أهمية دور أمن المعلومات في حماية الأنظمة والمنصات التعليمية الرقمية

أ. عبد الرؤوف محمد الغرياني
abdo.algharyani@gmail.com
عضو هيئة تدريس، جامعة الرفاق الأهلية للعلوم التطبيقية والإنسانية – ليبيا

المستخلص:

تستقصي هذه الورقة البحثية الدور المحوري لأمن المعلومات في تحصين أنظمة التعليم الإلكتروني، بالتزامن مع التحول الرقمي المتسارع واتساع رقعة الاعتماد على المنصات التعليمية محليًا في دولة ليبيا ودوليًا. وتهدف الدراسة إلى تحليل المفاهيم الجوهرية للأمن السيبراني، وتشخيص التهديدات الأمنية الناشئة التي تواجه الفضاء التعليمي الرقمي، مع استعراض حزمة من الأدوات والتقنيات الدفاعية، والسياسات الحكومية اللازمة لامتثال المؤسسات التعليمية للمعايير الأمنية. تعتمد الدراسة منهجية تحليلية تستعرض حالات دراسية واقعية (Case Studies) شهدتها البيئة التقنية في ليبيا خلال السنوات الأخيرة، موثّقةً الآثار المترتبة على الهجمات السيبرانية التي استهدفت المنصات التعليمية. وقد خلصت الدراسة إلى مجموعة من النتائج الجوهرية؛ أبرزها حتمية الاستثمار الاستراتيجي في البنية التحتية الأمنية، بوصفها ركيزة أساسية لضمان استمرارية الأعمال (Business Continuity). كما كشفت النتائج عن الدور الحاسم للعامل البشري، مؤكدةً أن رفع مستوى الوعي الأمني لدى المعلمين والطلاب يمثل خط الدفاع الأول للحد من مخاطر الهندسة الاجتماعية. علاوة على ذلك، توصلت الدراسة إلى أهمية دمج التقنيات الناشئة، مثل سلاسل الكتل (Blockchain) والذكاء الاصطناعي (AI)، لتعزيز مستويات التشفير واكتشاف الاختراقات بشكل استباقي. وتختتم الورقة بتقديم إطار عملي يتضمن استراتيجيات وتوصيات تهدف إلى تحقيق توازن متكامل بين متانة البنية التحتية التقنية، والوعي البشري، والحلول البرمجية المتقدمة، بما يضمن حماية خصوصية البيانات التعليمية واستدامة البيئة الرقمية.

الكلمات المفتاحية: أمن المعلومات، البلوك تشين، التعليم الإلكتروني، حماية البيانات الشخصية، الذكاء الاصطناعي، الهجمات السيبرانية.

Abstract:

This research paper investigates the pivotal role of information security in fortifying e-learning systems, amid the rapid digital transformation and the expanding reliance on digital educational platforms both globally and specifically within the State of Libya. The study aims to analyze the fundamental concepts of cybersecurity and diagnose emerging security threats facing the digital educational landscape. Furthermore, it reviews a suite of defensive tools, technologies, and governance policies essential for ensuring institutional compliance with established security standards. The study employs an analytical methodology, examining real-world case studies within the Libyan technological environment in recent years, documenting the ramifications of cyberattacks targeting educational platforms. The findings yield several core insights, most notably the imperative of strategic investment in security infrastructure as a

fundamental pillar for ensuring business continuity. Additionally, the results highlight the critical role of the human element, asserting that enhancing cybersecurity awareness among educators and students constitutes the primary line of defense in mitigating social engineering risks. Moreover, the study concludes that integrating emerging technologies, such as Blockchain and Artificial Intelligence (AI), is vital for bolstering encryption levels and enabling proactive intrusion detection. The paper culminates in proposing a practical framework that encompasses strategies and recommendations aimed at achieving an integrated balance between robust technical infrastructure, human awareness, and advanced software solutions, thereby ensuring the privacy of educational data and the sustainability of the digital environment.

Keywords: Artificial Intelligence (AI), Blockchain, Cyberattacks, E-learning, Information Security, Personal Data Protection.

1. المقدمة:

أصبحت منصات التعليم الإلكتروني إحدى الركائز الأساسية في تطوير المجتمعات الحديثة، إذ تتيح فرص التعلم المرن والوصـــول إلى المعرفة دون قيود زمانية أو مكانية. ومع ذلك، فإن الاعتماد المتزايد على المنصـــات الرقمية يفتح المجال أمام تهديدات أمنية قد تؤثر في جودة العملية التعليمية وخصوصية المستخدمين. وتهدف هذه الدراسة إلى تحليل دور أمن المعلومات في حماية أنظمة منصات التعليم الإلكتروني، من خلال استعراض المفاهيم الأساسية، والتهديدات، والأدوات، والسياسات، والدراسات التطبيقية (Chen, Ramamurthy, & Wen, 2012).

2. المنهجية وإطار العمل التحليلي:

تعتمد هذه الدراســة على المنهج الوصــفي التحليلي القائم على اســتخبارات المصــادر المفتوحة (Open Source Intelligence – OSINT)، وهو نهجٌ منهجيٌّ يعتمد على تجميع وتحليل البيانات المتاحة علنًا لإنتاج رؤى أمنية استباقية. وتهدف المنهجية إلى رسم خريطة للمهددات السيبرانية (Cyber Threat Landscape) في البيئة المحلية من خلال مسارات تقنية وإحصائية محددة.

1.2. مصادر البيانات وأدوات الرصد:

اعتمدت الدراسة على استراتيجية تثليث البيانات (Data Triangulation) لضمان دقة النتائج، من خلال دمج مصادر متعددة تشمل:

1.1.2. المنصــات العالمية والاســتخباراتية: تم اســتقاء البيانات من منصــات متخصــصــة في رصــد الثغرات (Vulnerability Scanning) والأنشطة الخبيثة، ومزوّدي حلول الحماية الاستباقية، مع التركيز على مؤشرات الخطورة الصادرة عن مختبرات عالمية مثل (SOCRadar Labs, 2025).

2.1.2. الاســتخبارات العميقة (Deep & Dark Web): شــملت المنهجية تتبّع البصــمات الرقمية والبيانات المسرّبة المرتبطة بالنطاقات الوطنية ضمن منتديات وقواعد بيانات الإنترنت المظلم.

3.1.2. المؤشرات الوطنية والدولية: لضمان مواءمة التحليل التقني مع السياق الاستراتيجي، تم الاستناد إلى تقارير الهيئة الوطنية لأمن المعلومات (NISSA, 2024) لتقييم الوضع المحلي، بالإضافة إلى "مؤشر الأمن السيبراني الوطني" الصادر عن أكاديمية الحوكمة الإلكترونية الإستونية (EGA, 2025) كمرجع للمقارنة المعيارية (Benchmarking).

2.2. معالجة البيانات وتحليل المؤشرات:

خضعت البيانات المجمعة لعمليات معالجة دقيقة ركزت على المؤشرات التقنية للسياق (Technical Context Indicators)، وشملت:

1.2.2. تصنيف الأصول الرقمية: تنظيم أسماء النطاقات (Domain Names)، وعناوين IP، وعناوين URL.

2.2.2. التحليل الكمي والنوعي: استخراج أنماط الهجمات وتصنيفها حسب نوع المهدِّد (Threat Actor) أو نوع الثغرة.

3.2.2. التحليل المقارن (Longitudinal Analysis): إجراء مقارنة زمنية بين عامي 2024 و2025 لرصد الفجوات الأمنية وقياس تطور منحنى التهديدات، مما يتيح تحديد فاعلية الإجراءات التصحيحية المتخذة خلال هذه الفترة.

3.2. المحددات والاعتبارات المنهجية:

تلتزم الدراسة بمبدأ الشفافية العلمية عبر توضيح المحددات التالية:

1.3.2. نطاق المسح: تمثل النتائج مسحًا شاملًا للأنشطة المرصودة عبر أدوات الـOSINT، وهي تخضع لعوامل تقنية مثل التوزيع الجغرافي لبروتوكولات الإنترنت وطبيعة العينات المتاحة وقت الرصد.

2.3.2. الطبيعة الاسترشادية: تُعد هذه النتائج مؤشرات استراتيجية تهدف إلى دعم صُنّاع القرار ورسم السياسات العامة، ولا تُعد بديلًا عن التحقيقات الجنائية الرقمية (Forensics) أو التحليلات التشغيلية العميقة التي تُجريها مراكز العمليات الأمنية (SOC) داخل المؤسسات.

3. الدراسات السابقة (Literature Review):

تم استخدام العديد من المنهجيات المشابهة في الدراسات السابقة، التي تعتمد على تحليل بيانات المصادر المفتوحة (OSINT) ورصد الهجمات والثغرات، خاصة في برامج الماجستير والبحوث الجامعية. ومن أبرزها ما صدر عن الجامعة الليبية الدولية (LIMU) في بنغازي، وجامعة طرابلس، حيث ركزت هذه الدراسات على تحليل المخاطر، وتقييم البنية التحتية الرقمية، واستخدام مؤشرات دولية مثل ISO/IEC 27001 وISO/IEC 27002 لتقييم الوضع الأمني. وقد تم تصنيف هذه الدراسات على النحو التالي:

1.3. برنامج الدراســـات العليا في الأمن الســـيبراني – الجامعة الليبية الدولية (LIMU): ركزت أبحاث هذا البرنامج على تحليل بيانات المصادر المفتوحة لرصد الهجمات السيبرانية في ليبيا. وتضمنت منهجية مشابهة لما ذُكر، حيث اعتمدت على تتبّع عناوين IP، والنطاقات، والثغرات الأمنية لرصد الأنشطة الخبيثة. كما تم الاستفادة من منصات عالمية لرصد الهجمات، مع إجراء مقارنات زمنية لقياس تطور الوضع الأمني.

