ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد الواحد والثمانون
تاريخ الإصدار: 2 – تموز – 2025م
www.ajsp.net

"تصميم مقرر مقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع"

اعداد الباحثات:

أ.د / هيلة بنت خلف الدهيمان

أستاذ المناهج وطرق التدريس بجامعة الإمام محمد بن سعود الإسلامية

الجوهرة بنت مرداس عليان المطيري / حصه بنت قياض عبدالله العنزي / ندى بنت عبدالعزيز المعشوق

باحثات دكتوراه بقسم المناهج وطرق التدريس بجامعة الإمام محمد بن سعود الإسلامية

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد الواحد والثمانون
تاريخ الإصدار: 2 – تموز – 2025م
www.ajsp.net

المستخلص:

هدفت هذه الدراسة إلى تصميم مقرر مقترح يهدف إلى تنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية، وذلك من خلال تطبيق التعلم القائم على المشاريع. كما سعت الدراسة إلى تقييم فعالية هذا المقرر في تعزيز تلك المهارات، اتبعت الدراسة المنهج شبه التجريبي باستخدام مجموعة تجريبية واحدة مع إجراء قياسين قبلي وبعدي، وتكونت عينة الدراسة من 30 طالبة تم اختيارهن بطريقة العينة القصدية. وشملت أدوات الدراسة المقرر المقترح لتنمية مهارات الأمن السيبراني، بالإضافة إلى استبيان صُمم خصيصًا لقياس مستوى هذه المهارات، أظهرت النتائج فعالية المقرر المقترح في تنمية مهارات الأمن السيبراني لدى الطالبات، حيث لوحظت فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين القياسين القبلي والبعدي في جميع مجالات المهارات المدروسة، والتي شملت: حماية البيانات الشخصية، إدارة كلمات المرور، مواجهة المخاطر المحتملة، التفاعل الآمن مع الآخرين، بالإضافة إلى الصيانة وطلب المساعدة. وتعزى هذه الفروق إلى تأثير المقرر المقترح لصالح القياس البعدي.

الكلمات المفتاحية: مقرر مقترح – مهارات الأمن السيبراني – التعلم القائم على المشاريع.

المقدمة:

تعد المناهج الدراسية أداة أساسية في بناء الأفراد الذين يشكلون دعامة المجتمعات، حيث يمثل الفرد العنصر الأهم في أي مجتمع. وتعتمد جودة المجتمع وكفاءته على ما تقدمه المناهج الدراسية من وسائل فعالة في صقل شخصية الإنسان وتطوير قدراته. لذلك، فإن تحديث المناهج بما يتناسب مع متطلبات العصر ومستجداته يحدد شكل المجتمع ومستقبله، ففي عصرنا الحالي، أصبح تطور الأمم يقاس بمدى تقدمها في العلوم الحديثة وقدرتها على الاستفادة من هذا التقدم وتوظيفه في خدمة التنمية. لذا، فإن تطوير المناهج الدراسية بما يواكب هذه المتغيرات لم يعد خيارًا، بل ضرورة لتمكين المجتمعات من مواكبة العالم وتحقيق التقدم.

وفي ظل التحول الرقمي المتسارع الذي يشهده العالم، أصبح الأمن السيبراني أحد الركائز الأساسية لضمان حماية البيانات والمعلومات، لا سيما في المملكة العربية السعودية التي تشهد نموًا غير مسبوق في الاعتماد على التقنية. وفقًا لـ رؤية المملكة 2030 (2016)، فإن بناء مجتمع رقمي آمن يُعدُّ أحد المحاور الرئيسية لتمكين التحول الوطني، حيث تؤكد الرؤية على "ضرورة تعزيز المهارات الرقمية للنشء لمواكبة متطلبات المستقبل"، ومع ذلك، تُظهر دراسة العنزي والعقاب (2019) أن مناهج الحاسب الآلي في المرحلة الثانوية لا تُولي الأمن السيبراني الاهتمام الكافي، حيث اقتصرت تغطية هذه المهارات على نسبة ضئيلة من المحتوى التعليمي، مما يعكس فجوةً بين الأهداف الاستراتيجية والواقع التعليمي.

في هذا السياق، تشير دراسة المحمادي (2023) إلى أن 96.3% من السعوديين يستخدمون الإنترنت يوميًا، بينما تعرض ثلثا السكان لمحاولات احتيال إلكتروني، أن دول الخليج ومن ضمنها المملكة العربية السعودية أقل قدرة على مواجهة مخاطر الهجمات السيبرانية بسبب انخفاض المهارات التقنية بها مقارنة بالدول المتقدمة، وفقًا لتقرير المركز الوطني لاستطلاعات الرأي العام (2022). هذه الأرقام تُبرز الحاجة الملحّة لتعزيز الوعي السيبراني لدى الطلاب، خاصةً في المرحلة الثانوية التي تُعدُّ مرحلةً حرجةً لتشكيل السلوك الرقمي. ومع ذلك، تُظهر دراسة تحليل المحتوى التي أجرتها الغملاس (2024) أن كتب التقنية الرقمية للصف الثاني ثانوي تخلو تمامًا من أي إشارةٍ إلى استراتيجيات الحماية من التهديدات الإلكترونية، وهو ما يتناقض مع توصيات السمحان (2020) الذي أكد أن الأمن السيبراني فرض نفسه في القرن الحادي والعشرين.

ولتعزيز جاهزية الطالبات لمواجهة هذه التحديات، تقدم هذه الدراسة مقررًا مقترحًا يعتمد على نموذج ADDIE، الذي عرّفه اللقاني والجمل (2003) بأنه إطار منهجي يمر بخمس مراحل: التحليل، التصميم، التطوير، التنفيذ، والتقويم. وقد دعمت دراسة السليماني وفرج (2021) فعالية هذا النموذج في تصميم المواد التعليمية، خاصةً عند دمجه مع التعلم القائم على المشاريع (PBL)، الذي يُعَدُّ أداةً فعّالةً لتنمية المهارات العملية، كما أوضحت دراسة علي وآخرون (2025) التي حققت تحسنًا ملحوظًا في أداء الطالبات عبر مشاريع واقعية. هذا النهج يتوافق مع ما أكدته رؤية 2030 من ضرورة ربط التعليم باحتياجات سوق العمل.

وترجمةً لنهج قيادة بلادنا الحكيمة لهذه المتغيرات وتفاعلاتها مع مستجدات العصر الرقمي وتطوراته، ومواكبة الرؤية الطموحة للمملكة العربية السعودية 2030م لذلك، صدر الأمر الملكي الكريم رقم 6801 وتاريخ 11/2/1439هـ بإنشاء الهيئة الوطنية للأمن السيبراني التي تعد أحد أهم روافد المشاريع الوطنية النوعية، وجاء هذا الأمر في الوقت المناسب لتكون هذه الهيئة مرجعًا وطنيًّا يهتم بحماية المصالح الحيوية للمملكة وأمنها السيبراني، وكافة خدماتها ومناشطها الإلكترونية.

حيث أكدت العديد من الدراسات والمؤتمرات على أهمية التوعية الرقمية، كدراسة محمد (2020) التي أوصت بأهمية توعية الطلاب والمعلمين بخطورة الحروب السيبرانية، وضرورة توجيههم إلى كيفية الاستخدام الآمن للإنترنت، بما يسهم في الحفاظ على أمنهم الشخصي ومعلوماتهم وخصوصياتهم، ويعزز وعيهم بحقوقهم ومسؤولياتهم الرقمية، وقواعد وسلامة التعامل الرقمي،وظهرت العديد من الدراسات مثل دراسة الغملاس (٢٠٢٤م) ودراسة القحطاني والشبل (٢٠٢٢) التي تدعو إلى ضرورة الاهتمام بتطوير منهج الحاسب الآلي من قبل متخصصي المناهج وطرق التدريس في الحاسب الآلي .

أما عن حدود الدراسة، فقد اقتصر التصميم المقترح على **طالبات الصف الثاني ثانوي في المملكة، نظرًا لكون هذه الفئة العمرية (16–17 عامًا) أكثر عرضةً للمخاطر الرقمية، وفقًا لتحليل الدوسري (2017)، الذي أشار إلى أن غياب التوعية في هذه المرحلة قد يؤدي إلى ممارسات رقمية غير آمنة. كما اعتمدت الدراسة على المنهج الوصفي التحليلي، الذي يُعدُّ الأنسب لتحليل المحتوى وتصميم المقررات، بحسب ما ذكره آل جديع (2021) في دراسته حول تطبيق نماذج التصميم التعليمي.

لذلك، يُقدِّم هذا البحث إطارًا عمليًا لسد الفجوة بين السياسات الطموحة لـ رؤية 2030 والواقع التعليمي، من خلال مقررٍ يُعزِّز مهارات الأمن السيبراني باستخدام نموذج مُجرَّبٍ ومدعومٍ بأدلة علمية، حيث أشارت دراسة الرويلي والحويطي (2024) التي أثبتت فاعلية النماذج التصميمية في تحسين نواتج التعلم.

مشكلة الدراسة:

تنبثق مشكلة الدراسة وأسئلتها مما تقوم به وزارة التعليم بأدوار مختلفة تجاه طلبتها ومن ذلك مسؤولية نشر الوعي التقني، واستشعارًا بأهمية الأنظمة التقنية والتكنولوجيا وتطبيقاتها المتجددة وارتباطها بالاستخدام الشخصي للأفراد، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء الإلكتروني، كان من المهم السعي لإثارة التساؤل حول تصميم مقرر مقترح لتنمية مهارات الأمن السيبراني في مقرر تقنية رقمية لدى طالبات الصف ثاني ثانوي؛ وتبني طرق تكنولوجية حديثة لإكساب الطلبة مهارات الأمن السيبراني معرفيا وأدائيا.

وفي ظل التوجه العالمي المتسارع نحو التحول الرقمي، والذي تُعَدُّ المملكة العربية السعودية أحد أبرز رواده عبر مبادرات رؤية 2030 (2016) الهادفة إلى بناء مجتمع معرفي قائم على الاقتصاد الرقمي، تبرز الحاجة المُلحّة لتعزيز مهارات الأمن السيبراني لدى النشء

كأحد الركائز الأساسية لضمان أمن الفضاء الإلكتروني. ومع ذلك، تُشير دراسة العنزي والعقاب (2019) إلى أن مناهج الحاسب الآلي وتقنية المعلومات في المرحلة الثانوية –رغم تحديثها المستمر– لا تُولي الاهتمام الكافي لمهارات الحماية الرقمية، حيث اقتصرت تغطية الأمن السيبراني على إشارات عابرة دون تعمق في المفاهيم أو التطبيقات العملية. هذا الواقع يتناقض مع توصيات المنتدى الدولي للأمن السيبراني (2024) الذي عُقد في الرياض، ودعا إلى "دمج مفاهيم الأمن السيبراني في المناهج التعليمية منذ المراحل المبكرة".

من جهة أخرى، كشفت الدراسة الاستطلاعية التي أجرتها الباحثة –عبر مقابلات مع 19 طالبةً من الصفوف العليا من المرحلة الإبتدائية– عن وجود قصورٍ كبيرٍ في الوعي السيبراني، حيث أظهرت النتائج أن 78% من الطالبات لا يُمكنهن التمييز بين التهديدات الإلكترونية الشائعة (مثل التصيد الاحتيالي أو البرمجيات الخبيثة)، في حين أن 65% منهن يستخدمن كلمات مرور ضعيفة لا تتوافق مع معايير الأمان الأساسية، هذه النتائج تتوافق مع ما أشارت إليه دراسة المحمادي (2023) التي وجدت أن 63% من الطلاب الجامعيين في المملكة يفتقرون إلى المهارات اللازمة لحماية بياناتهم الشخصية، وهو ما يعكس فجوةً مؤسسيةً في تعزيز الثقافة الرقمية الآمنة.

في السياق ذاته، يُظهر تحليل محتوى منهج التقنية الرقمية للصف الثاني ثانوي (مسار عام) –وفقًا لدراسة الغملاس (2024)– أن الوحدة الخاصة بالأمن السيبراني تشغل فقط 7% من إجمالي المحتوى، مع تركيزٍ شبه كاملٍ على الجانب النظري كتعريفات عامة دون تقديم أنشطة تطبيقية أو مشاريع التحديات الواقعية "simulate". هذا النقص يُعزز ما أكده القحطاني والشبل (2022) من أن المناهج الحالية لا تُنمّي المهارات الأدائية المطلوبة لسوق العمل الرقمي، خاصةً في ظل تصاعد الهجمات الإلكترونية التي تستهدف الأفراد، وبحسب تقرير الهيئة الوطنية للأمن السيبراني فقد احتلت المملكة المرتبة الثانية عالميًا في عدد الهجمات السيبرانية خلال عام 2023.

