العدد 6A مجلة دراسات في الإنسانيات والعلوم التربوية آب 2024
No. 6A Journal of Studies in Humanities and Educational Sciences August. 2024
Print ISSN 3006-3256 Online ISSN 3006-3264

التكنولوجيا السيبرانية ودورها في تأمين البيئة التعليمية الرقمية ـدراسة تحليلية لأراء عينة من أساتذة الجامعات العراقية

أ.م.د نضال عبد الله المالكي/ جامعة وارث الأنبياء، كربلاء، العراق
م.د محمد نبيل الحبوبي/ إدارة تقنيات المعلومات، الكلية التقنية الإدارية / كوفة، جامعة الفرات الأوسط التقنية
أ.م.د حسين محمد علي كشكول/ جامعة وارث الأنبياء، جامعة الكوفة، كربلاء، العراق
م.م فوزية حسين عبود الهلالي/ جامعة وارث الأنبياء، كربلاء، العراق
dr.nidhal.al.maliki@uowa.edu.iq
mohammed.haboobi@atu.edu.iq
husseinmohammed.1986@gmail.com
fawziah.al-helaly@uowa.edu.iq

المستخلص الدراسة

هدف الدراسة: تهدف هذه الدراسة إلى استكشاف دور وأهمية تكنولوجيا السيبرانية في تأمين البيئة التعليمية الرقمية، وفهم كيفية استخدامها لحماية بيانات الطلاب والأساتذة، وتوفير أمان وخصوصية في تعليم الطلاب عبر الإنترنت. **أهمية الدراسة:** في عصر التعلم الرقمي، تزايدت أهمية حماية البيئات التعليمية الرقمية من التهديدات السيبرانية المتزايدة. تمثل هذه الدراسة محاولة لتسليط الضوء على كيفية تأمين تلك البيئات وحماية البيانات التعليمية. **المنهج المتبع:** تم تنفيذ هذه الدراسة باستخدام منهج تحليلي تفسيري، حيث تم جمع وتحليل البيانات التي تم توزيعها على مجموعة من أساتذة الجامعات العراقية الاهلية والبالغ عددهم 243، كما تم تحليل البيانات باستخدام النهج الوصفي لاستخلاص المعلومات الرئيسية والاتجاهات. **أهم الاستنتاجات:** أظهرت الدراسة أن تكنولوجيا السيبرانية تلعب دورًا حيويًا في تأمين البيئة التعليمية الرقمية من التهديدات السيبرانية المتزايدة. تبني تلك التقنيات جدرانًا افتراضية لحماية البيانات وتوفير أمان للطلاب والأساتذة. **أهم التوصيات:** استنادًا إلى النتائج، يُنصح بتعزيز وتنفيذ سياسات وإجراءات أمان سيبراني دقيقة في البيئات التعليمية الرقمية. يجب توجيه الاهتمام إلى توفير التدريب المستمر للأساتذة والطلاب حول سلوكيات الأمان السيبراني. وعلاوة على ذلك، يُشدد على ضرورة التعاون المستمر مع مختصين في تكنولوجيا المعلومات للبقاء على اطلاع بأحدث التهديدات والتقنيات.

الكلمات المفتاحية: التكنولوجيا السيبرانية، البيئة التعليمية الرقمية، الجامعات العراقية.

Cyber Technology and its Role in Securing the Digital Educational Environment - An Analytical Study of the Opinions of a Sample of Iraqi University Professors

Assistant Professor Nidal Abdullah Al-Maliki/ University of Warith Al-Anbia, Karbala, Iraq
Assistant Professor Muhammad Nabil Al-Haboubi/ Information Technology Department, Technical Administrative College/Kufa, Middle Euphrates Technical University
Assistant Professor Hussein Muhammad Ali Kashkoul/ University of Warith Al-Anbia, University of Kufa, Karbala, Iraq
Assistant Professor Fawzia Hussein Abboud Al-Hilali/ University of Warith Al-Anbia, Karbala, Iraq

Abstract
Objective of the study: This study aims to explore the role and importance of cyber technology in securing the digital educational environment, understand how it is used to protect student and professor data, and provide security and privacy in student education online. Importance of the study: In the era of digital learning, the importance of protecting digital educational environments from increasing cyber threats has become increasingly important. This study represents an attempt to shed light on how to secure these environments and protect educational data.The approach followed: This study was implemented using an interpretive analytical approach, where the data that was distributed to a group of 243 professors at private Iraqi universities was collected and analyzed. The data was also analyzed using the descriptive approach to extract key information and trends. Most important conclusions: The study showed that cyber technology plays a vital role in securing the digital educational environment from increasing cyber threats. These technologies build virtual walls to protect data and provide security for students and professors. Most important recommendations: Based on the findings, it is recommended to enhance and implement careful cybersecurity policies and procedures in digital educational environments. Attention should be paid to providing ongoing training to professors and students on cybersecurity behaviors. Moreover, it stresses the need for continuous cooperation with IT specialists to stay informed of the latest threats and technologies.
Keywords: cyber technology, digital educational environment, Iraqi universities.

المبحث الأول
المنهجية العلمية للدراسة

أولاً: مشكلة الدراسة

تشهد البيئة التعليمية الرقمية تطورات سريعة مع تزايد استخدام التكنولوجيا السيبرانية لتأمين الأنظمة التعليمية. يثير هذا الارتفاع في التقنيات السيبرانية العديد من التحديات والفرص في سياق الجامعات العراقية. تهدف هذه الدراسة إلى إجراء تحليل تفصيلي لأراء أساتذة الجامعات العراقية حول دور التكنولوجيا السيبرانية في تأمين البيئة التعليمية الرقمية، لذا تتضمن تساؤلات الدراسة من خلال.

1. ما هي التقنيات السيبرانية المستخدمة حاليا في بيئة التعليم الرقمية في الجامعات العراقية؟
2. ما هو الدور المحتمل للتكنولوجيا السيبرانية في تعزيز أمان وحماية البيئة التعليمية الرقمية؟

ثانياً: أهمية الدراسة

1. يساهم الفهم العميق لآراء أساتذة الجامعات حول دور التكنولوجيا السيبرانية في تأمين البيئة التعليمية الرقمية في تعزيز الأمان الرقمي. يمكن للنتائج المستمدة من هذه الدراسة أن تسهم في تطوير استراتيجيات فعالة لمواجهة التحديات السيبرانية وتقديم بيئة تعليمية آمنة ومحمية.
2. من خلال فحص آراء الأساتذة، يمكن للدراسة أن تسلط الضوء على كيفية تحسين جودة التعليم الرقمي من خلال التكنولوجيا السيبرانية. ذلك يسهم في تعزيز تجربة التعلم للطلاب وتحقيق أهداف التعليم الفعّال.
3. يمكن للدراسة تحديد التحديات التي تواجه تكامل التكنولوجيا السيبرانية في البيئة التعليمية، وبالتالي، تقديم فرص لتطوير استراتيجيات تغلب على هذه التحديات. هذا يمكن أن يساهم في تحسين التخطيط والتنظيم لتكامل التقنيات.

