УДК 372.8:004.056.5

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ВИКЛАДАННЯ КУРСУ ЗА ВИБОРОМ «ОСНОВИ КІБЕРБЕЗПЕКИ»

Буц Катерина

Науковий керівник: доцент, кандидат педагогічних наук Лупан І.В.

Центральноукраїнський державний педагогічний університет імені Володимира Винниченка, м. Кропивницький, Україна

У статті наведено методичні рекомендації щодо вивчення курсу за вибором «Основи кібербезпеки» в старших класах школи. Підібрано літературу, яку можна порадити використовувати вчителям для підготовки до уроків та учням для кращого засвоєння навчального матеріалу. Вказано посилання на безкоштовні онлайн-курси з кібербезпеки. Для виконання практичних робіт з курсу рекомендовано застосовувати Packet Tracer, призначений для моделювання мережевих технологій. В статті наведено приклад практичної роботи для учнів та тестові завдання для перевірки знань.

Ключові слова: *курс за вибором, основи кібербезпеки, Packet Tracer.*

METHODICAL RECOMMENDATIONS FOR THE "BASICS OF CYBERSECURITY" SELECTIVE COURSE TEACHING

Buts Kateryna

Scientific supervisor: Candidate of Pedagogical Sciences, Docent Lupan I.V.

Volodymyr Vynnychenko Central Ukrainian State Pedagogical University, Kropyvnytsky, Ukraine

Abstract. *The article presents guidelines for teaching the "Basics of Cybersecurity" selective course. It is selected literature, which can be recommended to teachers to prepare for lessons and students for better learning material assimilation, links to free online cybersecurity courses, etc. To perform practical work it is recommended to use Packet Tracer designed to simulate network technologies. The article provides an example of practical work instruction for students and test tasks to test pupils' knowledge.*

Keywords: *selective course, cybersecurity, Packet Tracer.*

Постановка проблеми. Кіберзагрози існують повсюди, де застосовуються інформаційні технології, і, на жаль, далеко не всі, навіть дорослі люди, вміють їм протистояти. А для дітей небезпеки, які виникають в інформаційному середовищі, можуть стати фатальними: дуже часто ми чуємо, бачимо у новинах, що у соціальних мережах дітей доводять до самогубства, вербують в терористичні організації тощо. Отже, учень може в своїй діяльності стикнутися і зі спамом, і з вірусами, і з проникненням до комп’ютера сторонніх

осіб, і з багатьма іншими проблемами, на які потрібно вміти не тільки оперативно реагувати, але і наскільки можливо вміти запобігати їх появі.

У сучасному шкільному курсі інформатики на вивчення такої важливої теми, як безпечне використання комп'ютерних та мережевих технологій, відводиться замало годин. За цей час можливо лише ознайомитись з основними поняттями про шкідливе програмне забезпечення та засобами боротьби з ним. Тому більш глибоке занурення у зазначену тематику, а саме вивчення курсу за вибором (вибіркового модуля) "Основи кібербезпеки" [1] є і цікавим, і корисним, і актуальним. Основною метою курсу є формування в учнів фундаментальної теоретичної бази знань з основ кібербезпеки, умінь і навичок ефективного та безпечного використання сучасних інформаційно-комунікаційних технологій у своїй діяльності. Однак, оскільки курс з'явився у шкільній програмі відносно недавно, методична база для його вивчення учнями старших класів потребує доповнення та удосконалення.

Мета статті здійснити огляд літератури, інтернет-джерел та програмного забезпечення, які збагатять методичну базу курсу за вибором «Основи кібербезпеки» для вчителів і учнів, та навести приклади практичних робіт і тестових завдань з курсу.

Аналіз досліджень і публікацій. Серед джерел, що варто порекомендувати вчителям, які будуть викладати даний курс за вибором, слід в першу чергу назвати нормативні документи. Це Закон України «Про основні засади забезпечення кібербезпеки України» [2] та Навчальна програма курсу за вибором (вибіркового модулю) "Основи кібербезпеки" (авт. Войцеховський М.О., Гапонок Ю.М., Проценко Т.Г.) [1].

З введенням вибіркового курсу були видані підручник «Основи кібербезпеки та кібероборони» (Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега) [3] та методичні рекомендації «Кібербуллінг або агресія в інтернеті: способи розпізнання і захист дитини» [4].

