УДК 159.923.2:659.3-049.5(045)

Оксана Купіна

аспірантка спеціальності 011 Освітні, педагогічні науки

Комунального закладу «Харківська гуманітарно-педагогічна академія» Харківської обласної ради

ІНФОРМАЦІЙНА БЕЗПЕКА ОСОБИСТОСТІ ТА ІНФОРМАЦІЙНІ НЕБЕЗПЕКИ СУЧАСНОСТІ

У статті розглянуто ключові аспекти актуальності дослідження інформаційної безпеки, структуру основних категорій та підкатегорій, які пов'язані з інформаційною безпекою, найпоширеніші сучасні види інформаційних небезпек. Наведено комплекс заходів, що, на думку автора, сприятимуть підвищенню рівня інформаційної безпеки. Інформаційна безпека особистості розуміється як готовність і здатність індивіда зберігати недоторканість та сталість своїх поглядів, системи цінностей і ціннісних орієнтацій, переконань і стратегій у житті в умовах впливу інформаційної пропаганди й психологічних маніпуляцій, які впливають на свідомість та психіку.

***Ключові слова**: інформаційна безпека, інформаційні небезпеки, інформаційний вкид, ІПСО, фейк, цифровізація.*

The article discusses the key aspects of the relevance of information security research, the structure of the main categories and subcategories related to information security, and the most common modern types of information threats. The author provides a set of measures that will contribute to improving the level of information security. Personal information security is understood as the readiness and ability of an individual to maintain the integrity and stability of his or her views, system of values and value

orientations, beliefs, and strategies in life under the influence of information propaganda and psychological manipulations that affect the mind and psyche.

***Keywords**: information security, information hazards, information stuffing, IPSO, fake, digitalization.*

Дослідження проблеми інформаційної безпеки, зокрема, особистості є актуальним та нагальним завданням сучасності, особливо коли суспільство перебуває в процесі інформатизації та глибокого цифрового перетворення. Низка ключових аспектів підкреслюють актуальність дослідження цього питання.

Зростання кількості цифрових загроз. Бачимо, що сучасний світ відкриває багато можливостей для спілкування, навчання та розваг через Інтернет та інші технології, однак це також призводить до збільшення кількості кіберзагроз, таких як хакерські та фішингові атаки, крадіжка особистої інформації тощо.

Проблема конфіденційності. Використання онлайн-платформ, соціальних мереж та електронної пошти робить особисту інформацію більш доступною та призводить до порушення конфіденційності та незаконного використання приватних даних.

Цифровий слід. Варто зауважити, що кожна дія в інтернеті може залишити цифровий слід: дані про наші дії, звички та інтереси використовуються для створення персоналізованих рекламних пропозицій, а також можуть бути використані для впливу на наші дії та думки.

Освіта та свідомість. Дослідження показують незадовільний рівень знань щодо базових понять інформаційної безпеки, розуміння загроз та вміння захищати себе від них.

Захист від онлайн-шахрайства. Онлайн-шахраї стають все винахідливішими в своїх методах обману, а дослідження проблеми інформаційної безпеки допомагає захиститися від них.

Збереження психологічного здоров'я. Зловмисники також можуть використовувати інформацію для психологічного тиску, шантажу або булінгу. Розуміння та вміння уникати таких ситуацій може допомогти зберегти психологічне здоров'я.

Ці та інші аспекти привертають увагу науковців до вивчення питань інформаційної безпеки, зокрема: І. Арістової, М. Баран, В. Гіжевського, М. Демуцької, І. Дятлової, Я. Жаркова, І. Замаруєвої, Р. Калюжного, П. Квіткін, І. Кукіна, В. Петрика, Л. Петрова, М. Швеця та інших.

Розглядаємо інформаційну безпеку особистості як готовність і здатність індивіда зберігати недоторканість та сталість своїх поглядів, системи цінностей і ціннісних орієнтацій, переконань і стратегій у житті в умовах впливу інформаційної пропаганди і психологічних маніпуляцій, які впливають на свідомість та психіку. Вона також відображає цивілізаційну ідентичність суспільства та індивіда, враховуючи вплив соціокультурних трансформацій. Як цілісна і структурна сутність, інформаційна безпека особистості об'єднує в собі низку взаємопов'язаних складових: світоглядно-ментальну, когнітивну та культурологічну.

П. Квіткін, І. Дятлова та Л. Петрова розуміють інформаційну безпеку особистості як інтегральну якість та визначають забезпечення інформаційної безпеки особистості як функції держави, зокрема: «захист національного інформаційного простору від розповсюдження спотвореної або забороненої для поширення законодавством країни інформаційної продукції; проведення активної та цілеспрямованої контрпропагандистської діяльності; нейтралізація можливих негативних і деструктивних наслідків інформаційних та інформаційно-психологічних впливів; формування інформаційної безпеки особистості» [4].