4. يُظهر التركيز على آراء أساتذة الجامعات في هذا السياق كيف يمكن تحقيق تكامل فعّال للتكنولوجيا السيبرانية في النظام التعليمي. يمكن للدراسة أن تلعب دورًا حيويًا في تعزيز التكامل التكنولوجي ومواكبة التطورات الحديثة في عالم التعليم الرقمي.

ثالثاً: أهداف الدراسة

1. فحص الأدوات والتقنيات السيبرانية المستخدمة حالياً في البيئة التعليمية الرقمية في الجامعات العراقية.
2. تقييم فعالية ودور التكنولوجيا السيبرانية في تحقيق أمان وحماية للبيئة التعليمية الرقمية.
3. تحديد التحديات التي قد تواجه تكنولوجيا السيبرانية في تأمين البيئة التعليمية وتحليل كيفية التغلب عليها.
4. تقديم توصيات عملية ومبنية على النتائج لتحسين استخدام التكنولوجيا السيبرانية في تأمين البيئة التعليمية الرقمية.
5. تحليل كيف يؤثر استخدام التكنولوجيا السيبرانية في تأمين البيئة التعليمية على تجربة التعلم للطلاب والأساتذة.
6. توفير فهم شامل حول كيفية تكامل التكنولوجيا السيبرانية في بيئة التعلم الرقمية، مما يساعد في تحديد احتياجات المستقبل وتحسين استخدام التقنيات الحديثة.

رابعاً: مسوغات الدراسة

1. تزايد استخدام التكنولوجيا السيبرانية في مجالات متعددة يجعل دراستها ضرورية لفهم كيف يمكن تكاملها بشكل فعال في بيئة التعلم الرقمية.
2. زيادة التهديدات السيبرانية في مؤسسات التعليم تجعل من الضروري فحص كيفية تأمين البيئة التعليمية والتحديات التي تواجهها.
3. ازدياد الاعتماد على التعليم الرقمي يعني أن استخدام التكنولوجيا السيبرانية أصبح أحد الجوانب الرئيسية لتحسين جودة وأمان التعليم.
4. تزايد الاهتمام من قبل أساتذة الجامعات في تكامل التكنولوجيا السيبرانية يجعلهم مصدرًا ثريًا للآراء والتقييمات حول هذا الموضوع.
5. زيادة حاجة الجامعات إلى تحسين أمان بيئاتها التعليمية تجعل من الضروري دراسة تأثير واستخدام التكنولوجيا السيبرانية.
6. التحولات السريعة في السياق التعليمي في العراق تجعل من الضروري تحليل كيف يمكن تكامل التكنولوجيا السيبرانية في هذا السياق بشكل أفضل.
7. استخدام أساليب الاستقصاء وجمع آراء أساتذة الجامعات يعزز المدى الشامل والاستدلالي للدراسة.
8. توفير نتائج تشير إلى كيفية تحسين استخدام التكنولوجيا السيبرانية في السياق التعليمي يمكن أن يسهم في تطوير سياسات فعّالة في هذا المجال.

خامساً: فرضيات الدراسة

الفرضيــة الرئيســة: توجد علاقة ارتباط إيجابية بين التكنولوجيا السيبرانية وتأمين البيئة التعليمية الرقمية. وتنبثق عنها الفرضيات الآتية:

- توجد علاقة ارتباط معنوية بين الفيزياء السيبرانية وتأمين البيئة التعليمية الرقمية.
- توجد علاقة ارتباط معنوية بين التواصل الاجتماعي السيبراني وتأمين البيئة التعليمية الرقمية.
- توجد علاقة ارتباط معنوية بين الحياة السيبرانية وتأمين البيئة التعليمية الرقمية.
- توجد علاقة ارتباط معنوية بين الذكاء السيبراني وتأمين البيئة التعليمية الرقمية.
- توجد علاقة ارتباط معنوية بين الأمن السيبراني وتأمين البيئة التعليمية الرقمية.

سادساً: عينة ومجتمع الدراسة

تم تنفيذ هذه الدراسة باستخدام منهج تحليلي تفسيري، حيث تم جمع وتحليل البيانات التي تم توزيعها على مجموعة من أساتذة الجامعات العراقية الاهلية (وارث الأنبياء، البيان، المستقبل) والبالغ عددهم 243، كما تم تحليل البيانات باستخدام النهج الوصفي لاستخلاص المعلومات الرئيسية والاتجاهات.

المبحث الثاني
الإطار النظري للدراسة

اولاً: التكنولوجيا السيبرانية

1.مفهوم التكنولوجيا السيبرانية

برز مفهوم التكنولوجيا السيبرانية كقدرة عسكرية رقمية مصممة لإلحاق الضرر بالقوة العسكرية لعدو محتمل. لقد تم استخدامه كوسيلة لإضعاف القوة العسكرية للخصم من خلال شن هجمات إلكترونية وتعطيل أنظمة الكمبيوتر والشبكات الخاصة بهم. أصبح استخدام التكنولوجيا السيبرانية كمقدمة للحرب التقليدية، مع الهجمات الإلكترونية التي تسبق الضربات المادية، نهجًا استراتيجيًا. لقد تأثر تطوير ونشر القدرات السيبرانية بعوامل مثل تكلفة الحرب بالنسبة إلى العائد من النصر والتكلفة المتصورة للحرب. بالإضافة إلى ذلك، لعب توافر التكنولوجيا السيبرانية والوصول إليها، فضلاً عن عدم اليقين بشأن نجاحها، دورًا في تشكيل قرارات البلدان فيما يتعلق بتخصيص الموارد للبرامج السيبرانية والتسليح التقليدي. (Vesa, Kanniainen ،2019 :524)

ويرى (Amir, Lupovici ،2022 :154) أن التكنولوجيا السيبرانية هي استخدام أنظمة الكمبيوتر والشبكات والتقنيات الرقمية لأغراض مختلفة، بما في ذلك الاتصالات ومشاركة المعلومات وإجراء المعاملات عبر الإنترنت. وهي تشمل مجموعة واسعة من التقنيات، مثل الإنترنت وبرامج الكمبيوتر والأجهزة وأنظمة الاتصالات.

