد من نقاط الضعف في المؤسسات التربوية. يمكن أن يشكل هذا البحث أساسًا للسياسات المستقبلية في مجال إدارة الأمن السيبراني في الأنظمة التعليمية والإدارية.

خلفية البحث:

في السنوات الأخيرة و مع توسع التقنيات الرقمية والاستخدام المتزايد للفضاء الإلكتروني، أصبحت قضية الأمن السيبراني ومكافحة الهجمات الإلكترونية موضوعًا مهمًا. تناولت دراسات عديدة التحديات والحلول المتعلقة بالأمن السيبراني في المؤسسات التعليمية. ١. يشير دريفوس (٢٠١٠) في كتابه "حول الإنترنت" إلى خصائص الحياة في الفضاء الإلكتروني ويذكر أن هذا الفضاء يجذب الناس إلى فخ التبعيات المعقدة.

٢. قام الطارمي (١٣٨٩) في مقال بعنوان "الفضاء الإلكتروني والأضرار والمخاطر" قام بدراسة التهديدات الإلكترونية في المؤسسات التربوية و ذكر أن اختراق المعلومات والإفصاح عن الخصوصية و إنتشار الأخبار المزيفة وتغيير الأنماط السلوكية من بين التحديات الرئيسية في هذا المجال. أشار عبداللهي(١٣٩٢) في كتابه "دراسة الحرب الناعمة في فكر المرشد الأعلى" إلى دور وسائل الإعلام في الدفاع السلبي والأمن السيبراني و يؤكد علي أن وسائل الإعلام، باعتبارها أداةً مهمةً في الإعلام و التعليم و التثقيف العام، تلعب دورًا محوريًا في الحد من التهديدات السيبرانية. ٤. تناول بورعلي وبهمني (١٣٩٤) في مقالٍ بعنوان "دور وسائل الإعلام في الدفاع السلبي"، دور وسائل الإعلام في المؤسسات التربوية وأكدا أن وسائل الإعلام قادرة على منع انتشار التهديدات السيبرانية من خلال نشر الثقافة السيبرانية وتعزيز الوعي العام. يتطلب الأمن السيبراني في المؤسسات الإدارية والتعليمية اتخاذ تدابير وقائية وتدريبًا مكثفًا و استخدام أدوات دفاعية. و يمكن أن يُسهم تعزيز الأمن الرقمي من خلال حلولٍ مُتكاملة في الحد من التهديدات.

الأسس النظرية:

١. الفضاء الإلكتروني(السايبراني):

وتشير كلمة الفضاء في سياق الفضاء الإفتراضي أيضًا إلى معناها المجرد وأبعادها الواسعة جدًا. (الثقفي، ١٣٩١، ص ٣٦٤). "السايبر" اختصار لكلمة "السيبرنطيقا" التي تعني التوجيه والقيادة. وعند وصف هذه الكلمة، تُذكر عمليات الاتصال والإعلام والتحكم

كأدوات توجيه.

تم تقديم مصطلح "الفضاء السايبراني" أو "الفضاء الافتراضي" لأول مرة في رواية الخيال العلمي المسماة (Neuromancer) بقلم ويليام جيبسون (١٩٨٤). استلهم جيبسون فكرته من مشاهدة الشباب المنغمسين في ألعاب الكمبيوتر، فتصور شبكة من أجهزة الكمبيوتر وقواعد البيانات المترابطة التي يمكن للمستخدمين الدخول إليها ذهنيًا. هذه العملية، المسماة "jacking in"، تتيح للمستخدمين التحرك في فضاء ثلاثي الأبعاد والوصول إلى أبراج معلومات مصممة كناطحات سحاب سرية. (قائمي نيا، ١٤٠٠، ص ٢).

تم تعريف الفضاء الإلكتروني كبيئة خيالية حيث يقوم المخترقون والمستخدمون بالوصول بشكل غير قانوني إلى البيانات وقواعد البيانات. كان لهذه الصورة الخيالية العلمية تأثير كبير على تشكيل الإنترنت والشبكة العالمية، حيث أصبحت مصدرًا رمزيًا لفهم التقنيات الجديدة. (كرير ومارتن، ١٣٩٠، ص ٦٩-٧٠).

يشير مصطلح الواقع الافتراضي (VR)، والذي يرتبط أيضًا في كثير من الأحيان بالفضاء الإلكتروني، إلى عمليات المحاكاة الحاسوبية للأنظمة الحقيقية أو الخيالية التي تمكن المستخدمين من إجراء عمليات في بيئات رقمية. تعرض هذه المحاكاة تفاعلات المستخدمين كزمان حقيقي وتوفر مفهومًا للتجربة المعاشة في الفضاء الرقمي. (كرير ومارتن، ١٣٩٠، ص٧٠).

٢. نظام الأمان:

يشير نظام الأمن إلى مجموعة من العمليات والسياسات والأدوات والإجراءات المصممة والمنفذة للحفاظ على الأمن المادي والنفسي والاجتماعي و تعزيزه في بيئة تعليمية أو تنظيمية. يتضمن هذا النظام التخطيط والمراقبة والتحكم والتقييم المستمر لمنع وقوع الأحداث السلبية والتهديدات والأضرار المحتملة وتوفير الاستجابات المناسبة والسريعة في حالة حدوثها. في مجال الإدارة التربوية، لا يركز نظام الأمن على الأمن المادي فقط (مثل سلامة المباني والمعدات)، بل يركز أيضًا على الأمن النفسي والعاطفي للأفراد (مثل الطلاب والمعلمين والموظفين). ينبغي تصميم هذا النظام بما يوفر بيئة آمنة وهادئة وموثوقة للتعلم والنمو. (رضائي، ١٣٩٨، ص ٥٢). يتكون نظام الأمن من مجموعة من التقنيات والسياسات والعمليات المصممة لحماية المعلومات والشبكات والبنية التحتية الرقمية من

