співпраця з німеччиною
DEUTSCHE ZUSAMMENARBEIT

Співфінансується Європейським Союзом

Виконавець:
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

ПОСИЛЕННЯ СПРОМОЖНОСТІ ЛОКАЛЬНИХ ОРГАНІЗАЦІЙ

03/2026

Інформаційний
БЮЛЕТЕНЬ
№ 9

Дорогі колеги!

З початку воєнних дій на території України в 2014 році, безпека в різних її проявах стала питанням № 1. Усі громадяни стикнулися з потребою приділяти ще більше уваги фізичній безпеці, щоб вберегти здоров'я та життя. Для організацій громадянського суспільства (ОГС) цифрова безпека стала так само важливою, як і для державних структур, оскільки активізувалася робота з персональними даними людей, яким надають допомогу, особливо під час гуманітарного реагування.

Постійні атаки на об'єкти енергетики й цивільної інфраструктури змушують мати копії документів як у паперовому, так і в цифровому вигляді. Це вимагає особливої уваги до збереження цілісності й недоторканості даних. Саме тому цей бюлетень містить базові правила безпеки для ОГС, які слід знати й виконувати.

Олена Герус, *координаторка програми посилення спроможності локальних організацій*

Безпечні команди і процеси: фізична, цифрова й операційна безпека ОГС

empower

ПРАВО НА ЗАХИСТ
Благодійний фонд

Для ОГС турбота про безпеку — це не окремий документ і не реакція лише на кризу, а щоденна практика, яка допомагає не втрачати членів команди, їхню працездатність, дані й спроможність організації працювати безперервно.

В складних умовах найбільше навантаження часто припадає не лише на програми, а й на внутрішні процеси: комунікацію, прийняття рішень, збереження інформації, організацію поїздок, заходів і взаємодію команди.

Взаємопов'язані виміри базової системи безпеки ОГС

ФІЗИЧНА БЕЗПЕКА
Стосується людей, локацій, маршрутів і подій.

ЦИФРОВА БЕЗПЕКА
Охоплює захист акаунтів, пристроїв, документів і персональних даних.

ОПЕРАЦІЙНА БЕЗПЕКА
Пов'язана з наявністю правил, ролей, каналів комунікації, резервних рішень і здатністю команди діяти злагоджено навіть у разі збою.

Трикутник безпеки ОГС

ФІЗИЧНА БЕЗПЕКА

Фізична безпека починається з простих, але обов'язкових дій:

- оцінювання ризиків перед поїздкою або заходом;
- перевірки локації та наявності укриття;
- уточнення контактів відповідальних осіб;
- визначення зрозумілого порядку дій у разі зміни обставин.

Команді важливо заздалегідь знати, хто ухвалює рішення про перенесення, зупинку або зміну формату активності. Не менш важливо враховувати стан членів команди. Перевантаження, виснаження, тривалий стрес, робота без пауз і постійний поспіх знижують уважність, ускладнюють координацію та підвищують ризик помилок.

Безпека людей перед активністю

ЦИФРОВА БЕЗПЕКА

Цифрова безпека тримається на дисципліні доступів. Організації варто використовувати:

- складні паролі;
- двофакторну автентифікацію;
- окремі робочі акаунти;
- правило мінімально необхідного доступу до файлів, таблиць, пошти й баз даних.

Якщо доступи залишаються у колишніх членів команди, передаються в чатах або зберігаються безсистемно, ризик втрати контролю над інформацією різко зростає. Окремої уваги потребують резервні копії, захист персональних даних бенефіціарів/ок і обережність під час роботи з файлами, посиланнями й відкритими мережами.

4 ПРАВИЛА ЦИФРОВОЇ БЕЗПЕКИ

1. **СИЛЬНІ ПАРОЛІ**
2. **ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ**
3. **ДОСТУПИ ЗА РОЛЯМИ**
4. **РЕЗЕРВНІ КОПІЇ**

ОПЕРАЦІЙНА БЕЗПЕКА

Від рівня операційної безпеки залежить, чи зможе організація працювати далі, якщо:

- хтось із її ключових членів команди буде недоступним;
- зникне зв'язок;
- буде потрібно терміново змінити формат роботи;
- станеться інцидент.

