USAID ВІД АМЕРИКАНСЬКОГО НАРОДУ

ЄДНАННЯ

УНЦПД

ЦЕНТР ДЕМОКРАТІЇ ТА ВЕРХОВЕНСТВА ПРАВА

МЕТОДИЧНИЙ ПОСІБНИК

ІЗ ФІЗИЧНОЇ БЕЗПЕКИ

ДЛЯ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА, АКТИВІСТІВ/ОК І ВОЛОНТЕРІВ/ОК

КИЇВ
2023

ЗМІСТ

ВСТУП

Від початку війни в Україні у 2014 році організації громадянського суспільства (далі — ОГС), активісти/ки та волонтери/ки виконують безліч важливих ролей у наданні допомоги нашій країні. Громадські активісти/ки та волонтери/ки також є ефективними зв'язковими з бізнесом та владою, громадянами та військовими силами й захищають інтереси тих, хто потерпає від війни. Їхні зусилля сприяють підвищенню свідомості та формуванню громадянського суспільства в умовах важкої соціально-політичної ситуації.

Дії ОГС, правозахисників/ць, активістів/ок і волонтерів/ок охоплюють безліч напрямів в умовах небезпеки та постійних загроз життю й здоров'ю. Тож увага до безпекових аспектів роботи ОГС дуже важлива з погляду організаційної спроможності та базових умов роботи як під час війни, так і після її завершення.
Мета створення цього посібника — наголосити на важливості роботи над постійним покращенням саме фізичної безпеки ОГС, активістів/ок, волонтерів/ок і правозахисників/ць.

У межах роботи над покращенням безпеки ОГС, громадських активістів/ок, правозахисників/ць і волонтерів/ок варто розглядати фізичну, цифрову, правову, психологічну та інші види безпеки як комплексний процес, у якому все пов'язано з усім.

У контексті діяльності ОГС, громадських активістів/ок і волонтерів/ок фізична безпека — це стан, коли особа (працівник/ця) або організація усвідомлює потенційні небезпеки для фізичного здоров'я та майна і використовує стратегії посилення своєї захищеності від них. Ідеться про зменшення загроз, ризиків або потенційних небезпек, які можуть спричинити шкоду. Фізична безпека може стосуватися різних аспектів життя та професійної діяльності, таких як особиста безпека, безпека на робочому місці, безпека проведення заходів, безпека громадських просторів і безпека організацій тощо.

Цей посібник буде цікавим і корисним для керівників/ць ОГС, спеціалістів/ок з організаційного розвитку, безпекових менеджерів/ок. Він також стане в пригоді представникам/цям організацій, які працюють в Україні з різними цільовими аудиторіями.

Підходи до забезпечення безпеки ОГС, правозахисників/ць, активістів/ок і волонтерів/ок полягають у впровадженні заходів, стратегій для запобігання настанню ризиків і захисту від фізичних загроз, зокрема всіх видів насильства, розбою, крадіжки, проявів тероризму, нещасних випадків природного або техногенного характеру, а також інших небезпечних ситуацій.

Безпекові експерти/ки в Україні та за її межами наполягають розглядати підходи до безпеки, спираючись на три основні фактори:

- системність (розгляд певної ситуації максимально детально та прискіпливо);
- розуміння та усвідомленість (розгляд певної ситуації з позицій тверезого усвідомлення того, що відбувається, хто ми і що варто робити);
- здоровий глузд (розгляд конкретної ситуації / проблеми / виклику та пошук інструментів розв'язання саме конкретної ситуації з розумінням, що не можна стовідсотково контролювати ситуацію та усунути всі ймовірні ризики).

Використовуючи саме ці підходи, ми зазвичай формуємо плани безпеки та алгоритми дій надзвичайного реагування у випадку небезпек, які розглянемо в цьому посібнику далі.