التهديدات السيبرانية. وفي المؤسسات التربوية والإدارية، بالإضافة إلى حماية البيانات الحساسة، تلعب هذه الأنظمة دوراً هاماً في تعزيز الأمن النفسي والثقافي للمستخدمين.. (أحمد زاده كرماني، ١٣٨٨، ص ١٤٣). تشمل أنظمة الأمن الأدوات والتقنيات والتدابير المصممة لحماية البيانات والشبكات وأنظمة المعلومات من التهديدات السيبرانية. تتضمن هذه الأنظمة برامج مكافحة البرامج الضارة و جدران الحماية وأنظمة اكتشاف التطفل (IDS) وأنظمة منع التطفل (IPS). (عزيزي، ١٣٨٨، ص ١٢٢). الفضاء الإلكتروني هو بيئة تتشكل من خلال تكنولوجيا المعلومات والاتصالات وتوفر منصة للتفاعل وتبادل المعلومات والاتصالات العالمية. تتمتع هذه المساحة، بسبب حدودها غير المحدودة وبنيتها الرقمية بخصائص معينة مثل اللامركزية وعدم القدرة على التحكم. (بيل، ١٣٨٩، ص٢٢-٢٣).

٣. الأمن السيبراني:

يتضمن الأمن السيبراني مجموعة من التدابير الوقائية والدفاعية لحماية البيانات والأنظمة والشبكات الرقمية من التهديدات السيبرانية. يركز هذا المفهوم، إضافة علي الأجهزة والبرامج، على صنع السياسات والتدريب العملي وبناء ثقافة السلامة في الفضاء الإلكتروني. يلعب الأمن السيبراني دورًا رئيسيًا، خاصة في المؤسسات التربوية، نظرًا لأهمية حماية المعلومات الحساسة للطلاب والمعلمين. و تعد هذه المؤسسات أكثر عرضة للهجمات الإلكترونية بسبب البنية التحتية للمعلومات الأقل تطوراً لديها وسهولة الوصول إلى معلومات المستخدمين الشخصية (افتخاري، ١٣٨٢، ص٥؛ شعاري نجاد، ١٣٦٦، ص٢٤٣).

١-٣. الدفاع السلبي:

يشير الدفاع السلبي إلى مجموعة من التدابير التي تحمي البنية التحتية والأصول الحيوية من التهديدات دون الحاجة إلى المواجهة المباشرة. في المجال السيبراني، يسعى الدفاع السلبي إلى اتباع أساليب مثل الحد من نقاط الضعف وتعزيز أمن البنية التحتية والاستعداد للهجمات. الأمن السيبراني، باعتباره جزءًا من الدفاع السلبي في الفضاء الرقمي، يلعب دورًا هامًا في حماية البيانات وأنظمة المعلومات من خلال التركيز على التدابير الوقائية والتفاعلية. (موحدي نيا، ١٣٨٦، ص ٣).

٤. الهجمات الإلكترونية:

الهجمات الإلكترونية هي أنشطة مخربة في المجال الرقمي تهدف إلى التسلل إلى الشبكات أو التوصل غير المصرح إلى المعلومات أو تدمير الأنظمة أو تعطيل عملها. تتضمن هذه الهجمات أنواعًا مختلفة من التصيد الاحتيالي والبرامج الضارة وهجمات الحرمان من الخدمة الموزعة والهجمات القائمة على الشبكة. (جلالي الفراهاني، ١٣٨٦، ص٦).

٥. الإدارة التربوية:

التربية عملية تساعد على تكوين هوية الأفراد ونموها المستدام بشكل متكامل و وفقاً لمنظومة القيم الإسلامية و توجههم إلى تحقيق المستويات المنشودة من الحياة في كافة مناحيها بشكل واع و إرادي (المجلس الأعلى للثورة الثقافية، ١٣٩٠). الإدارة هي علم وفن تنسيق وتوجيه ومراقبة أنشطة المجموعة لتحقيق الأهداف المحددة بأقصى قدر من الكفاءة (اقتداري، ١٣٩٢، ص٦١). تعني الإدارة التربوية تطوير وتنفيذ السياسات والاستراتيجيات التي تعمل على ترقية البيئات التعليمية والاستفادة من التكنولوجيا الرقمية لتثقيف وتدريب الجيل الجديد. يشمل هذا المجال تصميم برامج تعليمية وتعزيز مهارات محو الأمية الإعلامية و تعزيز ثقافة الأمن السيبراني (الكلبايكاني، ١٣٨١، ص ٤٤؛ شرودر، ١٣٨٣، ص ١٢٠).

١. تحديد التهديدات السيبرانية في مجال الاداري-التربوي:

لقد أتاح التطور التكنولوجي و تطور الفضاء الإلكتروني فرصاً لتحسين الأنظمة الإدارية و التربوية، وقد صاحب هذه التطورات ظهور تهديدات جديدة لها تأثيرات كبيرة على الهياكل التعليمية. بالإضافة إلى تعريض أمن المعلومات والبيانات التعليمية للخطر، تُسبب هذه التهديدات مشاكل وتحديات للمسؤولين والمعلمين والطلاب. وتشمل أبرز التهديدات الإلكترونية ما يلي:

١-١. هجمات التصيد وسرقة المعلومات الإدارية في المراكز التعليمية:

تشكل هجمات التصيد الاحتيالي واحدة من أهم التهديدات الإلكترونية التي تواجه المراكز التعليمية. تتم هذه الهجمات عادة عن طريق إرسال رسائل بريد إلكتروني مزيفة وروابط ضارة وصفحات خادعة و الهدف منها هو سرقة المعلومات الحساسة من المدراء والأساتذة وموظفي الجامعة. ويستخدم المهاجمون السيبرانيون أساليب متطورة مثل تزوير

صفحات تسجيل الدخول للأجهزة التعليمية وخداع المستخدمين للكشف عن كلمات المرور وحتى إساءة استخدام أساليب الهندسة الاجتماعية للوصول غير المصرح به (كمالي زاده وآخرون، ١٣٩٤، ص ٣٠).