واكد (Reza .et ،2022 :9) أن التكنولوجيا السيبرانية هي استخدام التكنولوجيا في مجال الفضاء السيبراني ، والذي يشمل شبكات الكمبيوتر والإنترنت وأنظمة الاتصالات الرقمية. وهي تشمل جوانب مختلفة مثل الأمن السيبراني وتكنولوجيا المعلومات والبنية التحتية الرقمية.

في حين يرى (Xiaokang .et ،2020 :1090) أن مفهوم التكنولوجيا السيبرانية تشير إلى استخدام تقنيات الاتصالات والكمبيوتر لربط أجهزة الكمبيوتر والأجهزة الإلكترونية في مواقع مختلفة، مما يسمح بمشاركة البرامج والأجهزة وموارد البيانات وفقًا لبروتوكولات الشبكة. لقد حسنت بشكل كبير الفائدة العملية لأجهزة الكمبيوتر وتم تطبيقها على نطاق واسع في مختلف المجالات مثل النقل والتمويل وإدارة الأعمال والتعليم والاتصالات والتجارة.

- تعتبر التكنولوجيا الإلكترونية، التي تعتبر إعادة تشكيل للعوالم المادية والاجتماعية والعقلية الحالية، حقبة ناشئة لاستخدام التكنولوجيا السيبرانية لربط الأشياء الحقيقية ورسم خرائط لها بالوجود السيبراني في العالم السيبراني. لقد حدث بالفعل في مختلف المجالات مع تطوير نماذج الحوسبة الناشئة وتقنيات اتصالات المعلومات.

كما تلعب التكنولوجيا السيبرانية دورًا مهمًا في التحول الإلكتروني، حيث تعزز تكامل الأشياء الرقمية أو الكيانات السيبرانية في عالم الإنترنت. إنه مهم بشكل خاص في سياق الحوسبة الذكية والأشياء الذكية، وهي تقنيات ناشئة في البيئات الذكية.

كما تشير التكنولوجيا الإلكترونية إلى استخدام التكنولوجيا في مجال الفضاء الإلكتروني، والذي يشمل شبكات الكمبيوتر والإنترنت وأنظمة الاتصالات الرقمية. وهي تشمل جوانب مختلفة مثل الأمن السيبراني وتكنولوجيا المعلومات والبنية التحتية الرقمية. (Stosunki .et ،2022 :2)

في حسن أشار (Environ ،2022 :11) تشير الى تقنية الأمن السيبراني من خلال ممارسة حماية الشبكات والبرامج والأنظمة من الهجمات الإلكترونية. وهي تنطوي على تدابير لمنع الوصول غير المصرح به وتعديل البيانات أو حذفها وتعطيل العمليات العادية

كما تشير التكنولوجيا السيبرانية إلى استخدام أنظمة الكمبيوتر والشبكات والأجهزة الرقمية لتسهيل الاتصال ومشاركة المعلومات والأنشطة المختلفة عبر الإنترنت. (Allison .et ،2011: 298)
في حين أكد (Xiaokang .et ،2018: 119)
يمكن فهم مفهوم التكنولوجيا السيبرانية على أنه تطوير وتطبيق التقنيات التي تدمج المساحات المادية والاجتماعية والعقلية من خلال أنظمة فيزيائية إلكترونية موزعة بشكل كبير. وهي تنطوي على استخدام التقنيات الناشئة ونماذج الحوسبة مثل تقنية إنترنت الأشياء والحوسبة الذكية لإنشاء تطبيقات ممكّنة عبر الإنترنت.
كما وأضاف (Johanna .et ،2016: 32) أن مفهوم التكنولوجيا الإلكترونية هو عبارة عن استخدام التكنولوجيا وأنظمة الكمبيوتر لتسهيل الاتصالات والمعاملات والتفاعلات في الفضاء الافتراضي للفضاء السيبراني. يتضمن استخدام الشبكات الرقمية والبرامج والأجهزة لتمكين الأنشطة المختلفة مثل مشاركة المعلومات والمعاملات عبر الإنترنت والتفاعلات الاجتماعية والتجارب الافتراضية.
ويرى **الباحثون** أن التكنولوجيا السيبرانية هي استخدام التكنولوجيا وأنظمة الكمبيوتر لتسهيل الاتصالات والمعاملات والتفاعلات في الفضاء الافتراضي للفضاء الإلكتروني. يتضمن استخدام الشبكات الرقمية والبرامج والأجهزة لتمكين الأنشطة المختلفة مثل مشاركة المعلومات والمعاملات عبر الإنترنت والتفاعلات الاجتماعية والتجارب الافتراضية.

2.ابعاد التكنولوجيا السيبرانية

تشمل أبعاد التكنولوجيا السيبرانية جوانب مختلفة من عالم الإنترنت وتساهم في تقدم علوم وتكنولوجيا الإنترنت ومن هذه الابعاد وهي (Jianhua .et ،2016):

- **الفيزياء السيبرانية:** تشمل التكنولوجيا السيبرانية دراسة وتطوير الأنظمة التي تدمج المكونات المادية والإلكترونية، مثل المدن الذكية والمركبات المستقلة وأنظمة التحكم الصناعية.
- **التواصل الاجتماعي السيبراني:** تركز التكنولوجيا السيبرانية أيضًا على تأثير التكنولوجيا على التفاعلات الاجتماعية والمجتمع ككل، بما في ذلك مجالات مثل وسائل التواصل الاجتماعي والمجتمعات عبر الإنترنت ومنصات الاتصالات الرقمية.
- **الحياة السيبرانية:** يتضمن هذا البعد من التكنولوجيا السيبرانية استكشاف الواقع الافتراضي والمعزز والألعاب الغامرة والتقنيات الأخرى التي تعزز التجارب البشرية وتحولها.
- **الذكاء السيبراني:** تشمل التكنولوجيا السيبرانية تطوير أنظمة وخوارزميات ذكية يمكنها تحليل وتفسير كميات كبيرة من البيانات، وتمكين المهام مثل التعلم الآلي واستخراج البيانات والذكاء الاصطناعي.
- **الأمن السيبراني:** تتناول التكنولوجيا السيبرانية حماية الأنظمة والشبكات الرقمية من الوصول غير المصرح به وانتهاكات البيانات والتهديدات الإلكترونية الأخرى، بما في ذلك مجالات مثل التشفير وأمن الشبكة والاستجابة للحوادث.