М. Баран зазначає, що «діяльність державних інститутів, інститутів громадянського суспільства щодо вироблення та реалізації системи правових, організаційних, інформаційних і інших заходів, спрямованих

на забезпечення захищеності особи, соціальних груп та суспільства від деструктивного інформаційного впливу» визначається як забезпечення інформаційної безпеки [1, с. 47].

Узагальнюючи свої наукові пошуки, дослідники зазначають, що визначення інформаційної загрози: це «такий інформаційний вплив (внутрішній або зовнішній), при якому створюється потенційна або актуальна (реальна) небезпека зміни напряму або темпів прогресивного розвитку держави, суспільства, індивідів; небезпека заподіяння шкоди життєво важливим інтересам особистості, суспільства, держави шляхом інформаційного впливу на свідомість, інформаційні ресурси й інфосферу машинно-технічних систем; сукупність чинників, що перешкоджають розвитку і використанню інформаційного середовища в інтересах особистості, суспільства і держави» [3].

Поділяємо думку В. Петрика про те, що інформаційна безпека особистості є компонентом інформаційної безпеки країни та визначає захищеність людини від деструктивних інфовпливів, що призводять до спотвореного сприйняття дійсності. «Внесення деструктивних змін у свідомість особистості може здійснюватись цілеспрямованим застосуванням інформаційних технологій. Їх негативними наслідками можуть бути руйнування цілісності особистості, системи її відносин з іншими людьми та державою» [6, с. 22]. До таких деструктивних явищ відносимо фейки, ІПСО, інформаційні вкиди тощо.

Fake – з англ. – підробка, фальшивка. Сайт проєкту «Artefact» зазначає, що «фейки – продукт, в якому частково або повністю відсутня правдива інформація. Вони схожі на жовту пресу, але є набагато небезпечнішими, тому що з’являються навіть в респектабельних ЗМІ» [8].

На сайті «Український тиждень» бачимо, ІПСО – «проста розшифровка – інформаційно-психологічна операція. Це дещо видозмінений переклад поняття Psychological Operations, PSYOPS.

Значення, якщо максимально спростити, полягає в тому, щоб спочатку вплинути на настрої груп у суспільстві. На наступному етапі поширення таких настроїв прямо позначиться на діях представників цього ж суспільства. ІПСО застосовують і в мирний, і у воєнний час. Під час нинішньої війни йдеться про те, щоб передусім забезпечити загарбнику оптимальні умови для взяття під контроль територій, тобто зробити все, щоб українці не чинили опір російським окупантам. До елементів ІПСО відносяться дезінформація, пропаганда, перебільшення певної інформації або применшення іншої, диверсії в тилу, кібератаки» [7].

А. Демуцька стверджує, що високий рівень діджиталізації, який дозволяє кожному учаснику соціальної комунікації висловити свою думку на будь-яку тему, у будьякий момент, й «висловлене швидко стає доступним масовій аудиторії»; доступ особистості до комунікаційних технологій, «масовий вкид дезінформації у інформаційний простір світу, відсутність культури верифікації інформації або їх невисока якість, а ще низька свідомість аудиторії в частині інформаційної грамотності стали ознакою цього етапу інформаційної епохи» [2, с. 33].

Зрозуміти різні аспекти збереження безпеки в Інтернеті та реальному світі можливо через структуру основних категорій та підкатегорій, які пов’язані з інформаційною безпекою, зокрема:

- кібербезпека особистості (користування паролями, захист особистих облікових записів, безпечне підключення до Wi-Fi);

- комп'ютерна безпека (антивірусне програмне забезпечення, фаєрволі та інші засоби захисту, оновлення програмного забезпечення);

- безпека в мобільних застосунках (захист від шкідливих додатків, контроль над дозволами додатків, захист від втрати мобільного пристрою);

- захист персональних даних (конфіденційність інформації, захист від крадіжки особистої ідентифікації, збереження конфіденційності медичної інформації, захист банківських даних);

- культура безпеки (навички розпізнавання фішингових атак, запобігання соціальної інженерії, збереження безпеки під час онлайн-комунікацій, безпека користування соціальною мережею);

- освіта та підвищення обізнаності (інформаційна грамотність, знання з кібербезпеки, тренінги та семінари з інформаційної безпеки);

- безпека в реальному світі (захист фізичної ідентифікації, безпека у використанні грошових коштів та платіжних карток, захист від крадіжки пристроїв) тощо.

