DOI https://doi.org/10.36059/978-966-397-358-6-40

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ВОЄННОГО СТАНУ

Сьомак Сергій Васильович
здобувач освітньо-наукового рівня (доктор філософії),
Науково-дослідний інститут публічного права
м. Київ, Україна

Слюсарчук Павло Андрійович
здобувач освітньо-наукового рівня (доктор філософії),
Науково-дослідний інститут публічного права
м. Київ, Україна

Із початком воєнних дій на території нашої країни, сучасне суспільство України стало все більше часу проводити у месенджерах та в інтернеті, з метою пошуку новин, які яктуальні на даний момент. Тому слід пам'ятати, що інформаційна війна є також небезпечною. Наші гаджети, стають реальною загрозою у сучасних реаліях. Як цьому протидіяти?

«Однак не забувайте правила безпечного листування як у соцмережах, так і в месенджерах», – попереджають у Центрі протидії дезінформації.

Що не варто надсилати:

– Геолокацію. Власне місце знаходження, військ ЗСУ і техніки. Ворог може скористатись цими даними для заподіяння шкоди.
– Дані своїх банківських карток.
– Не пересилати свій номер телефону, паспортні дані, паролі

Таким чином ворог може взламати ваші облікові записи і вкрасти ваші дані і заподіяти вам неабиякої шкоди

Кібергігієна – це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації.

Щоб захистити дані потрібно дотримуватись або виконати такі умови:

1. Перевірка безпеки активних акаунтів.
2. Аналіз програм. Перевірити програми на наявність вірусів
3. Надійний пароль. Щоб забезпечити свої облікові записи якісною безпекою потрібно встановити надійний пароль. Важливо створити

складну комбінацію, яка містить не менше 12 символів, великі та малі літери, цифри та символи.

4. Додатковий рівень захисту. Для покращення безпеки облікових записів використовуйте двофакторну аутентифікацію, яка передбачає підтвердження особистості під час входу в певний акаунт. Двофакторна аутентифікація-це додатковий рівень захисту облікового запису.

5. Регулярне резервне копіювання. Важливим кроком для захисту ваших даних є резервне копіювання. Це допоможе уникнути втрати даних шкідливим програмним забезпеченням

6. Хмарні сховища. Новітній вид мережевих послуг, які дозволяють інформаційними засобами віртуального середовища розширити програмно-технічні ресурси комп'ютерного пристрою користувача.

Для ефективного забезпечення конфіденційності та надійності використання хмарних систем необхідно, перш за все, подбати про безпеку всіх учасників складових процесу передавання, зберігання інформації, починаючи від постачальника «хмарного» рішення, користувача та зв'язків, які їх пов'язують. Якщо говорити про поставлені завдання перед провайдером, то вони полягають у тому, щоб забезпечити недоторканність інформаційних даних третіми особами, як у фізичному, так і програмному сенсі.

Література:

1. Українцям нагадали про безпечне листування у соцмережах в умовах війни: чого не варто писати. *Новини Чернівці: Інформаційний портал «Молодий буковинець»*. URL: https://molbuk.ua/news/252735-ukrainciam-nagadaly-pro-bezpechne-lystuvannia-u-socmerezhakh-v-umovakh-viiny-chogo-ne-varto-pysaty.html

2. Кібергігієна – основні умови для захисту даних. рекомендації ESET. *ESET – офіційний сайт. Антивірусні програми Ісет в Україні. | ESET*. URL: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya