Journal of Educational and Psychological Sciences (JEPS) • Vol 7, Issue 13 (2023) • P: 98 - 73
https://journals.ajsrp.com/index.php/jeps
ISSN: 2522-3399 (Online) • ISSN: 2522-3399 (Print)

The Effectiveness of proposed electronic course to develop cognitive awareness of cybersecurity among secondary school students in the city of Jeddah

Mrs. Bayan Bakheet Almatrafi*[1], Co-Prof. Leena Ahmad Alfarani[1]
[1] Faculty of Educational Graduate Studies | King Abdulaziz University | KSA

Received: 27/11/2022
Revised: 06/12/2022
Accepted: 27/12/2022
Published: 30/04/2023

* Corresponding author: bayanmatrafiedu123@gmail.com

Citation: Almatrafi, B. B., & Alfarani, L. A. (2023). The Effectiveness of proposed electronic course to develop cognitive awareness of cybersecurity among secondary school students in the city of Jeddah. *Journal of Educational and Psychological Sciences, 7(13)*,73 – 98. https://doi.org/10.26389/AJSRP.K271122

2023 © AJSRP • National Research Center, Palestine, all rights reserved.

• Open Access

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license

Abstract: The study aimed to reveal the effectiveness of a proposed electronic course to develop the knowledge awareness of cybersecurity for female secondary school students in Jeddah, using the descriptive, analytical, and quasi-experimental approach. This is due to their relevance to the nature of the current study, and the study sample consisted of (26) female students who were deliberately chosen from the first-year secondary school students at the ninety-third secondary school in Jeddah. To achieve the objectives of the study, the two researchers applied the cybersecurity awareness test to the study sample before and after applying the proposed electronic course. The results showed that there were statistically significant differences at the significance level ($\alpha \le 0.05$) between the mean scores of secondary school students in the pre and post application of the cyber security awareness test in favor of The post application is due to the proposed electronic course And the effectiveness of the electronic course in developing cognitive awareness of cybersecurity, as the total gain value reached (1.3), which is high earning rates if compared to the minimum for Black (1.2), which indicates the effectiveness of the proposed electronic course to develop knowledge awareness of cybersecurity for secondary school students in Jeddah. The study set a set of recommendations, the most important of which is to benefit from the proposed electronic course prepared by the two researchers as a course for cyber security for female secondary school students in Jeddah and other regions of the Kingdom of Saudi Arabia.

Keywords: electronic courses- cybersecurity- high school students.

فاعلية مقرر إلكتروني مقترح لتنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية في مدينة جدة

أ. بيان بخيت المطرفي*[1]، أ.م.د/ لينا أحمد الفراني[1]
[1] كلية الدراسات العليا التربوية | جامعة الملك عبد العزيز | المملكة العربية السعودية

المستخلص: هدفت الدراسة الكشف عن فاعلية مقرر إلكتروني مقترح لتنمية الوعي المعرفي بالأمن السيبراني لطالبات المرحلة الثانوية بمدينة جدة، استخدم المنهج الوصفي التحليلي، وشبه التجريبي. وذلك لمناسبتهما لطبيعة الدراسة الحالية، وتكونت عينة الدراسة من (26) طالبة تم اختيارهن بطريقة قصدية من طالبات الصف الأول ثانوي بمدرسة الثانوية الثالثة والتسعين بجدة. ولتحقيق أهداف الدراسة قامت الباحثتان بتطبيق اختبار الوعي المعرفي بالأمن السيبراني على عينة الدراسة قبل وبعد تطبيق المقرر الإلكتروني المقترح، أظهرت النتائج وجود فروق دالة إحصائيًا عند مستوى الدلالة ($\alpha \le 0.05$) بين متوسطات درجات طالبات المرحلة الثانوية بالتطبيق القبلي والبعدي لاختبار الوعي المعرفي بالأمن السيبراني لصالح التطبيق البعدي تعزى للمقرر الإلكتروني المقترح، وفاعلية المقرر الإلكتروني في تنمية الوعي المعرفي بالأمن السيبراني، اذ بلغت قيمة الكسب الكلية (1.3)، وهي معدلات كسب عالية إذا قورنت بالحد الأدنى لبلاك Black (1.2) مما دل بفاعلية المقرر الإلكتروني المقترح لتنمية الوعي المعرفي بالأمن السيبراني لطالبات المرحلة الثانوية بمدينة جدة، وقدمت الدراسة مجموعة من التوصيات من اهمها الاستفادة من المقرر الإلكتروني المقترح الذي أعدته الباحثتان كمقرر للأمن السيبراني لطالبات مدارس المرحلة الثانوية بمدينة جدة ومناطق المملكة العربية السعودية الأخرى.

الكلمات المفتاحية: المقررات الإلكترونية- الأمن السيبراني- طالبات المرحلة الثانوية.

مقدمة.

يعد الأمن السيبراني من المفاهيم الحديثة نسبياً، وظهر في إطار الثورة الرقمية التكنولوجية المعاصرة، التي أسهمت في تدفق المعلومات بشكل كبير نظرًا لتعدد وسائل الاتصال عبر أجهزة الحواسيب، وغيرها من الأجهزة المحمولة، مما أدى إلى ظهور تحديات وتهديدات خطيرة، وظهر مفهوم الأمن السيبراني الذي أصبح محل اهتمام العديد من المؤسسات الرسمية والباحثين ومعبرًا عن الجانب الأمني المرتبط بحماية المعلومات.

إن الأمن السيبراني يشكّل جزءً أساسيًا من أي سياسة أمنية دفاعية دولية، لاسيما وأن أكثر من 130دولة حول العالم تخصص أقساماً ومرافق خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني لأي دولة لمحاربة الجرائم والقرصنة الالكترونية والاحتيال الالكتروني، وكل اشكال المخاطر السيبرانية الأخرى (شلوش، 2018).

ويستوجب الأمر توحيد الجهود في جميع الجهات لزيادة الوعي بين الأفراد بالأمن السيبراني من أجل الدفاع السريع ضد زيادة عدد الهجمات الإلكترونية. لذا من المهم تعزيز المعرفة بالأمن السيبراني من خلال برامج مصممة خصيصًا للأفراد وأيضاً للمجموعات، في كل من القطاعين الخاص والعام، ويمكن أن تكون هذه البرامج تم إنشاؤها لزيادة تثقيف الناس، ومن أجل تقليل فرص وقوعهم ضحية لمثل هذه الهجماتAlzubaidi (2021 ,).

وفي هذا الاطار فأن المملكة العربية السعودية استهدفت برؤيتها 2030 التطوير الشامل للمملكة، ومن الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية، بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية والشبكات العالمية المتجددة، وأنظمة تقنية المعلومات والتقنيات التشغيلية، ويتماشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتراسلها، وبما يهئ للتعامل مع معطيات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة، إن هذا التحول يتطلب انسيابية المعلومات وأمانها وتكامل أنظمتها، ويستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية، وتعزيزه، وحماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الاولوية والخدمات والأنشطة الحكومية، لذلك صدر امر ملكي برقم (6801) بإنشاء هيئة باسم (الهيئة الوطنية للأمن السيبراني) في تاريخ (11 صفر 1439هـ) الموافق (31 أكتوبر 2017م) ترتبط بمقام خادم الحرمين الشريفين، وهي الجهة المختصة بشؤون الأمن السيبراني في المملكة، وتعد مرجع الدولة لحماية أمنها الوطني، ومصالحها الحيوية، والبنية التحتية الحساسة فيها، وتوفير خدمات تقنية آمنه وطرق دفاعية لحماية أنظمة المعلومات والاتصالات ضد الهجمات الإلكترونية، والحفاظ على سرية وسلامة المعلومات (الهيئة الوطنية للأمن السيبراني، 2018).

وبينت دراسة جورانGoran (2017) وجود عدد من المخاطر السيبرانية لدى طلبة المرحلة الثانوية، وأهمية رفع مستوى وعي الطلبة بخصوص الأمن السيبراني، وتجنب المخاطر السيبرانية والانتهاكات التي يتعرضون لها أثناء استخدام الإنترنت. واشارت دراسة الشيتي (2019) إلى تقييم سياسات أمن وخصوصية المعلومات في مؤسسات التعليم بالمملكة العربية السعودية في مجال الأمن السيبراني، وضرورة وجود برامج توعية الموظفين وتشجيع البحوث في مجال الأمن السيبراني وأهمية تكامل وصحة البيانات في مؤسسات التعليم، وأكدت دراسة القحطاني (2019) على أهمية التوعية المستمرة بمشكلات الأمن السيبراني، وتدريس مقررات دراسية عنه أو إضافة أجزاء منه في المناهج الدراسية في المراحل التعليمية المختلفة، وبينت دراسة الصانع(2020) بضرورة تضمين أساليب واستراتيجيات حماية الطلبة من تهديدات ومخاطر الإنترنت، والتوعية بالأمن السيبراني ومفاهيمه في المقررات والمناهج الدراسية، وخلصت دراسة الزبيدي Alzubaidi(2021) إلى قياس مستوى الوعي بالأمن السيبراني للطلبة السعوديين، وأن الكثير ليس لديهم أي فكرة عن الوعي بالأمن السيبراني.

وعلى الرغم من الإيجابيات الكبيرة التي تحققت بفضل تقنية المعلومات، فإن تلك الثورة المعلوماتية المتصاعدة صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام، كظاهرة الجريمة

الرقمية نظرًا لقلة الوعي بالأمن السيبراني، والتي تصاعدت مخاطرها مما أفرز نوعًا جديدًا من الجرائم العابرة للقارات (أبو زيد، 2019).

ومن خلال البحث والتقصي، لاحظتا الباحثتان ندرة الدراسات المتخصصة في موضوع الدراسة، ومن الدراسات التي تناولت الوعي بالأمن السيبراني، دراسة الصائغ (2018)، ودراسة القحطاني (2019)، ودراسة فينتر وآخرون venter, &et al (2019)، ودراسة الجهني والفاضل Aljohani & Elfadil (2020)، ودراسة السواط وآخرون (2020)، ودراسة الزبيدي Alzubaidi (2021)، وتختلف الدراسة الحالية عن هذه الدراسات أنها تتناول مقرر إلكتروني لتنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة.

ومما لا شك فيه أن استخدام تقنيات العصر الرقمي في التعلم لم يعد أمراً اختيارياً للطلبة، ولذلك فأن الوعي والمعرفة بالأمن السيبراني يساهم في التعرف على تهديدات ومخاطر الإنترنت المرتبط بحماية المعلومات الرقمية والشبكات والخوادم، ومن المهم الحرص على وعي ومعرفة طالبات المرحلة الثانوية بالأمن السيبراني، وذلك من خلال تقديم مقرر إلكتروني؛ وبناء على ذلك فقد ظهرت الحاجة لإعداد مقرر إلكتروني مقترح لتنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية في مدينة جدة، وهذا ما تسعى الدراسة الحالية إلى تحقيقه.

مشكلة الدراسة:

مع تزايد الجرائم والهجمات الإلكترونية باختلافها وتنوعها بات لزاماً على جميع القطاعات والمنشآت توعية الأفراد بالأمن السيبراني، ويعد القطاع التعليمي من أكثر القطاعات استخداماً للإنترنت وتحديداً مع ظهور جائحة كوفيد19، أصبح الاعتماد كليًا على شبكة الإنترنت، وكون الطلبة شريحة كبيرة لا يستهان بها فكان لابد من تسليط الضوء على توعية هذه الشريحة، ونظرًا لأهمية موضوع الأمن السيبراني ومن واقع عمل الباحثتان وتخصصهما في تقنيات التعليم وملاحظتهما لتدني الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة، وعدم وجود مقرر خاص بالأمن السيبراني، مما شجع الباحثتان على طرق هذا الموضوع واختياره محوراً لدراستهما نظرًا لأهميته، وبناءً على ما سبق، واستناداً لما تم استعراضه من أدبيات ذات صلة، وما توصلت إليه الدراسات السابقة، وفي ظل التطورات التي يعيشها التعليم في المملكة العربية السعودية ترتب على ذلك ضرورة الوعي المعرفي بالأمن السيبراني في المجتمع التعليمي والمدارس التعليمية، وبرزت مشكلة الدراسة الحالية في عدم وجود مقرر إلكتروني خاص بالأمن السيبراني للوعي المعرفي به لدى طالبات المرحلة الثانوية بمدينة جدة. ولمواجهة هذه المشكلة تحاول الدراسة انشاء مقرر إلكتروني والكشف عن فاعليته في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة. وعليه يمكن ابراز مشكلة الدراسة في الأسئلة الأتية:

1- ما التصور المقترح للمقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة؟
2- ما فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة؟

فرض الدراسة: تختبر الدراسة الفرض التالي:

"توجد فروق دالة إحصائيًا عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات درجات طالبات المرحلة الثانوية في التطبيق القبلي والبعدي لاختبار الوعي المعرفي بالأمن السيبراني لصالح التطبيق البعدي تعزى للمقرر الإلكتروني المقترح".