أمام هذه التحديات، تبرز مشكلة الدراسة في التساؤل عن كيفية تصميم مقرر تعليمي فعّال قادر على سد الفجوة بين المستهدفات الاستراتيجية لرؤية 2030 –التي تُركّز على تمكين الشباب رقميًا– والواقع التعليمي الذي يُهمّش مهارات الأمن السيبراني، وخاصةً أن الدراسات السابقة –مثل بحث العنزي (2019)– اقتصرت على تحليل المحتوى دون تقديم حلول تصميمية قائمة على نماذج تربوية مُجرّبة، كنموذج ADDIE الذي أوصت به دراسة السليماني وفرج (2021) لضمان جودة المخرجات التعليمية. كما أن ندرة الأبحاث التي تجمع بين هذا النموذج واستراتيجية التعلم القائم على المشاريع (PBL) – كما في دراسة على وآخرون (2025)– تُضفي أهميةً إضافيةً لهذا البحث، كونه يقدّم إطارًا متكاملًا يُراعي الجانبين النظري والتطبيقي لتنمية المهارات الرقمية الآمنة.

مما سبق تتمثل مشكلة الدراسة في تصميم مقرر مقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع، بهدف تنمية مهاراتهن التقنية والفكرية، ومواءمتهن لمتطلبات سوق العمل، في ضوء رؤية المملكة 2030.

أسئلة الدراسة:

وبناء على ما سبق يمكن صياغة مشكلة الدراسة من خلال الاسئلة التالية:

1. ما تصميم المقرر المقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع؟

2. ما فعالية المقرر المقترح في تنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع؟

أهداف الدراسة:

تهدف الدراسة إلى تحقيق الأهداف التالية:

1. تصميم مقرر مقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع.

2. الكشف عن فعالية المقرر المقترح في تنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع.

أهمية الدراسة:

تتمثل أهمية الدراسة من خلال الأهمية النظرية والأهمية التطبيقية، ويمكن توضيحها بالآتي:

الأهمية النظرية:

وتتمثل أهمية الدراسة في الجانب النظري بأنها:

1. تعدّ هذه الدراسة استكمالاً لسلسلة الدراسات التي اهتمت بقضايا تطوير المنهج وتصميمه وفق نماذج المنهج.

2. ندرة الأبحاث والدراسات التي تناولت تصميم مقرر مقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع، وذلك في ظل ارتفاع الأصوات التي تنادي بضرورة تطوير وتصميم مناهج التقنية الرقمية.

3. توجيه الباحثين إلى تبني توجهات جديدة في أبحاثهم العلمية، لتساعدهم بتطوير مجتمعهم أمام تحديات العصر ومتغيراته، وذلك بآليات ورؤى جديدة تسهم في معالجة أوجه القصور المرتبطة بمناهج التقنية الرقمية.

الأهمية التطبيقية:

تبرز الأهمية التطبيقية للدراسة في الآتي:

1. ستُسهم الدراسة في اقتراح تطوير وصياغة محتوى منهج التقنية الرقمية في المرحلة المقبلة، وذلك من خلال تقديم تصميم مقرر مقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع.

2. قد تفيد القائمين على تأليف منهج التقنية الرقمية في المرحلة الإبتدائية عامة، الصفوف العليا منها خاصة عند التخطيط لتصميم المناهج.

3. تقديم بعض الإرشادات والمقترحات لمعلميّ ومعلمات التقنية الرقمية لتدريس محتوى المادة وفقا لمهارات الأمن السيبراني، مما يزيد من الوعي لدى الطالبات بالأمن السيبراني ومهاراته.

حدود الدراسة:

اقتصرت الدراسة الحالية على الحدود الآتية:

- **الحدود المكانية:** اقتصرت هذه الدراسة على تصميم مقرر مقترح لطالبات الصفوف العليا من المرحلة الابتدائية في المملكة العربية السعودية.
- **الحدود الزمانية:** سيتم تطبيق الدراسة في الفصل الدراسي الثالث من العام الدراسي 1446 هجري، والموافق 2025م.
- **الحدود الموضوعية:** اقتصرت الدراسة على تصميم مقرر مقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية في ضوء التعلم القائم على المشاريع.

مصطلحات الدراسة:

- **الأمن السيبراني:**

يعرّف بأنه "أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها" (الربيعة، 2018، ص6).

ويعرّفه الربيعة (2018) أيضاً بأنه "المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم ويشمل ذلك الأجهزة الالكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية الفضاء السيبراني ليس الإنترنت فقط وإنما شبكات أخرى كثيرة متصلة" (ص7).

وتعرفه الباحثات إجرائيا بأنه "الجوانب المختلفة لأمن المعلومات والأجهزة المرتبطة بشبكة الإنترنت، وذلك عن طريق استخدام الوسائل والأساليب المختلفة والتي توفر قدرًا مناسبًا من الأمان لبيانات وأجهزة طالبات المرحلة الثانوية، وتحول دون الوصول غير المصرح لتلك البيانات من قبل أطراف خارجية".

- **مهارات الأمن السيبراني:**

عرفها العلوان (2021) بأنها "مجموعة من القدرات والمعرفة التي تمكّن الأفراد من حماية الأنظمة والشبكات والبيانات من التهديدات والهجمات الرقمية، وتشمل القدرة على التعرف على المخاطر، تطبيق استراتيجيات الحماية، والاستجابة للحوادث الأمنية بفعالية " (ص.85)

وعرفها بأنها "بأنها مجموعة من الكفاءات التي تشمل المعرفة التقنية، المهارات العملية، والقدرات الشخصية، التي تمكّن الأفراد من التصدي للتهديدات الرقمية وحماية المعلومات والأنظمة (Chowdhury & Gkioulos 2021, p. 25).

وتعرفها الباحثات إجرائيا بأنها "مجموعة من المهارات المعرفية والتطبيقية التي تمكن طلاب الصف الثاني الثانوي من حماية معلوماتهم وأنظمتهم الرقمية من المخاطر السيبرانية، من خلال التعرف على التهديدات الإلكترونية، وتطبيق ممارسات الأمان الرقمي، واتخاذ الإجراءات الوقائية اللازمة لضمان سلامة البيانات والخصوصية على الإنترنت".

- التعلم **القائم على المشاريع:**

يعرف بأنه "نموذج ينظم التعلم حول المشاريع على هيئة مهام معقدة معتمداً على أسئلة أو مشكلات يشرك من خلالها الطلاب في التصميم أو حل المشكلات أو اتخاذ القرارات أو أنشطة الاستقصاء ويعطون فرصة للعمل بشكل مستقل نسبياً على مدار فترات زمنية محددة تظهر في صورة منتجات واقعية أو عروض تقديمية" (Thomas, 2000, p.1).

كما عرفه زهران (Zahran, 2018) بأنه مدخل تعليمي لتنمية مهارات القراءة والكتابة لدى الطلاب من خلال دمجهم في أنشطة جماعية تتضمن حل المشكلات واتخاذ القرارات ومهام فردية تقدم في صورة منتج أو عرض تقديمي" (ص.53).

وتعرفه الباحثات إجرائيًا بأنه أحد أساليب التعلم الحديث، والذي يتميز بإتاحة الفرصة للمتعلمين بالتفاعل النشط والمشاركة الفعالة في جميع خطوات المشروع من اختيار وتخطيط وتطوير وتنفيذ وتقويم، ويتميز ببقاء أثر التعلم لفترة طويلة.

الإطار المفاهيمي

يتناول هذا الفصل الإطار المفاهيمي، والدراسات السابقة، وقد استفادة الباحثة من هذه الأدبيات في تكوين تصور شامل عمّا يمكن أن يتناوله هذا البحث في ضوء أهدافه، من رسم لإجراءاته، وتصميم لأداته.

تمهيد:

يعد الحاسب في الوقت الحاضر مادة دراسية مهمة كغيره من المواد الدراسية؛ نظرا للحاجة إلى استخدامه في جميع مجالات الحياة وخصوصا مجال سوق العمل، ويختلف عن المواد الآخرى في أن استخداماته تدخل في مختلف العلوم والمواد الدراسة، فقد أشار الدوسري (2017) أن الحاسوب عبارة عن أحد الأجهزة الإلكترونية والتي تكون قادرة على أن تستقبل البيانات وتعالجها حتى تحولها إلى معلومات لها فاعليتها وقيمتها ومن ثم تخزينها حيث يمكن أن تستخدم في مجالات متعددة.

ووفقاً لذلك تبرز ضرورة الحاجة المستمرة إلى إعادة النظر في محتوى المقررات المدرسية ولاسيما مقررات الحاسوب لتواكب التغيرات السريعة التي تطرأ في هذا المجال بغية الوصول بها لتحقيق وظائفها، إذ يعد الحاسوب وسيلة فاعلة في العملية التعليمية في هذا العصر الذي تطور فيه أساليب الدراسة العلمية والتغير التقني السريع (العنزي والعقاب ،٢٠١٩).

السيبرانية:

تعتبر السيبرانية مأخوذة من كلمة (سيبر) Cyber، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية، تعني: فضاء الانترنت (الربيعة، 2018، ص. 6).

مفهوم الأمن السيبراني:

يعتبر مصطلح الأمن السيبراني مصطلح حديث، ووردت العديد من التعريفات للعلماء والباحثين حول مفهوم الأمن السيبراني، ومن تلك التعاريف ما يلي:

عرفه الاتحاد الدولي للاتصالات بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات االمؤسسات والمستخدمين" (فوزي، 2019: 103).

كما يعرف أيضًا بأنه "حماية الشبكات وأنظمة تقنية المعلومات، ومكوناتها من أجهزة وبرمجيات، وخدمات، وبيانات، من أي اختراق، أو تعطيل، أو استغلال غير مشروع" (الهيئة الوطنية للأمن السيبراني، 2020، ص 32)

ويعرف بأنه "الإجراءات والوسائل والتقنيات التي تهدف إلى حماية البيانات والمعلومات والأنظمة وما تقدمه من خدمات من أي شكل من أشكال التدخل غير المشروع الذي قد يؤدي إلى تعطيل الأجهزة أو اختراق البيانات والمعلومات والتلاعب بها أو سوء استخدامها مما يشكل خطرًا على المصالح الشخصية والعامة" (Hasweh & Hamed, 2023, 64).

وعرفه المحيميد (2023) بأنه "عبارة عن مجموعة من الوسائل التقنية التي تحقق أمن المعلومات الإلكترونية، وأمن الحاسبات، وأمن الأنظمة الإدارية والبرامج، وأمن الشبكات، وبناءً على ذلك يعد مفهوم الأمن السيبراني أوسع وأشمل من مفهوم أمن المعلومات الإلكترونية، إذ يعد أمن المعلومات الإلكترونية جزءًا من الأمن السيبراني" (ص. 90).

من خلال التعاريف السابقة نجد أنها رغم اختلاف الجوانب التي تناولها الباحثون إلا أنها تشترك في بعض النقاط الأساسية، ومنها:

1. حماية الأنظمة والشبكات من الهجمات الإلكترونية.
2. ضمان سرية وسلامة وتوافر المعلومات.
3. استخدام تقنيات وإجراءات لمنع الوصول غير المصرح به.
4. تأمين البنية التحتية الرقمية والمعلوماتية.
5. التركيز على السياسات والإجراءات التي تدير المخاطر السيبرانية.

مجالات الأمن السيبراني:

تتعدد مجالات الأمن السيبراني ومنها:

- **أمن الشبكات:** حماية الشبكات من التهديدات والهجمات مثل الهجمات الموزعة على الخدمة (DDoS) والتسلل غير المصرح به (Scarfone & Mell, 2007).
- **أمن التطبيقات:** ضمان أن التطبيقات البرمجية خالية من الثغرات التي قد تسمح بالاختراق أو سرقة البيانات (Howard & LeBlanc, 2003).
- **أمن المعلومات:** حماية البيانات من السرقة أو التلف أو التعديل غير المصرح به (Bishop, 2003).
- **أمن الأنظمة:** تأمين أنظمة التشغيل والبنية التحتية الحاسوبية ضد الهجمات والبرمجيات الخبيثة (Sharma & Sood, 2017).

- **الاستجابة للحوادث:** التعامل مع الحوادث الأمنية فور حدوثها للحد من الأضرار واستعادة الأنظمة (Killcrece et al., 2003).
- **التشفير:** استخدام تقنيات التشفير لضمان سرية البيانات أثناء النقل والتخزين (Menezes et al, 1996).