Фізична безпека громадських активістів/ок, правозахисників/ць, волонтерів/ок є важливою з багатьох причин:

- Гарантії охорони життя та здоров'я активістів/ок дозволяють якісно виконувати свою роботу без ризику для свого життя та життя близьких.
- Свобода думки та слова дозволяє активістам/кам боротися з несправедливістю, корупцією, неправомірними діями без страху перед насильством або репресіями.
- Багато активістів/ок працюють над зміною соціальних, політичних або економічних систем, що здебільшого призводить до переслідування та/або проявів насильства з боку владних структур або недоброчесного бізнесу. Робота над алгоритмами захисту фізичної безпеки допомагає зменшити ризики насильства та захистити активістів/ок від його наслідків.
- Турбота про фізичну (та інші види) безпеки активістів/ок дозволяє їм бути ефективними й продуктивними у своїй роботі. Вони можуть зосередитися на своїх завданнях без постійної тривоги про свою безпеку чи безпеку своїх близьких.
- Прорахунок ризиків і вироблення стратегій, як їх зменшити, дозволить зекономити ресурси (людські та грошові) ОГС у майбутньому, адже команди активістів/ок будуть планувати різні сценарії розвитку загрозливих ситуацій й продумувати стратегії реагування у «стабільному» стані (а не після нападу чи підпалу майна).
- Можливість стабілізуватися в будь-якому випадку кризи, закрити базові потреби в безпечному й захищеному просторі, що відкриває можливість подумати над іншими компонентами безпеки (психологічним здоров'ям, цифровою чи фінансовою безпекою) та стратегією розвитку ОГС.

Логічно було б у цьому контексті також говорити про важливість гарантій безпеки з боку держави. Ми вважаємо, що саме дотримання Конституції та законів України мало б гарантувати покарання за будь-яке переслідування активістів/ок чи правозахисників/ць, які стикаються із фізичними погрозами чи нападами.

Роль держави, окрім іншого, полягає в:

- невтручанні в діяльність ОГС, активістів/ок, правозахисників/ць як «агентів змін»;
- відхиленні навіть пропозицій законопроєктів, що можуть обмежити діяльність ОГС в Україні, і невикористанні лексики на зразок «грантоїди» чи «соросята»;
- формуванні конструктивного та продуктивного діалогу представників державної влади різних рівнів з представниками громадянського суспільства;
- швидкому реагуванні держави на загрози активістам/кам, правозахисникам/цям чи волонтерам/кам та забезпеченні заходів превенції порушень їхніх прав;
- посиленні координації між органами влади та забезпеченні розслідування випадків погроз, нападів чи інших проявів насильства проти активістів/ок і правозахисників/ць;
- формуванні підходів гідного фізичного, психологічного, правового та цифрового захисту й допомоги;
- формуванні спільно з ОГС та активістами/ками, правозахисниками/цями та волонтерами/ками безпекових програм, механізмів і стратегій захисту та превенції загроз діяльності сектору.

Як ОГС, волонтерам/кам та активістам/кам формувати персональні безпекові стратегії, плани безпеки та ставати самозараднішими в питаннях безпеки, ми проаналізуємо в наступних розділах.

Варто зазначити, що в посібнику зібрані найкращі безпекові матеріали та практики українських експертів/ок, які працюють з темами фізичної безпеки для ОГС та активістів/ок.

Методичний посібник підготувала Олександра Мельник, менеджерка проєктів ЦЕДЕМ, безпекова тренерка для ОГС та активістів/ок, спільно з командою ЦЕДЕМ.

Посібник рецензовано Анастасією Лихолат, радницею зі стратегічних комунікацій Центру прав людини ZMINA.

Цей методичний посібник створений ЦЕДЕМ у межах проєкту «Ініціатива секторальної підтримки громадянського суспільства», що реалізується ICAP Єднання у консорціумі з Українським незалежним центром політичних досліджень (УНЦПД) та Центром демократії та верховенства права (ЦЕДЕМ) завдяки щирій підтримці американського народу, наданій через Агентство США з міжнародного розвитку. ICAP Єднання несе повну відповідальність за зміст, який може не відображати поглядів АМР США або Уряду Сполучених Штатів Америки.