ثانياً: تأمين البيئة التعليمية الرقمية

1. مفهوم تأمين البيئة التعليمية الرقمية

يعد تأمين بيئة التعلم الرقمي أمرًا بالغ الأهمية في سياق الاستخدام المتزايد للتكنولوجيا في التعليم. من الضروري إنشاء نظام بيئة آمنة للمعلومات والاتصالات لضمان حقوق ونوعية حياة الأفراد في التحول الرقمي للعمليات التعليمية. (Анатолий .et ،2022: 233)
لذا أصبحت قضية الأمن السيبراني حادة بشكل خاص، لأنها تتعلق بجميع مجالات الحياة والنشاط البشري تقريبًا، لا سيما في التعليم الرقمي بالكامل، يحتاج الطلاب إلى أن يكونوا بارعين في محو الأمية المعلوماتية في البيئة الرقمية، بما في ذلك فهم أهمية السلامة وأمن المعلومات، يمكن أن تكون القصص الرقمية فعالة في زيادة الوعي واستيعاب أبعاد البيئات المدرسية او الجامعية الآمنة، مما يساهم في إنشاء بيئة جمعية آمنة. (Baeva&Liudmila ،2021: 111)

لذا يرى (Elena .et ،2022 :9) تأمين البيئة التعليمية الرقمية هو مفهوم مهم في سياق التعلم الرقمي ويؤكد على الحاجة إلى الكفاءة الرقمية واسعة النطاق بين المعلمين والطلاب في العملية التعليمية. في حين أن العقبات الرئيسية التي تحول دون تعميق وتطوير الكفاءة الرقمية بكفاءة تشمل هذه العقبات عوامل مثل منطقة الإقامة، واقتصاديات الأسرة، والخلفيات الثقافية، والدوافع المتضاربة لتطوير محو الأمية الرقمية، ووصول الطلاب إلى الأجهزة والبرامج الرقمية. لذلك، يمكن الاستدلال على أن تأمين البيئة التعليمية الرقمية سيشمل معالجة هذه العقبات وتنفيذ برامج المناهج التي تعزز المهارات الرقمية في الجامعات

كما أكد (Hania .et ،2023 :114) أن تأمين البيئة التعليمية الرقمية هي تنفيذ ضوابط وصول قوية وآليات مصادقة لضمان وصول الأفراد المصرح لهم فقط إلى الموارد والأنظمة التعليمية من خلال تحديث البرامج والأنظمة وتصحيحها بانتظام لمعالجة أي نقاط ضعف يمكن استغلالها من قبل المهاجمين، وإجراء عمليات تدقيق وتقييمات أمنية منتظمة لتحديد ومعالجة أي نقاط ضعف محتملة في البيئة التعليمية الرقمية.

وأضاف (George, Veletsianos ،2016 :243) أن تأمين البيئة التعليمية الرقمية هي اعتبارًا مهمًا في تصميم واستخدام بيئات التعلم الرقمية. من خلال مناهج واعية وجريئة في تصميم واستخدام بيئات التعلم الرقمية ويمكن الاستدلال على أن تأمين البيئة التعليمية الرقمية ينطوي على ضمان خصوصية وأمن بيانات ومعلومات المتعلمين.

في حين يرى (Balasundaram ،2011 :628) أن تأمين البيئة التعليمية الرقمية يتضمن حماية المحتوى والبيانات في أنظمة التعلم الإلكتروني من الهجمات الضارة أو الوصول غير المصرح به. في سياق التعلم الإلكتروني، يعد تأمين بيانات الاختبار أمرًا في غاية الأهمية. يمكن تحقيق ذلك من خلال أنظمة المصادقة المناسبة وأساليب حماية البيانات.

وأشار (Tse .et ،2018 :121) أن تأمين البيئة التعليمية الرقمية ينطوي على تنفيذ تدابير لحماية مواد التعلم الرقمية من القرصنة والوصول غير المصرح به. تتضمن بعض المفاهيم الأساسية المتعلقة بتأمين البيئة التعليمية الرقمية ما يلي:

✓ حماية حقوق الطبع والنشر: ضمان حماية مواد التعلم الرقمية، مثل الكتب الإلكترونية، بقوانين حقوق النشر لمنع النسخ والتوزيع غير المصرح به. يمكن تحقيق ذلك باستخدام تدابير تكنولوجية مثل أنظمة إدارة الحقوق الرقمية (DRM).

✓ المصادقة والتحكم في الوصول: تنفيذ آليات مصادقة آمنة للتحقق من هوية المستخدمين والتحكم في وصولهم إلى مواد التعلم الرقمية. يمكن أن يشمل ذلك استخدام أسماء المستخدمين وكلمات المرور وطرق المصادقة الأخرى لضمان أن الأفراد المصرح لهم فقط يمكنهم الوصول إلى المواد.

✓ التشفير: استخدام تقنيات التشفير لحماية سرية وسلامة مواد التعلم الرقمية. يمكن أن يمنع التشفير الوصول غير المصرح به إلى المعلومات الحساسة ويضمن عدم العبث بالمواد أثناء النقل أو التخزين.

✓ المراقبة والكشف: تنفيذ أنظمة لرصد واكتشاف أي وصول غير مصرح به أو محاولات قرصنة في البيئة التعليمية الرقمية. يمكن أن يشمل ذلك استخدام تقنيات مثل العلامات المائية الرقمية أو آليات التتبع لتحديد وتتبع الاستخدام غير المصرح به للمواد التعليمية.

✓ التعليم والتوعي: تعزيز التعليم والوعي بين الطلاب والمعلمين وغيرهم من أصحاب المصلحة حول أهمية احترام قوانين حقوق النشر وعواقب القرصنة. يمكن أن يساعد ذلك في خلق ثقافة التعلم الرقمي المسؤول وتثبيط القرصنة.

ويرى (Svetlana, Angelova ،2022 :1122) أن تأمين البيئة التعليمية الرقمية هو مفهوم مهم في خلق بيئة تعليمية شاملة والذي يلعب الاتصال بين التعلم الرقمي والتعليم غير الرسمي دورًا مهمًا وأن تكون منظمة بشكل جيد، ومنظمة، وشخصية، وشاملة، واجتماعية. من الضروري الاستفادة من التفاعل والتكامل بين التعلم الرقمي والتعليم غير الرسمي لدعم التنمية الشخصية للطلاب بشكل فعال.

كما يعرف (Sahin .et ،2021 :12) تأمين البيئة التعليمية الرقمية هو جانب مهم لخلق بيئة جامعية آمنة. يمكن أن يساهم استخدام القصص الرقمية في تحقيق هذا الهدف من خلال زيادة الوعي واستيعاب أبعاد المدرسة او الجامعة الآمنة في مؤسسات التعليم الخاص.

وأضاف الباحثون يعد تأمين البيئة التعليمية الرقمية مفهومًا مهمًا في عالم اليوم المتقدم تقنيًا ، كما أن تأمين البيئة التعليمية الرقمية ينطوي على ضمان سلامة وحماية الأفراد في سياق التحول الرقمي في التعليم، والذي يتضمن المفهوم تدابير للحماية من المخاطر والتهديدات في بيئة المعلومات، بالإضافة إلى إنشاء بيئة آمنة للمعلومات والاتصالات. لذا فأن هنالك بعض النقاط الرئيسية المتعلقة بتأمين البيئة التعليمية الرقمية هي:

- الحاجة إلى إنشاء نظام بيئة معلومات واتصالات آمنة لضمان حقوق ونوعية حياة الأفراد في التحول الرقمي للعمليات التعليمية.
- تحليل الحالات العملية الموجودة في وسائل الإعلام لتحديد الأساليب الناجحة للحماية من المخاطر في بيئة المعلومات.
- أهمية معالجة القضايا الأمنية في البيئة التعليمية الرقمية، بما في ذلك المخاطر الاجتماعية، مثل السلوك الإدماني والعزلة الاجتماعية والأمراض العقلية والجسدية والتهديدات للصحة بسبب نقص النشاط البدني والتعرض لفترات طويلة للشاشات.
- حاجة الجامعات والمؤسسات التعليمية إلى تنفيذ السياسات والمبادئ التوجيهية بنشاط لضمان حماية الطلاب في البيئة الرقمية.

2.أهمية تأمين البيئة التعليمية الرقمية

يعد تأمين البيئة التعليمية الرقمية أمرًا بالغ الأهمية في عالم اليوم المتقدم تقنيًا من خلال الاتي: (Liudmila& Baeva ،2021 :112)

- ✓ ضمان سلامة وحماية الأفراد في البيئة التعليمية الرقمية أمر بالغ الأهمية لرفاهية ونوعية حياة الطلاب والمعلمين.
- ✓ سلط التحول الرقمي للتعليم الضوء على الحاجة إلى معالجة القضايا الأمنية، بما في ذلك المخاطر الاجتماعية مثل السلوك الإدماني والعزلة الاجتماعية والتهديدات للصحة العقلية والجسدية.
- ✓ قلة النشاط البدني والتعرض الطويل للشاشة والضغط على الرؤية والجهاز العضلي الهيكلي هي بعض التهديدات الناشئة لصحة الطلاب في بيئة التعلم الرقمية.
- ✓ تحتاج الجامعات والمؤسسات التعليمية إلى تنفيذ السياسات والمبادئ التوجيهية بنشاط لحماية الطلاب في البيئة الرقمية، بما في ذلك تدابير الاتصال في البيئة السيبرانية وحماية البيانات الشخصية.
- ✓ يعد إنشاء بيئة آمنة للمعلومات والاتصالات أمرًا ضروريًا لضمان حقوق ونوعية حياة الأفراد في سياق التحول الرقمي في التعليم.

في حين أكد (Hoang .et ،2023 :11) على أهمية تأمين البيئة التعليمية الرقمية من خلال:

- ✓ يساعد على منع الوصول غير المصرح به إلى الموارد والبيانات التعليمية، مما يقلل من مخاطر خروقات البيانات والهجمات الإلكترونية.
- ✓ من خلال تنفيذ الإجراءات الأمنية، يمكن للمؤسسات التعليمية إنشاء بيئة تعليمية آمنة عبر الإنترنت، وتعزيز الثقة بين الطلاب وأعضاء هيئة التدريس.
- ✓ إن تأمين البيئة التعليمية الرقمية يعزز أيضًا المواطنة الرقمية المسؤولة، وتعليم الطلاب السلامة عبر الإنترنت، والسلوك الأخلاقي، وأهمية حماية المعلومات الشخصية.

كما ان يرى (Svetlana& Angelova،2022 :1132) أن أهمية تأمين البيئة التعليمية الرقمية تعود من خلال:

- ✓ يعد تأمين البيئة التعليمية الرقمية أمرًا بالغ الأهمية لخلق بيئة تعليمية شاملة.
- ✓ يجب استخدام الاتصال بين التعلم الرقمي والتعليم غير الرسمي لدعم التنمية الشخصية للطلاب بشكل فعال.

✓ يجب أن تتمحور البيئة حول المتعلم، وأن تكون منظمة بشكل جيد، ومنظمة، وشخصية، وشاملة، واجتماعية.
✓ توفر الوثائق المعيارية الحالية فرصًا لتسخير الاتصال بين التعلم الرقمي والتعليم غير الرسمي بشكل فعال لدعم التنمية الشخصية للطلاب.

3. أهداف تأمين البيئة التعليمية الرقمية

حيث أشار (Sahin .et ،2021 :12) أن أهداف تأمين البيئة التعليمية الرقمية هي:

- ضمان سلامة وحماية الطلاب والموظفين في بيئة التعلم الرقمية.
- منع الوصول غير المصرح به وانتهاكات البيانات والتهديدات السيبرانية في البيئة التعليمية الرقمية.
- حماية المعلومات الحساسة والبيانات الشخصية للطلاب والموظفين من التعرض للاختراق.
- تعزيز الاستخدام المسؤول والأخلاقي للتكنولوجيا بين الطلاب والموظفين.
- إنشاء بيئة تعليمية آمنة وجديرة بالثقة عبر الإنترنت تعزز المشاركة والمشاركة.
- تنفيذ تدابير فعالة لمعالجة وتخفيف المخاطر المرتبطة بمنصات وأدوات التعلم الرقمية.

كما أكد (Lyudmila& Bokova ،2020 :275) أن من أهداف تأمين البيئة التعليمية الرقمية هي:

- تحديد الاتجاهات الفعلية لتحسين التشريعات المتعلقة بأمن المعلومات في البيئة التعليمية.
- إنشاء وتنفيذ برامج لتثقيف الأطفال والمراهقين بقواعد السلوك الآمن في مساحة الإنترنت ومنع إدمان الإنترنت.
- فهم أفضل لمصطلح سلامة البيئة التعليمية.
- إدخال مفهوم سلامة البيئة التعليمية في التداول العلمي للفقه.
- اقتراح المبادرات التشريعية ذات الصلة في مجال أمن المعلومات في التعليم.
- تحسين علم قانون المعلومات باستخدام نتائج البحوث لتعزيز العلاقات القانونية السائدة في مجال استخدام تقنيات المعلومات في التعليم.