أهم أساليب هجمات التصيد في المراكز التعليمية:

١-١-١. رسائل التصيد الاحتيالي وانتحال هوية المدراء التعليميين:

يستهدف المهاجمون الإداريين والأساتذة من خلال رسائل بريد إلكتروني مزيفة تشبه إلى حد كبير الرسائل الجامعية الرسمية. تحتوي رسائل البريد الإلكتروني هذه عادةً على روابط مزورة تعمل على إعادة توجيه المستخدمين إلى صفحات تسجيل دخول مزيفة وسرقة معلومات تسجيل الدخول الخاصة بهم (زارع و ميرزائي، ١٣٩٨، ٢٥).

٢-١-١. هجمات التصيد الاحتيالي المبنية على مواقع الويب المزيفة:

يقوم بعض المهاجمين بتصميم مواقع ويب تبدو مشابهة لصفحات لأنظمة التعليمية الرسمية (مثل أنظمة إدارة التعلم ورسائل البريد الإلكتروني للأنظمة). وتقوم هذه المواقع بخداع المستخدمين وسرقة معلوماتهم الحساسة (صفدري، ١٤٠٢، ص ٤٢).

٣-١-١. الهندسة الاجتماعية وسرقة بيانات الاعتماد:

يستخدم المخترقون [الهاكرز] أساليب الهندسة الاجتماعية لخداع المستخدمين والحصول على معلومات تسجيل الدخول لأنظمة الجامعات من خلال المكالمات الهاتفية أو الرسائل النصية أو الشبكات الاجتماعية. هذه الطريقة ناجحة جداً خاصة بين الموظفين الذين ليس لديهم علم بالأمن السيبراني (سبزكار مقدم، ١٤٠٢، ص ٣٨).

٤-١-١. هجمات التصيد على مواقع التواصل والشبكات الاجتماعية:

تستخدم العديد من المؤسسات التعليمية وسائل التواصل الاجتماعي للتواصل. وهذا يوفر فرصة للمهاجمين لإرسال روابط مزورة ومصابة من خلال رسائل مزيفة في رسائل البريد الإلكتروني الخاص بالبرامج أو الأنظمة (رضا زاده وآخرون، ١٤٠٠، ص ٤٣).

١-٢. الإفصاح عن المعلومات المتعلقة بالطلاب والموظفين التعليميين والتربويين:

يعد الكشف عن المعلومات الشخصية للطلاب والموظفين التعليميين أحد أخطر التهديدات الإلكترونية والتي يمكن أن يكون لها عواقب واسعة النطاق، بما في ذلك سرقة الهوية والابتزاز وإساءة استخدام البيانات الشخصية. إن ضعف أمن أنظمة الإدارة التعليمية والإهمال في حماية البيانات يؤدي إلى تسرب المعلومات الحساسة الخاصة بالطلاب والمعلمين و المدراء. وقد يؤدي هذا إلى عواقب لا يمكن إصلاحها مثل تزوير الهوية و الإحتيال المالي والإضرار بسمعة الأفراد (عارفي نجاد و آخرون، ١٤٠٣).

٣-١. انتشار المحتوى الهدام وغير المصرح به في المجال التعليمي والتربوي:

يمكن أن تصبح منصات المتاحة عبر الإنترنت وخاصة شبكات التواصل الاجتماعي وأنظمة التعليم المفتوحة مكانًا لنشر المحتوى غير المناسب والأخبار المزيفة والمعلومات المضللة. و يؤدي هذا المحتوي إلى تقليل عمق المعرفة و انحرافات في التعليم و خلق مخاوف أخلاقية بين الطلاب و عائلاتهم (شاه ميري لجي، ١٤٠١).

٤-١. الهجمات الإلكترونية على أنظمة التعليم عبر الإنترنت:

مع الاعتماد المتزايد على التعليم الافتراضي، أصبحت البنية التحتية التعليمية أكثر عرضة للهجمات الإلكترونية. يمكن أن تتسبب هجمات مثل هجمات الحرمان من الخدمة الموزعة (DDoS) في تعطل أنظمة التعليم الإلكتروني وتعطيل عملية التعلم. كما تُعتبر البرمجيات الخبيثة وبرامج الفدية تهديداً خطيراً للخوادم والبيانات التعليمية (غفاري جردويشه و آخرون، ١٤٠٢).

٥-١. التجسس الإلكتروني والتدخل في السياسات التعليمية:

تهدف بعض الهجمات الإلكترونية ضد المؤسسات التعليمية إلى التجسس و جمع المعلومات الحساسة. يتم تنفيذ هذا النوع من الهجمات عادة من قبل مجموعات القرصنة المتطورة و حتى الحكومات المعادية ويمكن أن يؤدي إلى التلاعب بالسياسات التعليمية وسرقة البحوث العلمية وحتى التأثير على النظام التعليمي والإداري (عارفي نجاد و آخرون، ١٤٠٣).

٢. مراجعة أنظمة الأمان الموجودة:

ونظرا لانتشار التهديدات السيبرانية في البيئات الإدارية والتعليمية، فإن استخدام أنظمة

أمنية متقدمة يعد أمرا ضروريا للتخفيف من حدة هذه التهديدات. بعض طرق وأدوات الأمان:

٢-١. أطر الأمن السيبراني وإدارة المخاطر:

تعد الأطر مثل إطار عمل مثل NIST Cybersecurity Framework و ISO 27001 من بين معايير إدارة الأمن السيبراني الأكثر أهمية في مجال التربوي و التعليمي. توفر هذه الأطر حلولاً لتقييم التهديدات وتقليل المخاطر ومكافحة الهجمات الإلكترونية (نادري بور وبورابراهيمي، ١٤٠١، ص ٢٣).