أهداف الدراسة

تهدف الدراسة الحالية إلى:

1- اعداد المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة.

2- الكشف عن فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة.

أهمية الدراسة

من المأمول أن تفيد الدراسة في:

1- تقديم مقرر إلكتروني لتنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية، بالمفاهيم الأساسية للأمن السيبراني. وأنواع الجرائم والتهديدات السيبرانية التي يمكن التعرض لها في الفضاء السيبراني.

2- توجيه اهتمام المسؤولين في وزارة التعليم بأهمية الوعي المعرفي بالأمن السيبراني.

3- جذب انتباه المسؤولين وأصحاب القرار في وزارة التعليم بأهمية المقرر الإلكتروني وتعميمه على المدارس بشكل مستمر لنشر الوعي المعرفي في الأمن السيبراني لطلبة المرحلة الثانوية.

4- فتح المجال للباحثين نحو إجراء بحوث ودراسات أخرى تتعلق بموضوعات بالأمن السيبراني، وبمتغيرات الدراسة.

حدود الدراسة

- الحدود الموضوعية: ستقتصر الدراسة الحالية على موضوعات المقرر الإلكتروني المقترح(مفاهيم الأمن السيبراني، ضوابط الأمن السيبراني، الجرائم والتهديدات السيبرانية، الإجراءات المستخدمة لحماية الأمن السيبراني، ادارة حماية تقنيات الأمن السيبراني) لتنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة.
- الحدود البشرية: طالبات الصف الأول ثانوي بمدرسة الثالثة والتسعين في مدينة جدة.
- الحدود المكانية: مدرسة الثانوية الثالثة والتسعين بمدينة جدة.
- الحدود الزمنية: طبقت الدراسة الحالية خلال الفصل الدراسي الأول للعام الدراسي 1444 – 1445هـ.

مصطلحات الدراسة

- **المقرر الإلكتروني:** يعرف المقرر الإلكتروني بأنه:" المقرر الذي يربط بين المادة التعليمية وتكنولوجيا التعليم في تصميمه وتطبيقه وتقويمه، ويلزمه الاحتكام إلى مجموعة من المهارات" (موسى، 2020، ص. 203).
- ويعرف بأنه: "مجموعة من الوحدات والدروس، يتم نشره وادارته من خلال الإنترنت، ويتاح للمتعلمين الدراسة في أي وقت، ومن أي مكان"(الصعيدي والسعيد، 2016، ص.339).
- وتعرف الباحثتان المقرر الإلكتروني إجرائيًا بأنه: محتوى تعليمي يتضمن مجموعة الوحدات التعليمية، والأهداف والمعلومات، والأنشطة التعليمية، وأدوات التقويم تُقدم إلكترونيًا لتزويد طالبات الصف الأول ثانوي بالوعي المعرفي للأمن السيبراني من خلال المقرر الإلكتروني المقترح المستخدم في الدراسة الحالية.
- **الأمن السيبراني:** يعرف الأمن السيبراني حسب تعريف الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (2018) بأنه "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات، وأي اختراق، أو تعطيل أو تعديل أو دخول أو

استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك" (ص. 26).

- وتعرف الباحثتان الأمن السيبراني إجرائيًا بأنه: أمن المعلومات الرقمية ومعرفة التقنيات والمهارات اللازمة لحماية بيانات وخوادم وأنظمة وشبكات الكمبيوتر من التهديدات الإلكترونية والهجمات الضارة.

- **الوعي المعرفي بالأمن السيبراني:** عرفته الشامسي Alshamsi (2019) بأنه: "جميع الخطوات التي يتم اتخاذها لرفع مستوى المعرفة بالأمن السيبراني لدى المستخدمين النهائيين وتوجيههم للرد بشكل صحيح على الإنترنت"(P. 2).

- وتعرف الباحثتان الوعي المعرفي بالأمن السيبراني إجرائيًا بأنه: مستوى معرفة طالبات المرحلة الثانوية بالأمن السيبراني، ويقاس بالدرجة التي تحصل عليها الطالبة في أداة الدراسة(الاختبار) المعد لهذا الغرض والمكون من (61) فقرة.

2- الإطار النظري والدراسات السابقة.

أولاً- الإطار النظري

المحور الأول: المقررات الإلكترونية/ مفهوم المقررات الإلكترونية:

تعددت تعريفات المقررات الإلكترونية فعرفت بأنها: "مواد تعليمية تصمم وتنتج إلكترونيًا ثم يتم إدارتها من خلال الإنترنت وتتكون من مجموعة المعارف، والمهارات التي تم إعدادها، وإنتاجها، ليتم توزيعها وعرضها باستخدام تكنولوجيا التعلم الإلكتروني التشاركي، مما يؤدي إلى تجاوز مفهوم عملية التعليم والتعلم داخل جدران الفصول الدراسية ويتيح للمعلم دعم ومساعدة المتعلم في أي وقت سواء بشكل متزامن أو غير متزامن " (عبد القادر، 2019، ص. 139).

كما عرفتها المنديل (2020) بأنها "عبارة عن مقررات يتم تصميمها في بيئات التعلم الافتراضية تحتوي على العديد من أنماط التعلم المختلفة التي تناسب جميع الفروقات الفردية للمتعلمين، ويقدم المحتوى العلمي بشكل سهل ومشوق لما يحتويه على الفصول الافتراضية والأنشطة التعليمية المختلفة "(ص. 64).

يتضح مما سبق أن المقرر الإلكتروني عملية تحويل المحتوى التعليمي التقليدي للمقرر إلى شكل إلكتروني وفقاً لضوابط محددة، ويحتوي على عناصر الوسائط المتعددة المتنوعة، والتي تتكامل فيما بينها لدعم المحتوى، وتحقيق أهدافه، ويمكن للمتعلمة التفاعل معه بشكل تزامني أو غير تزامني.

أنواع المقررات الإلكترونية

قسم السجيني وخليل (2017) المقررات الإلكترونية إلى نوعان هما:

أ- المقررات الإلكترونية المعتمدة على الإنترنت: وهي مقررات تقوم على إيجاد موقع إلكتروني يتم تحميله على شبكة الإنترنت، ويعتمد في تكوينه على مكونات الوسائط المتعددة ذات الأشكال المختلفة من نصوص خاصة بالمقرر، وتعمل هذه المقررات على الترابط بين المتعلم وزملائه ومعلمه، سواء من خلال البريد الإلكتروني أو من خلال التحاور.

ب- المقررات الإلكترونية غير المعتمدة على شبكة الإنترنت: وتُقدم على أقراص مدمجة إلى المتعلم مباشرة، ويمكن تصميمها وفقاً لميوله وقدرته، و أسلوب التعلم الذي تقدم به المقررات وتعتمد عليه ولا تحتاج إلا لمهارات حاسوبية قليلة.

أهداف المقرر الإلكتروني

من أهداف المقرر الإلكتروني كما أوردها مطاوع والخليفة (2017):

1- تصميم المقرر الإلكتروني بطريقة آلية ورقمية وإلكترونية.
2- تحقيق مرونة التعلم الزمانية والمكانية من خلال إتاحة الفرصة للمتعلمين عبر المقرر الإلكتروني.
3- المساهمة في حل مشكلات القبول في مراحل التعليم العام والتعليم الخاص.
4- القضاء على مشكلة طرائق التدريس التقليدية لضمان دافعية المتعلم للتعلم بالتقنيات المستدامة.
5- إعداد المتعلم للحياة ونشر الثقافة المعلوماتية.
6- وضع أنشطة مصاحبة للمقرر الإلكتروني، وكذلك أسئلة ومواقف تساعد على الفهم والتذكر.
7- وضع وصلات links للموضوعات المرتبطة المقرر الإلكتروني لمزيد من الإثراء والتفصيل في حالة رغبة المتعلم.

يتضح من خلال تناول أهداف المقررات الإلكترونية أن لها العديد من الأهداف كالمساهمة في حل مشكلات القبول في مراحل التعليم العام والتعليم الخاص، وتحقيق مرونة التعلم، وأنها متاحة في أي زمان ومكان.

مميزات المقررات الإلكترونية

تلخص حلمي (2018) مميزات المقررات الإلكترونية أهمها:

1- عرض المعلومات بشكل غير خطي، واتاحة الانتقال المتشعب بين الدروس، وعناصر الدرس الواحد.
2- توافر الاختبارات البنائية لكل متعلم على حدة، وامكانية تصحيحها إلكترونيًا.
3- الاعتماد على النشاط الذاتي للمتعلم من خلال بحثه عن المعلومات.
4- ضمان تفاعل المتعلم مع باقي المتعلمين إلكترونيًا.
5- إعطاء فرص للمعلم لعرض وتنظيم المحتوى وادارة المقرر وسجلات الطلاب وارسال الواجبات واستقبالها إلكترونيًا.
6- الاستفادة من عناصر الوسائط المتعددة لعرض المعلومات.
7- إشراك المتعلم في أنشطة إلكترونية هادفة وجاذبة للانتباه، وتمكينه من التفاعل مع المحتوى.

وتضيف الباحثتان أن المقرر الإلكتروني يتمتع بعدة مزايا، أهمها:

1- توافر اختبارات تكوينية للمقرر.
2- توافر أساليب متنوعة للتقويم وتنوع الأنشطة التعليمية للمقرر.
3- يقدم المقرر الإلكتروني في أي وقت وفي أي مكان.
4- يحقق عرضًا أفضل للمادة التعليمية من خلال استخدام الوسائط المتعددة المستخدمة.

أهمية المقررات الإلكترونية:

للمقرر الإلكتروني دور مهم في تطوير عمليتي التعليم، وحدد هندي(2017) أهمية المقررات الإلكترونية بما يلي:

1- تدريب المتعلم على مهارات التواصل وصنع القرار وحل المشكلات تكنولوجيًا وعالميًا.
2- إمكانية عرض وتحميل عناصر الوسائط المتعددة، والملفات والمعلومات والقواميس ودوائر المعارف.
3- إعلام المتعلم بما يستجد في موضوع دراسته من خلال لوحة الأخبار أو الملاحظات على موقع المقرر الإلكتروني.
4- توفير جهد ووقت المعلم وتغير دوره إلى موجه ومرشد ومعدٍّ للأنشطة الطلابية.
5- توفير أشكال متنوعة من التفاعل بين المعلم والمتعلم سواء أكان هذا التفاعل تزامني أو غير تزامني.

6- تركيز المعلم على المهارات التي يحتاجها المتعلم فعليًا، وعلى التغذية الراجعة للمتعلم لتوجيهه للمسار الصحيح للتعلم.
7- توفير الوقت والجهد وتكاليف الورق والطباعة وغيرها، وانخفاض تكاليف النشر بالمقارنة بالنشر التقليدي.
8- سرعة تحديث المادة التعليمية وتزويد المتعلمين بها في نفس اللحظة مع سهولة تصحيح الأخطاء لحظة اكتشافها.
9- سرعة توزيع المحتوى الإلكتروني بمجرد إعداده وبرمجته وتوصيله للمتعلمين في أي مكان وزمان.

