УДК 004.738.5:004.056

ІНТЕРНЕТ БЕЗПЕКА: ЯК ЗАХИСТИТИ СВОЇ ДАННІ ТА СВОЄ ЖИТТЯ В ОНЛАЙН ПРОСТОРІ

Збітнєв Д.С.
Науковий керівник – к.т.н., доц. Пронюк Г.В.
Харківський національний університет радіоелектроніки,
61166, Харків, просп. Науки,14, каф. Охорона праці, тел. (057) 702-13-60
тел. +38(095) 664-25-74

Today, the number of Internet users is constantly growing. Especially for young people the Internet has become an information environment without which they cannot imagine life. The paper considers the key aspects that ensure the safety of the user on the Internet.

Безпека людини у техносфері вивчає різні за походженням та типом дії небезпеки виробничого та побутового середовища. Однак в останні десятиліття наша виробнича і побутова діяльність змінилася. Ми живемо в час швидкості, час стрімкої передачі інформації. Крім того, ковід пандемія і її наслідки кардинально змінили виробничі процеси: люди все більше працюють віддалено, використовуючи кожен день групові чати, платформи обміну даними і ін. Збиток від кіберзлочинності в 2022р. склав 8,4 трлн доларів та за даними експертів досягне 20 трлн доларів до 2026 р.

У зв'язку з цим особливого значення набувають питання, пов'язані з кібергігієною. Поняття кібергігієни набагато ширше, ніж тільки захист персональних даних, і включає в себе вивчення впливу на людину дигіталізації, розробку нормативів і заходів як з інформаційного захисту людини, так і з оздоровлення інформаційного середовища. Можна сформулювати набір елементарних правил інформаційної безпеки, які мають постійно актуалізуватися в міру розвитку технологій:

1. Не надавайте нікому свої дані. У мережі є багато спокусливих пропозицій: «Ваш номер виграв в лотереї!», при цьому вас можуть запитати PIN-код банковської картки, особисті данні і т.п. Найкраще припинити спілкування, навіть якщо пропозиція дуже спокуслива.

2. Перевіряйте інформацію. Не поширюйте новини із занадто великими заголовками, можливо, це фейк. Запитайте обізнаного друга чи перевірте інформацію на інших сайтах. Якщо вас просять пожертвувати гроші на операцію або поширити щось подібне, також важливо перевірити інформацію. Пам’ятайте, що шахраї часто видають себе за благодійників.

3. Захист паролем. Ви користуєтеся Instagram щодня чи робите покупки в інтернет-магазинах? І напевно, ви всюди використовуєте той самий пароль. Змінюйте пароль кожні 2-3 місяці та використовуй різні складні паролі. Зберігайте паролі в надійному місці, а ще краще - запам'ятовуйте їх, а не записуйте.

4. Використовуйте багатофакторну аутентифікацію, яка додає нові рівні безпеки з використанням біометричних даних (розпізнавання обличчя, відбитків пальців). Ви маєте пароль у Google, Facebook, Instagram, а вони пропонують двофакторну аутентифікацію? Погоджуйтеся! Вам зателефонують або надішлють код, тож ваші дані в соцмережах будуть у ще більшій безпеці.

5. Використовуйте офіційні додатки, тоді ви можете бути впевнені, що ваш комп'ютер чи смартфон не буде заражений жодними вірусами.

6. Не підключайтеся до публічної мережі Wi-Fi або використовуйте для цього VPN (не безкоштовний). Проте краще користуватися мобільною мережею.

7. Не натискайте на посилання, які вам незнайомі. Навіть якщо вони переслані вам від друзів. Часто зловмисникам достатньо, щоб ви натиснули на це посилання, і вони отримають доступ до вашого профілю і ваших особистих даних.

8. Не додавайте незнайомих людей до списку своїх контактів в соціальних мережах, бо вони можуть надсилати повідомлення іншим людям в статусі вашого друга.

9. Переконайся, що сайт, який ви використовуєте, має https, а не http. HTTPS – це розширення протоколу HTTP для підтримки шифрування з метою підвищення безпеки, HTTP "стає" HTTPS за наявності SSL-сертифікату. Це ознака того, що це не шахраї та користувач сміливо може проводити сплату на цьому сайті.

10. У свою чергу не довіряйте повідомленням від незнайомих акаунтів чи номерів, які представляються вашими друзями або знайомими ваших друзів. Спробуйте погуглити своє ім'я та подивіться, скільки особистої інформації про вас є в Інтернеті: де і з ким ви відпочивали, вчилися, як зовуть ваших родичів, і навіть як звали вашу домашню тварину. Усі ці дані можуть бути використані проти вас.

Дотримання кібергігієни сьогодні стає питанням особистої безпеки. Зрештою, кількість шахрайства в Інтернеті, факт втручання в особистий простір, поширення неправдивої інформації та інше зараз набуває ознак епідемії. Тому гігієна Інтернету стала не лише гарячою темою суспільних дискусій, а й предметом дослідження та формулювання правил його використання на державному рівні.

Список використаних джерел:

1. Безпека в інтернеті: найпростіші правила захисту даних. [Електронний ресурс]. – Режим доступу: https://www.bbc.com/ukrainian/blogs-51444737

2. Як захистити свої дані в інтернеті. [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua/news/yak-zakhistiti-svoi-dani-v-interneti