Дослідження проблеми інформаційної безпеки особистості є критично важливим завданням, оскільки воно сприяє забезпеченню безпеки, прозорості та довіри в цифровому світі, допомагає уникати потенційних небезпек і зміцнює цифрову грамотність серед користувачів.

І. Кукін визначає, що інформаційна безпека виявляється через систему її рівнів. До першої групи, що впливають на життєдіяльність людини науковець відносить природний, економіко-професійний, відтворювальний, світоглядний та захисний; ті, що пов'язані з розвитком особистості включають мотиваційний, інвестиційний, креативний та аналітичний; забезпечуючі життєдіяльність у суспільстві включають ретрансляційний, соціальний, соціальноаналітичний, інноваційний, харизматичний і технічний. При чому дослідник підкреслює їх взаємозвязок та наголошує, що вони зреалізовані в синергетичному (сумарному ефекті всіх рівнів) [5].

Вбачаємо можливість підвищення рівня інформаційної безпеки через упровадження комплексу заходів, таких як-от: захист від кіберзагроз (кіберзлочинці постійно вдосконалюють свої методи, тому важливо вивчати їх тактики та знаходити шляхи захисту від них, це допоможе зменшити ризик витоку особистих даних), цифрова грамотність (вивчення інформаційної безпеки сприяє формуванню навичок цифрової грамотності серед користувачів, що охоплює розуміння основних понять, якість

джерел інформації, здатність виявляти потенційно небезпечні ситуації), попередження ідентифікаційної крадіжки (вивчення проблеми допомагає виявляти та уникати підступів шахраїв), забезпечення безпеки дітей (діти та підлітки є особливо вразливими у цифровому середовищі, а дослідження інформаційної безпеки допомагає батькам та педагогам навчати дітей правильно користуватися технологіями та уникати потенційних небезпек), забезпечення довіри до технологій (інформаційна безпека впливає на загальну довіру до цифрових інструментів та сервісів: чим більше користувачі знають про заходи захисту та можливі ризики, тим більше вони будуть впевнені в своїй безпеці) й сприяння сталому розвитку (вивчення інформаційної безпеки в контексті сталого розвитку може допомогти зберегти ресурси, уникнути негативних наслідків для навколишнього середовища та забезпечення безпечної та стійкої цифрової екосистеми) тощо.

Таким чином, дослідження інформаційної безпеки особистості є важливим для забезпечення захисту особистих даних, підвищення цифрової грамотності та створення безпечного і надійного цифрового середовища. Це допомагає розвинути свідоме ставлення до інтернет-ресурсів, електронних комунікацій та цифрових інструментів, що своєю чергою сприяє покращенню якості життя та забезпеченню безпеки в онлайн-середовищі.

ЛІТЕРАТУРА

1. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні : дис. … доктор філософії : 081 Право. Львів, 2023. 244 с. URL : https://nrat.ukrintei.ua/searchdoc/0823U100338/ (дата звернення: 22.08.2023).

2. Демуцька А. В. Масові емоції в соціальних комунікаціях як ресурс посилення масово інформаційного впливу. *Baltija Publishing.* 2021. С. 32-39 URL : https://doi.org/10.30525/978-9934-26-042-1-7 (дата звернення: 19.08.2023).

3. Інформаційна безпека особистості, суспільства, держави : підручник / Я. М. Жарков та ін. Київ : Вид.-полігр. центр «Київ. ун-т», 2008. 274 с.

4. Квіткін П., Дятлова І., Петрова Л. Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісник НЮУ імені Ярослава Мудрого*. Серія: Філософія, філософія права, політологія, соціологія, 4 (51). 2021. С. 46-62. URL : https://doi.org/10.21564/2663-5704.51.241998 (дата звернення: 20.08.2023).

5. Кукін І. В. Рівні інформаційної безпеки особистості в системі національної безпеки держави. В*чені записки ТНУ імені В.І. Вернадського*. Серія: Державне управління Том 30 (69) № 5 2019 с. 85-90 URL : https://doi.org/10.32838/2663-6468/2019.5/15 (дата звернення: 20.08.2023).

6. Соціальна інженерія (системний аналіз) : навчальний посібник / Петрик В. М., Курганевич В. Г., Кононович В. Г. та ін. За заг. ред. В. І. Курганевича, В. М. Петрика. Київ, 2019. 200 с.

7. Що таке ІПСО, чому важливо це знати і які операції зараз проводить Росія проти України. *Український тиждень*. URL : https://tyzhden.ua/shcho-take-ipso-chomu-vazhlyvo-tse-znaty-i-iaki-operatsii-zaraz-provodyt-rosiia-proty-ukrainy/ (дата звернення: 20.08.2023).

8. Що таке фейк? *ARTEFACT*. URL : https://artefact.live/what-is-fake/ (дата звернення: 20.08.2023).