Також на користь учителям будуть онлайн курси, зокрема курс «Кібербезпека і десять сфер її застосування» (англ. мовою) [5] та курс «Безпека

в кіберпросторі» (англ мовою) [6]. При проходженні першого з них слухачі розглянуть питання контролю доступу до інформації та програмного забезпечення, аварійного відновлення інформації та планування, криптографії та мережевої безпеки; отримають практичні поради щодо організації власної кібербезпеки. У другому з них акценти зроблені на тому, щоб навчити слухачів проектувати і будувати безпечні інформаційні системи, в центрі яких буде людина.

Учням додатково можна порекомендувати такі онлайн курси:

– «Основи інформаційної безпеки» [7], призначений донести до слухачів базові правила поводження з персональною інформацією в умовах зближення фізичного і віртуального світів, інформаційної війни.

– «Введення в кібербезпеку» (англ. мовою) [8], який допоможе учням зрозуміти принципи онлайн безпеки: як розпізнати кіберзагрози, якої шкоди вони можуть заподіяти, які кроки необхідно зробити, щоб зменшити ймовірність впливів шкідливого ПЗ. Під час курсу учнів познайомлять з різними типами шкідливих комп’ютерних програм, включаючи віруси і трояни, а також буде розглянуто такі поняття як мережева безпека, криптографія та навчать, як захистити особисте життя у віртуальному світі.

– «Cyber Aces Online Courses» (англ. мовою) [9], який допоможе учням не тільки отримати базові знання з питань інформаційної безпеки, але істотно зміцнити власний комп’ютерний захист.

Також корисними для учнів будуть інтернет-джерела, наприклад [10, 11].

Оскільки основою міцних знань завжди була практика, то варто подбати про програмне забезпечення для виконання практичних завдань з курсу. Одним з них може стати пакет Packet Tracer.

Виклад основного матеріалу. Packet Tracer [12] – це гнучкий програмний засіб для моделювання та візуалізації дії IP мереж. Він призначений для навчання мережних технологій та оцінювання отриманих учнями знань.

Packet Tracer дозволяє будувати власні моделі мереж (віртуальні мережі), отримувати доступ до графічного представлення цих мереж, анімувати дію мережі, додаючи свої пакети даних, задавати питання про дію мереж та отримувати відповіді, і, нарешті, коментувати і зберігати свої розробки.

Для побудови моделі мережі Packet Tracer дозволяє моделювати основні типи мережевого обладнання: комп'ютерів, серверів, Ethernet комутаторів, маршрутизаторів, тощо.

Для формування практичних навичок учнів програмою курсу передбачено виконання 11 практичних та 11 лабораторних робіт, кожна тривалістю не більше 20 хвилин.

Тематика практичних робіт стосується ідентифікації загроз; шифрування файлів і даних; перевірки цілісності файлів і даних; опрацьовування алгоритму процесу обробки цифрових сертифікатів для надійного з'єднання з веб-сайтами; визначення рівня захисту; вивчення засобів та методів захисту бездротових та мобільних пристроїв, серверів, мереж; співставленню та аналізу доменів кібербезпеки, тощо.

З використанням Packet Tracer можна виконати також практичні роботи з налаштування WEP/WPA2, PSK/WPA2 RADIUS; налаштування транспортного режиму VPN; налаштування тунельного режиму VPN; резервування маршрутизаторів та комутаторів; налаштування брандмауерів на сервері та списків контролю доступу на маршрутизаторі (Access Control List, ACL); налаштування бездротового маршрутизатора; завантаження даних з використаннням FTP; безпечного підключення до віддаленого сайту з використанням VPN та інш.

Тематика лабораторних робіт стосується створення кіберсвіту, комунікації у кіберсвіті, встановлення віртуальної машини, вивчення аутентифікації, авторизації та обліку, виявлення загроз і вразливостей, використання стеганографії, методів та засобів зламу паролю, використання цифрових підписів.