٢-٢. أنظمة الكشف عن التطفل والوقاية منه (IDS/IPS):

يتم استخدام أنظمة IDS (نظام اكتشاف التطفل) للكشف عن الهجمات الإلكترونية، بينما يعمل IPS (نظام منع التطفل) بشكل فعال على منع وقوع الهجمات. تلعب هذه الأنظمة دوراً رئيسيًا في تحديد التهديدات وحظرها في مجالات التعليم والإدارة (بورفيضي وإيران زاده، ١٤٠١: ص ٤١).

٢-٣. الذكاء الاصطناعي(Ai) والتعلم الآلي(ML) في الأمن السيبراني:

يتم استخدام تقنية الذكاء الاصطناعي (AI) والتعلم الآلي (ML) بشكل متزايد في مجال الأمن السيبراني. وتستطيع هذه التقنيات تحليل أنماط سلوك المستخدم وتحديد التهديدات الإلكترونية مثل هجمات التصيد الاحتيالي أو البرامج الضارة (حجازيان، ١٤٠٢: ص٣٤).

٢-٤. أمن المعلومات وحماية البيانات:

تضع كتب مثل "الأمن السيبراني وحماية البيانات" الكثير من التركيز على أهمية حماية المعلومات الشخصية والتنظيمية. تساعد هذه الكتب المديرين على تنفيذ حلول أمنية مثل تشفير البيانات وإنشاء مصادقة متعددة العوامل وسياسات صارمة للتحكم في الوصول (كمالي، ١٤٠٣: ص ٢٨).

٢-٥. إدارة المخاطر السيبرانية في المنظمات:

ومن القضايا الرئيسية إدارة مخاطر الأمن السيبراني في المؤسسات التعليمية. ويعد تحديد

نقاط الضعف الأمنية وتنفيذ سياسات الحماية وتطوير خطط الاستجابة للأزمات من أهم التدابير للحد من تأثير التهديدات السيبرانية (حجازيان، ١٤٠٢: ص ٤٩). ويعد تطبيق أطر الأمن واستخدام أنظمة كشف التسلل والاستفادة من الذكاء الاصطناعي وتشفير البيانات من أهم أساليب الحفاظ على الأمن في البيئات الإدارية والتعليمية. تلعب زيادة وعي المستخدمين والموظفين بالتهديدات السيبرانية وتطوير سياسات أمنية قوية دوراً مهمًا في تقليل الأضرار المحتملة.

٣. تهديدات الفضاء الإلكتروني في مجال الإداري- التربوي:

يُشكّل الفضاء الإلكتروني إلى جانب فرصه العديدة في التعليم والإدارة التعليمية، تهديداتٍ خطيرة. يمكن أن تؤثر هذه التهديدات على جودة التعليم وتُضعف الثقة العامة و تُفضح المعلومات وتُسبب مشاكل تعليمية. و تشمل التهديدات الأكثر أهمية ما يلي:

٣.١. الإفصاح عن المعلومات:

إن أكبر التهديدات في الفضاء الإلكتروني هي تسرب المعلومات الإدارية والتعليمية الحساسة وأساليب التربية. إن نقاط الضعف في البنية التحتية الأمنية للمراكز التعليمية، إلى جانب الافتقار إلى وعي المستخدمين، تزيد من خطر سرقة المعلومات والإفصاح عنها مما يسبب انتحال الهوية والاستغلال المالي و حتى تهديدات نفسية للمجالات العلمية والروحية والتربوية. (عارفي نجاد وآخرون، ١٤٠٣، ص ٢٧).

٣.٢. تقليل عمق المعرفة:

إن الإفراط في استخدام الفضاء الإلكتروني يقلل من قدرات الطلاب التحليلية ويجعل التعلم سطحيا. في الواقع، إن وفرة المعلومات و سهولة الوصول إلى الإجابات الجاهزة يمكن أن تؤدي إلى ضعف في مهارات التفكير النقدي وتحليل المعلومات. كما أن الاعتماد المفرط على التكنولوجيا يقلل من التفاعل المباشر بين المعلم والطلاب ويضعف تجربة التعلم (الخلجي، ١٤٠٣، ص ٣٥).

٣.٣. الإخلال في الأنظمة التعليمية:

وتشكل الهجمات الإلكترونية على أنظمة إدارة التعلم (LMS) و الاختبارات عبر

الإنترنت وأنظمة التعليم الافتراضية تهديداً رئيسيًا آخر. وتشمل هذه الهجمات هجمات التصيد الاحتيالي والبرامج الضارة، وهجمات رفض الخدمة (DDoS) والتسلل غير المصرح به إلى الأنظمة التعليمية مما قد يؤدي إلى تعطيل عملية التعلم والإدارة (وظيفة دان، ١٣٩٥: ص ٣٢).

٣.٤. تقويض ثقة الجمهور:

يؤدي نشر المعلومات المزيفة والأخبار الكاذبة في الفضاء الإلكتروني إلى تقليل ثقة الجمهور في المؤسسات التعليمية والإدارية والتربوية. و تؤدي هذه المشكلة، وخاصة في البيئات التي لا تتوفر فيها سياسات أمنية مناسبة، إلى زيادة الفجوة بين المدراء و المعلمين و العوائل والطلاب (غفاري جردويشه وآخرون، ١٤٠٢: ص ٤٤).

٣.٥. التحديات التربوية:

يمكن أن يكون للفضاء الإلكتروني تأثير عميق على العملية التعليمية للأفراد. يُعدّ الوصول السهل إلى المحتوى غير اللائق والتواصل غير الخاضع للرقابة و ترويج أنماط ثقافية غربية غير لائقة من التحديات التي يواجهها المدراء و العوائل والمعلمون. كما أن ضعف برامج التربية الإعلامية و الأمية الرقمية يتسببان مشاكل في الشؤون التربوية والأخلاقية والسلوكية للأفراد. (محمدي ماشمياني وآخرون، ١٤٠٢: ص٣٩).

وتتضمن الحلول المهمة للحد من تهديدات الفضاء الإلكتروني وزيادة مستوى الأمن السيبراني؛ تطوير سياسات الحماية وتعزيز محو الأمية الإعلامية و تعليم المهارات الرقمية.