مما سبق نجد تعدد مجالات الأمن السيبراني بحيث تشمل بشكل عام حماية كل ما هو مرتبط بالبنية الحاسوبية وشبكات الإنترنت، ووضع الحلول المناسبة للحد من الاستخدام غير المشروع لتلك البنية.

مفهوم مهارات الأمن السيبراني:

وجدت العديد من التعريفات للباحثين حول مفهوم مهارات الأمن السيبراني، ومنها:

تعرف بأنها القدرات التقنية والمعرفية التي تمكن الأفراد من حماية الأنظمة والمعلومات الرقمية من الهجمات الإلكترونية والتهديدات السيبرانية (Alshaikh et al., 2020).

وتعرف بأنها مجموعة من المهارات الفنية والسلوكية التي تساعد في التعرف على المخاطر السيبرانية والتعامل معها بفعالية (Kumar & Carley, 2021).

كما تعرف بأنها القدرة على تطبيق المعرفة الأمنية في بيئة العمل الرقمية لضمان سرية وسلامة وتوافر المعلومات (Hadnagy, 2018)، وتشمل مهارات الأمن السيبراني تشمل فهم تقنيات الحماية، تحليل التهديدات، والاستجابة للحوادث الأمنية (Safa et al., 2016).

وتعرف أيضًا بأنها مجموعة من المهارات التي تمكن الأفراد من استخدام الأدوات الأمنية، تنفيذ السياسات، والتعامل مع التهديدات السيبرانية بشكل استباقي (Nguyen et al., 2022)

من خلال التعريفات السابقة لمهارات الأمن السيبراني نجد أنها تشترك في العديد من النقاط، ومنها:

- ضرورة الجمع بين المهارات التقنية والمعرفية.
- القدرة على التعرف على التهديدات السيبرانية وتحليلها.
- القدرة على اتخاذ الإجراءات الوقائية والاستجابة السريعة للحوادث.
- أهمية الجانب السلوكي والوعي الأمني لدى الأفراد.
- تطبيق المهارات في بيئات العمل الرقمية المختلفة للحفاظ على أمن المعلومات.

مهارات الأمن السيبراني:

لمواجهة التهديدات السيبرانية يتوجب امتلاك بعض المهارات التي تساهم في تحقيق ذلك، ومنها:

- **المهارات التقنية:** مثل فهم شبكات الحاسوب، أنظمة التشغيل، التشفير، وأنظمة كشف التسلل
- **مهارات التفاعل الأمن مع الآخرين:** بحيث يستطيع الفرد من خلالها التعامل والتفاعل الأمن مع الآخرين بصورة آمنة (Alshaikh et al., 2020).
- **مهارات تحليل المخاطر:** القدرة على تقييم نقاط الضعف والتهديدات المحتملة واتخاذ الإجراءات المناسبة.
- **مهارات التعرف على المحتوى الخطر:** حيث تتيح هذه المهارة التعرف على الروابط والمواقع التي تشكل تهديدًا وخطرًا على الفرد، وعدم فتح أو دخول تلك الروابط.

– **مهارات إدارة كلمات المرور:** وذلك من خلال استخدام كلمات مرور مناسبة وذات درجة منخفضة من التخمين، والابتعاد عن كلمات المرور الشائعة (Safa et al., 2016).

– **مهارات الاستجابة للحوادث:** التعامل مع الحوادث الأمنية بسرعة وفعالية لتقليل الأضرار.

– **مهارات الصيانة وطلب المساعدة:** حيث توفر للمستخدم صيانة الأجهزة بنفسه عندما يشعر بأنه معرض للتهديدات السيبرانية، وكيفية طلب المساعدة عندما يشعر بعجزه عن التعامل معها (Killcrece et al., 2003).

– **مهارات البرمجة والأتمتة:** معرفة لغات البرمجة الأساسية وأدوات الأتمتة لتعزيز الحماية (Nguyen et al., 2022).

– **مهارات الوعي الأمني:** فهم السياسات الأمنية وأهمية الالتزام بها، بالإضافة إلى تعزيز السلوكيات الآمنة في الاستخدام الرقمي (Hadnagy, 2018).

الحاجة إلى امتلاك مهارات الأمن السيبراني:

من المهم امتلاك الفرد لمهارات الأمن السيبراني وخصوصًا الطالبات في مختلف المراحل الدراسية، وذلك للأسباب التالية:

1– حماية الخصوصية الشخصية: حيث أن المراهقين معرضون بشكل كبير لهجمات التصيد والاختراق التي تستهدف بياناتهم الشخصية (Livingstone et al., 2017).

2– تعزيز الوعي الرقمي: تنمية الوعي حول المخاطر السيبرانية تساعد الطالبات على استخدام الإنترنت بشكل آمن ومسؤول (Kumar & Carley, 2021).

3– الاستعداد المهني: تزويد الطالبات بمهارات الأمن السيبراني يفتح أمامهن فرصاً مهنية في سوق العمل المتنامي في هذا المجال (Nguyen et al., 2022).

3– الحد من الجرائم الإلكترونية: من خلال التوعية والمهارات يمكن تقليل الوقوع ضحية للجرائم الإلكترونية مثل الاحتيال والابتزاز (Safa et al., 2016).

5– تعزيز الثقة في البيئة الرقمية: يساعد امتلاك المهارات على استخدام التكنولوجيا بثقة وأمان، مما يدعم التعلم الإلكتروني والتواصل الاجتماعي الآمن (Livingstone et al., 2017).

النموذج العام لتصميم التعليم ADDIE:

نموذج تصميم التعليم هو تمثيل مبسط لمجموعة من العلاقات بين العناصر التي يتألف منها موضوع الدرس، وتكون على شكل صورة أو مخطط أو شبكة، ويجب أن تتوافر بنماذج التصميم التعليمي عدة خصائص ومنها الاختزال والتركيز والاكتشاف (القميزي، 2017).

وأشار آل جديع (٢٠٢١) تمثل فلسفة نماذج التصميم التعليمي في أن التعلم يكون أكثر فاعلية عندما يتم تخطيطه وتصميمه بعناية لتلبية خصائص الطلاب، ويعد نموذج آدي ADDIE Model أساس جميع نماذج التصميم التعليمي وهو أسلوب نظامي لعمليه تصميم التعليم حيث يزود المصمم بإطار إجرائي يضمن أن تكون المخرجات التعليمية ذات كفاءة وفاعلية في تحقيق الأهداف.

وقد تم طرح نموذج ADDIE لأول مرة من قبل مركز تكنولوجيا التعليم بجامعة ولاية فلوريدا في منتصف السبعينيات، وبذلك أصبح نموذج ADDIE الآن نموذجاً تقنيا يستخدم على نطاق واسع في جميع أنحاء العالم، ويعتقد بعض الباحثين أن هذا النموذج مرن بما يكفي للتكيف مع بيئات تعليمية مختلفة، وبالتالي، فهو قابل للتطبيق بقوة لدمج التكنولوجيا في العملية التعليمية (Almelhi, 2021).

ISSN: 2663-5798 || Arab Journal for Scientific Publishing
الإصدار الثامن – العدد الواحد والثمانون
تاريخ الإصدار: 2 – تموز – 2025م
www.ajsp.net

ويستخدم نموذج ADDIE من قبل مصممي التعليم ومطوري الحقائب التدريبية، ويشتمل النموذج على خمس مراحل هي: التحليل Analysis Phase، والتصميم Design Phase، والتطوير Development Phase، والتنفيذ Implementation Phase، والتقييم Evaluation Phase (آل جديع ،٢٠٢١)، ويوضح الشكل التالي مراحل النموذج:

شكل (1) يوضح مراحل نموذج ADDIE (حويري ،٢٠٢٠، ص. ١٣٦)

وفيما يلي المراحل بالتفصيل وقد جاءت على النحو التالي:

أولاً: مرحلة التحليل Analysis Phase:

مرحلة التحليل هي المرحلة الأساسية وتمثل حجر الأساس لبقية المراحل الأخرى، فمن خلال هذه المرحلة يحدد المصمم التعليمي المشكلة والاحتياجات والأسباب والحلول الممكنة لها، وتحليل الحاجات والمهام وتحليل المحتوى، وتحليل الفئة المستهدفة، وكذلك يتم فيها تحديد الغاية أو الأهداف العلمية بصورة عامة ثم تحليلها إلى أجزاء ومكونات صغرى لتسهيل عملية تجميعها، ثم تحديد خصائص المتعلمين من خلال تحليل المتعلم ومعرفة احتياجاته والتغلب على المعوقات التعليمية التي تواجهه بالإضافة إلى تحليل الحاجات التعليمية، وكل هذه المعلومات ستساعد في تحديد الحلول والأهداف الممكنة (السليماني وفرج، 2021؛ Alsaleh, 2020).

ثانياً: مرحلة التصميم Design Phase:

هي عملية ترجمة مخرجات مرحلة التحليل إلى خطوات قابلة للتنفيذ، وذلك من خلال وضع مخططات ومسودات أولية لتطوير المواد التعليمية واختيار الأساليب والتقنيات المستخدمة للإنتاج، وفيها يتم وضع المخططات واستخدام المخرجات من مرحلة التحليل، بحيث تحدد هذه المخططات أهداف التعلم، والاستراتيجيات التعليمية، ووسائل التعلم المستخدمة في التدريب (السليماني وفرج، 2021).

ثالثاً: مرحلة التطوير Development Phase:

التطوير هو روح النظام التعليمي وقبل البدء في التطوير، يجب على المصمم إنشاء سيناريو تعليمي ويعرف السيناريو بأسماء مختلفة مثل التسلسل التربوي أو خطة الدرس أو القصة المصورة، ويعتبر أهم جزء في نموذج ADDIE، لأنه يقوم بوصف أنشطة التعلم والدعم، والأدوار، والفئة المستهدفة، والمتطلبات الأساسية، وأهداف التعلم، والأدوات اللازمة لتحقيق الأنشطة (آل جديع، ٢٠٢١).

وفي هذه المرحلة يقوم المصمم بتحديد المواد التعليمية المطلوبة، وأنشطة التعلم التي تم تصميمها في المرحلة السابقة، بالإضافة إلى تطوير إرشادات للطلاب على شكل منهج دراسي، كما يعد اختيار الوسائط المناسبة أحد مكونات هذه المرحلة ويجب أن يأخذ في الاعتبار اختيار الوسائط المتعددة المناسبة التي تساعد الطلاب على تعلم المحتوى المطلوب.

رابعاً: مرحلة التنفيذ Implementation Phase:

يتم في هذه المرحلة تنفيذ وتطبيق المواد التعليمية المنتجة في مرحلة التطوير على أرض الواقع، وتعد هذه المرحلة مرحلة التطبيق (السليماني وفرج، 2021).

خامساً: مرحلة التقييم Evaluation Phase:

وفي هذه المرحلة يتم قياس كفاءة المادة التعليمية المنفذة، ويكون التقويم مستمراً، بحيث يتم أثناء تنفيذ كل مرحلة من التصميم، وبين المراحل نفسها، ثم بعد انتهاء المراحل جميعها، وقد يكون التقويم تكوينياً أو ختامياً:

1- **التقويم التكويني Formative Evaluation:** تقويم مستمر في أثناء كل مرحلة، وبين المراحل المختلفة، ويهدف إلى تحسين المادة التعليمية المنفذة قبل وضعها بصيغتها النهائية موضع التنفيذ.

2- **التقويم الختامي Summative Evaluation:** ويكون في العادة بعد إنجاز النسخة النهائية من المادة التعليمية المنفذة، ويستفاد منه في اتخاذ قرار نهائي حول المادة التعليمية بالاستمرار في استخدامها أو التوقف عنه (الجهني، 2018).

مميزات نموذج التصميم العام ADDIE:

يتميز نموذج التصميم العام ADDIE كما يرى كل من (Almomen et al., 2016; Alodwan & Almosa, 2018؛ الجهيني، 2018) بالآتي:

1. البساطة في الاستخدام، ما جعل العديد من المصممين يعتمدون عليه.
2. إمكانية استخدامه لأي نوع من التعليم والتدريب.
3. الاتساق والاختزال والتعميم والتنظيم المجالات التعلم المختلفة.
4. يناسب المصممين والمعلمين الذين لا يملكون الخبرة الكافية في التصميم التعليمي.
5. .يوفر الوقت والمال والجهد ويسهل إصلاحه والتعديل عليه.

لذلك يعتبر هذا النموذج التصميمي من النماذج التي يمكن الاستفادة منه في تصميم الوحدات والمقررات الدراسية، حيث يتم تطبيق خطواته المحددة ومراعاة الشروط والمتطلبات اكل خطوة للوصول إلى التصميم المناسب والذي يلبي حاجات المتعلمين، وكذلك الاستفادة من المميزات التي يوفرها هذا التصميم والتي تتمثل بالسهولة والبساطة في التصميم، وتوفير الوقت والجهد أثناء التصميم.