ويتضح من خلال تناول أهمية المقررات الإلكترونية، أن لها دور مهم في تطوير العملية التعليمية، إذ أنها تجعل دور المتعلم ايجابيًا ومشاركًا في المحتوى التعليمي المقدم، وكونها تشتمل على العديد من الوسائط المتعددة، وتوفر جهد ووقت المعلم وتغير دوره إلى موجه ومرشد، وتساعد المؤسسة التعليمية على تحديث وسرعة توزيع المقررات الإلكترونية.

المحور الثاني: الأمن السيبراني

مفهوم الأمن السيبراني:

تطلق كلمة سيبراني (cyber) على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني يعني الفضاء الإلكتروني (Cyberspace) وهو كل ما يتعلق، بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالوتسآب، والفيس بوك، وغيرها من التطبيقات)، وكل الخدمات التي تقوم بتنفيذها (كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم (السمحان، 2020)،

وعرف الأمن السيبراني بأنه "التدخلات التقنية والتدابير المتخذة لحماية أجهزة الكمبيوتر وشبكات الإنترنت والبيانات ومعلومات الهوية من الوصول غير المصرح به وذلك بهدف الحفاظ على سلامة ونزاهة المعلومات المخزنة داخل هذه الأجهزة" (Richardson, et. al, 2020, P. 23).

المحاور التي يقوم عليها الأمن السيبراني

يرتكز الأمن السيبراني على اربعة محاور أساسية، بينتها الهيئة الوطنية للأمن السيبراني (2018) في الآتي:
1- الاستراتيجية (Strategy): ويقصد بها خطط العمل والأهداف والمبادرات والمشاريع للأمن السيبراني داخل الجهة، أو المؤسسة لتحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
2- الأشخاص (People): الذين يعملون في الجهة أو المؤسسة (بما في ذلك الموظفون الرسميون، والمؤقتون، والمتعاقدون).
3- الإجراء (Process): وثيقة تحتوي على وصف تفصيلي للخطوات الضرورية لأداء عمليات أو أنشطة محددة.
4- التقنية (Technology): الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية وبرامج مكافحة الفيروسات الضارة وغيرها.

أهداف الأمن السيبراني

بينت الهيئة الوطنية للأمن السيبراني (2018) الأهداف الأساسية لحماية الأمن السيبراني في الآتي:
1- سرية المعلومة (Confidentiality): ويقصد بها الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.

2- سلامة المعلومة (Integrity): ويقصد بها الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.

3- توافر المعلومة (Availability): الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.

أهمية الأمن السيبراني

للأمن السيبراني أهمية كبيرة، أشارت له السمحان (2020) وتتمثل في:

1- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك من العبث بها، وتحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها.

2- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات.

3- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

4- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيِق مبادئ الأمن السيبراني.

5- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.

أبعاد الأمن السيبراني

تشير الصائغ (2018) أن من أبعاد الأمن السيبراني ما يأتي:

1. الأبعاد العسكرية: تنشا أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي إلى كوارث.
2. الأبعاد الاقتصادية: يرتبط الأمن السيبراني ارتباطا وثيقا بالحفاظ على المصالح الاقتصادية لكل الدول، وحماية الاقتصاد من السرقة والملكية الفكرية.
3. الأبعاد القانونية: حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.
4. الأبعاد الاجتماعية: حماية وصيانة القيم الجوهرية في المجتمع كالانتماء، المعتقدات الدينية، والعادات والتقاليد.
5. الأبعاد السياسية: تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها.

الانتهاكات السيبرانية:

تشير الانتهاكات السيبرانية إلى كل نشاط خبيث يسعى إلى الحصول على تنازلات من جهة ما، أو يتسبب في إضعاف السرية، والنزاهة، وتعطيل توافر نظم الحواسيب، أو المعلومات، أو الاتصالات، أو الشبكات، والبنية التحتية المادية، والافتراضية التي تتحكم فيها أجهزة الحواسيب، وأنظمة المعلومات، أو المعلومات الموجودة فيها (بانقا، 2019).

وحدد (ابن تاج، 2018؛ الهزاني، 2018؛ بانقا، 2019) الانتهاكات السيبرانية بالآتي:

1. انتهاك الخصوصية Violation of Privacy: تعد الخصوصية من الحقوق الفردية التي نصت عليها التشريعات الداخلية والاتفاقات الدولية، ومن صور انتهاكها في الفضاء السيبراني ما يلي:
   - إدخال معلومات وهمية، وانتحال الشخصية بهدف حصول المعتدي على مبالغ مالية.
   - التجسس الإلكتروني بتتبع العيوب واصطياد الأخطاء.
   - التصنت ومحاولة الوصول إلى السجلات الخاصة والاعتداء على الحياة الخاصة.

2. انتهاك أمن المعلومات:Information Security Violationوتشمل جرائم الدخول إلى نظام المعلوماتي، وسرقة المعلومات وتزيفها وتظليلها، وإعاقة العمل المعلوماتي وتغيير المعلومات السرية وتعطيل الأنظمة وحجب الخدمة.
3. انتهاك الملكية الفكرية Violation of Intellectual Property: وتشمل وضع اسم على عمل وانتهاك تقليد ختم المؤلف، والاعتداء على أي حق من حقوقه.
4. انتهاك المواقع Violation of Sites: وتشمل انتهاك وتدمير المواقع الإلكترونية، والتلاعب بالبيانات، والمعلومات، والإضرار بها، وتهديدها بالفيروسات والبرامج الخبيثة والاختراقات.

الجرائم السيبرانية:

تعرف الجرائم السيبرانية بأنها: " أي جريمة تشتمل على جهاز حاسوب وشبكة اتصال، وهي جرائم ترتكب ضد الأفراد كالجماعات من قبل أفراد لديهم دافع إجرامي لتعمد إيذاء الضحايا من خلال تكنولوجيا المعلومات والاتصالات الحديثة" (التيماني، 2020، ص. 10).

وتصنف الجرائم السيبرانية إلى قسمين (Tiwari et al., 2017):

1. القسم الأول: يستهدف الحواسيب وشبكات المعلومات، كالفيروسات والديدان الخبيثة.
2. القسم الثاني: يستهدف مستخدمي الإنترنت ورواد الفضاء السيبراني، ويشمل ذلك الأفراد والمؤسسات الاقتصادية، والوزارات الحكومية، ومنها التنمر الإلكتروني، والتصيد، والهندسة الاجتماعية، والعديد من الأشكال الأخرى.

أنواع التهديدات الإلكترونية للأمن السيبراني

التهديدات الإلكترونية للأمن السيبراني متعددة منها ما بينه (ابو منصور، 2017؛ الرفاعي) في التالي:

- الفيروسات Viruses: برامج حاسوبية خبيثة تتنقل بين الحواسيب بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى.
- البرامج الخبيثة: تستخدم لوصف البرامج الضارة بما في ذلك برامج التجسس وبرامج الفدية والفيروسات.
- التنمر الإلكترونيBullying: استخدام تكنولوجيا الاتصالات لأغراض التهديد، الابتزاز، وغير ذلك من الإيذاء.
- التشهير الإلكترونيDefamation: بث أفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بالشخص أو الجهة.
- التصيد الإلكتروني Phishing: والمعروف أيضًا بالخداع، ويتم من خلال استهداف المستخدمين للحصول على معلوماتهم الحساسة مثل بطاقة الائتمان أو الضمان الاجتماعي أو المعلومات الشخصية، وكلمات السر وما إلى ذلك من معلومات.
- الهندسة الاجتماعية: Engineering Social ويُطلق عليها علم أو فن اختراق العقول، مجموعة الأساليب التي تستخدم في الحصول على المعلومات الحساسة، أو إقناع الضحايا بتنفيذ الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بها.
- الإرجاف الإلكتروني Destabilization: بث الأخبار المحبطة والمسيئة ونشر الشائعات بغرض إحداث الخوف والاضطرابات وزعزعة الأمن في نفوس الناس، لتحطيم مصادر الأخبار الحقيقية، وطُعم للحصول على الحقيقة.

- التغرير والاستدراج Grooming: غالب ضحايا هذا النوع من المخاطر هم صغار السن من مستخدمي شبكة الإنترنت، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت، وقد تتطور إلى التقاء مادي بين الطرفين.
- التجسس الإلكتروني Cyber-espionage: يتم بواسطة برامج معينة تحصل سرًا على معلومات لمستخدم عن طريق الربط بالإنترنت، وخاصة بدعاوي دعائية وإعلانية، أو برامج يمكن تنزيلها من شبكة الإنترنت، وبمجرد تركيب برنامج التجسس يبدأ بمراقبة حركة المستخدم على الإنترنت، وينقل المعلومات إلى الجهة المهاجمة.
- الاحتيال الإلكتروني Fraud: يستعمل البيانات الكاذبة التي تساعد في الخداع والاحتيال على الاشخاص والحكومات.

تقنيات الأمن السيبراني:

لمكافحة هجمات الأمن السيبراني توجد العديد من تقنيات الأمن السيبراني حددها باندي(Pande (2017 بالآتي:

1. التوثيق: عملية تحديد الفرد والتأكد من أنه هو نفسه عبر اسم المستخدم وكلمة السر.
2. التشفير: أسلوب لقفل البيانات عن طريق تحويلها إلى أكواد معقدة باستخدام خوارزميات رياضية، وتحويل البيانات في شكل غير قابل للقراءة قبل إرسالها عبر الإنترنت.
3. التوقيعات الرقمية: إنها تقنية للتحقق من صحة البيانات، ويتم إنشاء التوقيع الرقمي عن طريق تشفير البيانات بالمفتاح الخاص للمرسل.
4. مضاد فيروسات: تقنية استخدام برنامج خاص يسمى مكافح الفيروسات، وهو مصمم لحماية النظام من الفيروسات.
5. جدار ناري: تقنية جهاز/ برنامج يعمل كدرع بين شبكة المؤسسة والإنترنت وحمايته من التهديدات مثل الفيروسات والبرامج الضارة والمتسللين.
6. التصوير الشعاعي: تقنية لإخفاء الرسائل السرية في ملف مستند أو ملف صورة أو برنامج أو البروتوكول وغيرها.

إجراءات تعزيز الأمن السيبراني

توجد العديد من إجراءات تعزيز الأمن السيبراني، ومن هذه الإجراءات (Tiwari et al., 2017):

1. المحافظة على تحديث جدران الحماية، والتي تمثل أنظمة الدفاع عن البنية التحتية للبيئة المعلوماتية.
2. التأكد من إعدادات الحاسوب وشبكة الإنترنت.
3. اختيار كلمات مرور قوية، وعمليات تحقق أمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني، والحسابات الشخصية على الحاسوب أو الهواتف الذكية.
4. عدم الاستجابة لأي رسائل مجهولة المصدر ترد إلى البريد الإلكتروني.
5. استخدام برامج الحماية ومضادات الفيروسات وتحديثها باستمرار.
6. حماية المعلومات الشخصية ومنع الآخرين من الاطلاع عليها.
7. تحديث كلمات المرور بشكل مستمر، على الأقل مرة أو مرتين شهريًا.
8. عدم إرسال أي معلومات شخصية عبر البريد الإلكتروني، أو الإفصاح عن معلومات خاصة عبر مواقع التواصل الاجتماعي.

المحور الثالث: الوعي بالأمن السيبراني

مفهوم الوعي:

تباينت تعريفات الوعي، فعرفه صياد(2017) بأنه" الوعي الذي يؤسس على ثلاثة جوانب: الجانب المعرفي ويقصد به توفر المعلومات العلمية عن ظاهرة أو موضوع معين، والجانب الوجداني ويتمثل في تكوين الميول والاتجاهات، والجانب التطبيقي ويتمثل في كيفية التصرف في الموقف في المواقف الحياتية التي تواجه المتعلم، واذا اكتملت جوانب الوعي المعرفية والوجدانية والتطبيقية في شخص واحد وصف بأن لديه وعي علمي متكامل" (ص. 103).

