Забезпечення конфіденційності: важливо забезпечити конфіденційність результатів тестування та уникнути можливості підкупу чи підробки.

Стимулювання навчання: важливо враховувати, як використання тестів може вплинути на мотивацію учнів та їхнє активне навчання.

Незважаючи на ці виклики, тестові технології залишаються важливим інструментом для проведення моніторингових досліджень у сучасній освіті.

Тестові технології відіграють ключову роль у моніторингових дослідженнях в освіті, надаючи об'єктивні дані про навчальні досягнення учнів та допомагаючи у прийнятті обґрунтованих рішень щодо покращення якості освіти. Важливо постійно вдосконалювати та адаптувати тестові технології до потреб освітнього процесу для досягнення найкращих результатів.

Список використаних джерел:

1. Chen, B. (2018). Using data visualization to improve student learning: A meta-analysis. Educational Research Review, 24, 101-114.
2. Mayer, R. E. (2014). The Cambridge handbook of multimedia learning. Cambridge University Press.
3. Roschelle, J., & Pea, R. D. (2017). A dual-coding theory for multimedia learning and design research on students' understanding of complex concepts. Educational Psychologist, 52(1), 67-95.
4. Quinn, P. (2017). Data visualization for education. Journal of Educational Technology Development and Exchange (JETDE), 10(2), 117-129.

Сіткар Т. В.
доцент кафедри комп’ютерних технологій
Тернопільський національний педагогічний університет ім. В. Гнатюка
sitkar@gmail.com

РОЛЬ КІБЕРБЕЗПЕКИ У СУЧАСНІЙ ОСВІТІ: ВИКЛИКИ, ПЕРЕВАГИ ТА СТРАТЕГІЇ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

У сучасному цифровому світі, роль кібербезпеки у сфері освіти стає все більш визначальною та критичною. Зростання використання комп'ютерів, мобільних пристроїв та інших технологій у навчальних процесах створює серйозні виклики щодо забезпечення безпеки інформації та захисту від кіберзагроз [1].

Одним з головних аспектів, що підкреслює важливість кібербезпеки в освіті, є необхідність захисту конфіденційної інформації. У навчальних закладах зберігаються особисті дані учнів, викладачів, адміністрації, а також фінансова інформація. Зловмисники можуть спробувати зламати системи навчальних закладів, щоб отримати доступ до цієї чутливої інформації або вчинити кібератаки з метою витоку даних або вимагання викупу.

Крім того, інтенсивне використання цифрових технологій у навчальних цілях викликає потребу у посиленні захисту мереж та інформаційних систем. Завдяки доступу до мережі Інтернет, студенти та викладачі можуть здійснювати віддалений доступ до навчальних ресурсів, спілкуватися та співпрацювати в онлайн середовищі. Однак це також означає, що мережі навчальних закладів повинні бути надійно захищені від зловмисників, які можуть намагатися скомпрометувати ці системи або завдати шкоди шляхом кібератак.

Надто, зростання використання онлайн-платформ та хмарних сервісів у навчальних цілях ставить під загрозу безпеку даних. Важливо забезпечити захист конфіденційної інформації, яка зберігається в хмарних сервісах або передається через онлайн платформи, щоб уникнути витоку даних та неправомірного доступу до них.

У зв'язку з цим, основними викликами, з якими стикається кібербезпека в освіті, є:

Збільшення кількості кібератак: Зловмисники постійно намагаються зламати системи навчальних закладів для отримання конфіденційної інформації.

Недостатня освіченість з кібербезпеки: Важливо забезпечити навчання учасників навчального процесу з питань кібербезпеки для попередження фішингу, соціальної інженерії та інших кіберзагроз.

Використання застарілих технологій: Застосування застарілих систем та програмного забезпечення може стати причиною вразливостей у системах навчальних закладів.

Переваги впровадження кібербезпеки в освіті полягають у забезпеченні безпеки конфіденційної інформації, захисту мереж та систем від кібератак, а також підвищенні освіченості учасників навчального процесу з питань кібербезпеки. Це допомагає створити безпечне та надійне цифрове середовище для навчання та розвитку.

Одним із найбільших викликів кібербезпеки в освіті є постійний розвиток технологій та зростання кількості цифрових платформ у навчальних закладах [2]. Це призводить до збільшення загрози з боку кібератак та кіберзлочинів. Навчальні установи зберігають значну кількість чутливої інформації, включаючи особисті дані учнів та викладачів, фінансову інформацію та інші важливі дані, що робить їх мішенями для хакерів та зловмисників у кіберпросторі.

Найпоширенішими викликами, з якими стикаються навчальні заклади у сфері кібербезпеки, є кібератаки та зломи систем. Хакери та зловмисники можуть намагатися проникнути в системи навчальних закладів для отримання доступу до конфіденційної інформації або для здійснення кібератак на інші цілі. Це може призвести до витоку конфіденційних даних або навіть до недоступності важливих систем для користувачів.

Крім того, фішинг та соціальна інженерія є ще одним серйозним викликом [3]. Атаки, спрямовані на користувачів шляхом маніпуляції та обману, можуть призвести до витоку конфіденційної інформації або втрати доступу до важливих систем.

Недостатня освіченість з кібербезпеки також є великим викликом. Брак знань та навичок у сфері кібербезпеки серед учнів, викладачів та адміністраторів може призвести до недбалого ставлення до захисту інформації та створення вразливих моментів для кібератак.

