О. ЧЕРНИХ

КІБЕРБЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ В УМОВАХ ВОЄННОГО СТАНУ

На сьогоднішній день учителі, учні, їхні батьки активно використовують в освітньому процес мережу Інтернет як потужне джерело інформаційних ресурсів. Враховуючі, що динамічність розповсюдження інформації мережою Інтернет дуже висока, слід постійно контролювати загрози, які виникають повсякчас, а саме дезінформація, маніпуляція, фейкові новини, вірусні атаки, шахрайство, пропаганда терористичної та екстремістської діяльності. Особливо гостро це стало відчуватися під час карантину та військового стану.

З початком війни Україна стала ціллю чисельних кібератак, які охопили як державні установи, організації, так і звичайних громадян. Наразі створення безпечного освітнього середовища, збереження персональних даних учасників освітнього процесу, формування інформаційно-цифрової компетентності, дотри-мання правил захищеного користування інтернет-ресурсами в кіберпросторі є важливими показниками якості освіти.

Під кіберпростором слід розуміти середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціо-нування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «Кібербезпека – захищеність життєвоважливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1].

Оскільки об'єм даних збільшується й усе більше користувачів працюють і спілкуються, кіберзло-чинці розробляють складні методи, для отримання доступу до ресурсів, викрадення даних, саботажу роботи освітніх закладів або вимагання грошей. Щороку кількість атак збільшується, а зловмисники розробляють нові методи для уникнення виявлення.

Нині розмаїття небезпек і загроз зростає постійно. Найбільшу загрозу для здобувачів освіти мають приховані активні небезпеки, серед яких – мережні загрози. Активне використання мереж, особливо дітьми підліткового віку, супровод-жується збільшенням різних видів загроз. Найбільш активні приховані загрози, що походять із комп'ютерної мережі, можуть бути представлені наступною класифікацією:

- вірусні атаки;
- кіберзлочинність (спамерство, кардінг, фішинг, ботнети тощо);
- загрози від мережевого серфінгу (кібербулінг, «дорослий» контент, незаконний вміст, насильство в режимі онлайн, розголошення приватної інформації, платні послуги тощо).

Загрози, що надходять з мереж, можна розділити на наступні типи: активні та пасивні, відкриті та приховані, поточні та відкладені.

Зміщення цілей кіберзлочинності з технічних (інформаційних) об'єктів на людину спричинило появу соціальної інженерії як методів і технологій отримання необхідного доступу до інформації, заснованих на особливостях психології людей, зокрема, маніпуляція людськими страхами, зацікавленістю або довірою. Основними типами соціальної інженерії можна вважати наступні:

Претекстінг – це набір дій, відпрацьованих за певним, заздалегідь складеним сценарієм, у результаті якого жертва може видати будь-яку інформацію або вчинити певну дію. Для використання цієї техніки зловмисник спочатку збирає певні дані про жертву (ім'я, місце навчання та проживання; дату народження; дані про батьків), використовуючи реальні запити з іменами щодо оточення жертви, а після того, як увійде в довіру, отримує необхідну йому інформацію або дії.

Фішинг – техніка інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів авторизаційних даних різних систем. Основним видом фішингових атак є підроблений лист, відправлений жертві електронною поштою, який виглядає як офіційний. У листі міститься форма для введення персональних даних (пінкодів, логіна і пароля тощо) або посилання на web-сторінку, де розташовується така форма.

Троянський кінь – це техніка ґрунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти, як додаток, до якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або зміни інформації зловмисником.

Quiproquo (послуга за послугу) – ця техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці та необхідність їх усунення. У процесі «вирішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.

Дорожнє яблуко – цей метод є адаптацією троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій у загальнодоступних місцях. Для того, щоб виник інтерес до даного носія, зловмисник може нанести на носій логотип відомої популярної компанії.

Байтинг – метод, схожий на попередній, а також фішинг і троянський кінь, проте відрізняється тим, що байтер може запропонувати користувачеві реальну безкоштовну послугу (музику, фільм тощо) в обмін на конфіденційну (приватну) інформацію.

Зворотня соціальна інженерія – даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернутися до зловмисника за «допомогою». Наприклад, створити оборотні неполадки в ґаджеті жертви з попереднім інформуванням щодо служби «підтримки». Користувач у такому випадку зателефонує або зв'яжеться по електронній пошті зі зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.

Дружні листи – надсилання електронних листів, у яких особу повідомляють про отримання спадщини, призів, бонусів чи дружнього переказу грошей.

Вішинг – голосова версія фішингу. Як правило, дії пов'язані з телефонним шахрайством, метою якого є отримання реквізитів банківських карток або будь -якої іншої конфіденційної інформації або змушення жертви перевести гроші на банківський рахунок зловмисника.

Контакти – розсилання спаму від імені знайомих. Тобто, заволодівши чиїмось акаунтом, чи то в соціальній мережі, чи в електронній пошті, зловмисники можуть спробувати надсилати від його імені посилання. Психологічна дія, що побудована на схильності людини довіряти своїм знайомим і не дуже вагатися, коли отримують від них пропозицію відкрити посилання.

Щоб не стати жертвою кібератак, необхідно дотримуватися певних рекомендацій під час роботи у мережі Інтернет усім учасникам освітнього процесу.