وعرفته التيماني (2020) بأنه "معرفة الأشياء على نحو مستمر" (ص. 10).

وظائف الوعي بالأمن السيبراني:

يعزز الوعي بالأمن السيبراني تمكين الأفراد من حل المشكلات التي تواجههم، واشارت جميلة وبختة (2018) أن وظائف الوعي السيبراني يمكن تحديدها من خلال:

1. التعامل مع المتغيرات السريعة للمعلومات: برز الوعي المعلوماتي لتوافر كميات كثيرة من المعلومات من خلال الكتب والمجلات ووسائل الإعلام والأنترنيت مما ادى التعامل السريع للمعلومات.
2. الاستخدام الأخلاقي للمعلومات: يمكن أن تستخدم المعلومات بشكل سلبي أو إيجابي، لذا ينبغي الوعي المعلوماتي بما يضمن الاستخدام الامثل للمعلومات.
3. الإعداد للأفراد: الإعداد للعديد من الأفراد القادرين على استكشاف التغيرات في المعلومات والتقنيات وحل المشكلات.
4. التعلم مدى الحياة: الوعي المعلوماتي يجعل الأفراد قادرين على التعلم ذاتياً مباشرة في المدرسة او خارجها.
5. المشاركة في المعلومات: الوعي المعلوماتي يزود الأفراد بالمهارات الضرورية للعمل واتخاذ القرارات والتدخل الفعال للمشاركة في المعلومات.

أنواع الوعي بالأمن السيبراني

اشارت جميلة وبختة (2018) أن أنواع الوعي بالأمن السيبراني يمكن تحديدها بالتالي:

1. الوعي المكتبي: ويتضمن هذا النوع مجموعة من مهارات لاستخدام المكتبات للحصول على المعلومات مما يتضمنه بالتعامل مع الفهارس، واستخدام كافة المصادر والكشافات، والقدرة على استخدام المعلومات والبيانات والاستفادة منها.
2. الوعي البحثي: قدرة الفرد على تحديد موضوع البحث، وإنتاج النص أو الوسائط المتعددة له.
3. الوعي التقني: ويتضمن القدرة على استخدام الحواسيب الآلية وبرامجها.
4. الوعي الرقمي: معرفة وفهم التطور الرقمي في مجال المعلومات والاتصالات، وتوثيق المعلومات وإنتاجها وتوزيعها أو إرسالها واستقبالها واسترجاعها ومعالجتها بأشكال مختلفة.

أهمية الوعي بالأمن السيبراني

بين رحمان وآخرونRahman et al (2020) أهمية الوعي بالأمن السيبراني بالتالي :

1. تساعد التوعية بالأمن السيبراني على تجنب انتهاكات البيانات.
2. القدرة على تعليم الافراد للحفاظ على أنفسهم وبياناتهم من الأذى .

3. إنشاء ثقافة أمنية للحماية من الهجمات الإلكترونية.
4. يعزز الوعي الأمني للكفاءة التكنولوجية وتحديث البرامج للحفاظ على أمان المعلومات.
5. الوعي يعزز الدراية بالتهديدات الإلكترونية التي لا نهاية لها في عالم اليوم.
6. الوعي يساعد الفرد على الالتزام باللوائح والقوانين.
7. الوعي بالأمن السيبراني يجعل الفرد مسؤولاً امام المجتمع بعدم الهجمات الإلكترونية او التهديد للشبكات الأخرى.
8. القدرة على تنفيذ أفضل ممارسات أمان تكنولوجيا المعلومات بسهولة كإنشاء كلمات المرور وحمايتها.
9. الوعي بالأمن السيبراني يوفر المال والخسائر نتيجة للأضرار الناتجة عن الحوادث المتعلقة بالإنترنت.
10. الوعي بالأمن السيبراني يعزز الحماية ضد الهجمات السيبرانية.

دور وزارة التعليم في تنمية الوعي بالأمن السيبراني:

إن وزارة التعليم تؤدي دورًا مهمًا في مواكبة التطورات العلمية والتقنية المتسارعة، وإعداد المعلمين والمتعلمين للقيام بأدوارهم المستقبلية مع الأخذ في الاعتبار أن المدارس تعد من أكثر المؤسسات عرضة لخطر الانتهاكات السيبرانية.

وتشير الهيئة الوطنية للأمن السيبراني (2018) أن هدف أدوار ومسئوليات الأمن السيبراني هو ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة (المؤسسة)، وحددت الضوابط المخصصة لتلك الأدوار بأنه يجب على صاحب الصلاحية تحديد وتوثيق واعتماد الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للجهة، وتكليف الأفراد المعنيين بها، وتقديم الدعم اللازم لتنفيذ ذلك، والأخذ بالاعتبار عدم تعارض المصالح، اضافة إلى انه يجب مراجعة أدوار ومسؤوليات الأمن السيبراني في الجهة وتحديثها بفترات زمنية مخطط لها أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.

ويشير كريتزنجر وآخرون Kritizinger et al, (2017) إلى أدوار تنمية الوعي بالأمن السيبراني في المؤسسات التعليمية منها:

1. وضع الخطط للتوعية بالأمن السيبراني على مستوى المدارس، والتحذير من المخاطر والانتهاكات السيبرانية.
2. وجود خطة عمل لدى وزارة التعليم للجهات والمؤسسات للتعامل مع المخاطر والانتهاكات السيبرانية، ومواجهتها.
3. إشراف بعض الجهات المختصة في وزارة التعليم على تطبيق جميع المدارس للتعامل مع التكنولوجيا الرقمية بما يشمل الأمن السيبراني، وفق سياسات واضحة وتعميمها على جميع المدارس، مع التأكد منها.
4. عقد دورات تدريبية للمعلمين والمتعلمين للوعي بالأمن السيبراني، والإجراءات التي يُمكن اتباعها في حال وقوعهم ضحية للمخاطر والانتهاكات السيبرانية.
5. إدراج موضوع الأمن السيبراني ضمن المقررات الدراسية وأدلة المعلمين.
6. التعاون مع المؤسسات في وضع الخطط، وتوفير المصادر والدعم اللازم للتدريب ونشر الوعي بالأمن السيبراني.
7. إشراك اولياء الامور في خطط وبرامج عمل المدرسة ذات الصلة للتوعية بالأمن السيبراني.
8. نشر الوعي بالأمن السيبراني والاهتمام به على نطاق واسع من المجتمع، من خلال عقد ورش العمل وندوات مخصصة للأمن السيبراني، أو وضع ملصقات وتوزيع كتيبات ونشرات للتوعية، أو مواقع التواصل الاجتماعي.
9. اعتبار الوعي بالأمن السيبراني من المهارات الحياتية اللازمة للمتعلمين، وإدراجه أثناء التدريس والأنشطة المدرسية.

ويتضح من خلال تناول دور وزارة التعليم في تنمية الوعي بالأمن السيبراني أن صدور الاوامر الملكية بالمملكة العربية السعودية بإنشاء(الهيئة الوطنية للأمن السيبراني) وهي الجهة المختصة بشؤون الأمن السيبراني في المملكة، وترتبط بمقام خادم الحرمين الشريفين، أدى إلى الاهتمام بالأمن السيبراني على مستوى جميع الوزارات ومنها وزارة التعليم التي أبدت الاهتمام بالأمن السيبراني للمدارس والجامعات والعاملين بها، وأدوارها في تنمية الوعي بالأمن السيبراني والطرق التي تعززها لدى المعلمات والمتعلمات بما يمكنهن من الوعي والمسؤولية، والالتزام بالنواحي الأمنية والحماية والتعامل مع المعلومات الرقمية المختلفة، بالإضافة إلى الدور التي تؤديه في التوعية في مجال الأمن السيبراني لدى الأفراد في المجتمع السعودي.

ثانياً- الدراسات السابقة:

أ- دراسات تناولت المقررات الإلكترونية:

- **هدفت دراسة العنزي وآخرون (2020)** إلى تصميم وحدة تعليمية إلكترونية تفاعلية وقياس أثرها في التحصيل وتعزيز دافعية التعلم لدى طلاب الصف الأول الثانوي في المملكة العربية السعودية، استخدمت الدراسة المنهج التجريبي، واختبار تحصيلي، ومقياس دافعية التعلم كأدوات لجمع البيانات من عينة الدراسة التي تكونت من (60) طالبًا تم اختيارهم عشوائياً من طلاب الصف الأول الثانوي، وتوزيعهم في مجموعتان؛ تجريبية وضابطة بالتساوي، أظهرت نتائج الدراسة وجود فروق دالة إحصائيًا في مستوى التحصيل البعدي، لصالح المجموعة التجريبية التي درست من خلال الوحدة التعليمية الإلكترونية التفاعلية.
- **وبينت دراسة حلمي (2018)** بناء مقرر إلكتروني لتنمية التحصيل المعرفي والدافعية للتعلم لدى المتعلمات المعلمات بكلية التربية للطفولة المبكرة، أظهرت نتائج الدراسة وجود فروق دالة إحصائيًا بين متوسطات درجات المتعلمات اللواتي درست المقرر (إلكترونيًا – تقليديًا) في اختبار التحصيل المعرفي لصالح المتعلمات اللواتي درسن المقرر إلكترونيًا، فاعلية المقرر الإلكتروني في تنمية التحصيل المعرفي والدافعية للتعلم لدى المتعلمات.
- **وتوضح دراسة داود (2018)** بناء مقرر إلكتروني لمهارات الاتصال على نظام إدارة التعلم الإلكتروني (**Blackboard**) وفق معايير جودة التعلم الإلكتروني، والكشف عن فاعليته في تنمية التحصيل الدراسي والاتجاه نحو المقرر، وفق المعايير المتضمنة والمعتمدة من جامعة القصيم، استخدمت الدراسة المنهج التجريبي، واختبار تحصيلي ومقياس في الاتجاه كأدوات لجمع البيانات من عينة الدراسة التي تكونت من(37) طالبًا كمجموعة تجريبية درست المقرر الإلكتروني، والأخرى ضابطة عددها(40) طالبًا درست المقرر بالطريقة الاعتيادية، وتوصلت الدراسة إلى وجود فروق دالة إحصائيًا في مستوى التحصيل المعرفي ومقياس الاتجاه لصالح الطلبة الذين درسوا المقرر الإلكتروني، وفاعلية المقرر الإلكتروني لمهارات الاتصال في تنمية التحصيل والاتجاه الإيجابي نحوه، وأوصت الدراسة بضرورة تصميم جميع مقررات كلية الشريعة إلكترونيًا لما لها من أثر إيجابي على التحصيل والاتجاه نحو المقررات.

ب- دراسات تناولت الوعي المعرفي بالأمن السيبراني:

- **هدفت دراسة كريتزنجر وآخرون (Kritizinger et al, 2017)** إلى استعراض المبادرات الخاصة برفع مستوى الوعي المعرفي بالأمن السيبراني لدى طلبة مدارس بريطانيا وجنوب أفريقيا، وأظهرت نتائج الدراسة وجود عدد من المبادرات شملت دمج مفاهيم الأمن السيبراني ضمن المناهج الدراسية، وتدريب الطلبة، ووضع سياسات خاصة بالأمن السيبراني، وسن قوانين وتشريعات لمكافحة الانتهاكات السيبرانية، ودمج اولياء الامور ببرامج الوعي

بالأمن السيبراني، وعقد ورش العمل والندوات، والتوعية عبر وسائل الإعلام، وتدريب الطلبة في هذا المجال تساعد على رفع مستوى الوعي لديهم.

- **وبينت دراسة مارك ونجوين(2017) Mark & Nguyen** فعالية ورش العمل في رفع مستوى الوعي المعرفي بالأمن السيبراني لدى الإباء والتربويين، وتعزيز الأمن السيبراني في المنزل والمدرسة، تكونت عينة الدراسة من (51) فرد من الاباء والمعلمين والمرشدين التربويين ومديري المدارس في عدد من مدارس ولاية هاواي الأمريكية، وأظهرت نتائج الدراسة أن أهمية التوعية بالأمن السيبراني، وضرورة التعاون بين المنزل والمدرسة لتوفير بيئة انترنت أكثر أمانًا للطلبة، كما أظهرت نتائج الدراسة الدور المهم للمعلمين ولمديري المدارس في تعزيز الوعي بالأمن السيبراني.
- **وتوضح دراسة باستارد Bustard (2018)** إعداد وحدة دراسية تناولت الأخلاقيات والانتهاكات الخاصة بالأمن السيبراني، وقياس أثرها على اندماج الطلبة في تعلم أخلاقيات الأمن السيبراني، استخدمت الدراسة استبانة لقياس مدى رضا مجموعة من طلبة مرحلة الماجستير عن الوحدة الدراسية واندماجهم في تعلم الأخلاقيات، وكيفية التصدي لانتهاكات الأمن السيبراني، وأظهرت نتائج الدراسة رضا الطلبة بدرجة كبيرة عن الوحدة الدراسية، وأن عدم التوعية بالانتهاكات والهجمات السيبرانية والتصدي لها قد يكون له أثر سلبي على أمن المؤسسات، وضرورة معالجة القضايا الأخلاقية المتعلقة بالأمن السيبراني.
- **بينما هدفت دراسة كاي Cai (2018)** إلى فاعلية نموذج مقترح لتدريس الأمن السيبراني والانتهاكات السيبرانية، استخدمت الدراسة استبانة لتقييم أداء المحاضر والممارسات التدريسية، وأظهرت نتائج الدراسة وجود فروق وتحسناً واضحاً في التحصيل الدراسي للطلبة في مقرر الأمن السيبراني، وازدياد دافعية الطلبة نحو تعلم الأمن السيبراني والانتهاكات السيبرانية، وفاعلية النموذج المقترح في تنمية التحصيل للطلبة لمقرر الأمن السيبراني.
- **أما دراسة المنتشري وحريري (2020)** فسعت للتعرف على درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني بمدارس مدينة جدة، استخدمت الدراسة المنهج الوصفي، والاستبانة كأداة مكونة من (21) فقرة، وتشمل ثلاثة محاور: (مفاهيم الأمن السيبراني، مخاطر الأمن السيبراني، وانتهاكات الأمن السيبراني)، وطبقت على عينة مكونة من (362) معلمة، وأظهرت نتائج الدراسة عدم وجود فروق دالة إحصائيًا في درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني وفقاً لمتغيري المؤهل الدراسي وسنوات الخبرة.

تعقيب على الدراسات السابقة:

تنوعت الدراسات التي اهتمت بالمقررات الإلكترونية، والأمن السيبراني، والوعي بالأمن السيبراني، وبعض الدراسات استخدمت المنهج الوصفي ومنها المنهج التجريبي، ومن الدراسات استخدمت اختبار تحصيلي، ومنها الاستبانة كأداة دراسة. وتناولت الدراسات طلبة المرحلة الثانوية وبعض الدراسات تناولت معلمات كعينة، وحسب علم الباحثتان تميزت هذه الدراسة عن الدارسات الأخرى، إذ إنه لا توجد دراسات تناولت مقرر إلكتروني وقياس فاعليته في تنمية الوعي المعرفي بالأمن السيبراني لطالبات المرحلة الثانوية في جدة، وتأتي الدارسة الحالية إضافة المعلومات الجديدة والمفيدة التي لم تتطرق لها الدراسات السابقة.

3- منهجية الدراسة وإجراءاتها.

منهج الدراسة:

استخدمت الباحثتان المنهج الوصفي التحليلي كونه يستند على جمع المعلومات والبيانات عن ظاهرة ما، لمراجعة الدراسات السابقة العربية والأجنبية ذات العلاقة بمتغيرات الدراسة والاستفادة في بناء أداتها، والمنهج شبه التجريبي (ذي المجموعة الواحدة) وذلك لمناسبته لطبيعة الدراسة الحالية ومتغيراتها، لقياس فاعلية المتغير المستقل

المتمثل (بالمقرر الإلكتروني المقترح) على المتغير التابع المتمثل في (الوعي المعرفي بالأمن السيبراني) لدى طالبات المرحلة الثانوية بمدينة جدة.

التصميم التجريبي للدراسة:

استُخدم التصميم التجريبي المجموعة الواحدة ذي التطبيق القبلي والبعدي، وجدول (1) يوضح التصميم التجريبي.

جدول (1) يوضح التصميم التجريبي للدراسة

مجموعة	التطبيق القبلي	المعالجة التجريبية	التطبيق البعدي
التجربة	- اختبار الوعي المعرفي بالأمن السيبراني لطالبات المرحلة الثانوية.	المقرر الإلكتروني المقترح	- اختبار الوعي المعرفي بالأمن السيبراني لطالبات المرحلة الثانوية.

مجتمع الدراسة وعينتها:

يتكون مجتمع الدراسة من طالبات مدارس المرحلة الثانوية بمدينة جدة للعام الدراسي 1444 – 1445هـ، واختيرت عينة مكونة من (26) طالبة بطريقة قصدية من طالبات الصف الأول ثانوي بمدرسة الثانوية الثالثة والتسعين بمدينة جدة.

إعداد المقرر الإلكتروني المقترح:

هدفت الدراسة الحالية إلى إعداد المقرر الإلكتروني المقترح وقياس فاعليته في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية في جدة، وقامت الباحثتان بتحليل العديد من نماذج التصميم التعليمي Instructional Design models، للاستفادة منها في الخروج بنموذج تصميم تعليمي يناسب الدراسة الحالية، ومن هذه النماذج: النموذج العام (ADDIE)، ونموذج ديك وكاري(Dick & Carrey)، ونموذج جيرلاش وايلى(Gerlach & Ely)، ونموذج كمب (Kemp)، ونموذج الجزار، ونموذج هانج (Huang)، ونموذج فرناندو(Fernando) وغيرها من نماذج تصميم التعليم، واختارت الباحثتان نموذج (ADDIE) لاهتمامه بالجوانب الكلية لبناء المقرر الإلكتروني المقترح ومرونته والتأثير المتبادل بين عناصره.

الأسس والمبررات لبناء المقرر الإلكتروني المقترح:

من أسس ومبررات بناء المقرر الإلكتروني المقترح مواكبة الثورة العلمية والتكنولوجية الهائلة في مجال التعليم. والتقنيات الحديثة. وتوجه رؤية المملكة العربية السعودية 2030 التطوير الشامل للمملكة، ومواكبة التقدم العالمي المتسارع في الخدمات الرقمية، والشبكات العالمية المتجددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، وندرة الدراسات التي تناولت مقرر إلكتروني في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية في جدة. وتزويدهن بالمعارف لرفع مستوى المعرفة بالأمن السيبراني. وقد اتبعت الباحثتان في بناء المقرر الإلكتروني المقترح خطوات النموذج العام للتصميم التعليمي ADDIE ليكون كإطار عام لخطوات بناء المقرر، وفيما يلي مراحل وخطوات بناء المقرر الإلكتروني المقترح:

المرحلة الأولى: التحليل (Analysis) هي الأساس لجميع المرحل الأخرى لتصميم التعليم، ويتم بها تحديد مجموعة من مدخلات المقرر الإلكتروني المقترح وهي تحليل الخصائص العامة للطالبات، تحليل الأهداف العامة ومحتوى المقرر الإلكتروني، وتحليل بيئة التعلم.

المرحلة الثانية: التصميم (Design) تحديد الأهداف التعليمية الإجرائية والخاصة، ثم تحديد عناصر محتوى المقرر وتنظيمه، اختيار الاستراتيجيات والبيئة التعليمية، وفي ضوء قائمة أهداف المقرر الإلكتروني التفصيلية في صورتها النهائية، اعتبرت الباحثتان كل هدف بمثابة عنصر من العناصر الرئيسة للمحتوى، وقد راعت الدراسة الحالية التنظيم المنطقي في اختيار محتوى المقرر الإلكتروني وتنظيمه لضمان تحقيقه، وتم تحديد المحتوى في خمس وحدات:

الوحدة الأولى: مفاهيم الأمن السيبراني.

الوحدة الثانية: ضوابط الأمن السيبراني.

الوحدة الثالثة: الجرائم والتهديدات السيبرانية.

الوحدة الرابعة: الإجراءات المستخدمة لحماية الأمن السيبراني.

الوحدة الخامسة: ادارة حماية تقنيات الأمن السيبراني.

ومن ثم تصميم منصة تدريس المقرر الإلكتروني المقترح: إذ تم اختيار منصة wix من قبل الباحثتان لتدريس الطالبات المقرر الإلكتروني المقترح.

المرحلة الثالثة: التطوير (Development) تم بها ترجمة مخرجات عملية التصميم من مواد تعليمية حقيقية إلى إعداد وحدات المقرر الإلكتروني، وتنفيذه، وإنتاجه، وتتضمن المرحلة تجميع الوسائط المتاحة، ومن ثم إنتاج الوسائط المتعددة المطلوبة للمقرر الإلكتروني من نصوص وصوراً ثابتة، أو رسومات ثابتة ومتحركة، أو لقطات فيديو وفلاشات توضيحية، أو تطبيقات مساعدة للمقرر الإلكتروني والتي تُعين الباحثتان في التدريس.

المرحلة الرابعة: التطبيق(التنفيذ) (Implementation): تم في هذه المرحلة القيام الفعلي بالتدريس، وترجمة مخرجات عملية التطوير من مواد تعليمية حقيقية وتنفيذ وحدات المقرر الإلكتروني المقترح وادواته.

المرحلة الخامسة: التقويم (Evaluation) والمراجعة: شملت المرحلة تحكيم المقرر الإلكتروني المقترح، للتأكد من مناسبته لتحقيق الأهداف وعناصر المحتوى العلمي والأنشطة وتسلسلها، وسهولة الاستخدام وصلاحية المقرر الإلكتروني المقترح والأدوات التي تضمنها، ومن ثم تجريبه على مجموعة طالبات (عينة استطلاعية)، ومراجعة المقرر الإلكتروني وإضافة التعديلات التي تم الحصول عليها من خلال عملية التجريب المبدئي استعدادًا لإعداده النهائي، واجراء التقويم الختامي لقياس فاعليته.

أدوات قياس الدراسة (بناؤها وضبطها):

استلزم إجراء الدراسة الحالية بناء وضبط وتطبيق أدوات القياس والتي تتمثل في:

اختبار الوعي المعرفي بالأمن السيبراني: تم اعداد الاختبار لقياس الوعي المعرفي بالأمن السيبراني لطالبات الثانوية في جدة للكشف عن فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني، وفقاً لما يأتي:

أ- **تحديد هدف الاختبار**: يهدف الاختبار إلى قياس الوعي المعرفي بالأمن السيبراني لطالبات المرحلة الثانوية في جدة للكشف عن فاعلية المقرر الإلكتروني في تنمية الوعي المعرفي بالأمن السيبراني، قبل وبعد التجربة الميدانية.

ب- **إعداد الاختبار في صورته الأولية:** من خلال اطلاع الباحثتان على الأدب النظري والدراسات السابقة تم صياغة أسئلة الاختبار لتغطى جميع الأهداف العامة والإجرائية للوحدات التي تضمنها المقرر الإلكتروني المقترح، وبلغ عدد الأسئلة (61) سؤالاً في صورتها الأولية.

ج- **ضبط الاختبار:** قامت الباحثتان بالتحقق من صدق وثبات الاستبانة من خلال ما يلي:

التحقق من صدق الاختبار: جرى التحقق من صدق الاختبار من خلال الصدق الظاهري والاتساق الداخلي.

الصدق الظاهري للمحكمين بعد إعداد الاختبار في صورته الأولية، قامت الباحثتان بعرضه على مجموعة من الأساتذة المحكمين وعددهم (5) محكم، للاستفادة من آرائهم وتحكيمهم له، وأظهرت النتائج أن معظم الأسئلة حازت على نسبة (96%) من آرائهم واتفاقهم عليها، وأصبح الاختبار يتكون من (61) سؤالاً موزعة على الدروس الخمسة، وجاهز للتطبيق على العينة الاستطلاعية.

