РОЗВИТОК КІБЕРГРАМОТНОСТІ СУЧАСНОГО ЗДОБУВАЧА ОСВІТИ

Тетяна БРОШЕВАН

Сучасний кіберпростір дає великі можливості для користувачів, ставить нові вимоги до їхнього рівня підготовки, але водночас несе загрози, які впливають на благополуччя (фізичне, психологічне, матеріальне та соціальне) підлітка [4, с.8].

Інформаційно-психологічна безпека особи та суспільства в цілому є складовою частиною кібербезпеки України. Постає проблема в її створенні та впливу фактів на індивідуальну психіку особистості. Володіння певною інформацією, яку можна застосовувати для навчання та щоденного життя, забезпечує високий рівень кіберкультури [2, с.20]. Тому сучасний здобувач освіти повинен знати основні особливості, способи поширення та відомі приклади кіберзагроз, а також інструменти для захисту домашньої мережі.

Розглянемо інтернет-загрози, які спрямовані на домашніх користувачів:

- ✓ бекдор – шкідлива програма для отримання доступу до робочої станції шляхом обходу аутентифікації, загроза надає зловмисникам можливість несанкціоновано та дистанційно управляти інфікованим пристроєм жертви;
- ✓ прихований майнінг – шкідливі програми для прихованого майнінгу належать до категорії шкідливого коду, призначеного для використання обчислювальної потужності пристрою користувача з метою видобутку криптовалюти, при цьому жертви не дають згоду і навіть не підозрюють про таку діяльність;
- ✓ кетфішинг – це вид онлайн-шахрайства, коли людина або так званий кетфішер, створює фальшивий профіль у соціальній мережі чи на сайті знайомств з метою шахрайства чи обману;
- ✓ вішинг – вид телефонного шахрайства, під час якого зловмисники викрадають банківські дані або виманюють особисту інформацію, яка в подальшому може бути використана для доступу до ваших банківських рахунків;
- ✓ плечовий серфінг – спосіб викрадення конфіденційних даних шляхом спостереження за повідомленнями, які відображаються на смартфоні або ноутбуці жертви; зазвичай зловмисники використовують цей метод у публічних місцях, таких як транспорт чи кафе;
- ✓ рекламне ПЗ – це різні спливаючі рекламні оголошення, які відображаються на комп’ютері чи мобільному пристрої користувача; рекламне ПЗ може використовуватися у зловмисних цілях, наприклад, для завантаження вірусів та шпигунських програм на пристрій, або для отримання доступу до вашого браузера;
- ✓ мережевий черв’як – вид шкідливого програмного забезпечення, який здатний самостійно поширюватися в локальній або інтернет-мережі шляхом створення власних копій;

✓ програми-вимагачі – це шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв; за певну плату оператори шкідливого коду обіцяють відновити доступ до інфікованої машини або даних [1].

Із кожним роком складність кіберзагроз лише зростає, тому, навіть у досвідчених користувачів може виникати плутанина щодо їх особливостей. І саме педагог може грамотно донести до сучасних здобувачів освіти знання, уміння та навички кіберграмотності шляхом проведення семінарів, марафонів та тренінгів. Поглиблювати отримані знання можна за допомогою інформаційних сайтів (https://cutt.ly/h9LPxlK; https://cutt.ly/19LPDfA, https://v.gd/70Jlje); практичних завдань, які надають навчальні курси (https://cutt.ly/K9LLRAd, https://nt.ua/tag/it-security); конференцій (https://v.gd/rk3wM4), які знайомлять з ефективними практиками з розвитку кіберграмотності та навчальних посібників, де кібербезпека розкривається як інноваційна система віртуального сучасного інформаційного простору [3, с.50].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Енциклопедія Інтернет-загроз. *Eset* : вебсайт. URL: https://v.gd/aobE2B (дата звернення: 01.02.2023).

2. Кочарян А. Б., Гущина Н. І. Виховання культури користувача Інтернету. Безпека у всесвітній мережі : навч. посіб. Київ, 2011. 100 с.

3. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Видавничий дім «Кондор», 2019. 272 с.

4. Черних О.О. Онлайк : навч. посіб. Київ, BAITE, 2020. 108 с. URL: https://v.gd/TLJQ5q.