التعلم القائم على المشاريع:

مفهومه التعلم القائم على المشاريع:

التعلم القائم على المشاريع هو نهج تعليمي يركز على إشراك الطلاب في استقصاء طويل المدى لمشكلات أو أسئلة أو تحديات معقدة، تؤدي إلى إنتاجات أو حلول ملموسة. يتميز هذا النوع من التعلم بتركيزه على الطالب والعالم الحقيقي، مما يساعد الطلاب على اكتساب مهارات القرن الحادي والعشرين وتطبيق المعرفة في سياقات ذات معنى (العتيبي والوادعي، 2022).

خطوات التعلم القائم على المشاريع:

أشار كل من (العتيبي والوادعي، 2022؛ القحطاني والحارثي، 2022) إلى أنه يتم تنفيذ التعلم القائم على المشاريع وفق أربع خطوات رئيسية، وهي:

1. اختيار المشروع:

تعتبر أهم مرحلة من مراحل المشروع، إذ يتوقف عليها مدى جدية المشروع، ولذلك يجب أن يكون المشروع متوافقًا مع ميول التلاميذ، وأن يعالج ناحية مهمة في حياتهم، وأن يؤدي إلى خبرة وفيرة متعددة الجوانب، وأن يكون مناسبًا لمستواهم، وأن تكون المشروعات المختارة متنوعة، وتراعي ظروف المدرسة والتلاميذ وإمكانيات العمل.

2. التخطيط للمشروع:

في هذه المرحلة يقوم التلاميذ بإشراف معلمهم، بوضع الخطة ومناقشة تفاصيلها من أهداف النشاط والمعرفة والمهارات المتصلة به، والصعوبات المحتملة، على أن يقسم المتعلمون إلى مجموعات، وتدون كل مجموعة مهمتها وعملها في تنفيذ الخطة، ويكون دور المعلم في رسم الخطة هو الإرشاد والتصحيح وإكمال النقص فقط.

3. تنفيذ المشروع:

في هذه المرحلة يتم نقل الخطة والمقترحات من التفكير والتخطيط إلى التطبيق في حيز الوجود، وهي مرحلة النشاط والحيوية، ويبدأ المتعلمون الحركة والعمل، ويقوم كل منهم بالمسؤولية المكلف بها، ودور المعلم تهيئة الظروف، وتذليل الصعوبات، كما يقوم بعملية التوجيه التربوي، ويمنح الوقت المناسب للتنفيذ حسب قدرات كل منهم، ويلاحظهم أثناء التنفيذ ويشجعهم على العمل، ويجتمع بهم، إذا دعت الضرورة لمناقشة بعض الصعوبات، قصد تقويم وتعديل سير المشروع.

4. تقويم المشروع:

في هذه المرحلة يتم قياس وتقييم ما وصل إليه المتعلمون أثناء تنفيذ المشروع، والتقويم عملية مستمرة مع سير المشروع منذ البداية، وتتخلل المراحل السابقة، إذ في نهاية المشروع يستعرض كل متعلم ما قام به من عمل، وما استفاد منه من المشروع. ومن ثم يحكم المتعلمون على المشروع من خلال التساؤلات الآتية:

- إلى أي مدى أتاح لنا المشروع الفرصة لننمي خبراتنا من خلال الاستعانة بالكتب والمراجع؟
- إلى أي مدى أتاح لنا المشروع الفرصة للتدريب على التفكير الفردي والجماعي، في المشكلات الهامة؟
- إلى أي مدى ساعد المشروع على توجيه ميولنا، واكتساب ميول واتجاهات جديدة مناسبة؟

وبعد عملية التقويم الجماعي يمكن أن تعاد خطوة من خطوات المشروع، أو يعاد المشروع ككل بصورة أفضل، بحيث يعمل المتعلمون على تجنب الأخطاء السابقة.

مميزاته وفوائد التعلم القائم على المشاريع:

يقدم التعلم القائم على المشاريع فوائد تعليمية عديدة. إنه يطور مهارات الطلاب ويعزز تعلمهم بشكل فعال، ومنها:

- تنمية مهارات التفكير العليا كالتحليل والتركيب والتقييم لدى الطلاب.
- إكساب الطلاب مهارات القرن الحادي والعشرين كالتواصل والتعاون والإبداع.
- ربط التعلم بالحياة العملية من خلال تناول قضايا ومشكلات واقعية.
- تعزيز دافعية الطلاب وانخراطهم في العملية التعليمية.
- تطوير قدرات الطلاب على التعلم الذاتي والبحث والاستقصاء.
- بناء مجتمعات تعلم تفاعلية وتعاونية بين الطلاب (العتيبي والوادعي، 2022).

الدراسات السابقة

في هذه الدراسة قامت الباحثة بمراجعة العديد من الدراسات السابقة، وقد تنوعت هذه الدراسات في موضوعاتها ومجالاتها، وتعددت سبل استفادة الباحثة منها، حيث أثرى البعض منها منهجية الدراسة، والإطار المفاهيمي، ومنها ما استفادت منه الباحثات في النموذج التصميمي وما يتعلق به من إجراءات تصميمية، وفي ما يلي استعراض لبعض الدراسات التي ارتبطت بموضوع الدراسة الحالية:

أجرى الشريف (2023) دراسة هدفت إلى التعرف على فعالية برنامج تدريبي مقترح لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة، من خلال بناء برنامج تدريبي لتنمية وعي طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة في الأمن السيبراني، وذلك في حماية البيانات والأجهزة وسلامتها من مخاطر الانتهاكات السيبرانية والمحافظة على سلامة المعلومات وذلك بالحد من الدخول الغير مصرح به إليها، ولتحقيق أهداف الدراسة تم الاعتماد على المنهج التجريبي ذو المجموعة التجريبية والقياسين القبلي والبعدي مستخدما الاستبانة كأداة لجمع البيانات، وتم تطبيقها على عينة عشوائية بحيث بلغت (189) طالبة من طالبات كلية الآداب العلوم الإنسانية بجامعة طيبة، وأظهرت النتائج وجود فروقًا ذات دلالة إحصائية في معرفة طالبات المجموعة التجريبية على أداة الدراسة في القياسين القبلي والبعدي تعزى لتأثير البرنامج التدريبي لصالح القياس البعدي، وهذا يظهر فعالية ذلك البرنامج في تنمية

الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة، وأوصت الدراسة بضرورة تقديم برامج تدريبية توعوية مكثفة تختص بالأمن السيبراني وكذلك أهمية إضافة مواد ومقررات تعليمية تختص بالأمن السيبراني، وكذلك تفعيل إدارات الأمن السيبراني في توعية طلبة الجامعة بالأمن السيبراني.

وهدفت دراسة عبدالله (2023) إلى التعرف على فاعلية التعليم الموضوعي القائم على فيديو مشاركة المحتوى في الوعي بالأمن المعلوماتي وخفض الحمل المعرفي لدى طلاب مدارس المتفوقين في العلوم والتكنولوجيا، استخدم البحث المنهج التجريبي واعتمد على التصميم التجريبي ذو المجموعة الواحدة والقياسين القبلي والبعدي، تكونت العينة من (10) طالب وطالبة ممن أبدوا رغبة في الإشتراك، ولجمع البيانات استخدمت الدراسة اختبار تحصيلي، ومقياس الحمل المعرفي، ومنصة فصل جوجل (Google class) لتقديم المحتوى وفقا للتعليم الموضوعي، وجوجل فورم للاختبار والمقياس، وأظهرت النتائج وجود فروقًا ذات دلالة إحصائية في متوسط درجات أفراد العينة على اختبار الوعي بالأمن المعلوماتي في القياسين القبلي والبعدي تعزى لتاثير التعليم الموضوعي القائم على فيديو مشاركة المحتوى لصالح القياس البعدي، وأوصت الدراسة بالاهتمام بالتعليم الموضوعي القائم على فيديو مشاركة المحتوى، وتطبيق التعليم الموضوعي ببيئات تعليمية مختلفة، والاهتمام بتصميم بيئات تعليمية تراعي خفض الحمل المعرفي.

وقام قاسم والعنزي (2023) بدراسة هدفت إلى الكشف عن فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى المراهقين، ولتحقيق أهداف الدراسة تم اعتماد المنهج التجريبي ذو المجموعتين والقياسين القبلي والبعدي، وتكونت عينة الدراسة من (30) فردًا تم تقسيمهم إلى (15) طالبًا للمجموعة التجريبية، وعدد (15) طالبًا للمجموعة الضابطة من طلاب المدارس الثانوية بمدارس جيزان، واستعانت الدراسة باختبار الوعى بالأمن السيبراني من إعداد نورة الصانع وآخرين (2020)، إضافة إلى برنامج إرشادي لتنمية الوعى بالأمن السيبراني، وأظهرت النتائج وجود فروق دالة إحصائيًا عند مستوى دلالة (0.001) بين درجات القياسين البعدي والقبلي في اختبار الوعى بالأمن السيبراني، بعد تطبيق البرنامج الإرشادي في اتجاه القياس البعدي، كما كشفت الدراسة عن وجود فروق دالة إحصائيًا عند مستوى دلالة (0.001) بين درجات المجموعتين التجريبية والضابطة في اختبار الوعى بالأمن السيبراني، بعد تطبيق البرنامج الإرشادي في اتجاه المجموعة التجريبية، كما كشفت الدراسة عن عدم وجود فروق ذات دلالة إحصائية بين القياس البعدي، والتتبعي في الوعى بالأمن السيبراني بأبعاده المختلفة.

واما دراسة المطرفي والقراني (2023) فقد هدفت للكشف عن فاعلية مقرر إلكتروني مقترح لتنمية الوعي المعرفي بالأمن السيبراني الطالبات المرحلة الثانوية بمدينة جدة، استخدم المنهج شبه التجريبي ذو المجموعة الواحدة والقياسين القبلي والبعدي،، وتكونت عينة الدراسة من (26) طالبة تم اختيارهن بطريقة القصدية 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 إحصائيا عند مستوى الدلالة (0.05) بين متوسطات درجات طالبات المرحلة الثانوية بالتطبيق القبلي والبعدي لاختبار الوعي المعرفي بالأمن السيبراني تعزى للمقرر الإلكتروني المقترح لصالح التطبيق البعدي، كما أظهرت النتائج فاعلية المقرر الإلكتروني في تنمية الوعي المعرفي بالأمن السيبراني، اذ بلغت قيمة الكسب الكلية (13)، وهي معدلات كسب عالية إذا قورنت بالحد الأدنى لبلاك Black (12) مما دل بفاعلية المقرر الإلكتروني المقترح لتنمية الوعي المعرفي بالأمن السيبراني الطالبات المرحلة الثانوية بمدينة جدة، وقدمت الدراسة مجموعة من التوصيات من اهمها الاستفادة من المقرر الإلكتروني المقترح الذي أعدته الباحثتان كمقرر للأمن السيبراني الطالبات مدارس المرحلة الثانوية بمدينة جدة ومناطق المملكة العربية السعودية الأخرى.

أما دراسة Witsenboer et al (2022) فعملت على استكشاف مدى تطور سلوك الأمن السيبراني لدى الطلاب الهولنديين في المرحلتين الابتدائية والثانوية، ولتحقيق أهداف الدراسة تم تطبيق استبانة تطور سلوك الأمن السيبراني وكذلك المقابلة الشخصية الجماعية لتحسين تفسير النتائج، كشفت نتائج الدراسة أن المنهج الدراسي الهولندي لا يُولي هذا الموضوع اهتمامًا يُذكر، وأن الطلاب يكتسبون سلوكهم الإلكتروني بشكل رئيسي من خلال الخبرة والتعليمات على الإنترنت، ومن خلال أولياء أمورهم، ومن خلال أشقائهم. بالإضافة إلى ذلك، ازداد سلوك العديد من الطلاب تهورًا مع مرور الوقت، وأوصت الدراسة ببدء تعليم الأمن السيبراني في المرحلة الابتدائية بمجرد بدء الأطفال استخدام الأجهزة الإلكترونية. ومن المواضيع التي تستحق اهتمامًا خاصًا التعرّف على رسائل البريد الإلكتروني ومواقع التصيد الاحتيال، ويجب إقناع المتعلمين بأن السلوكيات الخطرة على الإنترنت قد تنقلب ضدهم وضد المنظمة التي ينتمون إليها.