صدق الاتساق الداخلي: بعد تأكد الباحثتان من الصدق الظاهري للاختبار، تم تطبيقه على عينة الدراسة الاستطلاعية وتحليل النتائج لمعرفة الصدق الداخلي، وذلك بحساب معامل الارتباط بيرسون (Pearson Correlation) لكل سؤال والدرجة الكلية للاختبار والتي تراوحت بين (0.80- 0.98) ووجد أن جميع قيم الأسئلة دالة إحصائيًا عند مستوى دلالة (0.01) مما يؤكد صدق الاتساق الداخلي للاستبانة، وأن جميع الأسئلة تتمتع بدرجة عالية من الصدق وصلاحيتها للتطبيق.

أ- **وضع تعليمات الاختبار:** قامت الباحثتان بإعداد التعليمات الخاصة بالاختبار، بحيث راعت **أن** تكون واضحة ومحددة، وتضمنت الهدف منها، وطريقة الإجابة عليها بالصواب والخطأ أو الاختيار من متعدد، حتى يتسنى لأي طالبة الاجابة عنها بدقة.

ب- **التجربة الاستطلاعية للاختبار** بعد التحقق من صدق الاختبار تم تطبيقه على عينة استطلاعية عددها خمس طالبات من الصف الأول ثانوي بمدرسة الثانوية الثالثة والتسعين بجدة، وهدفت التجربة الاستطلاعية إلى:

- حساب معامل السهولة والصعوبة: تم حساب معامل السهولة والصعوبة لأسئلة الاختبار عن طريق حساب معامل سهولتها ووجد أن معاملات السهولة ومعاملات الصعوبة للاختبار تراوحت ما بين (0.20- 0.80) وأنها ليست شديدة السهولة أو الصعوبة؛ وبقيت جميع اسئلة الاختبار كما هي (61) سؤال.
- معامل التمييز: تم حساب معامل التمييز لكل أسئلة الاختبار ووجد أن معامل التمييز لأسئلة الاختبار لا تقل عن (0.2) وتراوحت بين (0.4- 0.49) مما يبين أن أسئلة الاختبار ذات معامل تمييز مقبولة، وصالحة للتطبيق.
- حساب معامل ثبات الاختبار: بالتطبيق على العينة الاستطلاعية للدراسة تم حساب ثبات الاختبار، بمعامل الثبات ألفاكرونباخ (Cronbach's Alpha) ووجد أن معامل ثبات الاختبار الكلي(0.95) وهو معامل يشير إلى درجة ثبات عالية، مما يجعل الباحثتان تثق في استخدام الاختبار كأداة للقياس عند التطبيق على عينة الدراسة.
- زمن الاختبار: قامت الباحثتان بحساب الزمن التي استغرقته كل طالبة من طالبات (العينة الاستطلاعية) في الإجابة عن الاختبار، من خلال إيجاد متوسط الزمن المستغرق من قبل العينة الاستطلاعية لأول وأخر طالبة انتهت من الإجابة عن الاختبار، ووجد أن متوسط الزمن المستغرق في الإجابة عن الاختبار الكلى (20) دقيقة.

ج- **الصورة النهائية للاختبار:** بعد انتهاء الباحثتان من إعداد الاختبار والتأكد من صدقه وثباته أصبح في صورته النهائية مكون من (61) سؤالاً موزعة على الوحدات الخمس للمقرر الإلكتروني المقترح، وقد أعطيت لكل سؤال درجة واحدة وأصبحت الدرجة العظمى للاختبار (61) درجة.

بناء المقرر الإلكتروني المقترح

يتضمن المقرر الإلكتروني المقترح عدة مراحل هي:

المرحلة الاولى: التحليل (Analysis): تتضمن مرحلة التحليل الخطوات التالية:

- تحليل خصائص الطالبات: قامت الباحثتان بتحليل خصائص الطالبات (عينة الدراسة) كما يلي:

أ- المستوى التعليمي: من حيث المستوى التعليمي طالبات الصف الأول ثانوي للعام الدراسي 1444 – 1445هـ.

ب- العمر الزمني: يتراوح العمر الزمني للطالبات من 15 إلى 17عاماً.

ج- الخبرات السابقة: يتوافر لدى الطالبات خبرات سابقة لمهارات استخدام الكمبيوتر والإنترنت.

- تحديد اهداف المقرر الإلكتروني المقترح: قامت الباحثتان بتحديد الأهداف العامة المطلوب تحقيقها والتي تفيد عند بناء قائمة الأهداف الفرعية المرتبطة بهذه الأهداف، وتحديد عناصر المحتوى العلمي المناسب بحيث عند الانتهاء من المقرر الإلكتروني المقترح، ستتمكن الطالبة من:

1. المعرفة والوعي بمفاهيم الأمن السيبراني.
2. المعرفة والوعي بضوابط الأمن السيبراني.
3. المعرفة والوعي بالجرائم والتهديدات السيبرانية.
4. المعرفة والوعي بالإجراءات المستخدمة لحماية الأمن السيبراني.
5. المعرفة والوعي بإدارة حماية تقنيات الأمن السيبراني.

- تحديد عناصر المحتوى: من خلال تحديد اهداف المقرر الإلكتروني العامة، تم إعداد الصورة المبدئية لقائمة عناصر المحتوى وتمثلت بالموضوعات الآتية:

1. مفاهيم الأمن السيبراني.
2. ضوابط الأمن السيبراني.
3. الجرائم والتهديدات السيبرانية.
4. الإجراءات المستخدمة لحماية الأمن السيبراني.
5. إدارة حماية تقنيات الأمن السيبراني.

- تحليل بيئة التعلم: تم الاستعانة في تدريس الطالبات بمعمل يحتوي على اجهزة كمبيوتر متصلة بشبكة الإنترنت.

المرحلة الثانية: التصميم (Design): يندرج تحت هذه المرحلة الخطوات الفرعية التالية:

- تحديد الأهداف الخاصة: بناء على الاهداف العامة للمقرر الإلكتروني المقترح وتمثلت في (29) أهداف فرعي موزعة على (9) أهداف في الوحدة الأولى، (4) أهداف في الوحدة الثانية، (5) أهداف في الوحدة الثالثة، (3) أهداف في الوحدة الرابعة، (8) أهداف في الوحدة الخامسة.

- تحديد المحتوى وتنظيمه: في ضوء قائمة أهداف المقرر الإلكتروني المقترح التفصيلية في صورتها النهائية تم تحديد محتوى المقرر الإلكتروني المقترح في خمس وحدات، وتتضمن كل وحدة مهام وأنشطة تعلم تؤدى بشكل فردي، وفي نهاية كل وحدة نشاط، ثم يليه تقويم بنائي يتضمن أسئلة بحيث تحصل الطالبة على درجتها في التقويم فور الانتهاء من إجابتها، وتم عرض الصورة المبدئية للمحتوى على مجموعة من الاساتذة المحكمين وعددهم (5) وذلك لإبداء الرأي فيه، ومدى مناسبة موضوعات وصياغة محتوى المقرر الإلكتروني المقترح المناسبة للأهداف وتوزيعها على وحداته الخمس، التي أخذت 80% فأكثر من اتفاق المحكمين، وبذلك توصلت الباحثتان إلى المقرر المقترح.

المرحلة الثالثة: التطوير(Development) تم في مرحلة التطوير تجميع الوسائط المتعددة وإنتاجها، واختيار التطبيقات المساعدة المطلوبة للمقرر الإلكتروني المقترح.

المرحلة الرابعة: التطبيق(التنفيذ) (Implementation): تنفيذ وعرض المحتوي العلمي للمقرر الإلكتروني المقترح وجاء الشكل العام له كما يلى:

1. ظهور الصفحة الرئيسة للمقرر الإلكتروني المقترح المستخدمة لعرض العنوان والمكونات الرئيسية له.
2. ظهور واجهة التفاعل بصفحة المقرر الإلكتروني المقترح.
3. ظهور أهداف المقرر الإلكتروني المقترح.
4. ظهور تعليمات المقرر الإلكتروني المقترح.
5. ظهور الاختبار القبلي للمقرر الإلكتروني المقترح.
6. ظهور دروس المقرر الإلكتروني المقترح.
7. ظهور أدوات المقرر الإلكتروني المقترح.
8. ظهور أنشطة المقرر الإلكتروني المقترح.
9. ظهور الاختبار البعدي للمقرر الإلكتروني المقترح.

المرحلة الخامسة: التقويم (Evaluation) والمراجعة: وتم فيها تقويم المقرر الإلكتروني المقترح، إذ عرضته الباحثتان على مجموعة من الاساتذة المحكمين عددهم(3) للتأكد من صلاحيته للتطبيق وتقويم الأهداف التعليمية والدروس والأنشطة والتدريبات الخاصة بالمقرر الإلكتروني المقترح، وأجمع الاساتذة المحكمين على صحة محتوى المقرر الإلكتروني المقترح، وأصبح في صورته النهائية وصالح لتطبيقه على عينة الدراسة.

المراجعة النهائية: وتمثلت في مراجعة المقرر الإلكتروني المقترح وإضافة التعديلات والمقترحات التي تم الحصول عليها من خلال تطبيق المقرر الإلكتروني المقترح على عينة الدراسة الاستطلاعية المكونة من خمس طالبات بهدف التأكد من فاعلية المقرر الإلكتروني المقترح،وسلامته وصلاحيته للتجريب النهائي على عينة الدراسة.

شكل (1) النموذج المقترح لتصميم المقرر الإلكتروني

إجراءات الدراسة:

1. الإطلاع على الدراسات والبحوث السابقة المرتبطة بموضوع الدراسة الحالية، المتعلقة بالأمن السيبراني، بهدف إعداد الإطار النظري للدراسة وتصميم أدواتها.

2. إعداد رؤية ورسالة وأهداف المقرر الإلكتروني المقترح في ضوء نموذج (ADDIE) للتصميم التعليمي لشموليته ومناسبته للتطبيق بصورته الأولية، وعرضه على مجموعة من الأساتذة المحكمين.
3. بناء وإعداد أداة الدراسة (اختبار الوعي المعرفي بالأمن السيبراني) وتحكيمه من قبل الأساتذة المحكمين.
4. التأكد من الصدق الخارجي والداخلي لأداة الدراسة (الإختبار).
5. إجراء التعديلات في ضوء ملاحظات ومقترحات الأساتذة المحكمين للوصول إلى المقرر المقترح وأداة الدراسة النهائية.
6. تجريب المقرر الإلكتروني على عينة استطلاعية؛ للوصول إلى الصورة النهائية للمقرر المقترح وأداة الدراسة وثباتها.
7. اختيار عينة الدراسة من طالبات الصف الأول ثانوي بمدرسة الثانوية الثالثة والتسعين بجدة، وتطبيق المقرر الإلكتروني المقترح عليهن.
8. التطبيق القبلي للإختبار على عينة الدراسة.
9. تطبيق المقرر الإلكتروني المقترح على عينة الدراسة من طالبات المرحلة الثانوية بجدة.
10. التطبيق البعدي للإختبار على عينة الدراسة.
11. معالجة البيانات إحصائيًا وتحليلها للوصول إلى النتائج.
12. عرض نتائج الدراسة وتفسيرها ومناقشتها.
13. تقديم التوصيات والدراسات المقترحة في ضوء نتائج الدراسة.

المعالجات والأساليب الإحصائية

اجريت المعالجات الإحصائية لبيانات الدراسة باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS21) لاختبار صحة الفروض وفق الأساليب الإحصائية الأتية:

1. معامل الارتباط بيرسون لحساب صدق أداوت الدراسة.
2. معامل ألفا كرونباخ لقياس ثبات أداوت الدراسة.
3. اختبار ويلكوكسن "Wilcoxon Test" للمقارنة بين عينتين مرتبطتين بهدف التعرف على الفروق الدالة إحصائيًا بين متوسطات درجات الطالبات في التطبيق القبلي والبعدي لأدوات الدراسة.
4. معامل الكسب المعدل لبلاك Black لحساب درجة فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة.