РОЗДІЛ 1. АНАЛІЗ ОСНОВНИХ РИЗИКІВ І ЗАГРОЗ ФІЗИЧНІЙ БЕЗПЕЦІ АКТИВІСТІВ/ОК

Загрози фізичній безпеці ОГС включають різні види небезпек, які можуть спричинити фізичну шкоду команді організації або завадити її діяльності. До російсько-української війни серед активістів/ок і правозахисників/иць було звично вважати максимальною загрозою небезпечні дії людей, на інтереси яких впливає їхня діяльність. Це загрози від державних політичних діячів/ок, влади, недоброчесного бізнесу, органів правопорядку тощо.

Небезпечними діями з боку зазначених вище груп можуть бути незаконні затримання, обшуки, силовий розгін мирних зібрань, залякування, тиск, переслідування, перешкоджання в проведенні акцій і незабезпечення заходів безпеки в разі потреби чи інші загрозливі дії.

Але після початку російсько-української війни у 2014 році до переліку додалися ще загрози, які несе тимчасова окупація територій України, полон, фільтрація, депортація, загрози життю та здоров'ю під час здійснення волонтерської діяльності на деокупованих територіях або поблизу лінії фронту. І кожна з них може мати гірші наслідки від моменту, коли окупанти усвідомлюють приналежність їхньої жертви до правозахисної діяльності в Україні.

З окремою групою небезпек стикаються активісти/ки, громадські діячі/ки та правозахисники/ці, які вступили до лав Збройних Сил України і війна для яких несе комплексні та важчі загрози, ніж війна для цивільних активістів/ок в умовному тилу.

Окрім того, відчуття безпеки під час війни в Україні нівелюється через безперервну загрозу ракетних атак, атак дронами та інших видів обстрілів.

Для громадських діячів/ок, активістів/ок, волонтерів/ок в Україні та світі важливо аналізувати будь-які ризики та загрози винятково через призму контекстів — соціального, політичного, культурного, географічного тощо. І справді, лише перебуваючи в контексті, активісти/ки можуть знати про потенційні ризики, проаналізувати загрози й продумати стратегії їх пом'якшення.

Базові питання, які можуть допомогти проаналізувати контекст:

1 **Які головні проблеми впливають на права людини в країні чи громаді?**

(Ідеться про політичні, економічні, соціальні, безпекові та інші умови.)

2 **Хто стоїть за цими проблемами?**

(Ідеться про лідерів/ок думок та осіб, які відповідають за ухвалення рішень; установи, місцеві, національні, регіональні та міжнародні організації, бізнес та інших гравців.) Які потенційні інтереси вони переслідують (наприклад, дискредитація антикорупційних активістів/ок) і що можуть зробити (наприклад, почати дезінформаційну кампанію)?

3 **Як дотримання прав людини може негативно чи позитивно вплинути на інтереси цих ключових груп?**

(Ідеться про те, чи вже є якісь безпекові проблеми, пов'язані із цим.)

4 **Чи можна визначити час найбільшої вразливості активістів/ок і правозахисників/ць та найвищу ймовірність нападів?**

(Ідеться, наприклад, про вибори чи інші важливі події, ухвалення законів тощо.)

П'ять опорних питань, які можна поставити для аналізу контекстів безпосередньої загрози (не факт, що у вас будуть відповіді на всі ці питання, проте варто докласти максимум зусиль, щоб проаналізувати ситуації з різних точок зору). Обговорення краще проводити всією командою для кращого аналізу й залучення різних точок зору:

1. Які саме факти пов'язані із загрозою?

(Ідеться про те, чи загроза виникла внаслідок вашої професійної діяльності; чи були якісь погрози, загрозливі дзвінки; якщо так, якою була мова цих погроз тощо.)

2. Чи простежується закономірність наростання загроз, які супроводжують вашу діяльність?

(Ідеться про черговість подій, які з вами відбуваються. Наприклад, ви отримуєте серію дзвінків або повідомлень з погрозами або за вами чи вашими рідними стежать. Або ваших колег викликають на допит і наступним/ою викличуть вас тощо.)