2.3. ماجســـتير الأمن الســـيبراني – جامعة طرابلس: تناولت بعض الرســـائل الجامعية في هذا البرنامج تحليل المخاطر السيبرانية باستخدام أدوات OSINT، مع التركيز على المؤسسات الحكومية والمالية. واعتمدت على جمع البيانات من منصات كشف الثغرات، وتحليلها وفق معايير دولية مثل ISO/IEC 27001 وISO/IEC 27002. كما تضمنت دراسات حالة محلية حول الهجمات التي استهدفت البنية التحتية الرقمية في ليبيا.

3.3. دراسات تحليلية حول الأمن السيبراني في ليبيا (أبحاث أكاديمية مشتركة): ركزت بعض الأبحاث المنشورة ضمن تقارير أكاديمية محلية على استخدام OSINT لرصد الهجمات، خاصة في قطاع التعليم والقطاع الحكومي. واعتمدت على مقارنة بيانات من سنوات مختلفة (2023–2025) لرصد تطور التهديدات، كما أبرزت دور الوعي الأمني والبنية التحتية في مواجهة الهجمات.

4. مفهوم أمن المعلومات:

1.4. تعريف أمن المعلومات: هو مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية البيانات من الوصـول غير المصرح به، أو التعديل، أو التدمير.

2.4. المبادئ الأساسية:

1. **السرية:** ضمان عدم وصول غير المصرح لهم إلى المعلومات والبيانات الحساسة.
2. **السلامة:** الحفاظ على دقة البيانات وعدم تغييرها أو العبث بها.
3. **التوافر:** ضمان وصول المستخدمين إلى المعلومات والخدمات في الوقت المناسب وفي أي مكان.

3.4. العلاقة مع التعليم الإلكتروني: يعتمد التعليم الإلكتروني على بيانات حســـاســـة، مثل معلومات الطلاب والمعلمين، مما يجعل أمن المعلومات ضرورةً أساسيةً.

5. التهديدات الأمنية في الأنظمة والمنصات التعليمية الرقمية:

تشـــمل أبرز التهديدات الأمنية التي تواجه المنصـــات التعليمية هجمات التصـــيد الاحتيالي، والبرمجيات الخبيثة، وهجمات حجب الخدمة (Risk Based Security, 2023)، وهي على النحو التالي:

1.5. الهجمات الســيبرانية: تُعد الهجمات الســيبرانية من أبرز التهديدات، حيث تعتمد على العديد من الأســاليب، مثل التصيد الاحتيالي، والبرمجيات الخبيثة، وهجمات حجب الخدمة الموزعة (DDoS).

2.5. اختراق الحسابات: يؤدي اختراق الحسابات إلى تسريب العديد من البيانات، مثل سرقة الهوية الأكاديمية أو الوصول غير المصرح به إلى بيانات الطلاب.

3.5. التهديدات الداخلية: توجد العديد من التهديدات الداخلية التي قد تحدث، سواء من الموظفين أو الطلاب، الذين قد يستغلون صلاحياتهم بشكل غير قانوني.

6. أدوات وتقنيات أمن المعلومات لحماية الأنظمة والمنصات التعليمية الرقمية:

تُعد أدوات وتقنيات أمن المعلومات الركيزة الأساسية لحماية الأنظمة الرقمية وضمان سرية البيانات وسلامتها. ومن أبرز هذه الأدوات ما يلي:

1.6. التشفير (Encryption): يمثل التشفير إحدى أهم الوسائل المستخدمة لحماية البيانات، حيث يتم الاعتماد على خوارزميات متقدمة لضمان سرية المعلومات ومنع الوصول غير المصرح به إليها أثناء التخزين أو النقل.

2.6. أنظمة كشف ومنع التسلل (Intrusion Detection and Prevention Systems – IDS/IPS): تُستخدم هذه الأنظمة لرصد محاولات الاختراق، سواء كانت داخلية أو خارجية، كما تعمل على منع الهجمات المحتملة من خلال مراقبة حركة الشبكة وتحليل الأنشطة المشبوهة.

3.6. المصادقة متعددة العوامل (Multi-Factor Authentication – MFA): تُعد المصادقة الثنائية أو متعددة العوامل من أبرز الوسائل لتعزيز حماية الحسابات، حيث تضيف طبقات إضافية من التحقق إلى جانب كلمة المرور التقليدية، مما يقلل من احتمالية اختراق الحسابات.