وقامت الجندي ومحمد (2019) بدراسة هدفت إلى التعرف على دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة، واعتمدت الدراسة المنهج شبه التجريبي ذو المجموعتين التجريبية والضابطة والقياسين القبلي والبعدي، وتكونت عينة الدراسة من (80) طالبة من طالبات قسم الحاسب الآلي بالكلية الجامعية بأضم جامعة أم القرى تم اختيارهن بطريقة العينة القصدية، وأظهرت النتائج وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) بين متوسطات درجات المجموعة التجريبية والضابطة في القياس القبلي والبعدي لمستوى تنمية مهارات الأمن المعلوماتي لدى طالبات قسم الحاسب الآلي بالكلية الجامعية بأضم جامعة أم القرى، وأوصت الدراسة بتعميم تجربة الدراسة الحالية على مستوى فئات الطالبات التي تحتاج للاستفادة منها.

تعقيب على الدراسات السابقة:

من خلال مراجعة الدراسات السابقة نجد أنها اتفقت مع الدراسة الحالية في بعض الجوانب، واختلفت في البعض الآخر، ويمكن توضيح ذلك من خلال النقاط التالية:

من حيث متغيرات الدراسة:

اتفقت الدراسات السابقة مع الدراسة الحالية في اعتماد الوعي بالأمن السيبراني كمتغير تابع رئيسي، مع اختلفت في المتغير المستقل حيث اعتمدت الدراسة الحالية مقرر تعليمي مقترح في ضوء التعلم القائم على المشاريع، بينما دراسة المطرفي والقراني (2023) فكان المقرر الإلكتروني، بينما دراسة عبدالله (2023) استخدمت التعليم الموضوعي القائم على الفيديو، ودراسة قاسم والعنزي (2023) اختلفت في تضمين متغيرات سلوكية (مثل الوقاية من الاختراقات) إلى جانب المعرفية، بينما دراسة Witsenboer et al. (2022) فاهتمت بالسلوك الإلكتروني كمتغير تابع دون ربطه ببرنامج تدريبي محدد.

من حيث منهج الدراسة:

اتفقت الدراسة الحالية مع بعض الدراسات السابقة من حيث استخدام المنهج شبة التجريبي ذو المجموعة التجريبية الواحدة والقياسين القبلي البعدي مثل دراسة الشريف (2023)، ودراسة قاسم والعنزي (2023)، ودراسة المطرفي والقراني (2023)، واختلفت من حيث

اعتماد التصميم التجريبي ذو المجموعتين التجريبية والضابطة مع دراسة عبدالله (2023)، ودراسة الجندي ومحمد (2019)، بينما اختلفت مع دراسة Witsenboer et al (2022) والتي استخدمت المنهج الوصفي.

من حيث أدوات الدراسة:

اتفقت الدراسة الحالية من حيث استخدام الاستبانة كأداة لقياس حجم التغير في المتغير التابع بفعل المتغير المستقل مثل دراسة الشريف (2023)، ودراسة عبدالله (2023)، ودراسة المطرفي والقراني (2023)، ودراسة قاسم والعنزي (2023)، ودراسة الجندي ومحمد (2019)، بينما اختلفت مع دراسة Witsenboer et al (2022) والتي اضافت المقابلة كأداة لتحسين تفسير النتائج.

من حيث النتائج:

اتفقت الدراسة الحالية من حيث التوصل إلى فعالية المتغيرات المستقلة في إحداث تأثير واضح في تنمية المهارات والوعي بالأمن السيبراني مثل دراسة الشريف (2023)، ودراسة عبد الله (2023)، ودراسة المطرفي والقراني (2023)، ودراسة قاسم والعنزي (2023)، ودراسة الجندي ومحمد (2019)، بينما اختلفت مع دراسة Witsenboer et al (2022) والتي أظهرت أن المنهج الدراسي الهولندي لا يُولي هذا الموضوع اهتمامًا يُذكر، وأن الطلاب يكتسبون سلوكهم الإلكتروني بشكل رئيسي من خلال الخبرة والتعليمات على الإنترنت، ومن خلال أولياء أمورهم.

– ما يستفاد من الدراسات السابقة:

تم الاستفادة من الدراسات السابقة في العديد من الجوانب، ومنها:

- إثراء مقدمة ومشكلة والدراسة، وكذلك الإطار النظري للدراسة الحالية.
- التعرف على خطوات تصميم المقررات وفق نموذج التصميم (ADDIE).
- التعرف على مناهج البحث المختلفة، واختيار المنهج المناسب للدراسة الحالية.
- معرفة الأساليب الاحصائية المختلفة، واستخدام ما يناسب منها للدراسة الحالية.
- الاستفادة من نتائج تلك الدراسات لمقارنتها مع نتائج الدراسة الحالية.

– ما تميزت به الدراسة الحالية:

تتميز الدراسة الحالية بكونها من الدراسات القليلة التي تناولت تصميم مقرر دراسي لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الابتدائية، حيث يركز ذلك المقرر على اسلوب التعلم القائم على المشاريع، وضمن أحدث نموذج تصميمي والذي يعرف بنموذج (ADDIE) –على حد علم الباحثات– حيث لم تتطرق دراسة من قبل لتصميم ذلك المقرر بنفس أسلوب الدراسة الحالية.

منهجية الدراسة وإجراءاتها

منهج الدراسة:

يتحدد منهج الدراسة بناءًا على طبيعة الموضوع الذي تتناوله، وفي هذه الدراسة يتمثل موضوع الدراسة وهدفها بتصميم وحدة مقترحة لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الإبتدائية في ضوء التعلم القائم على المشاريع، لذلك

فإن المنهج شبه التجريبي هو المنهج المناسب لتحقيق ذلك، حيث تم اعتماد المنهج شبه التجريبي ذو المجموعة الواحدة، والقياسين القبلي والبعدي.

مجتمع الدراسة:

يتكون مجتمع الدراسة من جميع طالبات الصفوف العليا من المرحلة الإبتدائية بجميع المدارس بمنطقة تبوك.

عينة الدراسة:

شملت عينة الدراسة على عينتين، وهي:

العينة الاستطلاعية:

تم اختيار العينة الاستطلاعية بأسلوب العينة العشوائية البسيطة، حيث تكونت من (52) طالبة من طالبات الصفوف العليا للمرحلة الإبتدائية من مدارس منطقة تبوك، وذلك من أجل التأكد من الخصائص السيكومترية لاستبيان مهارات الأمن السيبراني لطالبات المرحلة الإبتدائية.

العينة الأساسية:

تم اختيار عينة البحث الأساسية عن طريق أسلوب العينة القصدية تكونت من (30) طالبة من مدرسة ابتدائية مويلح الأولى بضباء، وتم اختيار هذه المدرسة نظرًا لقربها من مكان إقامة الباحثات، ويمكن توضيح أكثر لخصائص العينة الأساسية على أساس الصف الدراسي من خلال الجدول التالي:

جدول رقم (1) يوضح خصائص عينة الدراسة

الصف	العدد	النسبة المئوية
الرابع الإبتدائي	10	33.33
الخامس الإبتدائي	10	33.33
السادس الإبتدائي	10	33.33
الإجمالي	**30**	**٪ 100**

من الجدول السابق نلاحظ بأنه تم اختيار عينة الدراسة بنسبة متساوية من الصفوف العليا (الرابع – الخامس – السادس) من المرحلة الإبتدائية، بواقع (10) طالبات من كل صف دراسي منها، حيث تم اختيارهن من الطالبات اللآتي حصلن على مستوى منخفض من مهارات الأمن السيبراني على الاستبيان المستخدم في هذه الدراسة.

أدوات الدراسة:

لتحقيق أهداف الدراسة تم الاعتماد على أدوات تم القيام بتصميمها، وتمثلت بالآتي:

استبيان مهارات الأمن السيبراني لطالبات المرحلة الابتدائية:

من خلال الرجوع إلى الأدب النظري والدراسات السابقة التي تناولت موضوع مهارات الأمن السيبراني تم تصميم الاستبانة حيث تكونت في صورتها الأولية من (25)، وأمام كل فقرة مقياس ليكرت الخماسي (دائمًا – غالبًا – أحيانًا – نادرًا – أبدًا)، حيث توزعت على خمسة أبعاد شملت (حماية المعلومات الشخصية – إدارة كلمات المرور – التعامل مع المحتوى الخطر – التفاعل الأمن مع الآخرين – الصيانة وطلب المساعدة)، حيث احتوى كل بعد على خمس فقرات.

الخصائص السيكومترية لاستبيان مهارات الأمن السيبراني:

للتأكد من ملائمة الاستبيان من خلال معاملات الصدق والثبات حيث تم ذلك من خلال الآتي:

1. صدق الاستبيان:

تم حساب صدق الاستبيان من خلال طريقتين، وشملت

- **الصدق الظاهري:** تم عرض الاستبيان على (5) من السادة المحكمين من ذوي الخبرة والاختصاص، للتأكد من ارتباط فقرات الاستبيان وقدرتها على قياس مهارات الأمن السيبراني، وقد كانت نسبة الاتفاق بين المحكمين عالية، حيث بلغت (80 ٪)، وتم الأخذ بالتعديلات التي أوصى بها المحكمون على فقرات الاستبيان.
- **صدق الاتساق الداخلي:** بعد تطبيق الاستبيان على العينة الاستطلاعية والمكرونة من (52) طالبة، تم حساب معامل الارتباط لبيرسون بين فقرات الاستبيان والدرجة الكلية للاستبيان، وتم التوصل إلى النتائج التالية:

جدول رقم (2) يوضح معامل الارتباط لبيرسون بين فقرات الاستبيان والدرجة الكلية له

حماية المعلومات الشخصية		إدارة كلمات المرور		التعامل مع المحتوى الخطر		التفاعل الأمن مع الآخرين		الصيانة وطلب المساعدة	
الفقرة	معامل الارتباط	الفقرة	معامل الارتباط	الفقرة	معامل الارتباط	الفقرة	معامل الارتباط	الفقرة	معامل الارتباط
1	**0.771	6	**0.791	11	**0.730	16	**0.443	21	**0.921
2	**0.763	7	**0.790	12	**0.678	17	*0.336	22	**0.454
3	**0.755	8	**0.784	13	**0.685	18	*0.325	23	*0.311
4	**0.530	9	**0.610	14	**0.673	19	*0.320	24	*0.306
5	**0.693	10	**0.705	15	**0.671	20	*0.307	25	**0.391

** تعني عند مستوى دلالة (0.01)، * تعني عند مستوى دلالة (0.05)

من الجدول السابق نلاحظ أن معامل الارتباط لبيرسون بين فقرات الاستبيان والدرجة الكلية له تراوحت بين (0.306 – 0.921)، عند درجة حرية (ن= 50)، ومستوى دلالة (0.01 – 0.05)، وهي قيم ارتباط مرتفعة لذلك يمكننا القول بأن الاستبيان يتمتع بدرجة صدق اتساق داخلي مناسبة ويمكن الإعتماد عليها.

2. ثبات الاستبيان:

تم التأكد من ثبات الاستبيان من خلال طريقة التجزئة النصفية ومعامل سبيرمان – براون، وكذلك من خلال معامل الثبات لالفاكرونباخ، وتم التوصل إلى النتائج التالية:

جدول رقم (3) يوضح معاملات الثبات لابعاد استبيان مهارات الأمن السيبراني

البعد	معاملات الثبات	
	التجزئة النصفية	الفاكرونباخ
حماية المعلومات الشخصية	0.761	0.908
إدارة كلمات المرور	0.909	0.955
التعامل مع المحتوى الخطر	0.871	0.950
التفاعل الأمن مع الآخرين	0.786	0.892
الصيانة وطلب المساعدة	0.878	0.941
مهارات الأمن السيبراني ككل	**0.923**	**0.922**

من الجدول السابق نلاحظ أن معاملات الثبات لابعاد الاستبيان بطريقة التجزئة النصفية تراوحت بين (0.761 – 0.909)، وكذلك معاملات الثبات لالفاكرونباخ لنفس الابعاد تراوحت بين (0.892 – 0.955)، وبالنسبة لمعاملة الثبات لاستبيان مهارات الأمن السيبراني ككل فقد بلغ بطريقة التجزئة النصفية والفاكرونباخ (0.923 – 0.922) على التوالي، وبالنظر لتلك المعاملات نجد أنها مرتفعة، وهذا يدل على أن الاستبيان يتمتع بدرجة ثبات مناسبة يمكن الإعتماد عليها في دراستنا الحالية.

3. الاستبيان في صورته النهائية:

بعد إجراء التعديلات التي أوصى بها المحكمون، والتأكد من صدق وثبات الاستبيان أصبح في صورته النهائية يتكون من (25) فقرة مصاغة بصورة إيجابية، وأمام كل فقرة مقياس ليكرت الخماسي (دائمًا – غالبًا – أحيانًا – نادرًا – أبدًا)، حيث توزعت على خمسة أبعاد (حماية المعلومات الشخصية – إدارة كلمات المرور – التعامل مع المحتوى الخطر – التفاعل الأمن مع الآخرين – الصيانة وطلب المساعدة)، حيث احتوى كل بعد على خمس فقرات، ولأن جميع فقرات الاستبيان تم صياغتها بصورة إيجابية تأخذ البدائل القيم الكمية (5 – 4 – 3 – 2 – 1) على التوالي.

