УДК 004.056.5
Сніжной Г.В. [1], Грабова М.Р. [2]
[1] проф. НУ «Запорізька політехніка»
[2] студ. гр. БК-713 НУ «Запорізька політехніка»

РОЛЬ ОФІЦЕРА З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ ЗАХИСТУ ІНФОРМАЦІЇ

Офіцер з інформаційної безпеки (Information Security Officer, ISO) — це фахівець, який відповідає за розробку та впровадження політик захисту даних, управлінням ризиками, моніторингом інфраструктури, реагуванням на кіберінциденти та підвищенням рівня обізнаності співробітників [1]. Основна мета цієї посади – забезпечення конфіденційності, цілісності та доступності інформації.

У своїй роботі він не лише формує правила та процедури поводження з даними, а й систематично адаптує їх до актуальних викликів і загроз. Значна увага приділяється аналізу можливих ризиків та внутрішньому аудиту — це допомагає вчасно знаходити слабкі місця й розуміти, наскільки дієвими є встановлені бар'єри захисту. Це дозволяє швидше реагувати на потенційні загрози. Паралельно забезпечується технічна безпека: налаштовуються системи захисту, контролюється резервне копіювання, а також відстежується підозріла активність у мережі.

Під час інцидентів офіцер координує дії щодо їх усунення, мінімізує наслідки та запобігає повторним атакам. Окремий акцент він робить на управлінні правами доступу та навчанні команди, оскільки саме людські помилки найчастіше стають найбільш уразливим елементом. Уся діяльність здійснюється з дотриманням правових норм і законодавчих вимог, що регулюють безпеку та конфіденційність даних.

У той самий час обов'язки офіцера з інформаційної безпеки не обмежуються лише технічними завданнями. В умовах активного розвитку цифрового середовища він також долучається до протидії кібербулінгу, особливо коли йдеться про захист дітей [2, 3]. Експерти допомагають вчасно помічати про-яви онлайн-цькування, оперативно реагують на появу образливих чи небез-печних матеріалів, співпрацюють із профільними службами та онлайн-платформами, а також проводять роз'яснювальну роботу [4, 5].

Зазвичай кібербулінг проявляється через постійні образи, погрози чи розповсюдження вигаданих і принизливих відомостей, використання чужих фото без дозволу чи створення фейкових акаунтів для тиску. У подібних випадках критично важливо не просто припинити цькування, а й забезпечити захист постраждалих, зокрема їхніх персональних даних. Тому сьогодні інформаційна безпека стосується не тільки технологій, а й створення безпечного середовища для спілкування та розвитку, зокрема для молоді.

Для більш глибокого розуміння проблеми важливо також звернути увагу на ознаки кібербулінгу та способи реагування на нього.

Ознаки кібербулінгу не завжди є очевидними, однак існує ряд поведінкових змін, які можуть свідчити про те, що дитина зазнає онлайн-цькування. Зокрема, це може проявлятися у зменшенні спілкування з однолітками та родиною, небажанні відвідувати навчальні заклади або інші місця, де є ровесники, а також у різких змінах настрою. Дитина може ставати більш замкнутою, тривожною, втрачати інтерес до звичних занять і хобі. Іноді спостерігаються й фізичні прояви, такі як головний біль, порушення сну чи загальна нервозність.

У таких ситуаціях важливо своєчасно та правильно реагувати. Передусім необхідно підтримати дитину, вислухати її без осуду та створити атмосферу довіри.

Важливо також зберігати докази випадків кібербулінгу, зокрема скріншоти повідомлень чи коментарів.

Доцільним є блокування кривдника та звернення до адміністрації онлайн-платформ із відповідною скаргою [6, 7]. У разі потреби варто змінити контактні дані та налаштування конфіденційності, а також навчати дитину правилам безпечної поведінки в інтернеті, зокрема захисту особистої інформації.

Таким чином, робота офіцера з інформаційної безпеки охоплює широкий спектр напрямів: вона поєднує технічний захист, організаційні заходи та освітню роботу, спрямовану на формування культури безпечної поведінки в цифровому просторі, що ґрунтується на взаємній повазі, дотриманні особистих меж і недопущенні завдання шкоди іншим.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кіберполіція України. Офіційний сайт [Електронний ресурс]. URL: https://cyberpolice.gov.ua (дата звернення: 02.03.2026).

2. Міністерство освіти і науки України. Протидія булінгу. [Електронний ресурс]. URL: https://mon.gov.ua (дата звернення: 02.03.2026).

3. Державна служба спеціального зв’язку та захисту інформації України. [Електронний ресурс]. URL: https://dsszzi.gov.ua (дата звернення: 02.03.2026).

4. Національна гаряча лінія «Ла Страда — Україна» [Електронний ресурс]. URL: https://la-strada.org.ua (дата звернення: 02.03.2026).

5. StopBullying. Інформаційна платформа з протидії булінгу [Електронний ресурс]. URL: https://stopbullying.com.ua (дата звернення: 02.03.2026).

6. UNICEF Україна. Кібербулінг: як розпізнати та що робити [Електронний ресурс]. URL: https://www.unicef.org/ukraine (дата звернення: 02.03.2026).

7. Освітній проєкт «Дія.Цифрова освіта». Безпека дітей в інтернеті [Електронний ресурс]. URL: https://osvita.diia.gov.ua (дата звернення: 02.03.2026).