4.6. الذكاء الاصطناعي (Artificial Intelligence – AI): يُستخدم الذكاء الاصطناعي في تحليل الأنماط السلوكية واكتشاف الهجمات المتقدمة التي يصعب على الأنظمة التقليدية التعرف عليها بسرعة، مما يساهم في تعزيز قدرة المؤسسات على الاستجابة الفورية للتهديدات السيبرانية (Hosam El-Sofany et al., 2024; Sri Watini et al., 2024).

5.6. البلوك تشين (Blockchain): يُعد البلوك تشين من أبرز الابتكارات التقنية الحديثة التي أحدثت تحولًا في مجال أمن المعلومات، فهو عبارة عن قاعدة بيانات موزعة (Distributed Ledger) تُخزن المعلومات في شكل كتل مترابطة ومؤمنة باستخدام تقنيات التشفير (Encryption)، مما يجعل من الصعب تعديلها أو التلاعب بها بعد تسجيلها. وتعتمد هذه التقنية على مبدأ اللامركزية (Decentralization)، حيث يتم حفظ البيانات عبر شبكة من العُقد (Nodes) بدلًا من الاعتماد على خادم مركزي واحد. ويسهم هذا النموذج في تعزيز مستوى الأمان والشفافية، ويقلل من احتمالية تعرض النظام للاختراق أو الهجمات الموجهة نحو نقطة مركزية. كما يمثل البلوك تشين أداةً استراتيجيةً لتعزيز أمن التعليم الإلكتروني، من خلال ضمان نزاهة الشهادات، وحماية البيانات، وتعزيز الثقة المجتمعية. ومع ذلك، فإن نجاح تطبيقه يعتمد على الاستثمار في البنية التحتية الرقمية، وتطوير سياسات

وطنية داعمة، وتدريب الكوادر البشـــرية على إدارة هذه التقنية (Estonian e-Government Academy, 2025).

7. السياسات والإجراءات الأمنية:

تُعد السياسات والإجراءات الأمنية إطارًا تنظيميًّا ضروريًّا لضبط استخدام الأنظمة الرقمية وتعزيز مستوى الحماية داخل المؤسسات التعليمية، ومنها:

1.7. وضع سياسات أمنية واضحة: يتم تحديد مسؤوليات المستخدمين والإدارة، كلٌّ حسب مهامه وصلاحياته.

2.7. التدريب والوعي الأمني: يتم تدريب الموظفين ونشر ثقافة الأمن السيبراني بين الطلاب والمعلمين.

3.7. إدارة الحقوق والصلاحيات: يتم منح صلاحيات محدودة لكل مستخدم وفقًا لطبيعة عمله.

8. حماية خصوصية الطلاب والمعلمين:

تمثل حماية الخصوصية عنصرًا أساسيًّا في بناء بيئة تعليمية رقمية آمنة وموثوقة، تحافظ على حقوق جميع المستخدمين، وتتم هذه الحماية من خلال:

1.8. حماية البيانات الشخصية: يتم فيها حماية البيانات، مثل الأسماء، والعناوين، والسجلات الأكاديمية.

2.8. التشريعات الدولية: يتم فيها دراسة التشريعات الدولية المعتمدة، مثل القوانين الصادرة عن منظمة الإنتربول وغيرها.

3.8. التوازن بين الخصوصية وسهولة الوصول: يتم فيها ضمان حماية البيانات دون تعطيل العملية التعليمية.

9. دراسة حالات اختراق الأنظمة والمنصات التعليمية الرقمية في دولة ليبيا:

شهدت ليبيا خلال السنوات الأخيرة توسعًا ملحوظًا في استخدام المنصات التعليمية الرقمية نتيجة للتحول الرقمي في قطاع التعليم العام والخاص. إلا أن هذا التحول لم يكن مصحوبًا دائمًا بإجراءات أمنية كافية، مما جعل هذه المنصـــات عرضـــة لهجمات إلكترونية أدت إلى تســـريب بيانات آلاف الطلاب والمعلمين (SOCRadar, NISSA, 2024; Labs, 2025).

1.9. خلفية الحادثة:

تتناول هذه الفقرة الســـياق العام الذي أدى إلى ظهور الثغرات الأمنية في البيئة التعليمية الرقمية. بما أن الجامعات والمدارس الليبية بدأت تعتمد على أنظمة إدارة التعلم عن بُعد، فقد أدى ذلك إلى ظهور ثغرات أمنية نتيجة ضـــعف البنية التحتية الرقمية. وأشـــارت تقارير أمنية محلية ودولية إلى تعرض بعض المنصـــات التعليمية لاختراقات أدت إلى تسريب بيانات حساسة. كما تم تحليل بيانات 63 مؤسسة تعليمية ليبية، حيث كشف التقرير

عن وجود تهديدات سيبرانية خطيرة تتعلق بتسريب بيانات الموظفين واختراق الأجهزة. ويُعد تسريب سجلات الموظفين على مواقع خارجية من أبرز هذه التهديدات، مما يشير إلى ضعف حماية بيانات المستخدمين. كما يعكس العدد الكبير من الأجهزة المصابة (أكثر من 60 ألف جهاز) انتشار البرمجيات الخبيثة في بيئة العمل. وقد تم العثور على مؤشرات في الإنترنت المظلم (Dark Web) تدل على اهتمام جهات خبيثة بهذه المؤسسات، مما يستدعي تدخلًا عاجلًا. وشملت البيانات المسربة معلومات شخصية، مثل الأسماء، وأرقام الهوية، والسجلات الأكاديمية، والعناوين.