المقرر المقترح لتنمية مهارات الأمن السيبراني:

تم تصميم مقرر مقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا للمرحلة الابتدائية اعتمادًا على النموذج التصميم التعليمي ADDIE، وذلك لما له من مميزات تجعله مناسبًا لهذه الدراسة، بالإضافة إلى إعتماد أسلوب التعلم القائم على المشاريع كونه من أحدث الأساليب التدريسية، وفيما يلي توضيح لتصميم المقرر المقترح بالتفصيل:

أولاً: مرحلة التحليل Analysis Phase: وتم في هذه المرحلة تحديد الآتي:

1. تحديد خصائص المتعلمات:

قامت الباحثات بذلك من خلال النزول الميداني والمقابلات الشخصية لعدد من الطالبات ومعلمات الصفوف (الرابع – الخامس – السادس) من المرحلة الإبتدائية، وتم تحديد خصائص المتعلمات وهي كالآتي:

2. تحديد احتياجات المتعلمات:

وتمثلت الاحتياجات الأساسية للمتعلمات في مجال مهارات الأمن السيبراني بالاحتياجات التالية:

ثانياً: مرحلة التصميم Design Phase:

بعد الانتهاء من مرحلة التحليل تم عمل خطة لتصميم المقرر المقترح، مع مراعات السهولة والواقعية وقابلية التنفيذ في تلك الخطة، ويمكن توضيح ذلك با

1. تحديد الهدف العام للمقرر:

يتمثل الهدف العام للمقرر المقترح في تنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا (الرابع – الخامس – السادس) من المرحلة الإبتدائية.

2. تحديد الأهداف الإجرائية للمقرر المقترح:

بعد الانتهاء من المقرر المقترح يتوقع بأن تكون الطالبة قادرة على:

- تعريف مفهوم الأمن السيبراني.
- ذكر المخاطر السيبرانية المتعددة التي يمكن أن تتعرض لها.
- توضيح أهمية امتلاك مهارات الأمن السيبراني.
- امتلاك مهارات حماية المعلومات الشخصية في برامج التواصل المختلفة.
- امتلاك القدرة على إدارة كلمات المرور الخاصة بها في جميع حساباتها.
- امتلاك القدرة على التحقق من المحتوى الخطر على شبكات التواصل المختلفة.
- امتلاك مهارة التفاعل الأمن مع الآخرين من خلال شبكات التواصل المختلفة.

- التعرف على الطرق المختلفة لطلب المساعدة عند مواجهة أي طارئ.

3. المحتوى التعليمي:

ويتمثل المحتوى المناسب لتحقيق أهداف المقرر المقترح بالآتي:

4. طرائق التدريس والوسائل التعليمية المستخدمة:

لتنفيذ محتوى المقرر المقترح بشكل فعال تم اعتماد بعض طرائق التدريس والوسائل التعليمية، وهي:

- طرائق التدريس: اعتمدت الباحثات أسلوب والحوار، وأسلوب التعلم القائم على المشاريع لما يوفره ذلك الأسلوب من بيئة تعليمية تفاعلية تتيح لجمع الطالبات بالمشاركة الفاعلة في تنفيذ المشروعات المختلفة، وينمي جوانب معرفية ووجدانية ومهارية مختلفة لديهن، وقد تنوعت المشاريع التي تم تحديدها للطالبات بحيث تراعي الفروق الفردية بينهن، وشملت المشاريع التالية:
  1. تصميم بروشورات توعوية للتعريف بالأمن السيبراني، وأهمية امتلاك مهارات الأمن السيبراني.
  2. تصميم حملة توعوية رقمية حول حماية الحسابات الشخصية، وإدارة كلمات المرور الشخصية.
  3. إعداد فيديو تعليمي عن كيفية اكتشاف الرسائل الاحتيالية، وطرق التعامل معها.
  4. تنفيذ دراسة حالة حول اختراق أمني وتحليل أسبابه وطرق الوقاية.
  5. برمجة نموذج أولي لتطبيق بسيط يقدّم نصائح أمنية تفاعلية.
- الوسائل التعليمية: يعتمد هذا المقرر على العديد من الوسائل التعليمية المساعدة، ومنها:
  1. أجهزة الحاسوب.
  2. عروض باوربوينت.
  3. فيديوهات تعليمية.

5. التقييم والتقويم:

تم تحديد وسائل وأساليب التقييم والتقويم، وتمثلت بالآتي:

- استبيان مهارات الأمن السيبراني لطالبات الصفوف العليا من المرحلة الإبتدائية والمصمم في هذه الدراسة.
- معايير الإلتزام بمعايير تصميم وتنفيذ المشاريع المختلفة.
- التغذية الراجعة: وتشمل تغذية راجعة فورية لتوجيه الطالبات أثناء تنفيذ المقرر المقترح، وتصميم وتنفيذ المشاريع.

ثالثاً: مرحلة التطوير Development Phase:

في هذه المرحلة تم تحديد المواد التعليمية المصممة، تم إعداد المواد التعليمية الرقمية والورقية، وتشمل الآتي:

1. دليل المعلمة:

تم تصميم دليل المعلمة في صورة كتاب إلكتروني، واحتوى على الآتي:

- الهدف العام لتدريس المقرر المقترح.

- اللازم لتدريس المقرر المقترح.
- خطة تدريسية عامة لتوزيع محتوى المقرر والحصص المطلوبة لكل جزء منه، والأهداف الإجرائية والوزن النسبي لكل جزء.
- توضيح لطرائق التدريس الواجب استخدامها في تدريس المقرر المقترح، مع نصائح لتحسين استخدامها.
- توضيح للوسائل التعليمية المساعدة في تدريس المقرر، وطرق الاستفادة منها بالشكل الأمثل.
- شرح تفصيلي للتعلم القائم على المشاريع وأهميته، والخطوات اللازمة لتنفيذ المشاريع (اختيار المشروع – التخطيط للمشروع – تنفيذ المشروع – تقييم المشروع)، وكذلك طرق تقييم المشاريع، مع إرفاق استمارة لتقييم المشاريع المنفذة.

2. كتاب المتعلم:

تم تصميم كتاب الطالبة بحيث روعي عند إخراجه تناسق الألوان وجاذبيتها، ودعم الكتاب بالصور والفيديوهات التوضيحية، بالإضافة إلى التطبيق العملي الذي يعزز تعلم المهارات الأمن السيبراني المختلفة، وأيضا احتوى الكتاب على أسئلة مثيرة للتفكير، واسئلة تقويمية متنوعة نهاية كل درس، وكذلك نهاية المقرر المقترح، واحتوى الكتاب على خمسة دروس شملت:

- الدرس الأول: مقدمة عن الأمن السيبراني.
- الدرس الثاني: التهديدات السيبرانية الشائعة في عصرنا الحالي.
- الدرس الثالث: نبذة عن التعلم القائم على المشاريع وآلية تنفيذه.
- الدرس الرابع: مهارات الأمن السيبراني وأهميتها.
- الدرس الخامس: تطبيق مهارات الأمن السيبراني بصورة عملية.
- الدرس السادس: تنفيذ مشاريع لتنمية مهارات الأمن السيبراني.

رابعاً: مرحلة التنفيذ Implementation Phase:

تم تنفيذ وتطبيق المنهج المقترح على عينة طالبات الصفوف العليا والبالغ عددهم (30) طالبة تم اختيارهن من الثلاثة الصفوف بشكل متساوي، وذلك من مدرسة ابتدائية مويلح الأولى بضباء، حيث تم تطبيق المقرر في الفصل الدراسي الثالث للعام الدراسي 1446هـ، حيث تم تطبيق المقرر في (10) حصص دراسية، مدة كل حصة (45) دقيقة، وبمعدل حصتين في الأسبوع، وبذلك استغرق التطبيق مدة (5) أسابيع.

خامساً: مرحلة التقييم Evaluation Phase:

للتأكد من تحقق أهداف المقرر المقترح تم اعتماد العديد من أساليب التقويم، ومنها:

- التقويم القبلي: ويهدف إلى تحديد الخلفية النظرية والمهارية للطالبات في مجال مهارات الأمن السيبراني المختلفة، وكذلك لتحديد النقطة التي يجب أن يبدأ منها المقرر المقترح، حيث تم ذلك من خلال تطبيق استبيان مهارات الأمن السيبراني المعد في هذه الدراسة.
- التقويم التكويني: وذلك خلال تنفيذ المقرر المقترح بهدف توجيه الطالبات نحو تحقيق أهداف المقرر، ولتقديم تغذية راجعة فورية لهن، والإجابة على تساؤلاتهن، حيث يتم ذلك من خلال المناقشة والحوار الهادف معهن، وكذلك لتقييم تقدمهن في تنفيذ المشاريع الموكلة إليهن.

- التقويم النهائي (البعدي): ويهدف هذا التقويم إلى تحديد مدى فعالية المقرر المقترح في تنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا من المرحلة الإبتدائية، وذلك من خلال تطبيق استبيان مهارات الأمن السيبراني المعد في هذه الدراسة على الطالبات بعد الانتهاء من تدريس المقرر المقترح.

التأكد من ملائمة المقرر المقترح:

للتأكد من ملائمة المقرر المقترح تم عرض كل من دليل المعلم وكتاب المتعلم الإلكتروني على (5) من السادة المحكمين من ذوي الاختصاص في مجال تصميم المقررات الدراسية وخاصة تصميم مقررات الحاسب الآلي، وذلك لابداء الرأي، وإضافة أو حذف أو تعديل ما ورد فيهما، وقد أورد المحكمون بعض الملاحضات للتحسين والتي تم الأخذ بها، وأصبح المقرر المقترح ملائم للتنفيذ والتأكد من فعاليته.

الأساليب الإحصائية:

تم استخدام برنامج تحليل الحزم الإحصائية SPSS وذلك لتحليل وحساب الأساليب الإحصائية التالية:

1. التكرار والنسبة المئوية لعرض عينة الدراسة، وكذلك نسبة إتفاق المحكمين.
2. معامل الارتباط لبيرسون لحساب صدق الاتساق الداخلي لأداة الدراسة.
3. معامل الارتباط لسيبرمان–براون ومعامل الفاكرونباخ للتأكد من ثبات أداة الدراسة.
4. اختبار ت T–test للعينات المرتبطة، وذلك لتحديد فعالية المنهج المقترح من خلال حساب دلالة الفروق بين متوسط درجات المجموعة التجريبية على استبيان مهارات الأمن السيبراني في القياسين القبلي والبعدي.

الفصل الرابع

عرض النتائج ومناقشتها

يتناول هذا الفصل عرض نتائج الدراسة، وفيه يتم استعراض النتائج التي توصلت إليها والتأكد من صحة فروض الدراسة.

فروض الدراسة:

1. لا توجد فاعلية للمقرر المقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا للمرحلة الابتدائية في ضوء التعلم القائم على المشاريع.

2. لا توجد فروق ذات دلالة إحصائية عند ($\alpha \leq 0.05$) بين متوسط درجات المجموعة التجريبية في مهارات (حماية المعلومات الشخصية – إدارة كلمات المرور – التعامل مع المحتوى الخطر – التفاعل الأمن مع الآخرين – الصيانة وطلب المساعدة) لدى طالبات الصفوف العليا من المرحلة الابتدائية في القياسين القبلي والبعدي تعزى للمقرر المقترح في ضوء التعلم القائم على المشاريع.

اولا: النتائج المتعلقة بالفرض الأول والذي ينص على "**لا توجد فاعلية للمقرر المقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا للمرحلة الابتدائية في ضوء التعلم القائم على المشاريع**"

للتأكد من صحة هذا الفرض تم تطبيق اختبار ت T–test للعينات المرتبطة لتحديد دلالة الفروق في متوسط درجات المجموعة التجريبية على استبيان مهارات الأمن السيبراني في القياسين القبلي والبعدي، وتم التوصل إلى النتائج التالية:

جدول رقم (4) يوضح اختبار ت T–test لتحديد الفروق بين متوسط درجات المجموعة التجريبية على استبيان مهارات الأمن السيبراني في القياسين القبلي والبعدي.

