



КОНТРОЛЬНА РОБОТА: «БЕЗПЕКА ТА ЗАХИСТ ДАНИХ У ЦИФРОВОМУ СЕРЕДОВИЩІ»

8 КЛАС

I рівень. Початковий (Тестові завдання)

1. Спеціальна програма або апаратний пристрій, який контролює та фільтрує мережевий трафік за встановленими правилами безпеки, це:

- а) Браузер
- б) Антивірус
- в) Брандмауер (Firewall)
- г) Диспетчер завдань



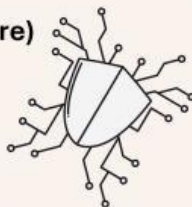
2. Який протокол передачі даних свідчить про безпечне та зашифроване з'єднання з вебсайтом у браузері?

- а) HTTP
- б) FTP
- в) IP
- г) HTTPS



3. Що з переліченого є прикладом шкідливого ПЗ, яке шифрує файли користувача та вимагає викуп?

- а) Спам
- б) Програма-вимагач (Ransomware)
- в) Фішинг
- г) Файрвол



4. Вид шахрайства, метою якого є отримання конфіденційних даних користувачів (паролів, номерів карток) через підроблені сайти чи листи, називається:

- а) Фішинг
- б) Спуфінг
- в) Фармінг
- г) Скейтбординг

5. Яке з дій порушує авторське право в Інтернеті?

- а) Цитування фрагмента статті із зазначенням джерела
- б) Використання зображення з ліцензією Creative Commons з вказуванням автора
- в) Посилання на офіційний сайт автора
- г) Публікація чужої електронної книги під своїм ім'ям

6. Яка з поданих комбінацій є НАЙБІЛЬШ захищеним паролем?

- а) 12345678
- б) kR#9!mX2\$vLP
- в) qwerty2026
- г) P@ssw0rd!



II рівень. Середній (З'єднання та чекбокси)

1. Установіть відповідність між поняттям та його визначенням:

1. Комп'ютерний вірус	☐	Програма, що примусово демонструє небажані рекламні банери.
2. Троянська програма	☐	Шкідливий код, що здатний саморозмножуватися та прикріплюватися до інших програм.
3. Шпигунське ПЗ	☐	Програма, що непомітно збирає інформацію про дії користувача та передає її третім особам.
4. Рекламне ПЗ	☐	Програма, що маскується під корисний софт, але виконує приховані деструктивні дії.

2. Оберіть ТРИ ознаки того, що електронний лист є фішинговим:

- ☐ ЛИСТ МІСТИТЬ ЛИШЕ ТЕКСТОВЕ ПРИВІТАННЯ ЗІ СВЯТОМ БЕЗ ПОСИЛАНЬ
- ☐ АДРЕСА ВІДПРАВНИКА МАЄ ДИВНІ СИМВОЛИ АБО ПОМИЛКИ В ДОМЕНІ (НАПРИКЛАД, SUPPORT@PAYPA1-SECURITY.COM)
- ☐ НАЗВУ САЙТУ В ПОСИЛАННІ НАПИСАНО ЧЕРЕЗ ПРОТОКОЛ HTTPS
- ☐ У ЛИСТІ Є ТЕРМІНОВА ВИМОГА ПЕРЕЙТИ ЗА ПОСИЛАННЯМ ПІД ЗАГРОЗОЮ БЛОКУВАННЯ АКАУНТА
- ☐ ДО ЛИСТА ДОДАНО ПІДОЗРІЛИЙ АРХІВ ЧИ ФАЙЛ ІЗ РОЗШИРЕННЯМ .EXE АБО .SCR
- ☐ ЛИСТ НАДІЙШОВ ВІД ОФІЦІЙНОЇ СЛУЖБИ ПІДТРИМКИ З ВАШИМ ПЕРСОНАЛЬНИМ ЗВЕРНЕННЯМ ПО ІМЕНІ

III рівень. Достатній (Заповнення пропусків та відкриті запитання)

Доповніть речення необхідними термінами (впишіть відповідь у поле):

- а) Для захисту акаунтів рекомендується вмикати _____ автентифікацію, яка вимагає підтвердження входу через додатковий пристрій або СМС.
- б) Резервне копіювання даних за правилом «3-2-1» передбачає збереження як мінімум ____ копій даних на ____ різних носіях, з яких ____ копія зберігається поза домом/офісом.



IV рівень. Високий (Ситуаційний аналіз з автоперевіркою)

Проаналізуйте ситуацію та виконайте завдання:

Учень 8 класу Олексій шукав у мережі безкоштовну зламану версію гри. На одному з форумів знайшов завантаження .zip-архіву. Антивірус видав попередження про загрозу, але на сторінці написано: «Вимкніть антивірус, це помилкове спрацювання». Олексій вимкнув захист і запустив setup.exe. Через годину всі його файли змінили розширення на .locked, а на екрані з'явилася вимога переказати криптовалюту.

А) ВКАЖІТЬ ВИД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВІД ЯКОГО ПОСТРАЖДАВ ПК:

- ☐ ФІШИНГ
- ☐ ПРОГРАМА-ВИМАГАЧ (RANSOMWARE)
- ☐ РЕКЛАМНЕ ПЗ (ADWARE)

Б) Оберіть УСІ ТРИ помилки, яких припустився Олексій:

- [] Завантаження файлів із неперевіреного піратського джерела
- [] Вимкнення антивірусного захисту
- [] Запуск невідомого виконуваного файлу .exe
- [] Використання браузера для пошуку інформації
- [] Раптове відключення комп'ютера від мережі Wi-Fi

В) Яку ПЕРШУ та найважливішу дію має виконати Олексій одразу після виявлення загрози, щоб зупинити поширення хробака?

- а) Оплатити викуп у криптовалюті
- б) Негайно відключити ПК від мережі Інтернет (Wi-Fi/кабель)
- в) Оновити операційну систему
- г) Перезавантажити комп'ютер кілька разів