2.9. تفاصيل الاختراق:

استهدف الهجوم المنصات التعليمية الرقمية من خلال قاعدة بيانات مركزية غير مشفرة، حيث تم استغلال ثغرات أمنية في برمجيات غير محدثة، وفي بعض الحالات غير مرخصة. وقد أدى ذلك إلى تسريب البيانات ونشرها عبر الإنترنت، وبيعها في السوق السوداء والإنترنت المظلم (Dark Web).

3.9. التداعيات:

تتناول هذه الفقرة الآثار المترتبة على الهجمات السيبرانية على المستوى الفردي والمؤسسي، ومنها:

1. انتهاك خصوصية الطلاب والمعلمين، مما جعلهم عرضة للابتزاز والاحتيال الرقمي.
2. فقدان ثقة أولياء الأمور والطلاب في استخدام المنصات التعليمية الرقمية.
3. حدوث آثار اجتماعية سلبية نتيجة انتشار شهادات مزورة عبر الإنترنت.
4. تهديد الأمن القومي الرقمي نتيجة تزوير الشهادات والوثائق التعليمية.

4.9. أسباب الاختراق:

تسلط هذه الفقرة الضوء على العوامل الرئيسية التي ساهمت في حدوث هذه الاختراقات، ومنها:

1. ضعف البنية التحتية الأمنية للمنصات التعليمية الرقمية.
2. غياب سياسات واضحة لحماية البيانات.
3. الاعتماد على منصات خارجية غير مؤمنة، وبرمجيات غير معروفة المصدر أو غير مرخصة.
4. نقص الوعي الأمني لدى الموظفين والطلاب والمسؤولين.

5.9. الدروس المستفادة:

تقدم هذه الفقرة مجموعة من التوصيات المستخلصة لتعزيز الأمن السيبراني في البيئة التعليمية، ومنها:

1. ضرورة تطبيق تشفير قوي للبيانات داخل المنصات التعليمية الرقمية.
2. تدريب الكوادر التعليمية على تطبيق سياسات الأمن السيبراني بشكل صحيح.

3. إجراء اختبارات اختراق دورية لاكتشاف الثغرات ومعالجتها.
4. سنّ قوانين وطنية لحماية بيانات المنصات التعليمية ومستخدميها.

10. مقارنة مؤشرات الأمن السيبراني في الأنظمة والمنصات التعليمية في دولة ليبيا لسنة (2024-2025)

وفقًا لمؤشر الأمن السيبراني الوطني (Estonian e-Government Academy, 2025) وتقارير SOCRadar (2024, 2025)، لم تحقق دولة ليبيا تقدمًا جوهريًّا بين عامي 2024 و2025م، حيث ظل الأداء ضعيفًا في السياسات الوطنية وحماية البيانات، مع وجود بعض المبادرات الإيجابية في مجال البحث والتطوير الأكاديمي. حيث تم استنتاج هذه البيانات الموجودة في الجدول الأكاديمي من مقارنة بين مؤشرات الأمن السيبراني في دولة ليبيا لسنتي (2024-2025) وهي على النحو التالي:

جدول (1): مقارنة بين مؤشرات الأمن السيبراني في دولة ليبيا لعامي (2024-2025)

ر.م	المحور أو المؤشر	القيمة أو الترتيب لعام (2024)	القيمة أو الترتيب لعام (2025)	التحليل والملاحظات الختامية
1	المؤشر الوطني للأمن السيبراني (NCSI)	المرتبة 111 (21.67%)	تحسن طفيف (23.5% تقديري)	فجوة في السياسات الوطنية الشاملة وتحديث التشريعات.
2	المؤشر العالمي للأمن السيبراني (GCI)	68% (Score)	استقرار نسبي دون تقدم	انخفاض في معايير التعاون الدولي والعمليات التقنية.
3	تطوير الحكومة الإلكترونية (EGDI)	المرتبة 125 (55%)	ثبات في التصنيف	بطء في وتيرة التحول الرقمي الآمن للخدمات العامة.
4	الجاهزية الشبكية (NRI)	0%	0%	غياب البيانات أو الافتقار التام لمقومات الاستعداد الشبكي.
5	الاستراتيجية والسياسات الوطنية	غير مفعلة أو شبه غائبة	في طور الصياغة الأولية	الحاجة الماسة لإطار وطني يحكم الفضاء السيبراني.
6	حماية البنية التحتية الحيوية (CII)	25%	25%	ضعف في بروتوكولات حماية القطاعات (الطاقة، المصارف).
7	الممكنات الرقمية (Digital Enablers)	0%	0%	غياب منظومة الهوية الرقمية والتوقيع الإلكتروني.
8	الاستجابة للحوادث (Incident Response)	0%	0%	غياب فرق طوارئ وطنية (CERT) معتمدة دوليًّا.
9	إدارة الأزمات وحماية البيانات	19%	19%	غياب قانون حماية البيانات الشخصية والخصوصية.

ر.م	المحور أو المؤشر	القيمة أو الترتيب لعام (2024)	القيمة أو الترتيب لعام (2025)	التحليل والملاحظات الختامية
10	البحث والتطوير (D&R)	%60	%62	نقطة قوة نسبيّة: ناتجة عن تزايد الدراسات الأكاديمية.
11	الوعي الأمني وبناء القدرات	%0	تحسن محدود (مبادرات)	الإنسان يظل الحلقة الأضعف لغياب الحملات المنظمة.

وعليه، ومن خلال النتائج المتحصل عليها من المقارنة بين مؤشرات الأمن السيبراني في دولة ليبيا لسنتي (2024–2025)، يتضح أن الدولة لم تُحقق تقدمًا جوهريًا خلال هذه الفترة في معظم المؤشرات، حيث ظل الأداء ضعيفًا في مجالات السياسات الوطنية، وحماية البيانات، والجاهزية الشبكية. ومع ذلك، يُلاحظ وجود بعض المبادرات الإيجابية في مجال البحث والتطوير الأكاديمي، والتي يمكن أن تُشكّل قاعدةً لبناء قدرات وطنية أكثر فاعلية في المستقبل.

11. التهديدات السيبرانية المستقبلية المرتبطة بالأنظمة والمنصات التعليمية الرقمية:

تواجه المنصات التعليمية الرقمية مجموعة من التهديدات السيبرانية المعقدة والمتنوعة، من أبرزها:

1.11. التعليم عبر الأجهزة المحمولة (Mobile Learning Threats): إن الاعتماد المتزايد على الأجهزة المحمولة في العملية التعليمية يفتح المجال أمام تهديدات جديدة وخطيرة، أبرزها انتشار التطبيقات الخبيثة التي قد تستغل ثغرات أمنية في أنظمة التشغيل أو التطبيقات التعليمية نفسها، مما يؤدي إلى تسريب البيانات أو تعطيل الخدمات (Shonola & Joy, 2014).

2.11. استخدام الذكاء الاصطناعي في الهجمات (AI-driven Attacks): على الرغم من أن الذكاء الاصطناعي يمثل أداة فعالة في تعزيز الأمن السيبراني، إلا أنه يُستخدم أحيانًا في تنفيذ هجمات موجهة ضد المنصات التعليمية الرقمية. إذ يمكن للمهاجمين استغلال تقنيات الذكاء الاصطناعي في تحليل الأنماط السلوكية للمستخدمين وتطوير هجمات يصعب على الأنظمة التقليدية اكتشافها (Alotaibi, 2021).

3.11. الهجمات المتقدمة المستمرة (Advanced Persistent Threats – APT): تُعد الهجمات المتقدمة من أخطر التهديدات التي تواجه المؤسسات التعليمية الكبرى، حيث تستهدف هذه الهجمات تعطيل الأنظمة التعليمية أو سرقة البيانات الحساسة أو ابتزاز المسؤولين. وتتميز هذه الهجمات بكونها طويلة الأمد، ومنظمة، وتستخدم تقنيات متطورة للوصول إلى أهدافها بشكل دقيق (SOCRadar Labs, 2025).

4.11. الفوضى الرقمية وفقدان المصداقية التعليمية: إن استمرار الهجمات السيبرانية على المنصات التعليمية الرقمية يُشكل تهديدًا مباشرًا لاستقرار العملية التعليمية، حيث يمكن أن يؤدي إلى تعطيل الأنظمة، فقدان البيانات، أو إيقاف الخدمات التعليمية لفترات طويلة. هذه الاضطرابات التقنية تُفضي إلى ما يُعرف بـ"الفوضى الرقمية"، وهو

وضع يضعف ثقة المستخدمين في المنصات التعليمية ويُفقدها المصداقية الأكاديمية، الأمر الذي قد ينعكس سلبًا على اعتماد التعليم الإلكتروني كبديل فعّال ومستدام للتعليم التقليدي.