المتغير	القياس	المتوسط الحسابي	الانحراف المعياري	قيمة ت	مستوى الدلالة	الدلالة
مهارات الأمن السيبراني ككل	القبلي	51.23	6.80	28.103	0.000	دال
	البعدي	100.63	6.82			

من الجدول السابق نلاحظ أن متوسط درجات طالبات المجموعة التجريبية على استبيان مهارات الأمن السيبراني في القياس القبلي بلغ (51.23)، بانحراف معياري (6.80)، بينما بلغ متوسط درجاتهن في القياس البعدي (100.63)، بانحراف معياري (6.82)، وبلغت قيمة ت المحسوبة (28.103)، عند مستوى دلالة محسوب بلغ (0.000)، وهو أقل بكثير من مستوى الدلالة المعتمد في هذه الدراسة (0.05)، وهذا يدل على أن الفروق بين متوسطات درجات الطالبات المجموعة التجريبية في القياسين القبلي والبعدي ذات دلالة إحصائية لصالح القياس البعدي، وهذا يدل على فعالية المقرر المقترح في تنمية مهارات الأمن السيبراني لدى طالبات المجموعة التجريبية، ونتيجة لذلك يتم رفض الفرض الصفري السابق واعتماد الفرض البديل والذي ينص على "توجد فاعلية للمقرر المقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا للمرحلة الابتدائية في ضوء التعلم القائم على المشاريع"، ونتفق هذه النتيجة مع نتائج دراسة الشريف (2023)و دراسة المطرفي والقراني (2023)، ودراسة عبدالله (2023) ودراسة الجندي ومحمد (2019)، التي أظهرت وجود فروق دالة إحصائيا عند مستوى الدلالة (0.05) بين متوسطات درجات عينة الدراسة بالتطبيق القبلي والبعدي لاختبار الوعي المعرفي بالأمن السيبراني لصالح التطبيق البعدي تعزى للبرنامج المقترح، وكذلك مع دراسة قاسم والعنزي (2023)، التي كشفت عن وجود فروق دالة إحصائيًا عند مستوى دلالة (0.001) بين درجات القياسين البعدي والقبلي في اختبار الوعى بالأمن السيبراني، بعد تطبيق البرنامج الإرشادي في اتجاه القياس البعدي.

وتُعزى هذه النتيجة إلى قدرة المقرر المقترح على اكتساب أفراد المجموعة التجريبية المعرفة الكافية حول الأمن السيبراني ومهاراته المختلفة، حيث استطاع إحداث تغيير واضح في خبراتهن ومهاراتهن التي يستطعن من خلالها مواجهة المخاطر السيبرانية التي توجههن، ويعود ذلك إلى طريقة تصميم ذلك المقرر والتي تمت من خلال خطوات محددة أثبتت فعاليتها في تصميم المقررات المختلفة، حيث انطلق تصميم ذلك المقرر من أسس جوهرية اعتمدت على الخصائص والحاجات الفعلية لأفراد مجتمع الدراسة، كما روعي عند التصميم الفروق الفردية لدى الطالبات واستخدام أساليب تدريسية فعالة تمثلت بالمشروعات التعليمية والتي تجعل التعلم أكثر فعالية من خلال إتاحة الفرصة أمام الطالبات للمشاركة والتعاون لتنفيذ تلك المشاريع، وقد اثبت هذا الأسلوب التدريسي بقدرته على تنمية قدرة المتعلم المعرفية والمهارية، وبقاء أثر التعلم لفترة طويلة.

ثانيًا: النتائج المتعلقة بالفرض الثاني والذي ينص على "**لا توجد فروق ذات دلالة إحصائية (الفا أقل أو تساوي 0.05) بين متوسط درجات المجموعة التجريبية في مهارات (حماية المعلومات الشخصية – إدارة كلمات المرور – التعامل مع المحتوى الخطر – التفاعل الأمن مع الآخرين – الصيانة وطلب المساعدة) لدى طالبات الصفوف العليا من المرحلة الابتدائية في القياسين القبلي والبعدي تعزى للمقرر المقترح في ضوء التعلم القائم على المشاريع**".

وللتأكد من صحة هذا الفرض تم تطبيق اختبار ت T–test للعينات المرتبطة لتحديد دلالة الفروق في متوسط درجات المجموعة التجريبية على ابعاد استبيان مهارات الأمن السيبراني في القياسين القبلي والبعدي، وتم التوصل إلى النتائج التالية:

جدول رقم (5) يوضح اختبار ت T–test لتحديد الفروق بين متوسط درجات المجموعة التجريبية على أبعاد استبيان مهارات الأمن السيبراني في القياسين القبلي والبعدي.

المهارة	القياس	المتوسط الحسابي	الانحراف المعياري	قيمة ت	مستوى الدلالة	الدلالة
حماية المعلومات الشخصية	القبلي	9.58	1.98	**11.575	0.000	دال
	البعدي	19.64	1.99			
إدارة كلمات المرور	القبلي	9.53	1.97	**19.580	0.000	دال
	البعدي	19.53	1.97			
التعامل مع المحتوى الخطر	القبلي	11.10	3.23	**12.786	0.000	دال
	البعدي	20.50	2.40			
التفاعل الأمن مع الآخرين	القبلي	9.83	1.49	**26.037	0.000	دال
	البعدي	19.93	1.49			
الصيانة وطلب المساعدة	القبلي	9.10	1.73	**22.399	0.000	دال
	البعدي	19.10	1.73			

من الجدول السابق نلاحظ أن متوسط درجات طالبات المجموعة التجريبية في مهارة حماية البيانات الشخصية في القياس القبلي بلغ (9.58)، بانحراف معياري (1.98)، بينما بلغ متوسط درجاتهن في القياس البعدي (19.64)، بانحراف معياري (1.99)، وبلغت قيمة ت المحسوبة (11.575)، عند مستوى دلالة محسوب بلغ (0.000)، وهو أقل بكثير من مستوى الدلالة المعتمد في هذه الدراسة (0.05)، وهذا يدل على أن الفروق بين متوسطات درجات الطالبات المجموعة التجريبية في القياسين القبلي والبعدي تعزى لتأثير المقرر

المقترح ذات دلالة إحصائية لصالح القياس البعدي، وكذلك نلاحظ أن متوسط درجات طالبات المجموعة التجريبية في مهارة إدارة كلمات المرور في القياس القبلي بلغ (9.53)، بانحراف معياري (1.97)، بينما بلغ متوسط درجاتهن في القياس البعدي (19.53)، بانحراف معياري (1.97)، وبلغت قيمة ت المحسوبة (19.580)، عند مستوى دلالة محسوب بلغ (0.000)، وهو أقل بكثير من مستوى الدلالة المعتمد في هذه الدراسة (0.05)، وهذا يدل على أن الفروق بين متوسطات درجات الطالبات المجموعة التجريبية في القياسين القبلي والبعدي تعزى لتأثير المقرر المقترح ذات دلالة إحصائية لصالح القياس البعدي، وكذلك بلغ متوسط درجات طالبات المجموعة التجريبية في مهارة التعامل مع المحتوى الخطر في القياس القبلي بلغ (11.10)، بانحراف معياري (3.23)، بينما بلغ متوسط درجاتهن في القياس البعدي (20.50)، بانحراف معياري (2.40)، وبلغت قيمة ت المحسوبة (12.786)، عند مستوى دلالة محسوب بلغ (0.000)، وهو أقل بكثير من مستوى الدلالة المعتمد في هذه الدراسة (0.05)، وهذا يدل على أن الفروق بين متوسطات درجات الطالبات المجموعة التجريبية في القياسين القبلي والبعدي تعزى لتأثير المقرر المقترح ذات دلالة إحصائية لصالح القياس البعدي، وبلغ متوسط درجات طالبات المجموعة التجريبية في مهارة التفاعل الأمن مع الآخرين في القياس القبلي بلغ (9.83)، بانحراف معياري (1.49)، بينما بلغ متوسط درجاتهن في القياس البعدي (19.93)، بانحراف معياري (1.49)، وبلغت قيمة ت المحسوبة (26.037)، عند مستوى دلالة محسوب بلغ (0.000)، وهو أقل بكثير من مستوى الدلالة المعتمد في هذه الدراسة (0.05)، وهذا يدل على أن الفروق بين متوسطات درجات الطالبات المجموعة التجريبية في القياسين القبلي والبعدي تعزى لتأثير المقرر المقترح ذات دلالة إحصائية لصالح القياس البعدي، وأخيرًا بلغ متوسط درجات طالبات المجموعة التجريبية في مهارة الصيانة وطلب المساعدة في القياس القبلي بلغ (9.10)، بانحراف معياري (1.73)، بينما بلغ متوسط درجاتهن في القياس البعدي (19.10)، بانحراف معياري (1.73)، وبلغت قيمة ت المحسوبة (22.399)، عند مستوى دلالة محسوب بلغ (0.000)، وهو أقل بكثير من مستوى الدلالة المعتمد في هذه الدراسة (0.05)، وهذا يدل على أن الفروق بين متوسطات درجات الطالبات المجموعة التجريبية في القياسين القبلي والبعدي تعزى لتأثير المقرر المقترح ذات دلالة إحصائية لصالح القياس البعدي، مما سبق يمكننا رفض الفرض الصفري السابق واعتماد الفرض البديل والذي ينص على "توجد فروق ذات دلالة إحصائية ($\alpha \leq 0.05$) بين متوسط درجات المجموعة التجريبية في مهارات (حماية المعلومات الشخصية – إدارة كلمات المرور – التعامل مع المحتوى الخطر – التفاعل الأمن مع الآخرين – الصيانة وطلب المساعدة) لدى طالبات الصفوف العليا من المرحلة الابتدائية في القياسين القبلي والبعدي تعزى للمقرر المقترح في ضوء التعلم القائم على المشاريع لصالح القياس البعدي"، وهذا يدل على التأثير الواضح للمقرر المقترح في تنمية مهارات الأمن السيبراني، ونتفق هذه النتيجة مع نتائج دراسة الشريف (2023)و دراسة المطرفي والقراني (2023)، ودراسة عبدالله (2023) وكذلك مع دراسة قاسم والعنزي (2023) ودراسة الجندي ومحمد (2019)، والتي أثبتت التأثير الواضح للمقرر المقترح في تنمية مهارات الأمن السيبراني، وتختلف مع دراسة Witsenboer et al (2022) التي بينت نتائجها أن المنهج الدراسي لا يُولي هذا الموضوع اهتمامًا يُذكر، وأن الطلاب يكتسبون سلوكهم الإلكتروني بشكل رئيسي من خلال الخبرة والتعليمات على الإنترنت.

وتُعزى هذه النتيجة إلى المميزات التي يتمتع بها أسلوب التعلم القائم على المشاريع وقدرته على تنمية جوانب مهارية مختلفة لدى المتعلمات، حيث يتميز هذا الأسلوب بكونه أحد أساليب التعلم النشط والذي يتمحور حول المتعلم ويجعله محور العملية التعليمية، وأيضًا لعب التصميم المنهجي للمقرر المقترح دورًا أساسيًا في تأثيره الفعال في تنمية مهارات الأمن السيبراني حيث اتبع ذلك التصميم المراحل والخطوات العلمية لتصميم المقررات التعليمية، مع مراعاة الشروط والمبادئ لكل مرحلة منها.

ملخص النتائج:

يمكن تلخيص النتائج التي توصلت إليها الدراسة الحالية بالنقاط التالية:

1. توجد فاعلية للمقرر المقترح لتنمية مهارات الأمن السيبراني لدى طالبات الصفوف العليا للمرحلة الابتدائية في ضوء التعلم القائم على المشاريع.
2. توجد فروق ذات دلالة إحصائية ($\alpha \leq 0.05$) بين متوسط درجات المجموعة التجريبية في مهارات (حماية المعلومات الشخصية – إدارة كلمات المرور – التعامل مع المحتوى الخطر – التفاعل الأمن مع الآخرين – الصيانة وطلب المساعدة) لدى طالبات الصفوف العليا من المرحلة الابتدائية في القياسين القبلي والبعدي تعزى للمقرر المقترح في ضوء التعلم القائم على المشاريع لصالح القياس البعدي.

التوصيات:

بناءًا على النتائج التي توصلت إليها الدراسة نوصي بالآتي:

1. دمج المقرر المقترح في مناهج التعليم الابتدائي في مناهج الحاسب الآلي وذلك لتنمية مهارات الأمن السيبراني لدى المتعلمين في وقت مبكر.
2. إقامة دورات تدريبية لمعلمات المرحلة الابتدائية حول أهمية مهارات الأمن السيبراني لعصرنا الحالي، وأهمية تنمية مهاراته لدى المتعلمين.
3. إقامة ندوات توعية للمجتمع بالمخاطر السيبرانية الشائعة في عصرنا الحالي، والمهارات اللازمة للتعامل معها.