٤. الإدارة التربوية و حلول الأمن في الفضاء الإلكتروني:

ونظراً للنمو المتزايد للتكنولوجيا وتوسع الفضاء الإلكتروني في البيئات التعليمية، فإن هناك حاجة ملحة إلى إدارة تربوية فعالة و حلول لتأمين الأمن لحماية الطلاب و المدراء التعليميين و التربويين تشمل "العمل التعليمي لمحو الأمية الإعلامية وبناء ثقافة الأمن الرقمي وإنشاء سياسات مرنة" وتفسير هذه الحلول هو:

٤.١. العمل على محو الأمية الإعلامية:

يُعدّ محو الأمية الإعلامية من أكثر السبل فعاليةً لمكافحة التهديدات السيبرانية في البيئة التعليمية. و قد أدي انتشار محو الأمية الرقمية إلى الوقاية من الكشف عن المعلومات والحدّ من عمليات الاحتيال و إساءة الإستخدام الإلكتروني. (كمالي، ١٤٠٣: ص ٣٤). ومن شأن إدراج مقررات محو الأمية الإعلامية في مناهج المدارس والجامعات والمؤسسات التعليمية أن يزيد وعي الطلاب بمخاطر الفضاء الإلكتروني. (غفاري جردويشه وآخرون، ١٤٠٢: ص ٣٤). ومن أهم الإجراءات تدريب معلمين أخصائيين في مجال الثقافة الرقمية مما يزيد من مستوى الأمان في البيئة الإدارية والتعليمية والتربوية (رزمخواه، ١٤٠٣: ص ٢٩).

٤.٢. بناء ثقافة الأمن الرقمي:

يتطلب بناء ثقافة الأمن الرقمي ترسيخَ رؤية سليمة تجاه الخصوصية وأمن المعلومات ومراعاة أخلاقيات الإنترنت. و يُساعد عقدُ ورش عملٍ في المدارس والجامعات للطلابَ والمعلمين على إدراك أهمية الأمن السيبراني ومراعاة مبادئ الخصوصية (حجازيان، ١٤٠٢: ص ٢٩). و قد تم اقتراح إنشاء نوادي طلابية رقمية كمكان لتعلم وممارسة مهارات الأمن السيبراني (حسيني وآخرون، ١٤٠٣: ص ٢٨). إن إنشاء إرشادات سلوكية وتربوية في المركز للاستخدام الآمن للإنترنت وشبكات التواصل الاجتماعي والأنظمة التعليمية يعد حلاً مهماً (نصيري ووليكبني، ١٤٠٢: ص ٢٥).

٤.٣. إنشاء سياسات مرنة:

ولضمان الأمن السيبراني في البيئات التعليمية، فإن السياسات المرنة والشاملة ضرورية. ينبغي تصميم هذه السياسات بطريقة، مع الحفاظ على الأمن، تضمن منع فرض قيود غير ضرورية على التعلم. يُعدّ تطبيق سياسات أمنية تكيفية قائمة على سلوك المستخدم وسيلةً مهمةً لمنع الهجمات الإلكترونية في البيئات التعليمية (حجازيان، ١٤٠٢: ص ٤٥). إضافة إلى ذلك، يُمكن أن يُساعد وضع قواعد و لوائح مُحددة لخصوصية المستخدم في الأنظمة التعليمية على الحدّ من تسريب المعلومات واحتمالية إساءة استخدامها (غفاري-جردويشه وآخرون، ١٤٠٢: ص ٣٢). و يعد تطوير تعليم محو الأمية الإعلامية وخلق ثقافة الأمن الرقمي و وضع سياسات مرنة من التدابير الأساسية في الإدارة التعليمية للفضاء الإلكتروني. ولن تؤدي هذه الحلول إلى الحد من التهديدات السيبرانية في البيئات التعليمية

فحسب، بل يمكنها أيضًا توفير أساس لرفع مستوى الوعي وتعزيز المسؤولية الرقمية وزيادة أمن الفضاء التعليمي.

٥. دور وسائل الإعلام في الدفاع السلبي والأمن السيبراني:

تعتبر وسائل الإعلام أدوات مؤثرة في الفضاء الإلكتروني و تلعب دوراً رئيسياً في الدفاع السلبي والأمن السيبراني بل و يمكن أن تساهم أيضًا في استقرار الفضاء الإلكتروني من خلال خلق ثقافة الأمن الرقمي ومواجهة الحرب الناعمة والعمليات النفسية للعدو (خواجة، ١٣٩٩، ص ٩). الدفاع السلبي هو وسائل الإعلام والإعلان. تلعب وسائل الإعلام في المؤسسات التعليمية دوراً أساسيًا في نقل المعلومات وتدريس الثقافة السيبرانية في المراكز العلمية والدينية. ويُعتبر الأمن السيبراني جزءًا من الدفاع السلبي وذلك من خلال تصميم أنظمة وقائية وتفاعلية لحماية وسائل التعليم (بورعلي، بهمني، ١٣٩٤، ص ١٥-٢٠).

١-٥. دور وسائل الإعلام في رفع الوعي وخلق ثقافة الأمن السيبراني:

تلعب وسائل الإعلام دوراً مهمًا في المؤسسات التعليمية في نقل المعلومات و التعليم لمحو الأمية السيبرانية و رفع الوعي بين الطلاب والمعلمين. و تتعرض وسائل الإعلام لهجمات إلكترونية يمكن أن تؤدي إلى الكشف عن معلومات حساسة وانتشار الأخبار المزيفة و تآكل ثقة العامة. ويعتبر الأمن السيبراني جزءًا من الدفاع السلبي من خلال تصميم أنظمة وقائية وتفاعلية لحماية الوسائل التعليمية. (بورعلي، بهمني، ١٣٩٤، ص ١٥-٢٠). يمكن لوسائل الإعلام تعزيز ثقافة الأمن السيبراني بين المستخدمين من خلال إنتاج ونشر المحتوى التعليمي. وبحسب الدراسات فإن استخدام وسائل الإعلام العامة فعال للغاية في تعزيز المعرفة العامة حول التهديدات السيبرانية وتعليم أساليب منع هجمات التصيد وزيادة الوعي بشأن الخصوصية (تمنايي فر وتوليت، ١٣٩٣: ص ٤٢). يمكن لوسائل الإعلام في المؤسسات التعليمية أن تلعب دوراً هاماً في خلق ثقافة الأمن الرقمي. وفي هذا المجال، يمكن لوسائل الإعلام الرقمية أن تعلم مفاهيم الأمن السيبراني للمعلمين والطلاب و العوائل. (بوررضا كريم سرا، ١٣٩٢، ص ١٠-٢٤؛ قائمي نيا، ١٤٠٠، ص ٧٢).

٢-٥. وسائل الإعلام ومواجهة الحرب الناعمة في الفضاء الإلكتروني:

ومن أهم التحديات الأمنية في الفضاء الإلكتروني الحرب الإعلامية والعمليات النفسية للعدو. و تستطيع وسائل الإعلام منع انتشار المعلومات الكاذبة وتقويض ثقة الجمهور من خلال إنتاج محتوى سليم ومحاربة الشائعات والأخبار المزيفة (أباذري وآخرون، ١٣٩٥: ص ٣٨). أحد أهم التهديدات في الفضاء الإلكتروني هو الحرب الناعمة والهجمات المعلوماتية. يؤثر انتشار المعلومات المضللة أو الأخبار المزيفة على تفكير الناس ومعتقداتهم. يُعدّ محور الإعلام في الدفاع السلبي فعّالاً في الحدّ من آثار هذه الهجمات من خلال إنشاء وسائط آمنة واستخدام الأمن السيبراني لمنع التلاعب بالمعلومات. (عبداللهي، ١٣٩٢، ص ٢٨٥).

٣-٥. حماية البنية التحتية للإعلام من الهجمات الإلكترونية:

تشكل الوسائط التعليمية، بما في ذلك أنظمة التعلم عبر الإنترنت وشبكات المعلومات في المدارس والجامعات، أهدافا مهمة للهجمات الإلكترونية. إن حماية هذه البنى التحتية في إطار الدفاع السلبي يتطلب استخدام برامج مكافحة البرامج الضارة وجدران الحماية وتصميم بروتوكولات الوصول الآمن وإنشاء نسخ احتياطية من بيانات الوسائط (أنوشاو وآخرون، ١٤٠٠، ص ٢-٦). و تمنع هذه الإجراءات تسرب المعلومات الحساسة و تحد من الهجمات الإلكترونية على أنظمة إدارة التعلم. وتعتبر وسائل الإعلام الرقمية والمؤسسات الإخبارية أيضًا أهدافا رئيسية للهجمات الإلكترونية. ويعد تطوير الدفاع السيبراني في وسائل الإعلام الوطنية وزيادة أمن البنية التحتية للمعلومات أمرا ذا أهمية خاصة. وأظهرت الدراسات أن وسائل الإعلام الوطنية ينبغي أن تعطي الأولوية لاستراتيجيات الدفاع السلبي مثل تشفير البيانات ومكافحة اختراقات البرامج الضارة وإنشاء بروتوكولات أمنية قوية. (نوروستا و السلطاني، ١٤٠٢: ص ٥٠).

٤-٥. تحديات وسائل الإعلام في مجال الأمن السيبراني والدفاع السلبي:

وبالإضافة إلى دورها الإيجابي، تواجه وسائل الإعلام أيضًا بعض التحديات، بما في ذلك استخدام وسائل الإعلام في عمليات التسلل الإلكتروني والدعاية الخبيثة من قبل مجموعات القرصنة ونشر الأخبار الكاذبة والتأثير على الرأي العام، والافتقار إلى التثقيف المناسب للمستخدمين حول التهديدات الأمنية والخصوصية (خواجة وأنباراكي، ١٣٩٩: ص٤٨).

٥-٥. عناصر الأمن السيبراني المتعلقة بالدفاع السلبي:

يشمل الدفاع السلبي في مجال الأمن السيبراني حلولاً وقائية ودفاعية وتفاعلية يتم تنفيذها بهدف تقليل نقاط الضعف وزيادة القدرة على الصمود في مواجهة التهديدات السيبرانية. في مجالين رئيسيين:

١-٥-٥. التدابير الوقائية:

هدف الدفاع السلبي؛ تقليل احتمالية التهديدات السيبرانية ومنع المهاجمين من الاختراق والذي يتضمن تدابير مثل:

- أمان الأجهزة: استخدام معدات مقاومة للهجمات الإلكترونية مثل جدران الحماية المادية وأجهزة التوجيه الآمنة و وحدات الأمان التي تمنع التطفل غير المصرح به.
- أمان البرامج: تثبيت وتحديث برامج الأمان وبرامج مكافحة البرامج الضارة وبروتوكولات التشفير بشكل مستمر لحماية البيانات والأنظمة.
- تثقيف المستخدمين: زيادة مستوى الثقافة السيبرانية لدى المعلمين والطلاب والمدراء التعليميين للتعرف على تهديدات الفضاء الإلكتروني ومراقبة السلوكيات الآمنة في البيئة الرقمية (الأباذري وآخرون، ١٣٩٥: ص ٤٢).

٢-٥-٥. التدابير الدفاعية والتفاعلية:

تم تصميم هذه التدابير لتحديد ومراقبة و تخفيف تأثير التهديدات السيبرانية بعد وقوع الهجوم وتتضمن الحلول ما يلي:

- أنظمة اكتشاف التطفل (IDS): تعمل هذه الأنظمة على اكتشاف أي نشاط غير عادي في شبكات المعلومات وتحذر من أي تطفل محتمل.
- استعادة البيانات والنسخ الاحتياطي:

إنشاء نسخ احتياطية منتظمة للمعلومات الحساسة في المؤسسات التعليمية لتقليل الأضرار الناجمة عن الهجمات الإلكترونية وتسريع عملية استعادة البيانات.

