Міністерство освіти і науки України
Національна академія наук України
Південний науковий центр НАН та МОН України
Чорноморський національний університет імені Петра Могили
Первинна профспілкова організація ЧНУ імені Петра Могили
Інститут української археографії та джерелознавства ім. М.С. Грушевського НАНУ
Державний архів Миколаївської області
ДУ «Національний науковий центр радіаційної медицини НАМН України»
Державний аграрний університет Молдови (Кишинів)
Університет гуманітарних та природничих наук ім. Яна Длугоша (Польща)
Університет імені Адама Міцкевича (Польща)
Leipzig University of Applied Sciences (Німеччина)
Ca` Foscari University, Venice (Італія).

ОЛЬВІЙСЬКИЙ ФОРУМ – 2023: стратегії країн Причорноморського регіону в геополітичному просторі

XVII Міжнародна наукова конференція

ТЕЗИ

ТЕХНІЧНІ НАУКИ
СТАЛИЙ РОЗВИТОК УНІВЕРСИТЕТСЬКОЇ СИСТЕМИ ОСВІТИ

15–18 червня 2023 р., м. Миколаїв,Україна

Миколаїв – 2023

Ольвійський форум – 2023 : стратегії країн Причорноморського регіону в геополітичному просторі.Технічні науки. Сталий розвиток університетської системи освіти: XVII Міжнар. наук. конф. 15–18 черв. 2023 р., м. Миколаїв : тези / М-во освіти і науки України ; Нац. акад. наук України ; Півд. наук. центр НАН та МОН України ; ЧНУ ім. Петра Могили ; Первинна профспілкова орг. ЧНУ ім. Петра Могили ; Ін-т укр. археографії та джерелознавства ім. М. С. Грушевського НАНУ ; Держ. архів Миколаївської обл. ; ДУ «Нац. наук. центр радіаційної медицини НАМН України» ; Держ. аграрний ун-т Молдови (Кишинів) ; Ун-т гуманітарних та природн. наук ім. Яна Длугоша (Польща) ; Ун-т ім. Адама Міцкевича (Польща) ; Leipzig University of Applied Sciences (Німеччина) ; Ca` Foscari University, Venice (Італія). – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2023. – 252 с.

Збірник містить тези доповідей учасників XVII Міжнародної науково-практичної конференції «Ольвійського форуму-2023 : стратегії країн Причорноморського регіону в геополітичному просторі. Технічні науки. Сталий розвиток університетської системи освіти».

УДК 004.056.53

Венгрін О. О.,
студент факультету інформаційних технологій
спеціальності «Кібербезпека»,
ХНЕУ імені С. Кузнеця, м. Харків, Україна
Старкова О. В.,
д-р техн. наук, професор, зав. кафедри КІТ,
ХНЕУ імені С. Кузнеця, м. Харків, Україна

КІБЕРЗАХИСТ САЙТІВ ЗАКЛАДІВ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ УКРАЇНИ

Тривалий карантин та війна в Україні призвели до того, що переважна більшість закладів загальної середньої, професійної та професійно-технічної освіти перейшли на дистанційну форму навчання. Але, навіть за таких умов, в інтернеті вони представлені не на належному рівні. Багато з них мають зовсім неінформативні сайти з дизайном, який був актуальним більше 10 років тому. Очевидно, що цим сайтам можуть бути притаманні і актуальні на той час вразливості, які вже виправлені в більш сучасних рішеннях, але можуть зберігати свій потенціал в застарілих.

На думку авторів, дослідження вразливостей інтернет-ресурсів означених закладів освіти є актуальним, оскільки за останні роки наше суспільство неодноразово могло відчути на собі наслідки різноманітних інформаційних спецоперацій. Тому, щоб ефективно протидіяти цьому, дуже важливо приділяти належну увагу кібербезпеці в усіх сферах нашого життя.

Для батьків, діти яких навчаються в школі або ліцеї, інтернет-ресурси цих закладів зазвичай є авторитетним джерелом інформації. І поява певних новин на їх сайтах, підкріплених повідомленнями з каналів в Telegram та коментарями у Facebook, може підбурити суспільство до деструктивних дій або викликати паніку. Також певну небезпеку несе в собі злам сайту з метою розміщення на ньому реклами певного змісту, демонстрація якої є неприпустимою для дітей.

Питанням аналізу кіберзагроз присвячена велика кількість досліджень, але цілком очевидно, що переважна більшість авторів розглядають проблеми кіберстійкості критичної інфраструктури [1] та банківських систем [2]. Важливість цих галузей в сучасному світі неможливо переоцінити, але є багато інших ресурсів, вразливість яких також може призвести до негативних наслідків, хоча і меншого масштабу. Так, в роботі [3] звернуто увагу на те, що вищі навчальні заклади на-

копичують великі обсяги персональних даних і фінансової інформації про студентів, викладачів та співробітників, а також інформацію про наукові дослідження, і це робить їх привабливою мішенню для кіберзлочинців. Особливо привабливим об'єктом для кібератак виступають військові вищі навчальні заклади [4] через те, що там циркулюють дані не тільки звичайних громадян, але й діючих та майбутніх військовослужбовців.

У порівнянні з наслідками атак критичної інфраструктури, банківського сектору та ВНЗ, атака на ресурси закладів середньої освіти не виглядає такою привабливою. Але вона може стати одним із елементів певної нової стратегії, ще незнайомої нашому суспільству.

Метою даного дослідження є визначення найбільш розповсюджених вразливостей, які зустрічаються на сайтах закладів загальної середньої освіти в Україні, оцінка їх впливу на стійкість сайту і виявлення певних закономірностей, якщо вони існують.