المقترحات:

1. إجراء دراسة حول مقرر مقترح على أساس التعلم التفاعلي لتنمية مهارات الأمن السيبراني لدى طالبات المرحلة المتوسطة بالمملكة.
2. إجراء دراسة حول مخاطر الأمن السيبراني الناجمة عن استخدام وسائل التواصل الاجتماعي المختلفة وطرق التعامل معها.
3. تطبيق هذه الدراسة على بيئات سعودية مختلفة للتأكد من فعالية المقرر المقترح المطبق فيها.

المراجع العربية:

آل جديع، مفلح بن قبلان بن بجاد. (٢٠٢١). مدى تطبيق معايير تصميم التعليم في المقررات الجامعية الإلكترونية وفق نموذج ADDIE Model من وجهة نظر أعضاء هيئة التدريس بجامعة تبوك. مجلة كلية التربية،،٣٧)١٠(٥٦-١٠٠.

التقرير السنوي للرقمنة السعودية. (٢٠٢٥). تاريخ الاسترجاع :٣١-٣-٢٠٢٥م،من : https://trendx.co/1014650

الجندي، علياء بنت عبدالله، ومحمد، نهير طه حسن. (٢٠١٩). دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة. عالم التربية، ٦٧)٣(، ١٤. – ٨٤

الجهني، ليلى سعيد سويلم. (.(٢٠١٨تصميم المواد البصرية تقنيات وتطبيقات. العبيكان للنشر

حويري، عليش عبدالرحيم البشير. (.٢٠٢٠ أثر وحدة تدريسية قائمة على إستراتيجية التعلم المعكوس وفقا لنموذج التصميم العام ADDIE على التحصيل الدراسي في مقرر المدخل إلى تكنولوجيا التعليم لدى طلاب المستوى الثاني بكلية التربية جامعة الخرطوم. مجلة جيل العلوم الإنسانية والاجتماعية، ((٦٦ ، ١٢٩–١٥٠.

الدوسري ,حسين بن سعيد. ((٢٠١٧.تحليل محتوى مقرر الحاسب الآلي وتقنية المعلومات للصف الأول ثانوي بالمملكة العربية السعودية في ضوء مهارات القرن الحادي والعشرين. [رسالة ماجستير غير منشورة]. جامعة الإمام محمد بن سعود. كلية العلوم الاجتماعية. الرياض.

الربيعة,صالح بن علي بن عبدالرحمن (٢٠١٨).الأمن الرقمي وحمايةالمستخدم من مخاطر الإنترنت.هيئة الاتصالات وتقنية المعلومات.مكة المكرمة..

الرويلي، مزيدة بنت براك، و الحويطي، محمد بن مفرج فريج. (.(٢٠٢٤فاعلية وحدة تعليمية قائمة على التعلم المدمج في تنمية مهارات التفكير الرياضي لدى طالبات الصف الرابع الابتدائي. المجلة العربية للتربية النوعية، ((٣٢، .٣٤٣–٣٧٠

سليم، مريم. (.٢٠٠٤ علم النفس التربوي، دار النهضةالعربية، بيروت.

السليماني، نسرين، فرج ميراهان. (.٢٠٢١ تصميم كتاب إلكتروني تفاعلي لتعلم تصميم الأزياء الوظيفية وفقاً للنموذج العام للتصميم التعليمي ADDIE Model. مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع، (٦٤)، ٢٧١–٢٨٥.

الشريف، مرام خالد يحيى، الحربي، ليان سعد عوض الله، الحربي، العنود عبدالعزيز مصلح، و السليماني، أمل عبيدالله عبدالعزيز. (.٢٠٢٣ فعالية برنامج تدريبي مقترح لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية: دراسة تجريبية "الجزء الأول". المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات، .٣)٤(، ٩٧–١٤٠

عبد الله، مصطفى أحمد. (.٢٠٢٣ فاعلية التعليم الموضوعي القائم على فيديو مشاركة المحتوى في الوعي بالأمن المعلوماتي وخفض الحمل المعرفي لدى طلاب مدارس المتفوقين في العلوم والتكنولوجيا.مجلة جنوب الوادي الدولية للعلوم التربوية. ٦)١٠(، ٤٩٦–٥٣٩.

العتيبي، ماجد، والوادعي، مسفر. (.٢٠٢٢ أثر التعلم القائم على المشاريع لتدريس اللغة الإنجليزية في تنمية مهارات الكتابة الإبداعية لدى طلاب المرحلة الثانوية. المجلة السعودية للعلوم التربوية، .١)٨(، ٢٣–٣٨

العلوان، جعفر أحمد عبد الكريم. ((٢٠٢١. الألعاب الرقمية الجادة و تنمية مهارات الأمن السيبراني : دراسة استكشافية. مجلة المثقال للعلوم الاقتصادية و الإدارية و تكنولوجيا المعلومات، .٧)٣(، ٨٢–١١٤

علي، سهير عبدالسميع السيد، محمود، صابر حسين، و محمد، عزة محمد عبدالسميع. (.(٢٠٢٥برنامج مقترح قائم على التعلم بالمشروع لتنمية مهارات ريادة الأعمال لدى طلاب المدارس الثانوية التجارية. دراسات في التعليم الجامعي، (٦٦)،٢٣٦–٢٧١.

العنزى، حصة بنت قياض، والعقاب، عبدالله بن محمد. (٢٠١٩). تحليل محتوى مقرر الحاسب وتقنية المعلومات (1) للصف الأول ثانوي في ضوء المهارات الحاسوبية اللازمة لسوق العمل. مجلة البحث العلمي في التربية، ٢٠(٦)، ٤٥٧-٤٨٠

العنزي، أحمد محمد علي. ((٢٠٢٤. درجة تضمين أنماط الذكاءات المتعددة كتب الحاسوب في المرحلة الأساسية العليا في الأردن. مجلة البلقاء للبحوث والدراسات، ٢٧.)٢(، ٨٨-١٠٧

فوزي، إحمد. (.(٢٠١٩ الأمن السيبراني: الأبعاد الاجتماعية والقانونية، تحليل سوسيولوجي. المجلة الاجتماعية القومية، ٥٦)٢(، ٩٩-١٣٩.

قاسم، عبدالمريد عبدالجابر، العنزي، تركي بن بندر. (٠٢٣٢). فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى مستخدمي الإنترنت من طلاب المرحلة الثانوية بمنطقة جازان. مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية. ١٢(٣)، ١٦.٥-٥٥١

القحطاني، سمية، والحارثي، ماجد. (٠٢٢٢). أثر استراتيجية التعلم الإلكتروني القائم على المشاريع في خفض التجول العقلي لدى طالبات الصف الثالث المتوسط بجدة. مجلة العلوم التربوية والنفسية، ٦(٩٥)، ٥٩-١٨١.

القحطاني، مها بنت مسمار، و الشبل، منال بنت عبدالرحمن يوسف. (٠٢٢٢). تحليل محتوى كتب المهارات الرقمية للصف الأول المتوسط بالمملكة العربية السعودية في ضوء مبادئ النظرية البنائية وأسسها. مجلة المناهج وطرق التدريس، ١((١٢، ٧٣ – ٨٥.

القميزي، حمد. (٢٠١٧). تقنيات التعليم ومهارات الاتصال. دار روابط للنشر وتقنية المعلومات ودار الشقري للنشر.

اللقاني، أحمد حسين؛ والجمل، علي أحمد. (٢٠٠٣). معجم المصطلحات التربوية المعرفة في المناهج وطرق التدريس.ط ٣، القاهرة: عالم الكتب..

المحمادي، غدير بنت علي. (٠٢٣٢). فاعلية وحدة الكترونية تفاعلية في توظيف مهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية. مجلة جامعة أم القرى للعلوم التربوية والنفسية، ٥١)١(،١٤٢-١٦٥.

محمد,وائل عبدالله ؛العظيم ,ريم أحمد(٠١٢٢).تحليل محتوى المنهج في العلوم الإنسانية . عمان: دار المسيرة.

المحيميد، باسم. (٢٠٢٣). دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية مجلة العلوم التربوية، ٩(٤)، ٣٨-١٦١.

الهيئة الوطنية للأمن السيبراني. ((٢٠٢٠. الضوابط الأساسية للأمن السيبراني، تم الاسترجاع من موقع : https://nca.gov.sa/files/ecc-ar.pdf

وزارة التعليم .دليل الخطط الدراسية لعام ١٤٤٥ .مسترجع في ٣١ مارس ٢٠٢٥ ،من https://www.moe.gov.sa/ar/education/generaleducation/StudyPlans/Documents/Study-plans-1445.pdf:

المراجع الأجنبية:

-Hadnagy, C. (2018). Social engineering: The science of human hacking. Wiley .

-Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). State of practice of computer security incident response teams (CSIRTs). Carnegie Mellon University .

-Kumar, N., & Carley, K. M. (2021). Cybersecurity awareness and skills: A review. Computers & Security, 101, 102116. https://doi.org/10.1016/j.cose.2020.102116

-Livingstone, S., Stoilova, M., & Nandagiri, R. (2017). Children's data and privacy online: Growing up in a digital age. UNICEF Office of Research .

-Nguyen, T., Kim, D., & Lee, J. (2022). Cybersecurity skills development for youth: A review of educational approaches. Journal of Cybersecurity Education, Research and Practice, 2022(1), 1-15 .

-Safa, N. S., Maple, C., & Watson, T. (2016). Information security awareness: A review of literature. Computers & Security, 63, 101-115. https://doi.org/10.1016/j.cose.2016.07.002

Almelhi, A. M. (2021). Effectiveness of the ADDIE Model within an E- Learning Environment in Developing Creative Writing in EFL Students. English Language Teaching, 14(2), 20-36.

Alodwan, T., & Almosa, M. (2018). The Effect of a Computer Program Based on Analysis, Design, Development, Implementation and Evaluation (ADDIE) in Improving Ninth Graders' Listening and Reading Comprehension Skills in English in Jordan. English Language Teaching, 11(4), 43-51.

Alsaleh, N. (2020). The Effectiveness of an Instructional Design Training Program to Enhance Teachers' Perceived Skills in Solving Educational Problems. Educational Research and Reviews, 15(12), 751-763.

Bishop, M. (2003). Computer security: Art and science. Addison-Wesley.

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: a systematic literature review. Information and Computer Security.

Hasweh, R. S., & Hamed Al- Qudah, Mohammed A. (2023). The Role of Secondary School Teachers in Developing Cybersecurity Awareness among Its Students from the Perspective of Teachers in Private Schools in Amman. Dirasat: Educational Sciences, 50(3), 61–75.

Howard, M., & LeBlanc, D. (2003). Writing secure code. Microsoft Press.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). State of practice of computer security incident response teams (CSIRTs). Carnegie Mellon University.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC Press.

Sharma, S., & Sood, S. K. (2017). A survey on security issues in cloud computing. Journal of Network and Computer Applications, 79, 88-115.

Thomas, J. W. (2000). A review of research on project-based learning. Online. Retrieved April 8, 2019, from http://www.bobpearlman.org/BestPractices/PBL_Research.pdf.

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers & Education, 186, 104536.

Zahran, F. A. (2018). TheImpact of Project Based Learning on EFL Critical Reading and Writing Skills. Studies in curriculum and instruction, 232.(72-39),

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد الواحد والثمانون
تاريخ الإصدار: 2 – تموز – 2025م
www.ajsp.net

"Designing a Proposed Curriculum to Develop Cybersecurity Skills among Female Students in The Upper Grades of Primary School in Light of Project-Based Learning"

Prepared by:

Prof. Dr. Haila bint Khalaf Al-Duhaiman

Al-Joharah Mirdas Alian Al-Mutairi

Hessa bint Qayyad Abdullah Al-Anzi

Nada bint Abdulaziz Al-Mashou

Abstract:

This study aimed to designing a proposed curriculum to develop cybersecurity skills among female students in the upper grades of primary school, using project-based learning. The study also sought to evaluate the effectiveness of this course in enhancing these skills. The study followed a quasi-experimental approach using a single experimental group with pre- and post-tests. The study sample consisted of 30 female students selected through a purposive sampling method. The study tools included the proposed course for developing cybersecurity skills, in addition to a questionnaire specifically designed to measure the level of these skills. The results demonstrated the effectiveness of the proposed course in developing students' cybersecurity skills. Statistically significant differences were observed at a significance level of ($\alpha \leq 0.05$) between the pre- and post-tests in all skill areas studied, including: protecting personal data, managing passwords, confronting potential risks, interacting safely with others, and maintaining and seeking assistance. These differences are attributed to the proposed course's favorable effect on the post-test. Keywords: Proposed Course - Cybersecurity Skills - Project-Based Learning.

Keywords: Proposed Course - Cybersecurity Skills - Project-Based Learning.