Приклад практичної роботи: ***Термінологія хешування. Порівняння даних за допомогою хешу.***

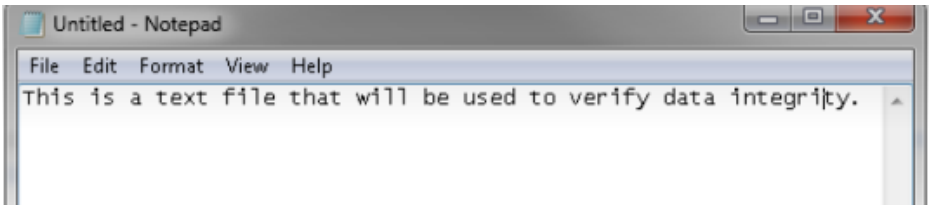
Мета: використати програму хешування для перевірки цілісності даних.

Завдання 1: *Створіть текстовий файл*

Інструкція:

a. Знайдіть на своєму комп'ютері програму Блокнот (Notepad) і відкрийте її.

b. Введіть текст у програмі.

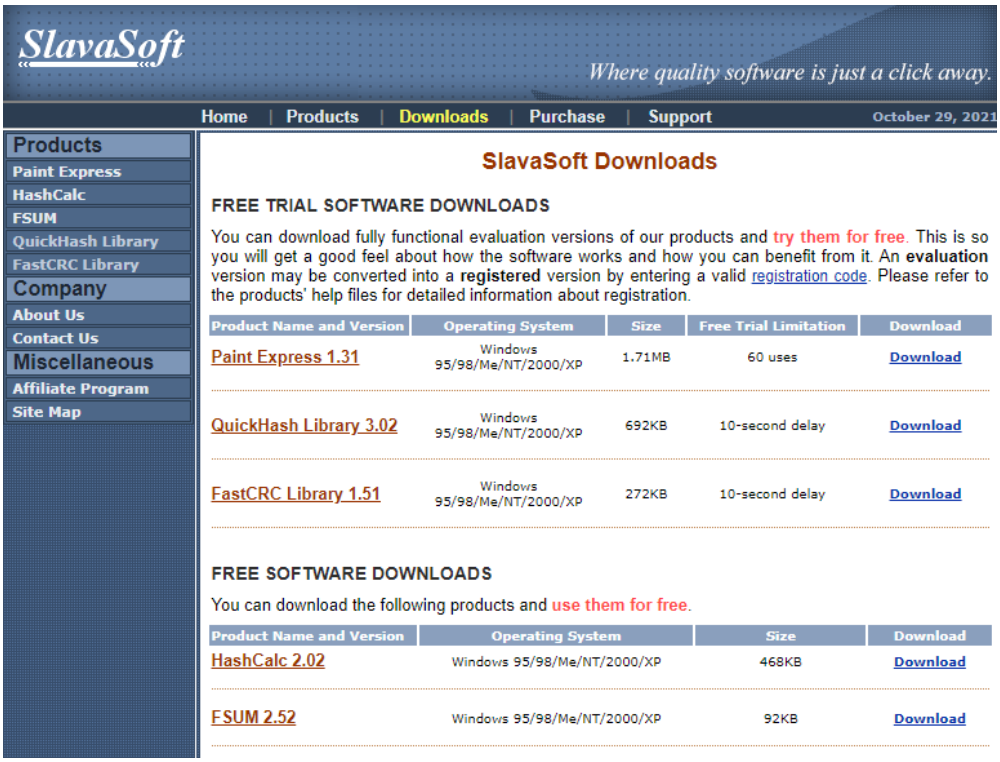


c. Виберіть ***Файл > Зберегти (File > Save)***

d. Введіть ***Hash*** *у поле* ***Ім'я файлу*** *і натисніть* ***Зберегти (Save).***

Завдання 2*. Встановіть HashCalc*

a. Відкрийте веб-браузер і перейдіть за посиланням http://www.slavasoft.com/download.htm.



