



Безпека життя та охорона здоров'я - головні завдання сучасного суспільства

**Збірник доповідей студентської
регіональної наукової конференції**

Психологічна безпека особистості у кіберпросторі

Бульчик Тамара, студентка IV курсу факультету психології та соціології СНУ ім. Лесі Українки, голова НТАіС факультету психології та соціології

Науковий керівник: Мигдасюк Л.І., кандидат психологічних наук

Ні для кого не секрет, що життя сучасної людини плавно та впевнено «перемістилося» у простір Інтернету, соціальних мереж, меседжерів, онлайн знайомств, зустрічей, покупок, платежів та інших життєво необхідних справ. Говорити про позитивні та негативні аспекти таких змін можна годинами, проте важливо сказати про захист особистості, її матеріального, психічного та навіть фізичного стану у системі модернізованого суспільства.

Поряд з розвитком та збагаченням Інтернет-соціуму є ті хто прагне легкої наживи, тобто шахраї, гопники, бандити, злодії та лиходії, сфера кіберпростору, Інтернету, не стала для них чимось недосяжним.

Практично немає користувача Інтернету, який хоча б раз не ставав об'єктом кібератаки. У цьому аніскільки не сумніваються і фахівці в області кібербезпеки, відзначаючи, що людей і компанії зазвичай можна розділити на два види: таких, які знають, що стали жертвою подібних дій, і тих, що цього не зрозуміли. Від атак кібертерористів ніхто не застрахований.

Це зумовлює важливість та актуальність розгляду питання психологічної безпеки у кіберпросторі, чому виникають кіберзлочини та як не стати жертвою такого сучасного злочинця.

Перш за все, варто з'ясувати значення дефініцій «психологічна безпека», «кібернетична безпека», «інформаційно-психологічна безпека особистості».

• **Кібернетична безпека** – це захищеність належного функціонування інформаційно-телекомунікаційних систем від небажаного для користувачів порушення процесу обробки даних і результатів такої обробки (кіберзагроз).

• **Психологічна безпека** - стан суспільної свідомості, при якому суспільство та особистість сприймають існуючий стан дійсності й життя як адекватний та надійний, оскільки складаються реальні можливості для задоволення природних і

соціальних потреб громадян сьогодні та існує впевненість у майбутньому.

- **Інформаційно-психологічна безпека особистості** – це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо.

Також, важливим для нас поняттям є розуміння того, що включає в себе кіберпростір:

- **Кіберпростір** – це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережні системи та пов'язані з ними фізичні інфраструктури.

- **Кіберзагроза** - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам особистості у кіберпросторі.

Відповідно до цього давайте з'ясуємо, у чому полягає безпечна робота у кіберпросторі:

- Отримання своєчасного доступу до необхідних даних.
- Дотримання конфіденційності певних даних.
- Забезпечення вірогідності даних.
- Захист від дезінформації, недостовірних і перекручених даних.

- Захист певного виду даних від незаконного тиражування.
- Встановлення відповідальності за порушення законних прав суб'єктів відносин у кіберпросторі.

Кіберзлочини, на відміну від злочинів у реальному житті, завжди умисні та передбачають такі мотиви:

- Користь (86%)
- Помсту (6%)
- Потребу у самоствердженні (3%)
- Хуліганські мотиви (2%)
- Кар'єризм (1%)
- Інша особистісна нематеріальна зацікавленість (2%)

Для уникнення кіберзлочинів варто застосувати наступну тріаду механізмів:

- Фізичні заходи – хто може мати доступ до приміщення, де знаходяться документи;

- Технологічний контроль – обладнання та програмне забезпечення;

• Механізми адміністративного контролю – просвіта та політика.

Важливо не ігнорувати гігієну свого перебування у мережі Інтернет та своїх гаджетів загалом. Науковці рекомендують застосовувати наступні поради щодо кращого захисту своїх даних:

• Постійне вдосконалення та інтерес до новинок у сфері ІТ, правил безпеки і соціальної інженерії (фішингу);

• Паролі не повинні бути легкими, адже тоді їх можна буде легко підібрати. («Ніяких admin-admin, 12345, qwerty, імен мамі, тата, собаки»). Краще, щоб доступ взагалі проходив через двофакторну автентифікацію, тобто пароль плюс пін-код, який надходитиме на телефон у момент підключення;

• Встаючи з робочого місця, заблокуйте комп'ютер (lock-out). Це має увійти у звичку;

• Пересилаючи конфіденційну інформацію, архівуйте її так, щоб ключ від архіву був лише у вас і вашого контрагента;

• Завжди оновлюйте свій антивірус та інші життєвоважливі програми;

• Копіюйте важливі дані на окремі оффлайнові носії (бекап даних) і відновлюйте інформацію при необхідності.

Виконуйте ці прості правила, і шанси, що вас хакнуть та нанесуть шкоду як вашим персональним даним, так і вашому психічному благополуччю будуть в рази менше!

Список використаних джерел:

1. Брито Д. Кибератаки: угроза преувеличена для контроля Интерне та [Электронный ресурс] / Джерри Брито, Тэйт Уоткинс. – 2009. – Режим доступа :<http://papinaziat.ru/?tag=кибербезопасности>.

2. Інформаційна та кібербезпека: соціотехнічний аспект. Бурячок В. Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Бурячок В. Л., Толубко В.Б., Хорошко В. О., Толюпа С.В.. «Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]». – Київ - 2015.

3. Шеломенцев В. П. Основні напрями і суб'єкти забезпечення кібернетичної безпеки Ураїни /В. П. Шеломенцев // збірник праць Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2013. №1 (29), - Київ – С. 348 – 355.