Для цього потрібні:

- зафіксовані базові процедури;
- визначені ролі;
- резервні контакти;
- зрозумілі канали внутрішньої комунікації;
- простий план дій для критичних ситуацій.

Операційна безпека також підтримує ментальну стійкість команди — коли ролі, правила й канали комунікації зрозумілі, люди менше працюють у режимі постійної невизначеності й виснаження.

5 ЗАПИТАНЬ ПЕРЕД ПОЧАТКОМ АКТИВНОСТІ

1. Чи в безпеці члени команди й учасники заходу?
2. Чи захищені дані?
3. Чи зрозумілі ролі?
4. Чи є план Б?
5. Хто ухвалює рішення у разі збою?

Надійність створюється не складністю правил, а їх ясністю, реалістичністю та застосуванням на практиці. Для втілення цих правил важливо мати звички, які формують безпечну організаційну культуру. Одна з них — ставити базові запитання перед кожною активністю для вчасного виявлення та зниження ризиків, адже надійна ОГС — це не та, яка може усунути всі ризики, а та, яка здатна їх передбачати, зменшувати й діяти злагоджено.

Чек-лист «Чи має наша ОГС базовий рівень безпеки?»

- [ ] Команда має погоджені канали комунікації для звичайних і термінових ситуацій.
- [ ] Доступ до пошти, дисків, таблиць і баз даних розподілений за ролями.
- [ ] Для важливих акаунтів увімкнено двофакторну автентифікацію.
- [ ] Критично важлива інформація зберігається впорядковано й захищена резервним копіюванням.
- [ ] Перед поїздками, заходами й польовою роботою команда оцінює ризики.
- [ ] Команда знає, хто є відповідальною особою під час активності й інциденту.
- [ ] Базові процедури для критичних процесів зафіксовані й доступні.
- [ ] Після змін у команді доступи переглядаються і зайві закриваються.
- [ ] У команді прийнятно говорити про втому, перевантаження та потребу в перепланування навантаження.
- [ ] Правила безпеки не лише існують, а й використовуються у щоденній роботі.

Безпека в ОГС починається не з довгих інструкцій, а з узгоджених щоденних дій. Найкраще працюють ті правила, які команда розуміє, приймає й застосовує на практиці. Саме такі звички формують стійкість організації в складних умовах.

Авторка:
Катерина Рижкова-Сєбєлєва,
експертка з організаційного розвитку

Якщо ви хочете долучитися до створення наступних інформаційних бюлетенів або запропонувати питання, яке важливо висвітлити, будь ласка, напишіть нам:

Катерина Вихівська,
фахівчиня з управління знаннями БФ «Право на захист»
k.vykhivska@r2p.org.ua

Більше про діяльність БФ «Право на захист» ви можете дізнатися на сайті: ***r2p.org.ua***

КОРИСНІ МАТЕРІАЛИ

> Методичний посібник із фізичної безпеки для організацій громадянського суспільства, активістів/ок і волонтерів/ок

> Порадник з безпеки для організацій громадянського суспільства та активістів: алгоритми дій у різних ситуаціях

> Методичний посібник із Цифрової безпеки для організацій громадянського суспільства, активістів/ок і волонтерів/ок

Це видання створено в межах проєкту «Посилення спроможності громад через локалізовані дії та багатосекторальну екстрену підтримку в південних і східних регіонах України», що здійснюється в межах мультидонорського проєкту «Посилення постраждалих від війни громад України через місцеві ініціативи (EMPOWER)», що фінансується Федеральним міністерством економічного співробітництва та розвитку Німеччини (BMZ) спільно з Генеральним Директоратом Європейської Комісії з питань цивільного захисту та гуманітарної допомоги та реалізується Німецьким товариством міжнародного співробітництва (GIZ) ГмбХ.