За результатами дослідження буде сформульовано рекомендації щодо побудови інтернет-ресурсів. Оскільки автори не отримували згоди від власників на детальний аналіз їх сайтів і це дослідження виконується не за дорученням Міністерства освіти і науки України або інших державних установ, то з метою дотримання вимог законодавства прийнято наступний алгоритм виконання роботи:

1. З сайту ЄДБО [5] завантажуються відкриті реєстри закладів освіти.

2. Створюється бот, який відвідує сайти і виконує збір певної інформації для подальшого аналізу.

3. Слід зауважити, що відбувається саме відвідування сайту, а не його атака спеціальними сканерами, тобто бот веде себе як звичайна людина і аналізує лише те, що відображається на екрані. Жодних спроб взаємодії з кодом сайту не виконується.

4. Результати відвідувань заносяться в таблицю, після чого обробляються і формуються візуалізації, за допомогою яких можна буде визначити найбільш характерні особливості сайтів (на якій платформі створені, тип серверу, захищеність підключення, показники відвідуваності, особливості дизайну і, у відповідності до них, можливі вразливості тощо).

5. За отриманими результатами буде створений і розміщений в інтернеті макет сайту, на який буде здійснено певну кількість атак.

6. За результатами експерименту будуть сформовані рекомендації щодо методів протидії, на основі яких будуть внесені зміни в макет. За допомогою повторних атак буде визначено ефект від впровадження рекомендацій.

7. Також метою дослідження є спроба визначення, чому саме такі конфігурації є привабливими для закладів освіти та, за можливості, буде запропоновано більш раціональне та безпечне рішення.

Автори розуміють, що інформація, яку буде отримано в результаті дослідження, є конфіденційною і може нашкодити власникам сайтів. Тому візуалізація результатів дослідження буде виконана таким чином, щоб унеможливити ідентифікацію сайтів за будь-якою ознакою: IP-адресою, місцем розташування закладу освіти тощо. Більш детальні дані можуть бути оприлюднені лише після отримання авторами всіх належних дозволів.

Список використаних джерел

1. Мальцева І. Р., Черниш Ю. О., Овсянніков В. В. Аналіз методик оцінки кіберстійкості критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2021. Т. 4, № 12. С. 29–35.

2. Євсєєв С. П., Рзаєв Х. Н., Мамедова Т. А., Самедов Ф. Г., Ромащенко Н. В.Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем. *Кібербезпека: освіта, наука, техніка*. 2018. Т. 2, № 2. С. 47–67.

3. Трофименко О. Г., Логінова Н. І., Манаков С. Ю., Дубовой Я. В. Кіберзагрози в освітньому секторі. *Кібербезпека: освіта, наука, техніка*. 2022. Т. 4, № 16. С. 76–84.

4. Кива В. Ю. Аналіз чинників, які впливають на кібербезпеку вищого військового навчального закладу. *Кібербезпека: освіта, наука, техніка*. 2022. Т. 3, № 15. С. 53–70.

5. Єдина державна електронна база з питань освіти. URL: https://registry.edbo.gov.ua/zagalna-serednya-osvita/ (дата звернення: 10.05.2023).

УДК 004.67

Гончаров Д. С.,
аспірант, завідувач навчальної лабораторії ІКЦ,
ЧНУ імені Петра Могили, м. Миколаїв, Україна

ОБРОБКА ДАНИХ З ПРИЛАДІВ ЗА ДОПОМОГОЮ WEKA НА ПРИКЛАДІ РАКУ МОЛОЧНОЇ ЗАЛОЗИ

Рак молочної залози – це злоякісне утворення, яке посідає перше місце серед захворювань жінок. За даними Всесвітньої організації охорони здоров'я (ВООЗ), щороку діагностують близько 2,3 мільйонів

ЗМІСТ

Секція
ТЕХНІЧНІ НАУКИ

Підсекція: Комп'ютерна інженерія

Басов Д. Є., Пузирьов С. В. Побудова нейронної мережі для детектування малопомітних рухомих об'єктів.....3

Доценко Д. В., Бурлаченко І. С. Продуктивність ORM серверних фреймворків вебзастосунків…….....7

Венгрин О. О., Старкова О. В. Кіберзахист сайтів закладів загальної освіти України….....11

Гончаров Д. С. Обробка даних з приладів за допомогою Weka на прикладі раку молочної залози……...…....11

Данилова О. М., Горішна О. М., Бурлаченко І. С. Регресійні дерева рішень для навігації безпілотного наземного транспорту на перехресті доріг….....17

Дарнапук Є. С. Використання моделей штучного інтелекту для розпізнавання мовлення……...…..20

Дунець А. С. Кіберфізична система виявлення дефектів медичних виробів…….....24

Жуланов М. О., Пузирьов С. В. Діяльність ООН-жінки в Україні: здобутки та перспективи…….……28

Калашніков Д. С., Тимченко В. В., Шутько В. О. Позиція ООН щодо ядерної програми КНДР……..…….31

Крайник Я. М., Доценко Д. В Стиснення вузлових точок зображення за допомогою алгоритму Хаффмана……..…….35

Михайлов О. О., Пузирьов С. В. Автоматизація моніторингу приміщень за допомогою IP-камер та OpenCV……...…….39

Салтовський Б. Г. Візуалізація картографічної інформації на малопотужних пристроях……...……...……...……...42

Семенов В. В. Проєктування друкованих плат в програмі Altium Designer…….……...…….45