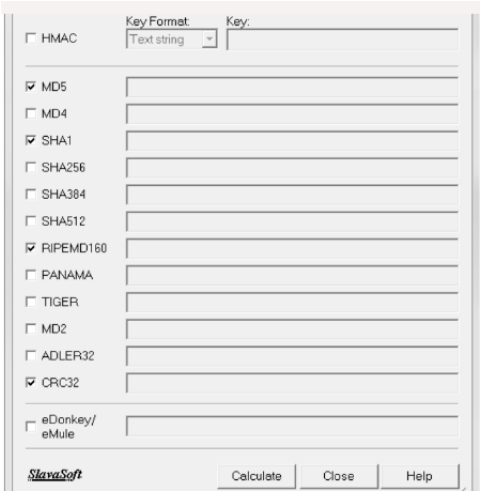
b. Натисніть ***Завантажити (Download)*** *у рядку* ***HashCalc.***

c. Відкрийте ***hashcalc.zip*** *файл та запустіть файл* ***setup.exe*** *всередині.*

d. Дотримуйтеся вказівок ***Майстра установки****, щоб встановити* ***HachCalc****.*

e. Натисніть кнопку ***Готово (Finish)*** *на останньому екрані та закрийте файл* ***README,*** *якщо він відкритий. Ви можете прочитати файл, якщо захочете.*

g. ***HashCalc*** *тепер встановлено та запущено.*



Завдання 3: *Обчисліть хеш файлу Hash.txt*

a. Вкажіть наступні елементи у HashCalc:

1) *Формат даних (Data Format):* ***Файл (File)***
2) *Дані: натисніть… Поруч із полем Дані (Data), перейдіть на* ***Робочий стіл (Desktop)*** *і виберіть файл* ***Hash.txt.***
3) *Зніміть прапорець* ***HMAC***
4) *Зніміть усі типи хешів, крім* ***MD5***

b. Натисніть кнопку ***Обчислити (Calculate)***

c. Яке значення поряд з ***MD5****?*

Завдання 4*: Внесіть зміни у файлі* ***Hash.txt.***

a. Перейдіть на ***Робочий стіл*** *і відкрийте файл* ***Hash.txt.***

b. Зробіть невелику зміну тексту, наприклад, видалення літери або додавання пробілу.

c. Натисніть ***Файл> Зберегти (File > Save)*** *та закрийте Блокнот.*

Завдання 5*: Обчисліть новий хеш файлу Hash.txt*

a. Знову натисніть кнопку ***Обчислити (Calculate****) в* ***HashCalc.***

Яке значення поряд із ***MD5?.***

Чи значення відрізняється від значення, що одержано на кроці 3?

b. Поставте прапорець біля усіх типів хеш-функцій.

c. Натисніть ***Обчислити (Calculate)***

d. Зверніть увагу, що багато типів хеш-функцій створюють хеш різної довжини. Чому?

Для перевірки знань учнів з курсу можна запропонувати, зокрема такі тестові завдання (курсивом виділено правильні відповіді):

1. Який з паролів є надійнішим?
    a) 23568294
    b) kate22
    c) The.Best.Password.Ever.256
2. Позначте правила безпечного користування Інтернетом:
    a) не змінюйте налаштування Інтернетом самостійно;
    b) не заходьте на підозрілі сайти, якщо про це попереджує захист комп'ютера;
    c) не заважайте іншим користувачам, не робіть протизаконних вчинків в Інтернеті;
    d) відповідайте на будь які інформаційні повідомлення;
    e) повідомляйте та оприлюднюйте без дозволу близьких особисту інформацію.
3. Що таке Фейк?
    a) сфальсифікована неправдива інформація
    b) викрадена інформація
    c) неактуальна інформація
    d) неточна інформація
4. Що є вагомою підставою перевірити коректність медійного повідомлення?
    a) повідомлення викликає сильні негативні чи позитивні емоції
    b) повідомлення базується на події річної давнини
    c) повідомлення надходить із джерела, про яке раніше не було відомо
    d) у повідомленні подана думка або позиція лише однієї сторони конфлікту
    e) усі відповіді правильні