У цілому, кібербезпека в освіті вимагає комплексного підходу та постійного вдосконалення стратегій захисту для ефективного протидії різноманітним кіберзагрозам.

Впровадження ефективних стратегій кібербезпеки в освіті має численні переваги [4]:

- Захист конфіденційної інформації: Гарантується захист особистих та фінансових даних учасників навчального процесу.
- Забезпечення безпеки мереж і систем: Захищається інфраструктура навчального закладу від кібератак та витоків даних.
- Підвищення освіченості з кібербезпеки: Сприяється розвитку навичок учасників освітнього процесу у сфері безпеки в мережі.

Для успішного захисту від кіберзагроз у сфері освіти необхідно впроваджувати комплекс стратегій, спрямованих на підвищення рівня кібербезпеки. Основні стратегії включають:

Освічення з кібербезпеки: Важливим елементом є проведення навчань, семінарів та тренінгів для учасників навчального процесу з питань кібербезпеки. Це допоможе підвищити рівень усвідомлення ризиків і збільшити навички користувачів у виявленні та запобіганні кіберзагроз.

Використання сучасних технологій захисту: Необхідно встановлювати та активно використовувати програмні засоби для виявлення та запобігання кібератак. Це може включати антивірусне програмне забезпечення, файрволи, системи виявлення вторгнень та інші технології захисту даних.

Регулярні аудити та тестування на проникнення: Важливо періодично проводити аудити та тестування на проникнення для перевірки систем на наявність вразливостей та виявлення можливих загроз. Це допоможе вчасно виявляти потенційні проблеми та приймати необхідні заходи для їх вирішення.

Впровадження цих стратегій дозволить підвищити рівень кібербезпеки у навчальних закладах та забезпечити надійний захист від кіберзагроз. Однак важливо також пам'ятати про постійне вдосконалення заходів безпеки відповідно до змін у кіберпросторі та зловмисницьких тенденцій.

Усвідомлення важливості кібербезпеки в сучасній освіті є критичним аспектом у забезпеченні безпеки та захисту конфіденційної інформації в навчальних закладах. Впровадження відповідних стратегій захисту є необхідним кроком у цифрову епоху, де зростає кількість кіберзагроз та кібератак на освітні інституції.

Проведення систематичних навчань, семінарів та тренінгів з питань кібербезпеки серед учасників навчального процесу є ключовою стратегією. Це дозволяє підвищити рівень усвідомлення ризиків та навички виявлення та запобігання кіберзагрозам. Важливо, щоб кожен учасник освітнього процесу був ознайомлений із загрозами в кіберпросторі та знав, як правильно діяти у разі виявлення аномальної активності чи підозрілих повідомлень.

Паралельно з освіченням, використання сучасних технологій захисту є важливою стратегією. Встановлення та постійне оновлення програмних засобів для виявлення та запобігання кібератак є обов'язковим. Зокрема, важливо встановлювати антивірусне програмне забезпечення, файрволи та інші технології захисту даних.

Такі сталі зусилля у напрямку кібербезпеки в освіті дозволять уникнути серйозних кіберзагроз та забезпечити безпеку всіх учасників освітнього процесу в умовах сучасного цифрового середовища.

Список використаних джерел:

1. Коваленко А. А. Кібербезпека для дітей та підлітків: Як захистити себе в Інтернеті. – Х.: Ранок, 2021. – 144 с.
2. Кравченко Т. В. Кібербезпека в освіті: виклики та шляхи їх вирішення // Комп'ютерні науки та інформаційні технології. – 2023. – № 1. – С. 5-7.
3. Мороз О. С. Роль кібербезпеки в сучасній освіті // Освіта і наука. – 2022. – № 1. – С. 3-4.
4. Петренко С. М., Шевченко О. В., Гук І. П. Кібербезпека в освіті: Посібник для викладачів. – К.: Літера ЛТД, 2022. – 128 с.

Скрипко С.О.,
старший викладач
ННІ професійної освіти та технологій
Національний університет
«Чернігівський колегіум» імені Т. Г. Шевченка (м. Чернігів)
sskripro0807@ukr.net
Повечера І.В.
кандидат педагогічних наук, доцент кафедри
технологічної освіти та інформатики
Національний університет
«Чернігівський колегіум» імені Т. Г. Шевченка (м. Чернігів)
iryna_povechera@meta.ua

ОРГАНІЗАЦІЯ ДИСТАНЦІЙНОГО НАВЧАННЯ МАЙБУТНІХ ВЧИТЕЛІВ ТЕХНОЛОГІЙ

На сьогоднішній день питання використання дистанційної форми навчання в роботі ВНЗ стають надзвичайно актуальними. Це пов’язано з тим, що в умовах воєнного стану, дистанційна форма освіти може запроваджуватися як єдино можлива з безпекових міркувань форма здобуття освіти на всій території України або в окремих місцевостях.

Дистанційна форма навчання дає сьогодні рівні можливості всім студентам, незалежно від місцезнаходження в будь-яких районах країни і за її межами реалізувати права на освіту. Особливо актуальними означені питання постають у сфері підготовки майбутніх вчителів технологій, адже значна кількість студентів, які навчаються на сьогоднішній день у Національному університеті «Чернігівський колегіум» імені Т.Г. Шевченка знаходяться в областях, що постраждали від військових дій.

Зважаючи на це, дослідження питань організації дистанційного навчання є доцільним та своєчасним. Різними аспектами вивчення дистанційної освіти займалися такі вчені, як