5.11. تزوير الشهادات والاحتيال الرقمي: تُعد بيانات الطلاب والمعلمين من أكثر الأصول الرقمية حساسية، إذ يمكن استغلالها في عمليات تزوير الشهادات التعليمية أو الاحتيال الرقمي. فالوصول غير المصرح به إلى قواعد البيانات التعليمية يتيح للمهاجمين تعديل السجلات الأكاديمية أو إنشاء شهادات مزيفة، مما يُقوض نزاهة النظام التعليمي ويُضعف الثقة في مخرجاته. هذا النوع من الهجمات لا يهدد فقط المؤسسات التعليمية، بل يمتد أثره إلى سوق العمل والمجتمع بأكمله، حيث تصبح الشهادات غير موثوقة وتفقد قيمتها (Hosam El-Sofany et al., 2024).

6.11. تهديد الثقة المجتمعية في التعليم الرقمي: تُعتبر الثقة المجتمعية ركيزة أساسية لنجاح التعليم الإلكتروني، إلا أن تعرض بيانات الطلاب والمعلمين الشخصية للاختراق أو التسريب يُشكل تهديدًا مباشرًا لهذه الثقة. فعندما يشعر المستخدمون بأن سلامة معلوماتهم الشخصية مهددة، يتراجع الإقبال على المنصات التعليمية الرقمية، ويزداد القلق بشأن الخصوصية والأمان. هذا الانخفاض في مستوى الثقة المجتمعية يُعرقل جهود التحول الرقمي في قطاع التعليم، ويُضعف قدرة المؤسسات التعليمية على تبني استراتيجيات رقمية طويلة الأمد.

12. استراتيجيات تعزيز أمن المعلومات بالأنظمة والمنصات التعليمية الرقمية:

فيما يلي مجموعة من الاستراتيجيات المقترحة لتعزيز أمن المعلومات في الأنظمة والمنصات التعليمية الرقمية:

1.12. الاستثمار في البنية التحتية الأمنية: يمثل الاستثمار في البنية التحتية الأمنية للمنصات التعليمية الرقمية أحد أهم الركائز لضمان استمرارية العملية التعليمية وحماية البيانات الحساسة. ويشمل ذلك اقتناء أنظمة حديثة للحماية مثل جدران الحماية المتقدمة، أنظمة كشف ومنع التسلل (IDS/IPS)، وحلول التشفير عالية الكفاءة. هذا الاستثمار لا يقتصر على الجانب التقني فحسب، بل يُسهم أيضًا في تعزيز قدرة المؤسسات التعليمية على مواجهة الهجمات السيبرانية المتطورة وتقليل احتمالية تعطيل الخدمات التعليمية.

2.12. التعاون مع شركات الأمن السيبراني: تُعد الشراكات الاستراتيجية مع شركات الأمن السيبراني من الوسائل الفعّالة لتطوير المنصات التعليمية الرقمية وتعزيز حمايتها. إذ تتيح هذه الاتفاقيات الاستفادة من الخبرات العالمية في مجال الأمن السيبراني، وتوفير حلول متقدمة لرصد التهديدات وتحليلها، بالإضافة إلى إجراء تقييمات دورية للبنية التحتية الأمنية. كما يُسهم التعاون في بناء قدرات محلية من خلال التدريب ونقل المعرفة، مما يعزز جاهزية المؤسسات التعليمية لمواجهة التحديات السيبرانية بشكل مستدام.

3.12. تطوير حلول متخصصة للتعليم الرقمي: يتطلب قطاع التعليم الرقمي حلولًا أمنية مصممة خصيصًا لتلبية احتياجاته الفريدة. ومن أبرز هذه الحلول أنظمة إدارة الهوية الأكاديمية، التي تضمن التحقق من هوية الطلاب والمعلمين بشكل آمن وتمنع محاولات التزوير أو الانتحال. كما يمكن تطوير منصات تعليمية مزودة بآليات حماية

متقدمة مثل المصادقة متعددة العوامل (MFA) وأنظمة مراقبة الأنشطة المشبوهة، بما يضمن بيئة تعليمية رقمية آمنة وموثوقة تدعم جودة العملية التعليمية وتحافظ على نزاهتها.

13. التوصيات:

1. إنشاء مراكز مراقبة الشبكات وحماية الأنظمة داخل المؤسسة التعليمية (NOC and SOC Room).
2. الاستعانة بالشركات والمؤسسات التي لديها خبرات في مجال الأمن السيبراني والتعليم الرقمي.
3. اعتماد تقنيات حديثة في تشفير البيانات وحمايتها من العبث او التزوير.
4. وضع خطط استجابة للطوارئ تشمل التدريب العملي والنظري على المنصات التعليمية.
5. تعزيز الوعي الأمني والتقني لدى الطلاب والمعلمين والموظفين الذين يتعاملون مع هذه المنصات التعليمية الرقمية.