Для безпечної роботи в кіберпросторі педагогам можна надати наступні рекомендації:

1. Не користуйтесь забороненим и поштовими сервісами (Mail.ru, Yandex) та соціальним мережами (Vkontakte, Одноклассники).

2. Використовуйте антивірусні програми.

3. Користуйтесь надійними паролями, періодично змінюйте їх.

4. Оновлюйте програмне забезпечення.

5. Залучайте батьків до профілактичної роботи з дітьми, проводьте бесіди для батьків щодо проблем кіберзагроз та засобів їх упередження.

6. Використовуйте систему превентивних заходів для вирішення проблеми кіберзахисту в шкільному середовищі.

7. Використовувати активні та інтерактивні форми роботи, такі як: перегляд кінострічок, роликів на тему кібербезпеки, обговорення переглянутого, моделювання ситуацій, які схожі на ті, які реально відбуваються, та пошуки виходу з них.

8. Проводити діагностику стану психологічного клімату класу, виявляти дітей, які зазнавали

віртуального цькування або можуть піддаватися кібербулінгу.

Батькам потрібно починати говорити з дітьми про кібербезпеку з того моменту, коли ви даєте дитині в руки телефон, планшет, ноутбук. Вік дитини може бути різним: одні діти починають користуватися сучасними гаджетами в 3-4 роки, інші перед початком навчання в школі. Особливу увагу слід звертати на дітей підліткового віку, саме вони є особливо уразливою категорією для кіберзлочинців.

Батькам слід дотримуватися наступних рекомендацій:

1. Інформуйте дитину про ризики, які можуть виникнути під час користуванням Інтернетом.
2. Цікавтеся віртуальним життям своєї дитини, спілкуйтеся з нею про її інтернет-враження.
3. Поясніть дитині, що необхідно радитися з вами перед тим, як здійснювати покупки через мережу Інтернет.
4. Ознайомлюйтеся з сайтами, які відвідує ваша дитина.
5. Привчайте дитину з повагою і тактовністю ставитися до інших користувачів мережі Інтернет.
6. Навчайте дитину розповідати про свої знайомства в соціальних мережах.
7. Користуйтесь програмами батьківського контролю, використовуйте інформаційні фільтри.
8. Допоможіть дитині створити безпечний пароль і поясніть, що це є необхідним для того, щоб захистити особисту інформацію.
9. Поясніть дитині що таке спам, вірус, які ризики пов'язані з цим.

Дуже важливо навчати дітей основним правилам безпечного користування гаджетами. У своєму віці вони ще не знають, як безпечно користуватися мережею Інтернет. Тому діти мають розуміти, як себе захистити. У цьому їм повинні постійно і систематично допомагати як батьки, так і вчителі. Учням слід дотримуватися наступних рекомендацій:

1. Завжди консультуватися з батьками про незрозумілі для вас речі в Інтернеті.
2. Не розповідайте інформацію про себе, ваших близьких і знайомих незнайомцям.
3. Не погоджуйтеся на зустрічі з незнайомими вам людьми без дозволу батьків, вчителів.
4. Використовуйте відеозв'язок лише з тими людьми яких ви знаєте особисто.
5. Якщо отримуєте листа чи повідомлення образливого змісту обов'язково повідомте батьків, вчителів.
6. Якщо отримали листа чи повідомлення з незнайомої адреси, номеру телефону не відкривайте його. Повідомте про це батькам та або вчителям, щоб уникнути вірусної атаки.
7. Обдумано публікуйте фото чи відео в Інтернеті, їх може подивитися будь-хто.
8. Враховуйте, що віртуальні знайомі можуть бути не тими, за кого себе видають.
9. Не повідомляйте стороннім людям свої паролі, користуйтеся лише надійними паролями та логінами.
10. Ніколи не робіть того, що може коштувати вашій родині фінансової шкоди.
11. Не користуйтесь забороненими поштовими сервісами (Mail.ru, Yandex) та соціальними мережами (Vkontakte, Одноклассники).

Постійно з'являються нові рішення у відповідь на кібератаки, весь час зростає поінформованість учасників освітнього процесу. Саме пильність і систематичне використання рекомендацій для педагогів, батьків і учнів може бути потужним ресурсом для виявлення та пом'якшення кіберзагроз, що виникають.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про кібернетичну безпеку України» // Відомості Верховної Ради України, 2017. № 45. ст.403.
2. Довгань О.Д., Тарасюк А.В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. Інформація і право. 2018. № 3(26). С. 94-103.
3. Довгань О.Д. Щодо деяких правових аспектів культури кібербезпеки: зб. тез наукових доповідей IX Всеукраїнської науково-практичної конференції ["Актуальні проблеми управління інформаційною безпекою держави"]. К., 2018. С. 60-62.
4. Доценко С. О., Прокопенко А. І. Цифрова грамотність майбутніх учителів у контексті STEM-освіти. Психолого-педагогічні проблеми вищої і середньої освіти в умовах сучасних викликів : теорія і практика : матеріали III Міжнародної науково-практичної конференції (Харків, 10 квітня 2018 р.). Харк. нац. пед. ун-т імені Г. С. Сковороди. Харків : «Стиль-Издат», 2018. 476 с., С. 298-300.
5. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С.В.Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.