واكد الباحثون أن أهداف تأمين البيئة التعليمية الرقمية هي:

- حماية البيانات وضمان سرية الطلاب والمعلمين في المؤسسات التعليمية.
- منع الهجمات الإلكترونية والحد من الأضرار التي تسببها هذه الهجمات في قطاع التعليم.
- تنفيذ مجموعة دنيا من التدابير لمنع الهجمات الإلكترونية والحفاظ على ميزة تنافسية في بيئة المعلومات.
- تقديم توصيات للاستخدام الآمن للشبكات الاجتماعية والممارسات عبر الإنترنت في المؤسسات التعليمية.
- تحليل إعدادات الخصوصية للأجهزة المحمولة وتقديم نصائح للاستخدام الآمن للشبكات الاجتماعية.
- التأكد من تشفير النشاط عبر الإنترنت عند الاتصال بنقاط اتصال Wi-Fi العامة.
- الحفاظ على تحديث الأنظمة لجعل اختراقها أكثر صعوبة للمهاجمين الإلكترونيين.
- اتباع سياسات وإجراءات أمان المؤسسة عند تثبيت البرامج أو المكونات الإضافية أو الإضافات.

المبحث الثالث

الإطار العلمي للدراسة

اولاً: التحليل الوصفي لاستجابات العينة

يتناول في هذا المبحث التحليل الوصفي لبيانات متغيرات الدراسة، وقد اعتمد على الوسط الحسابي الموزون والإنحراف المعياري الموزون والأهمية النسبية، وقد تم وضع معيار الحكم على درجة الموافقة على محاور الدراسة وفقا للمقياس الخماسي الذي يتضمن:

أ. إذا كان الوسط الحسابي من (1.00 – 1.80) فإن أفراد العينة هم غير متفقين جدا
ب. إذا كان الوسط الحسابي من (1.81 – 2.60) فإن أفراد العينة هم غير متفقين.
ت. إذا كان الوسط الحسابي من (2.61 – 3.40) فإن أفراد العينة هم محايدون.
ث. إذا كان الوسط الحسابي من (3.41 –4.20) فإن أفراد العينة هم متفقون.
ج. إذا كان الوسط الحسابي من (4.21 –5.00) فإن أفراد العينة هم متفقون جدا.

1.التحليل الوصفي لمتغير التكنولوجيا السيبرانية

من متابعة نتائج التحليل الوصفي ضمن الجدول (1) لبيانات التكنولوجيا السيبرانية يتضح بأن هذا المتغير سجل توجه إيجابي بشكل عام فقد بلغت قيمة الأهمية النسبيــة (75.696 %) ، بوسط حسابي عام بلغت قيمته (3.8006) ، وإنحــراف معياري (0.9404) ، وفيما يخص الأبعاد كانت كالآتي :

أ. **الفيزياء السيبرانية:** تشير النتائج إلى أنّ هنالك توجه إيجابي حول هذا البعد، فقد بلغـت قيمة الأهمية النسبية (76.907%) وسجلت قيمة الوسط الــموزون (3.845) وهي قيمة مرتفعة تتجاوز قيمة الوســط الفرضي للدراسة البالغ (3)، كما أن قيمة الإنحــراف المعياري تشير إلى ان هنالك تجانس بين البيانات فقد سجل (0.842).

ب.**التواصل الاجتماعي السيبراني:** من متابعة المؤشرات التحليلية يتضح أن هنالك توجه إيجابي حول هذا البعد فقد بلغـت الأهمية النسبية (76.257%) وسجلت قيمة الوسط الــموزون (3.813) وهي قيمة مرتفعة وتتجاوز قيمة الوســط الفرضي للدراسة البالغ (3)، كما أن قيمة الإنحــراف المعياري تشير إلى ان هنالك تجانس بين البيانات فقد سجل (0.887).

ت.**الحياة السيبرانية:** تشير النتائج إلى أنّ هنالك توجه إيجابي حول هذا البعد فقد بلغـت قيمة الأهمية النسبية (74.81%) وسجلت قيمة الوسط الــموزون (3.7407) وهي قيمة مرتفعة وتتجاوز قيمة الوســط الفرضي للدراسة والبالغ (3)، كما أن قيمة الإنحــراف المعياري تشير إلى ان هنالك تجانس بين البيانات فقد سجل (0.8913).

ث.**الذكاء السيبراني :**من متابعة المؤشرات التحليلية يتضح ان هنالك توجه إيجابي حول هذا البعد فقد بلغـت الأهمية النسبية (75.257%) وسجلت قيمة الوسط الــموزون (3.763) وهي قيمة مرتفعة وتتجاوز قيمة الوســط الفرضي للدراسة والبالغ (3)، كما أن قيمة الإنحــراف المعياري تشير إلى ان هنالك تجانس بين البيانات فقد سجل (1.0417).

ج. **الأمن السيبراني:** من متابعة المؤشرات التحليلية يتضح ان هنالك توجه إيجابي حول هذا البعد فقد بلغـت الأهمية النسبية (75.257%) وسجلت قيمة الوسط الــموزون (3.7563) وهي قيمة مرتفعة وتتجاوز قيمة الوســط الفرضي للدراسة والبالغ (3)، كما أن قيمة الإنحــراف المعياري تشير إلى ان هنالك تجانس بين البيانات فقد سجل (1.0324).

