РОЗРОБКА МУЛЬТИМЕДІЙНОГО КУРСУ З КІБЕРБЕЗПЕКИ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ

Онищенко Ю. М., Муллалієва Д. С.
Харківський національний університет внутрішніх справ, Харків, Україна

Актуальність кібербезпеки в сучасному світі надзвичайно висока, оскільки кіберзагрози та кібератаки постійно зростають у складності та масштабах. Відсутність належного захисту може призвести до серйозних наслідків для корпорацій, державних структур та громадян. Узагальнена статистика підтверджує цю тенденцію.

За даними Звіту про кібербезпеку Verizon за 2022 рік [1], порівняно з 2021 роком кількість атак програм-вимагачів в 2022 році зросла на 13%, що є значним збільшенням, якщо порівняти цей відсоток з останніми 5 роками разом [2].

Стосовно України, протягом 2022 року Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році.

Кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла у 18,3 та 2,2 рази відповідно [3].

Ця статистика вказує на необхідність надійного навчання та підготовки фахівців у галузі кібербезпеки для подолання зростаючих загроз та ефективного захисту інформації та інфраструктури в сучасному цифровому середовищі.

У цьому контексті розробка мультимедійного курсу з кібербезпеки на платформі вебсайту є актуальним завданням, адже має низку переваг:

1. Збільшення обізнаності: здобувачі вищої освіти можуть швидко ознайомитися зі змінами в кіберзагрозах та відповідних стратегіях захисту, відвідавши даний вебсайт.
2. Реалістичне навчання: мультимедійні ресурси на вебсайті дозволяють створити ситуації, що імітують реальні кібератаки, допомагаючи здобувачам вищої освіти розвивати практичні навички в області кібербезпеки, користуючись вебплатформою.
3. Гнучке навчання: здобувачі вищої освіти можуть навчатися у власному темпі, вибираючи час і місце для навчання, і отримувати доступ до матеріалів з будь-якого пристрою з підключенням до Інтернету.
4. Оновлення змісту: вебсайт можна легко оновлювати, щоб відображати нові загрози та стратегії захисту, забезпечуючи постійно актуальну інформацію.
5. Візуалізація складних концепцій: мультимедійний формат дозволяє візуалізувати складні кібербезпекові концепції, діаграми та графіки, що полегшує розуміння матеріалу і покращує сприйняття інформації.

6. Інтерактивність: мультимедійні курси можуть включати інтерактивні вправи, вікторини та завдання, що допомагають здобувачам вищої освіти активно залучатися до навчання та встановлювати практичні навички.

7. Можливість дистанційного навчання: мультимедійний курс може бути доступним онлайн, що дозволяє здобувачам вищої освіти навчатися з будь-якого місця і в будь-який час, зменшуючи географічні та часові обмеження.

8. Персоналізоване навчання: мультимедійні курси можуть враховувати індивідуальні потреби здобувачів вищої освіти, надаючи можливість обирати шляхи навчання та фокусуватися на конкретних аспектах кібербезпеки.

9. Відстеження прогресу: платформа мультимедійного курсу може надавати звіти про прогрес здобувачаів вищої освіти, що допомагає науково-педагогічним працівникам, тренерам та інструкторам в оцінці успішності та адаптації курсу.

10. Ефективне поширення інформації: мультимедійний курс може бути легко поширюваним та доступним для широкої аудиторії, що сприяє розповсюдженню знань та навичок в області кібербезпеки.

Отже, розробка та впровадження мультимедійного курсу з кібербезпеки на вебсайті є необхідним етапом для зміцнення знань та навичок у цій надважливій галузі, щоб забезпечити надійний захист від кіберзагроз і зберегти цифрову безпеку в нашому сучасному глобалізованому світі.

Список літератури

1. Джерело: Verizon. (2022). 2022 Data Breach Investigations Report. [Посилання на джерело: https://enterprise.verizon.com/resources/reports/dbir/] (дата звернення: 10.11.2023)

2. https://blog.desdelinux.net/uk/segun-el-informe-de-2022-de-verizon-el-ransomware-aumento-un-13-en-comparacion-con-el-ano-pasado/ (дата звернення: 10.11.2023)

3. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України, https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit (дата звернення: 10.11.2023)