5. В яких випадках може відбутись крадіжка особистих даних в Інтернеті?
    a) якщо перейти за незнайомим посиланням
    b) якщо переслати пароль електронною поштою
    c) якщо пересилати особисті дані через публічний Wi-Fi
    d) особисті дані неможливо вкрасти в Інтернеті
6. Як захистити свій комп’ютер від хакерських атак?
    a) використовувати антивірусні програми
    b) використовувати блокувальник реклами
    c) чистити історію відвідування веб-сайтів
    d) використовувати брандмауер
7. На що вказує літера «s» у префіксі «https»?
    a) на те, що тут з’єднання немає
    b) на те, що з’єднання є безпечним та зашифрованим
    c) на те, що з’єднання є безпечним
    d) на те, що з’єднання є зашифрованим
    e) на те, що з’єднання є небезпечним
    f) на те, що з’єднання є розшифрованим
8. Що таке двофакторна автентифікація?
    a) метод захисту, який передбачає подвійну процедуру входу в обліковий запис
    b) метод захисту від хакерів
    c) метод захисту від фішингу
9. Який вид загроз демонструє наступний приклад: в наслідок хакерського нападу на сайт інтернет магазину певний час користувачі не могли виконувати в ньому покупки, що завдало магазину чималого збитку?
    a) отримання доступу до секретних конфіденційних даних
    b) отримання доступу до керування роботою комп'ютерною інформаційною системою
    c) порушення або повне припинення роботи комп'ютерної інформаційної системи

10. Інформаційна безпека базується на таких принципах

a) достовірність;

b) захищеність;

c) конфіденційність;

d) доступність;

e) цілісність;

11. При отриманні перерахунку на твою картку від іншої людини достатньо повідомити….

a) CVV-2 код картки

b) номер картки свого друга

c) всі варіанти правильні

d) номер картки

e) термін дії картки

f) пароль картки

12. Ви намагаєтеся підключитися до Wi-Fi, який працює без пароля. Браузер каже, що підключення не захищене. Що робити?

a) знайти іншу точку доступу

b) знайти кнопку "Продовжити", вона захована, але десь є, я вже так робив

c) перезавантажити ноутбук/телефон

Висновки. Використання мережі Packet Tracer дозволить формувати практичні навички учнів під час вивчення основ кібербезпеки. Наведені у статті приклади інструкції до практичної роботи та тестових завдань, а також огляд додаткових онлайн-джерел будуть на користь вчителям у викладанні вибіркового курсу «Основи кібербезпеки» у закладах загальної середньої освіти.

Список використаної літератури

1. Навчальна програма курсу за вибором (вибіркового модулю) “Основи кібербезпеки” (авт. Войцеховський М.О., Гапонок Ю.М., Проценко Т.Г.) (Лист ІМЗО №22.1/12-Г-328 від 06.06.2019). – URL: https://drive.google.com/drive/u/0/folders/1MA0HxjYodlTrNpiXGmgXJcv

MYI1bseiA?fbclid=IwAR1unGvQeDSo4bSP6ivs81yxRmmw411qzxbIU8Zzx2W3lQWUmgMSL7ssfm0

2. Закон України «Про основні засади забезпечення кібербезпеки України» – URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса: ОНАЗ ім. О.С.Попова, 2019. – 320 с. – URL: https://metod.onat.edu.ua/download/686

4. Найдьонова Л. А. Кібербуллінг або агресія в інтернеті: способи розпізнання і захист дитини./ Найдьонова Л.А. //Методичні рекомендації. – К., 2014. – 80 с. – URL: http://mediaosvita.org.ua/wp-content/uploads/2017/11/KIBERBULLING-ABO-AGRESIYA-V-INTERNETI-SPOSOBY-ROZPIZNANNYA-I-ZAHYST-DYTYNY-.pdf

5. Онлайн курс «Кібербезпека і десять сфер її застосування» (англ. мовою). – URL: https://www.coursera.org/course/ksucybersec

6. Онлайн курс «Безпека в кіберпросторі» (англ. мовою). – URL: https://www.coursera.org/course/usablesec

7. Онлайн курс «Основи інформаційної безпеки». – URL: http://zillya.ua/prometheus

8. Онлайн курс «Введення в кібербезпеку» (англ мовою). – URL: https://www.futurelearn.com/courses/introduction-to-cyber-security

9. Онлайн курс «Cyber Aces Online Courses» (англ мовою). – URL: http://www.cyberaces.org/courses/

10. Як не налажати в Інтернеті: поради експерта з цифрової безпеки. – URL: https://life.pravda.com.ua/society/2019/07/26/237678/

11. 15 фактів про кібербезпеку, які змушують хвилюватися. – URL: https://yur-gazeta.com/golovna/15-faktiv-pro-kiberbezpeku-yaki-zmushuyut-hvilyuvatisya.html (24 липня 2020).

12. https://cisco-packet-tracer.informer.com