14. الخاتمة:

يعد أمن المعلومات حجر الأساس في حماية أنظمة التعليم الرقمي وضمان استمرارية العملية التعليمية. ومن خلال تطبيق السياسات الأمنية والتقنيات الحديثة، يمكن للمؤسسات التعليمية مواجهة التهديدات المتزايدة وتعزيز ثقة للمستخدمين في استخدام المنصات التعليمية الرقمية. وفي ضوء ما تناولته هذه الدراسة من تحليل لمفاهيم أمن المعلومات وأثرها المباشر على حماية أنظمة التعليم الإلكترونية، اتضح أن الأمن السيبراني لم يعد خيارًا ثانويًّا، بل أصبح ضرورة ملحة لضمان استمرارية العملية التعليمية في ليبيا. لذلك أبرزت النتائج أن الاستثمار في البنية التحتية الأمنية يمثل الركيزة الأساسية لأي منظومة حماية فعّالة، وأن غياب هذا الأساس يترك المؤسسات عرضة لمخاطر جسيمة. كما أكدت الدراسة أن العنصر البشري يظل الحلقة الأضعف في مواجهة التهديدات، مما يجعل تعزيز الوعي الأمني لدى الطلاب والمعلمين جزءًا لا يتجزأ من الاستراتيجية الشاملة للأمن السيبراني.

ومن جانب آخر، أظهرت الدراسة أن التقنيات الحديثة مثل البلوك تشين والذكاء الاصطناعي يمكن أن تُحدث نقلة نوعية في تعزيز أمن المنصات التعليمية، من خلال توفير حلول مبتكرة قادرة على التصدي للهجمات المعقدة وضمان حماية البيانات. وعليه، فإن الجمع بين بنية تحتية قوية، ووعي بشري متنامٍ، وتبني أحدث التقنيات، يشكل المزيج الأمثل لتحقيق بيئة تعليمية رقمية آمنة ومستدامة.

وبذلك، تخلص الورقة إلى أن مستقبل التعليم الإلكتروني يعتمد بشكل مباشر على مدى قدرة المؤسسات التعليمية على دمج الأمن السيبراني في صميم استراتيجياتها، بما يضمن حماية المستخدمين، ويعزز الثقة في المنصات الرقمية، ويدعم استمرارية العملية التعليمية في مواجهة التحديات المتزايدة.

15. قائمة المراجع:

1.15. المراجع العربية:

1. الجامعة الليبية الدولية (LIMU). (2024). برنامج الدراسات العليا في الأمن السيبراني. تم الاسترجاع من https://mnc.limu.edu.ly/ar.
2. جامعة طرابلس. (2024). ماجستير الأمن السيبراني – قسم الشبكات. تم الاسترجاع من https://lan.uot.edu.ly/it/programdetails.php?id=594&lang=ar.

2.15. المراجع الإنجليزية:

1. Alotaibi, M. B. (2021). Cybersecurity challenges in e-learning systems: A systematic review. *Education and Information Technologies, 26*(5), 6157–6176. https://doi.org/10.1007/s10639-021-10539-2
2. Alwi, N. H., & Fan, I. S. (2010). E-learning and information security management. *International Journal of Digital Society, 1*(2), 148–156. https://doi.org/10.20533/ijds.2040.2570.2010.0020
3. Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305
4. Estonian e-Government Academy. (2025). *National Cyber Security Index (NCSI)*. Retrieved from https://ncsi.ega.ee/country/ly/?pdfReport=1
5. Hosam El-Sofany, H., El-Seoud, S. A., Karam, O. H., Bouallegue, B., & Ahmed, A. M. (2024). A proposed secure framework for protecting cloud-based educational systems from hacking. *Egyptian Informatics Journal, 27*, Article 100505. https://doi.org/10.1016/j.eij.2024.100505
6. National Information Security & Safety Authority (NISSA). (2024). *State of Libya cyber security report 2024*. Retrieved from https://nissa.gov.ly/gavedug/State_of_Libya-Cyber-Security-Report-2024.pdf
7. Risk Based Security. (2023, February 15). *DDoS attacks statistics 2022*. Retrieved from https://www.riskbasedsecurity.com/2023/02/15/ddos-attacks-statistics-2022/
8. Shonola, S. A., & Joy, M. (2014). Mobile learning security issues based on students' experiences. *International Journal of Computer & Information Technology, 3*(2), 227–237.
9. SOCRadar Labs. (2023). *Last country threat landscape report 2023*. SOCRadar.
10. SOCRadar Labs. (2025a). *Country threat landscape report 2025*. SOCRadar.
11. SOCRadar Labs. (2025b). *Cyberattack campaigns database*. Retrieved from https://socradar.io/labs/campaigns
12. SOCRadar Labs. (2025c). *Threat report – Libya*. SOCRadar.
13. Sri Watini, S., George, D., & Andersen, N. (2024). Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments. *International Transactions on Education Technology (ITEE)*. Retrieved from https://paperity.org/p/359447290/cybersecurity-in-learning-systems-data-protection-and-privacy-in-educational-information