4- عرض نتائج الدراسة ومناقشتها.

- **الإجابة عن السؤال الأول**: "ما التصور المقترح لبناء للمقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة؟"

وللإجابة عى السؤال؛ تناولت الباحثتان إجراءات وخطوات إعداد المقرر الإلكتروني المقترح لتنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة، والممثلة بمرحلة التحليل (Analysis)، ومرحلة التصميم (Design)، ومرحلة التطوير(Development)، ومرحلة التطبيق(التنفيذ) (Implementation)، ومرحلة التقويم (Evaluation)، والموضح خطوات بنائه في منهجية وإجراءات الدراسة.

- **الإجابة عن السؤال الثاني:**"ما فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة؟

وللإجابة عن السؤال قامت الباحثتان بصياغة الفرض ونصه " توجد فروق دالة إحصائيًا عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات درجات طالبات المرحلة الثانوية في التطبيق القبلي والبعدي لاختبار الوعي المعرفي بالأمن السيبراني لصالح التطبيق البعدي تعزى للمقرر الإلكتروني المقترح ".

وللتحقق من صحة الفرض استخدمت الباحثتان اختبار ويلكوكسن "Wilcoxon Test" للمقارنة بين عينتين مرتبطتين بهدف التعرف على الفروق الدالة إحصائيًا بين متوسطات درجات الطالبات في التطبيق القبلي والبعدي لأداة الدراسة، ويوضح جدول (2) دلالة الفروق بين متوسط درجات الطالبات البالغ عددهن (ن = 26) في التطبيق القبلي والبعدي لاختبار الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة.

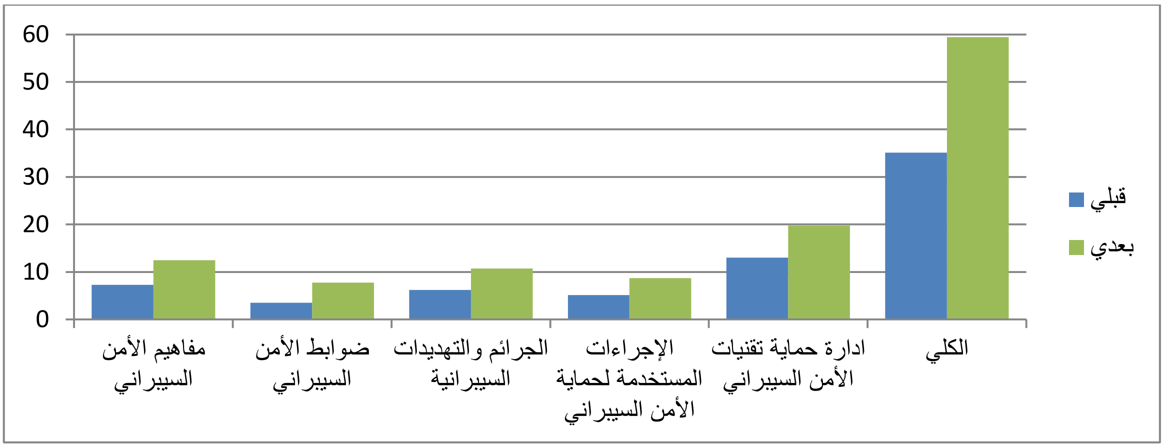
جدول (2) دلالة فروق بين متوسطات درجات الطالبات في التطبيق القبلي والبعدي للاختبار

م	الوحدات	المتوسط الحسابي		درجة الاختبار العظمى	قيمة Z	قيمة الدلالة	الدلالة
		قبلي	بعدي				
1	مفاهيم الأمن السيبراني	7.27	12.50	13	-4.328	.000	دالة
2	ضوابط الأمن السيبراني	3.50	7.77	8	-4.483	.000	دالة
3	الجرائم والتهديدات السيبرانية	6.19	10.69	11	-4.471	.000	دالة
4	الإجراءات المستخدمة لحماية الأمن السيبراني	5.15	8.73	9	-4.303	.000	دالة
5	ادارة حماية تقنيات الأمن السيبراني	13.00	19.77	20	-4.462	.000	دالة
	الكلية	35.12	59.46	61	-4.460	.000	دالة

دالة عند مستوى (0.05)

يتضح من الجدول (2) ان اجمالي متوسط درجات طالبات المرحلة الثانوية في التطبيق البعدي الكلي لاختبار الوعي المعرفي بالأمن السيبراني اكبر من اجمالي متوسط درجات التطبيق القبلي للاختبار، إذ بلغ اجمالي متوسط درجات طالبات المرحلة الثانوية في التطبيق البعدي الكلي لاختبار الوعي المعرفي بالأمن السيبراني (59.46)، بينما بلغ اجمالي متوسط درجات طالبات المرحلة الثانوية في التطبيق القبلي الكلي لاختبار الوعي بالأمن السيبراني (35.12)، وأن اجمالي قيمة مستوى الدلالة الإحصائية المحسوبة بلغت (0.000)=Asymp.Sig(Z)وهي أقل من قيمة مستوى الدلالة المفروضة($\alpha \leq 0.05$)، مما يدلل على وجود فروق دالة إحصائية لصالح التطبيق البعدي الكلي لاختبار الوعي المعرفي بالأمن السيبراني، وبهذا تم التحقق من صحة الفرض بشكل كامل وقبوله.

وشكل (1) يوضح دلالة الفروق بين متوسط درجات الطالبات البالغ عددهن (ن = 26) في التطبيق القبلي والبعدي لاختبار الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة لجميع وحدات المقرر الإلكتروني المقترح.



شكل (1) دلالة الفروق لمتوسط درجات الطالبات في التطبيق القبلي والبعدي لاختبار الوعي المعرفي بالأمن السيبراني

ولحساب فاعلية المقرر الإلكتروني في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية تم حساب درجات الاختبار القبلي والبعدي بكل وحدة على حدة وبشكل كلي، وحسبت فاعلية المقرر الإلكتروني بواسطة معامل الكسب المعدل لبلاكBlack بالمعادلة:

$$\text{معامل بلاك} = \frac{\text{المتوسط البعدي} - \text{المتوسط القبلي}}{\text{النهاية العظمى} - \text{المتوسط القبلي}} + \frac{\text{المتوسط البعدي} - \text{المتوسط القبلي}}{\text{النهاية العظمى}}$$

ويوضح جدول (3) قيمة الكسب المعدل لبلاك Black للوعي بالأمن السيبراني لدى طالبات المرحلة الثانوية لكل وحدة من الوحدات وبشكل كلي.

جدول (3) قيمة الكسب المعدل لكل وحدة من الوحدات وبشكل كلي

م	الوحدات	المتوسط الحسابي		درجة الاختبار العظمى	قيمة الكسب	الدلالة
		قبلي	بعدي			
1	مفاهيم الأمن السيبراني	7.27	12.50	13	1.32	عالي
2	ضوابط الأمن السيبراني	3.50	7.77	8	1.48	عالي
3	الجرائم والتهديدات السيبرانية	6.19	10.69	11	1.34	عالي
4	الإجراءات المستخدمة لحماية الأمن السيبراني	5.15	8.73	9	1.33	عالي
5	ادارة حماية تقنيات الأمن السيبراني	13.00	19.77	20	1.31	عالي
	الكلية	35.12	59.46	61	1.34	عالي

يتضح من الجدول (3) أن قيمة الكسب المعدل لكل وحدة من وحدات المقرر الإلكتروني لجميع القيم أعلى من (1.2)، وهي معدلات كسب عالية إذا قورنت بالحد الأدنى لنسبة الكسب المعدل المقبولة لبلاك وهي (1.2)، كما يتضح أن قيمة الكسب الكلية بلغت (1.3)، وهي معدلات كسب عالية إذا قورنت بالحد الأدنى لقيمة الكسب المعدل لبلاك Black (1.2) مما يدلل على فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية (عينة الدراسة). وبذلك تكون الباحثتان قد أجابتا على السؤال الثاني للدراسة والذي ينص على: "ما فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة؟

مناقشة النتائج

أظهرت نتائج الدراسة ما يأتي:

- وجود فروق دالة إحصائيًا عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات درجات طالبات المرحلة الثانوية في التطبيق القبلي والبعدي لاختبار الوعي بالأمن السيبراني لصالح التطبيق البعدي تعزى للمقرر الإلكتروني المقترح.

تتفق هذه النتيجة مع دراسة حلمي(2018) والتي توصلت إلى وجود فروق دالة إحصائيًا بين درجات اختبار التحصيل المعرفي لصالح المتعلمات اللواتي درست المقرر الإلكتروني، ودراسة داود (2018) والتي توصلت إلى وجود فروق دالة إحصائيًا في مستوى التحصيل المعرفي لصالح الطلبة الذين درسوا المقرر الإلكتروني، ودراسة كاي Cai (2018) والتي توصلت إلى وجود فروق وتحسناً واضحاً في مستوى التحصيل للطلبة في مقرر الأمن السيبراني تعزى للنموذج المقترح للأمن السيبراني، ودراسة العنزي وآخرون(2020) والتي توصلت إلى وجود فروق دالة إحصائيًا في مستوى التحصيل البعدي، لصالح الطلاب الذين درسوا من خلال الوحدة التعليمية الإلكترونية التفاعلية.

كما تختلف النتيجة مع دراسة المنتشري وحريري (2020) والتي توصلت إلى عدم وجود فروق دالة إحصائيًا في درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني تُعزى إلى متغيري المؤهل الدراسي وسنوات الخبرة.

وتعزو الباحثتان النتيجة إلى:

1. أن أسئلة الاختبار المعرفي تعد من الأسئلة التي يبنى عليها الاختبار البعدي ومعرفة المتعلمة بها في التطبيق القبلي ساعد في التقليل من الإجابات الخطأ في الاختبار البعدي.
2. احتواء المقرر الإلكتروني المقترح على الأنشطة التعليمية التفاعلية بالشكل المناسب، والتنوع في اساليب إيصال المحتوى زود المتعلمات بالكثير من المعلومات والمفاهيم والتي لم تكن متوفرة لديها قبل دراستها لمحتوى المقرر الإلكتروني المقترح مما أدى لوجود فروق في التطبيق القبلي والبعدي للاختبار المعرفي الخاص بوعي الطالبات بالأمن السيبراني لصالح التطبيق البعدي تعزى للمقرر الإلكتروني المقترح.
3. تضمن المقرر الإلكتروني المقترح العديد من العناصر المسموعة والمرئية التي عملت على جذب وتركيز انتباه المتعلمات مما ساعد في تنمية المعرفة والوعي بالأمن السيبراني لديهن مما أدى لوجود فروق في التطبيق القبلي والبعدي للاختبار المعرفي الخاص بوعي المتعلمات بالأمن السيبراني لصالح التطبيق البعدي تعزى للمقرر الإلكتروني المقترح.
4. التنظيم الذي يوفره المقرر الإلكتروني المقترح بطريقة متدرجة، وكذلك إتاحة العديد من المواقف الاختبارية (قبلية – بعدية – تقويم ذاتي)، ساعد المتعلمات على تحصيل المعلومة بسهولة ويسر، وجذب انتباهها والاحتفاظ بالمادة التعليمية أطول فترة ممكنة مما أسهم في تنمية الوعي المعرفي بالأمن السيبراني. وساعد في وجود فروق في التطبيق القبلي والبعدي للاختبار المعرفي الخاص بوعي الطالبات بالأمن السيبراني لصالح التطبيق البعدي يعزى للمقرر الإلكتروني المقترح.

- فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة.

أظهرت نتائج الدراسة ان قيمة معامل الكسب المعدل لبلاك Black الكلية بلغت (1.3)،مقارنة بالتطبيق القبلي والبعدي للاختبار المعرفي، وفاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة. وتتفق هذه النتيجة مع دراسة حلمي (2018) والتي توصلت إلى فاعلية مقرر إلكتروني لتنمية التحصيل المعرفي لصالح المتعلمات اللواتي تعرضن للمقرر الإلكتروني، ودراسة داود (2018) والتي توصلت إلى فاعلية المقرر الإلكتروني في تنمية التحصيل المعرفي، ودراسة كاي Cai (2018) والتي توصلت إلى فاعلية النموذج المقترح في تنمية التحصيل للطلبة لمقرر الأمن السيبراني.