الجدول (1) نتائج التحليل الوصفي لمتغير التكنولوجيا السيبرانية

الفقرات	الوسط الموزون	الإنحراف المعياري	الأهمية النسبية
1	3.907	0.847	78.14
2	3.814	0.799	76.29
3	3.814	0.88	76.29
الفيزياء السيبرانية	**3.845**	**0.842**	**76.907**
4	4.026	0.854	80.52
5	3.66	0.909	73.2
6	3.753	0.894	75.05
التواصل الاجتماعي السيبراني	**3.813**	**0.887**	**76.257**
7	3.747	0.929	74.95
8	3.686	0.857	73.71
9	3.789	0.888	75.77

74.81	**0.8913**	**3.7407**	**الحياة السيبرانية**
76.08	0.94	3.804	**10**
75.44	1.099	3.799	**11**
73.71	1.086	3.686	**12**
75.257	**1.0417**	**3.763**	**الذكاء السيبراني**
76.23	0.87	3.855	**13**
75.98	1.056	3.769	**14**
73.71	1.098	3.645	**15**
75.257	**1.0324**	**3.7563**	**الأمن السيبراني**
75.696	**0.9348**	**3.8006**	**التكنولوجيا السيبرانية**

2.التحليل الوصفي لمتغير تأمين البيئة التعليمية الرقمية

من متابعة نتائج التحليل الوصفي لمتغير تأمين البيئة التعليمية الرقمية ضمن الجدول (2) يتضح بان هذا المتغير سجل توجه إيجابي بشكل عام، فقد بلغت قيمة الأهمية النسبيــة (73.436%)، بوسط حسابي عام بلغت قيمته (3.6713)، وانحــراف معياري (0.8933).

الجدول (2) نتائج التحليل الوصفي لمتغير تأمين البيئة التعليمية الرقمية

الفقرات	الوسط الموزون	الإنحراف المعياري	الأهمية النسبية
1	3.804	0.853	76.08
2	3.691	0.838	73.81
3	3.784	0.73	75.67
4	3.933	0.928	78.66
5	4.052	0.832	81.03
6	3.747	0.912	74.95
7	3.887	0.844	77.73
8	3.799	0.792	75.98
9	3.799	0.897	75.98
10	3.99	0.858	79.79
تأمين البيئة التعليمية الرقمية	**3.6713**	**0.8933**	**73.436**

ثانياً: إختبار علاقات الإرتباط

تم اجراء تحليل الإرتباط لبيانات البحث وذلك من أجل الوقوف على قيمة الإرتباطات البينية بين المتغيرات قبل المضي في اجراء تحليل التأثير بينها ، وكلما اقتربت درجة الإرتباط من الواحد الصحيح فإنّ يعني ان درجة الإرتباط قوية ، وفقد ابتعدت عن الواحد الصحيح واقتربت من الصفر فإن ذلك يشير إلى ضعف العلاقة بين المتغيرات ، وتشير الدراسات إلى ان العلاقات بشكل عام تكون ضعيفة في حالة كانت قيمة معامل الإرتباط اقل من (0.30) ، وان العلاقة الإرتباطية تكون متوسطة فقد كانت القيمة بين (0.30-0.70) ، وتكون العلاقة قوية في حالة قيمة الإرتباط اكبر من (0.70) .

أولا: الفرضيــة الرئيســة الأولــى

تشير نتائج التحليل ان هنالك علاقة ارتباط إيجابية بلغت قيمتها (0.810) وهي علاقة معنوية بالاعتماد على قيمة مستوى الدلالة والتي تقع قيمته ضمن قيمة القبول التي تشترط ان تكون قيمته أصغر من (0.05). وهذه النتيجة تدعم تحقق الفرضية البديلة كذلك بالنسبة للعلاقات الفرعية كانت هنالك النتائج كالآتي:

الفرضية الفرعية (1) : يتضح من النتائج تحقق هذه الفرضية حيث كانت قيمة الارتباط مرتفعة وإيجابية بلغت (0.793) وهي قيمة معنوية بالإعتماد على قيمة مستوى الدلالة الذي وقعت نتيجته ضمن منطقة القبول التي تشترط ان تكون القيمة أصغر من (0.05).

الفرضية الفرعية (2): من مراجعة النتائج التحليلية لمصفوفة الإرتباط يتضح ان هذه الفرضية قد تحققت حيث كانت قيمة الإرتباط بلغت (0.601) وهي قيمة مرتفعة وإيجابية معنوية بالإعتماد على قيمة مستوى الدلالة التي وقعت نتيجته ضمن منطقة القبول التي تشترط ان تكون القيمة أصغر من (0.05).

الفرضية الفرعية (3): يتضح من النتائج تحقق هذه الفرضية حيث كانت قيمة الإرتباط مرتفعة وإيجابية بلغت (0.700) وهي قيمة معنوية بالإعتماد على قيمة مستوى الدلالة التي وقعت نتيجته ضمن منطقة القبول التي تشترط ان تكون القيمة أصغر من (0.05).

الفرضية الفرعية (4): من مراجعة النتائج التحليلية لمصفوفة الإرتباط يتضح ان هذه الفرضية قد تحققت حيث كانت قيمة الإرتباط بلغت (0.407) وهي قيمة مرتفعة وإيجابية معنوية بالإعتماد على قيمة مستوى الدلالة الذي وقعت نتيجته ضمن منطقة القبول التي تشترط ان تكون القيمة أصغر من (0.05).

الفرضية الفرعية (5): من مراجعة النتائج التحليلية لمصفوفة الإرتباط يتضح ان هذه الفرضية قد تحققت حيث كانت قيمة الإرتباط بلغت (0.543) وهي قيمة مرتفعة وإيجابية معنوية بالإعتماد على قيمة مستوى الدلالة الذي وقعت نتيجته ضمن منطقة القبول التي تشترط ان تكون القيمة أصغر من (0.05).

المبحث الرابع
الاستنتاجات والتوصيات

اولاً: الاستنتاجات

1. توضح الدراسة أهمية استخدام التكنولوجيا السيبرانية في تأمين البيئة التعليمية الرقمية، وكيف يمكن لهذه التقنيات تحسين الأمان والحماية.
2. يظهر تحليل الدراسة وجود تحديات تكنولوجية وأمانية تواجه عملية تكامل التكنولوجيا السيبرانية في بيئة التعلم الرقمية.
3. يشير التحليل إلى أن استخدام التكنولوجيا السيبرانية يؤثر بشكل كبير على تجربة التعلم للطلاب ويساهم في تحسين فعالية التعلم الرقمي.
4. تقديم آراء أساتذة الجامعات يمثل محورًا هامًا للفهم العميق لتحديات وفرص تكامل التكنولوجيا السيبرانية في السياق الجامعي.
5. تشير الدراسة إلى ضرورة وجود استراتيجيات فعّالة لتحسين أمان البيئة التعليمية الرقمية وتعزيز استخدام التكنولوجيا السيبرانية.
6. تقديم توصيات عملية لتحسين الأمان الرقمي في السياق التعليمي يعزز إمكانية تطبيق النتائج على أرض الواقع.
7. يبرز دور الدراسة في المساهمة في تحسين السياسات التعليمية وتوجيه الجهود نحو تكامل فعّال للتكنولوجيا السيبرانية في مجال التعليم.