- خطط إدارة الأزمات: وضع سياسات استجابة سريعة وخطط طوارئ للحد من آثار الهجمات السيبرانية والحفاظ على استقرار الأنظمة التعليمية والمعلوماتية (مرداني و عيوضي، ١٣٩٥: ص ٦٠). تلعب التدابير الوقائية والدفاعية والتفاعلية في إطار الدفاع السلبي دورًا هامًا في تعزيز الأمن السيبراني، والحد من التهديدات، والحفاظ على استقرار المعلومات في المؤسسات التعليمية والإدارية والتربوية. سيساعد تنفيذ الحلول في تقليل نقاط الضعف وزيادة جاهزية المستخدم والاستجابة السريعة للهجمات الإلكترونية.

الخاتمة:

الفضاء الإلكتروني، باعتباره أحد أهم مكونات الحياة الحديثة، طرح تحديات واسعة في مجالات الأمن والتعليم والإدارة والأخلاق والتربية. و وفقًا لنتائج وإنجازات هذا البحث فإن المؤسسات التعليمية والتدريبية والإدارية، باعتبارها مراكز مسؤولة عن تثقيف وتدريب جيل المستقبل، معرضة لتهديدات إلكترونية، مثل: اختراق المعلومات و كشف الخصوصية ونشر الأخبار الكاذبة والتغيرات في الأنماط السلوكية والعادات الاجتماعية والأسرية والثقافات والأفكار والحجاب والعفة و الحياء. وقد أثرت هذه التهديدات على أمن المعلومات و الصحة النفسية و و سائر الأمور الثقافية للمستخدمين. ولمعالجة هذه التحديات، هناك حاجة إلى تصميم وتنفيذ أنظمة أمنية فعالة وشاملة في المؤسسات التعليمية (في المجالين التعليمي والنفسي).

الحل: تعزيز أمن الأجهزة والبرمجيات وتعليم الثقافة السيبرانية و وضع سياسات رقابية على وسائل الإعلام والمنصات التعليمية و استخدام وسائل الإعلام لتعزيز ثقافة الأمن الرقمي وتعزيز الدفاع السلبي والأمن السيبراني. إن تعليم الثقافة الإعلامية وتعزيز الوعي العام يمنعان انتشار التهديدات السيبرانية. يتطلب الأمن السيبراني في المؤسسات التعليمية اتخاذ تدابير وقائية وتدريب مكثف واستخدام أدوات دفاعية. الحل الأهم لتعزيز أمن الأجهزة والبرمجيات هو محو الأمية السيبرانية و وضع سياسات رقابية على وسائل الإعلام والمنصات التعليمية واستخدام وسائل الإعلام لتعزيز ثقافة الأمن الرقمي. يتطلب تعزيز الأمن الرقمي في المؤسسات التعليمية والإدارية تعاونًا بين مختلف الإدارات والمديرين

والمسؤولين والمعلمين. يُسهم استخدام الأدوات الدفاعية في تقليل نقاط الضعف وتعزيز الأمن في الفضاء الإلكتروني. ويُعد دور وسائل الإعلام في الدفاع السلبي والأمن السيبراني بالغ الأهمية. ومن خلال تدريس محو الأمية الإعلامية وتعزيز الوعي العام، فإنه يساعد على منع التهديدات الإلكترونية. وباعتبارها أداة مهمة في الإعلام وبناء الثقافة فإنها تلعب دوراً رئيسياً في الحد من آثار الهجمات الإلكترونية والحرب الناعمة في الفضاء الإفتراضي.

قائمة المصادر والمراجع

١. اباذري، علي و خاك‌پور، محمدعلي و آزادخواه، شهريار، تبيين نقش رسانه‌ها در نهادينه كردن فرهنگ پدافند غيرعامل، كنفرانس پدافند غيرعامل و توسعه پايدار، تهران،١٣٩٥.

٢. احمدزاده كرماني، روح الله محمد صادق اسماعيلي، فرهنگي شدن سياست خارجي رويكردي نرم اقتدارانه تهران پژوهشكده ي مطالعات و تحقيقات بسيج دانشگاه امام صادق عليه السلام ١٣٨٧.

٣. افتخاري، اصغر، استراتژي ملي براي تأمين امنيت در فضاي مجازي، تهران، پژوهشكده ي مطالعات راهبردي، ١٣٨٢.

٤. اقتداري، علي‌محمد. سازمان و مديريت. تهران: مولوي، ١٣٩٢.

٥. انوشا، سهيل ومهنوش نيكجو و روح اله كوليوند، استراتژی امنيت سايبری، سومين همايش ملي تحقيقات ميان رشته اي در علوم مهندسي ومديريت،١٤٠٠.

٦. بل، ديويد،در آمدي بر فرهنگ هاي سايبر، ترجمه مسعود كوثريو حسين حسني،تهران: جامعه شناسان،١٣٨٩.

٧. پوررضا كريم سراء ناصر (١٣٩٢) تاثيرپذيري تغييرات فرهنگي و سبك زندگي از فضاهاي مجازي فصلنامه رسانه هاي نوين و فرهنگ، سال اول شماره ٣، ١٣٩٢.

٨. ثقفي، كاميار، فضاي مجازي؛ فرصت يا تهديدي براي خانواده مجله پاسدار إسلام، شماره سيصد و شصت و هفت پايگاه اطلاع رساني حوزه، ١٣٩١.

٩. جلالي فراهاني امير حسين، تأملي بر فيلترينگ: ١ اقدام پيشگيرانه از جرايم رايانه اي مركز پژوهش هاي مجلس شوراي إسلامي، شماره ي ٨٣٧١، ١٣٨٦.