وتعزو الباحثتان النتيجة إلى:

1. المعلومات والوسائط المتعددة من نصوص وصوت وصور ثابتة ولقطات فيديو والمؤثرات الصوتية والتفاعلية التي يتضمنها المقرر الإلكتروني المقترح والنشاطات المرتبطة به جعلت التعلم أكثر جاذبية للمتعلمات، واتاح لها التعلم باستخدام أكثر من حاسة، وبالتالي ارتفع وعيها وأداؤها واتجاهها، وانعكس إيجابياً في تنمية وعيها بالأمن السيبراني مما ادى إلى فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني للمتعلمات.
2. احتواء المقرر الإلكتروني المقترح على اختبار الوعي المعرفي ووجود فروق دالة بين التطبيقيم القبلي والبعدي لصالح البعدي يدلل على فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات الثانوية.

3. تصميم المقرر الإلكتروني المقترح وفقاً لخصائص طالبات المرحلة الثانوية ومستواهن الدراسي، ساعد في التفاعل مع محتواه التعليمي برغبةٍ زادت من حدوث التعلم بالأمن السيبراني مما ادى إلى فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى الطالبات المرحلة الثانوية.
4. اهتمام المقرر الإلكتروني المقترح بتقديم الجوانب المعرفية المرتبطة بتنمية الوعي المعرفي بالأمن السيبراني، أدى إلى تنمية الوعي والمعرفة بالأمن السيبراني مما ادى إلى فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لدى الطالبات المرحلة الثانوية.

التوصيات والمقترحات.

في ضوء ما توصلت إليه الدراسة من نتائج توصي الباحثتان وتقترحان ما يلي:

1- الاستفادة من المقرر الإلكتروني المقترح الذي أعدته الباحثتان كمقرر للأمن السيبراني لطالبات مدارس المرحلة الثانوية بمدينة جدة ومناطق المملكة العربية السعودية الأخرى.

2- الاستفادة من نتائج الدراسة التي بينت فاعلية المقرر الإلكتروني المقترح وأداة الدراسة (اختبار الوعي المعرفي بالأمن السيبراني) في تنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية بمدينة جدة.

3- ضرورة استفادة الجهات التعليمية المختصة بالمملكة العربية السعودية من المقرر الإلكتروني المقترح وتحويله إلى برنامج تدريبي في الأمن السيبراني في اقامة دورات تدريبية لتدريب وتنمية الوعي المعرفي بالأمن السيبراني لطلبة مدارس المرحلة الثانوية في مختلف مناطق المملكة العربية السعودية.

4- ضرورة تزويد طالبات المرحلة الثانوية بكل جديد في الوعي المعرفي بالأمن السيبراني من خلال تكثيف الدورات التدريبية، وتقديم مهارات الوعي المعرفية بالأمن السيبراني.

5- كما تقترح الباحثتان إجراء الدراسات الآتية:

1. برنامج تدريبي لتنمية الوعي بالأمن السيبراني لدى معلمات المدارس الحكومية والأهلية في مدينة جدة.
2. درجة وعي طالبات المرحلة الثانوية بالأمن السيبراني والاتجاه نحوه بمدينة جدة.
3. الصعوبات التي تواجه طالبات المرحلة الثانوية للوعي بالأمن السيبراني بالمملكة العربية السعودية.

قائمة المراجع.

أولاً- المراجع بالعربية:

- ابن تاج، لحمر عباس. (2018). أخلاقيات الأعمال الإلكترونية وتحديات الأمن المعلوماتي في ظل الاقتصاد الرقمي. المجلة المصرية للدراسات القانونية والاقتصادية، مصر،10، 299-329.
- أبو زيد، عبد الرحمن عاطف. (2019). الأمن السيبراني الوطن العربي: دراسة حالة المملكة العربية السعودية. آفاق سياسية، ع48، 55–61
- أبو منصور، حسين يوسف. (2017). توظيف تقنية التصنيف الربطي للكشف عن مواقع التصيد الإلكتروني. المجلة العربية الدولية للمعلوماتية. جامعة نايف العربية للعلوم الأمنية. 5 (9)، 32-40.
- بانقا، علم الدين. (2019). مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي. الكويت: المعهد العربي للتخطيط، سلسلة دراسات تنموية، ع.36.
- التيماني، مداخل زيد عبد الرحيم. (2020). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني.
- جميلة، عبيدة؛ بختة، فواطمية. (2018). الوعي المعلوماتي لدى أخصائي المعلومات.. رسالة ماجستير. كلية العلوم الاجتماعية. جامعة عبد الحميد بن باديس- مستغانم- الجزائر.

- حلمي، رانيا وجيه. (2018). مقرر إلكتروني لتنمية التحصيل المعرفي والدافعية للتعلم لدى المتعلمات المعلمات بكلية التربية للطفولة المبكرة. مجلة الطفولة، (29)، 1295- 1366.
- خليفة، إيهاب. .(2017). القوى الإلكترونية كيف يُمكن أن تدير الدول شؤونها في عصر الإنترنت. القاهرة: العربي للنشر والتوزيع.
- داود، سليمان حمودة محمد. (2018). فاعلية مقرر إلكتروني لمهارات الاتصال وفق معايير جودة التعليم الإلكتروني في التحصيل الدراسي والاتجاه نحو المقرر لدى طلاب كلية الشريعة جامعة القصيم- المملكة العربية السعودية. المجلة الدولية للأبحاث التربوية، 42(1)، 1-34.
- الرفاعي، تغريد حمد. (2018). درجة ممارسة وتعرض طلبة المرحلة المتوسطة في مدارس دولة الكويت للتنمر الإلكتروني وأثر متغير الجنس. مجلة العلوم التربوية. جامعة الكويت، 4 (3)، 111- 145.
- السجيني، وليد؛ خليل، حنان. (2017). تصميم المناهج والمقررات الإلكترونية عبر شبكة الويب. عمان، دار المسيرة.
- السمحان، منى عبدالله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية، جامعة المنصورة، 111، 1- 29.
- السواط، حمد؛ الصانع، نورة؛ ابو عيشة، زاهدة. (2020). العلاقة بين الوعي بالأمن السيبراني القيم الوطنية والاخلاقية والدينية لتلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. مجلة البحث العلمي في التربية للعلوم الاجتماعية، 21(4)، 278-306.
- شلوش، نورة. 2018. القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول. مجلة مركز بابل للدراسات الإنسانية، 8(2)، 185-206.
- الشيتي، إيناس ابراهيم. (2019). تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربي السعودية دراسة تطبيقية علي جامعة القصيم. رسالة ماجستير غير منشورة، جامعة القصيم.
- الصانع، نورة (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. Journal of Faculty of Education Assiut University-المجلة العلمية بكلية التربية-جامعة أسيوط، 36(6)، 41-90.
- الصائغ، وفاء بنت حسن عبد الوهاب. (2018). وعي أفراد الآسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية. المجلة العربية للعلوم الاجتماعية، 14(3)، 18-70.
- الصعيدي، عمر سالم؛ السعيد، محمد. (2016). منهجية مقترحة لتطوير وانتاج المقررات الإلكترونية بجامعة المجمعة وأثرها على تنمية كفايات إعداد المقررات الإلكترونية لدى أعضاء هيئة التدريس، تكنولوجيا التربية دراسات وبحوث، ع 29، 327-378.
- صياد، سامية. (2017). فاعلية برنامج تدريبي قائم على التعليم المدمج في تنمية الوعي المعلوماتي بإدارة المراجع إلكترونيا لدى طلبة الدراسات العليا. المجلة المصرية للتربية العلمية، 20 (9)، 101-144.
- عبد القادر، حنان. (2019). المعايير التربوية والفنية اللازمة لتصميم وإنتاج المقررات الإلكترونية لبرنامج Articulate Storyline . المؤتمر العربي، 12، 133- 159.
- العنزي، حاكم بشير؛ القاعود، إبراهيم القادر؛ الهرش، عايد حمدان. (2020). تصميم وحدة تعليمية إلكترونية تفاعلية وقياس أثرها في التحصيل وتعزيز دافعية التعلم في مادة الدراسات الاجتماعية لدى طلاب الصف الأول الثانوي في المملكة العربية السعودية. المجلة الفلسطينية للتعليم المفتوح والتعلم الإلكتروني، 8(24)، 120- 134.
- القحطاني، نورة بنت ناصر. (2019). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية جمعية الاجتماعيين في الشارقة، 36(144)، 85 – 120.
- مطاوع، ضياء الدين؛ الخليفة، حسن. (2017). استراتيجيات التدريس الفعال. مكتبة المتنبي. الرياض، المملكة العربية السعودية.
- المنتشري، فاطمة يوسف؛ حريري، رندة. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية، 4(13)، 95- 140.
- المنديل، خلود خالد. (2020). أثر استخدام بيئة الواقع الافتراضي (Blackboard) في تحسين الكفاءة الذاتية لإنتاج المقررات الإلكترونية لدى أعضاء هيئة التدريس بجامعة المجمعة. المجلة العربية للعلوم ونشر الأبحاث، مجلة العلوم التربوية والنفسية. 4(36)، 61- 88.
- موسى، سميرة. (2020). المقررات الإلكترونية لتعليم اللغة العربية، مجلة العربية، 7(1)، 200- 213.
- الهزاني، محمد ناصر. (2018). المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني: دراسة تأصيلية مقارنة بالقانون الإماراتي. رسالة ماجستير غير منشورة. جامعة نايف العربية للعلوم الأمنية: كلية العدالة الجنائية، قسم الشريعة والقانون.

- هندي، أسامة حسن. (2017). أثر نمط التفاعل والأسلوب المعرفي في التدريب الإلكتروني لإنتاج المقررات الإلكترونية المتاحة عبر الإنترنت MOOCs لدى أعضاء الهيئة المعاونة بجامعة الأزهر. اطروحة دكتوراه منشورة، كلية التربية، جامعة الأزهر، مصر.
- الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبراني، المملكة العربية السعودية.

ثانياً- المراجع الإنجليزية:

- Aljohani, W., & Elfadil, N. (2020). Measuring Cyber Security Awareness of Students: A Case Study at Fahad Bin Sultan University.
- Alshamsi, A. A. (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. International Journal of Information Technology and Language Studies, 3(2).
- Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), 06-16.
- Bustard, J. (2018). Improving student engagement in the study of professional ethics: concepts and an example in cyber security. Scientific engineer ethics. 24, 683-698.
- Cai, Yu (2018). Using case studies to teach cybersecurity courses. Journal of cybersecurity education, research and practice. 2, 1-24
- Goran, I. (2017). Cyber security risks in public high school. Unpublished master thesis. City university of New York: John Jay college of criminal justice
- Kritizinger, E., Bada, M., & Nurse, J. (2017). A study into the cybersecurity awareness initiatives for school learners in south africa and the uk. 10th world conference on information security education. Rome: May 29-31
- Mark, L. & Nguyen, T. (2017). An Invitation to Internet Safety and Ethics: School and family collaboration. journal of invitational theory and practice. 23, 62-75.
- Pande, Jeetendra. (2017). Introduction to Cyber Security, Uttarakhand Open University.
- Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F.(2020) The Importance of Cybersecurity Education in School. International Journal of Information and Education Technology, Vol. 10, No. 5, 378-382.
- Richardson, M., Lemoine, P., Stephens, W., & Waller, R. (2020). Planning for Cyber Security in Schools: The Human Factor. Educational Planning,
- Tiwari, S., Bhalla, A., & Rawat, R. (2017). Cyber-crime and security. International journal of advanced research in computer science and software engineering. 6(4), 46-5227(2), 23-39.
- Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as “the three R's”. Heliyon, 5(12), 28-55.