ثانياً: التوصيات

1. توجيه الجهود نحو تعزيز البنية التحتية السيبرانية في الجامعات العراقية لتحقيق أمان أفضل ومواكبة التقنيات الحديثة.
2. إطلاق برامج تدريبية لأعضاء هيئة التدريس لتعزيز فهمهم لتكنولوجيا السيبرانية وكيفية استخدامها بفعالية في بيئة التعلم.

3. تشجيع على تطوير ثقافة الأمان السيبراني بين الطلاب والموظفين، وذلك من خلال ورش العمل والحملات التوعية.
4. دعم الأبحاث والابتكار في مجال التكنولوجيا السيبرانية لتطوير حلول جديدة وفعّالة لتحسين الأمان في بيئة التعلم الرقمية.
5. تشجيع على التعاون مع مؤسسات دولية ذات خبرة في مجال السيبرانية لتبادل المعرفة والخبرات.
6. ضرورة تكامل استخدام التكنولوجيا السيبرانية مع سياسات التعليم الوطنية لضمان تناغم وفعالية.
7. إقامة آليات فعّالة للرد السريع على التهديدات السيبرانية، مما يعزز الاستعداد للحماية والتصدي للهجمات المحتملة.
8. ضرورة توفير دعم فني وتقني مستمر للجهات المعنية لضمان صيانة وتحديث الأنظمة السيبرانية بشكل دوري.

المصادر المراجع

1. A Comparative Study on Cyber security Technology in Big data Cloud Computing Environment. .(2022) doi: 10.1109/ic3i56241.2022.10072552
2. Cyber Technology and the European Union’s Gestaltian Approach to China. Stosunki międzynarodowe(2022), 2:10-10. doi: 10.12688/stomiedintrelat.17431.2
3. Allison, G., Dempsey., Michael, L., Sulkowski., Jack, Dempsey., Eric, A., Storch. (2011). Has cyber technology produced a new group of peer aggressors. Cyberpsychology, Behavior, and Social Networking, 14(5):297-302. doi: 10.1089/CYBER.2010.0108
4. Amir, Lupovici. (2022). Ontological security, cyber technology, and states’ responses. European Journal of International Relations, 29(1):153-178. doi: 10.1177/13540661221130958
5. Elena, Tikhonova., Marina, A., Kosycheva., Galina, I., Efremova. (2022). Digital learning environment: digital literacy, e-exclusion and cyber-wellness. doi: 10.1145/3551708.3551716
6. George, Veletsianos. (2016). Digital Learning Environments. 242-260. doi: 10.1002/9781118736494.CH14
7. Hania, Mohamed., Nickolaos, Koroniotis., Nour, Moustafa. (2023). Digital Forensics based on Federated Learning in IoT Environment. doi: 10.1145/3579375.3579387
8. Jianhua, Ma., Kim-Kwang, Raymond, Choo., Hui-Huang, Hsu., Qun, Jin., William, Liu., Kevin, I-Kai, Wang., Yufeng, Wang., Xiaokang, Zhou. (2016). Perspectives on Cyber Science and Technology for Cyberization and Cyber-Enabled Worlds. 1-9. doi: 10.1109/DASC-PICOM-DATACOM-CYBERSCITEC.2016.17
9. Johanna, Thompson, Wynne. (2016). Wired Fast And Thinking Slow: Cyber Technology And The US Army .
10. Le, Thi, Hoang, Ha. (2023). An Assessment of Information Literacy of Students in Digital Learning Environment. VNU Journal of Science: Education Research, doi: 10.25073/2588-1159/vnuer.4687

11. Liudmila, V., Baeva. (2021). The "black swan" of covid-19 and the security issues in digital learning. 3(2):110-140. doi: 10.46539/GMD.V3I2.161
12. Liudmila, V., Baeva. (2021). The "black swan" of covid-19 and the security issues in digital learning. 3(2):110-140. doi: 10.46539/GMD.V3I2.161
13. Lyudmila, N., Bokova. (2020). Legal regime of creation of a secure digital educational environment. 24(2):274-292. doi: 10.22363/2313-2337-2020-24-2-274-292
14. Reza, Hasmath., Una, Aleksandra, Bērziņa-Čerenkova. (2022). Cyber technology and the European Union's gestaltian approach to China. Stosunki międzynarodowe, 2:10-10. doi: 10.12688/stomiedintrelat.17431.1
15. S., R., Balasundaram. (2011). Securing tests in E-learning environment. 624-627. doi: 10.1145/1947940.1948070
16. Sahin, Akdag., Zehra, Altinay. (2021). Learning Through Digital Stories for Safe School Environment.. Frontiers in Psychology, 12:738954-. doi: 10.3389/FPSYG.2021.738954
17. Sahin, Akdag., Zehra, Altinay. (2021). Learning Through Digital Stories for Safe School Environment.. Frontiers in Psychology, 12:738954-. doi: 10.3389/FPSYG.2021.738954
18. Svetlana, Angelova. (2022). Digital learning and non-formal education in their connectivity for creating the inclusive learning environment. Pedagogika, 1121-1131. doi: 10.53656/ped2022-9.03
19. Svetlana, Angelova. (2022). Digital learning and non-formal education in their connectivity for creating the inclusive learning environment. Pedagogika, 1121-1131. doi: 10.53656/ped2022-9.03
20. Tse, Ho, Keung. (2018). Anti-piracy in digital learning environment .
21. Vesa, Kanniainen. (2019). Cyber Technology and the Arms Race. German Economic Review, 20(4):523-544. doi: 10.1111/GEER.12181
22. Xiaokang, Zhou., Flavia, C., Delicato., Kevin, I-Kai, Wang., Runhe, Huang. (2020). Smart computing and cyber technology for cyberization. World Wide Web, 23(2):1089-1100. doi: 10.1007/S11280-019-00773-Y
23. Xiaokang, Zhou., Guangquan, Xu., Jianhua, Ma., Ivan, Ruchkin. (2018). Scalable platforms and advanced algorithms for IoT and cyber-enabled applications. Journal of Parallel and Distributed Computing, 118:1-4. doi: 10.1016/J.JPDC.2018.03.002
24. Анатолий, Семенович, Олейник., А.Н., Шилов., Д.А., Светличный., Р.А., Макаров., А.А., Мартазаева. (2022). Cybersecurity in a digital learning environment. Управление образованием: теория и практика, 231-239. doi: 10.25726/7435-3301-1451-c