١٠. حجازيان، پيام، مديريت خطرهاي سايبري انتشارات دانشگاه و پژوهشگاه دفاع ملي، ١٤٠٢.

١١. خلجي، ليلا، بررسي تهديدها و فرصت‌هاي فضاي مجازي بر جامعه و افراد، اولين همايش ملي راهبردهاي آموزشي و پژوهشي در آموزش و پرورش، اهواز، ١٤٠٣.

١٢. خواجه، احمدو ليلا انباركي، بررسي جايگاه و نقش رسانه درتوسعه فرهنگ پدافندغيرعامل،١٣٩٩.

١٣. دريفوس،هيوبرت.درباره اينترنت، ترجمه علي فارسي نژاد،تهران:ساقي، ١٣٨٩.
١٤. رضازاده، محمد و مرادنژادي، يوسف و مرادنژادي، محمدرضا، نقش پليس در مقابله با جرم فيشينگ،،١٤٠٠.
١٥. رضايي، علي،مديريت امنيت در محيطهاي آموزشي، انتشارات مدرسه، ١٣٩٨.
١٦. زارع، امير و ميرزائي، كمال، مكانيزم حملات فيشينگ و ويژگي حملات در سرقت اطلاعات، سومين كنفرانس بين‌المللي نوآوري و تحقيق در علوم مهندسي،١٣٩٨.
١٧. شرودر،كيت اي،كليدهاي همراهي و مراقبت از نوجوانان در اينترنت. ترجمه فرناز فرود. نشر صابرين، تهران،١٣٨٣.
١٨. شعاري نژاد علي اكبر، مياني روان شناختي تربيت، تهران، موسسه مطالعات و تحقيقات فرهنگي، ١٣٦٦.
١٩. شه ميري لجي، سهيلا، بررسي فرصت‌ها و تهديدهاي تربيتي در فضاي مجازي، نشريه مطالعات علوم اجتماعي،١٤٠١.
٢٠. شوراي عالي انقلاب فرهنگي،سند تحول بنيادين آموزش و پرورش،١٣٩٠.
٢١. صفدري، اميرحسين، نگاهي مختصر به جرم فيشينگ، سيويليكا، ١٤٠٢.
٢٢. طارمي، محمد حسين، فضاي سايبر، آسيب ها و مخاطرات فصلنامه ره آورد نور، شماره ٣٢، ١٣٨٧.
٢٣. عارفي نژاد، سيدمجيد و كمالي، علي و رحماني بلوط حصار، ابراهيم، بررسي امنيت سايبري؛ چالش‌ها و راهكارها، پانزدهمين كنفرانس ملي و دومين كنفرانس بين‌المللي فرماندهي و كنترل ايران، تهران،١٤٠٣.
٢٤. عبداللهي، ابوطالب،بررسي جنگ نرم در انديشه مقام معظم رهبري،قم، انتشارات زمزم هدايت.١٣٩٢.
٢٥. عزيزي، مرتضي، سايبر تروريسم يا تروريسم اينترنتي، تهران: معاونت سياسي نهاد نمايندگي مقام معظم رهبري در دانشگاها، ١٣٨٨.
٢٦. غفاري گردويشه، زكريا و محمدي ماشمياني، آرمين و محبي مقدم ناشي، مهوش، رويكردهاي آموزشي براي مقابله با تهديدات فضاي مجازي و حفاظت از دانش آموزان، اولين همايش بين‌المللي افق‌هاي نوين در آموزش و پرورش، ١٤٠٢.
٢٧. قائمي نيا،عليرضا، الهيات سايبري، تهران: كتابخانه موزه و مركز اسناد مجلس شوراي إسلامي،١٤٠٠.
٢٨. كمال، حامد و كمال، محمد، امنيت سايبري، سيماي فلق،١٤٠٢.
٢٩. كمالي زاده، سلمان و شاه محمدي، غلامرضا و كمال زاده تختي، حسام‌الدين، مروري بر روش‌هاي حمله فيشينگ و مقابله با آن‌ها، سومين همايش ملي كامپيوتر، سنندج،١٣٩٤.

٣٠. كمالي، سيد تقي، ١۴٠٣، امنيت سايبري و حفاظت از داده‌ها، پشتيبان، ١٤٠٣.
٣١. گل‌پايگاني، اكبر، جامعه صنعتي و جامعه اطلاعاتي، فصلنامه فرهنگ سال دوازدهم شماره ۴٣، ١٣٨١.
٣٢. لين‌چ،مايكل پاتريك.اينترنت ما:اطلاعات زيادو فهم كم در عصركلان داده ها،ترجمه حامد قديري، تهران: اسم،١٣٨٩.
٣٣. محمدي ماشمياني، آرمين، فرصت‌ها و تهديدهاي فضاي مجازي بر هويت و آموزش دانش‌آموزان و دانشجويان، سيويليكا، ١٤٠٢.
٣٤. مرداني، علي و عيوضي، رضا، مديريت امنيت سايبري و پدافند غيرعامل در زيرساخت‌هاي آموزشي، پژوهشكده مديريت راهبردي،١٣٩٥.
٣٥. موحدي نيا، جعفر،اصول و مباني پدافندغيرعامل، دانشگاه صنعتي مالك اشتر، تهران، ١٣٨٦.
٣٦. موسوي، سيد علي، امنيت سايبري، انتشارات نسل روشن،١٤٠٢.
٣٧. نوروززاده گيل ملك، علي محمد، آموزش كاربردي امنيت فناوري اطلاعات، كتابراه،١٤٠١.
٣٨. نوروستا، حسين و سلطاني، ايمان، راهبردهاي پدافند غيرعامل در حوزه محافظت از زيرساخت رسانه ملي، سيويليكا، ١٤٠٢.
٣٩. وظيفه دان، سارا، انواع تهديدات در فضاي سايبري و راهكارهاي مقابله با آن، كنفرانس ملي پدافند غيرعامل در قلمرو فضاي سايبر، مراغه، ١٣٩٥.