3. Чи розумієте ви мету загроз, які супроводжують вашу діяльність?

4. Чи знаєте ви особу або осіб — ваших кривдників/ць?

(Ідеться про те, що дуже важливо проаналізувати спроможності ваших потенційних кривдників/ць і чи можуть вони перейти від погроз до конкретних нападів або інших дій.)

5. Чи вважаєте ви, що загроза буде втілена в життя?

(Аналіз епізодів вашої роботи та життя, включаючи історію нападів на правозахисників/ць в Україні, аналіз випадків безкарності тощо.)

Під час аналізу різноманітних загроз і рівня шкоди від них також не варто забувати про важливість такого явища, як «безпековий аудит».

АУДИТ БЕЗПЕКИ ОГС — це процес комплексного оцінювання рівнів систем безпеки організації за трьома факторами — оцінювання персоналу, процесів і технічного забезпечення.

ПЕРЕВАГИ:

- надає керівникам/цям ОГС і їхнім співробітникам/цям важливу інформацію, на основі якої можна визначити сильні та слабкі сторони систем безпеки, дозволяючи зосередити ресурси там, де це найбільше потрібно;
- є інструментом для проведення належної перевірки внутрішніх процесів управління та визначення відповідності системи управління безпекою;
- проводиться кваліфікованими експертами/ками, чиї знання підтверджено неодноразовим досвідом проведення, що дозволяє об'єктивно проаналізувати слабкі та сильні сторони вашої безпекової стратегії і надати точкові рекомендації;
- проводиться за напрямами фізичної, цифрової, правової, психологічної та інших сфер безпеки ОГС;
- за результатами таких аудитів напрацьовуються рекомендації щодо покращення всіх безпекових систем, рекомендації щодо покращення діяльності безпекових менеджерів/ок тощо.

Чому організації проводять безпекові аудити:

1. ОГС мають зобов'язання гарантувати своїм працівникам/цям безпеку в процесі виконання їхньої роботи.
2. У багатьох контекстах донори та партнери зобов'язують ОГС піклуватися про працівників/ць, вимагаючи чітко визначених систем і процесів для управління ризиками на робочому місці.
3. Це також заощаджує фінансові витрати в разі, якщо ймовірність настання ризику — висока.

Безпекові аудити проводяться раз на рік (якщо колектив сталий і не оновлювався впродовж року) або за іншим розкладом, визначеним внутрішніми положеннями організації. Якщо колектив за певний період діяльності оновився принаймні на 30–40 %, варто знову провести безпековий аудит.

Процес безпекового аудиту зазвичай доволі тривалий і може розтягнутися в часі від декількох тижнів до декількох місяців.

Етапи проведення аудиту безпеки для ОГС:

1. Спільне усвідомлення процесів аудиту (безпековий/а аудитор/ка, керівник/ця та працівники/ці організації та інші дійові особи, залучені до аудиту, однаково розуміють процес безпекового аудиту, його мету та очікувані результати).
2. Узгодження часових рамок (безпековий/а аудитор/ка, керівник/ця та працівники/ці організації узгоджують тривалість кожного з етапів).
3. Формування плану та охоплення аудиту (залежить від розмірів організації, бюджетів, тематики діяльності, політичного, географічного охоплень, цінностей, місії організації та інших факторів).
4. Мапування ризиків і загроз у кожній зі сфер безпеки.
5. Формування індикаторів для кожного з етапів безпекового аудиту.
6. Підготовка до збору даних.
7. Розгляд документації, потрібної для аудиту.
8. Залучення співробітників/ць організацій.
9. Залучення інших дійових осіб (залучених консультантів/ок, правління, членів/кинь наглядових рад тощо).
10. Підготовка фокус-групових досліджень.
11. Підготовка онлайн-опитувальників (за потреби).
12. Проведення всіх видів опитувань з усіма дійовими особами.
13. Картографування всіх відповідей на декілька сфер (згідно зі зручною шкалою).
14. Визначення сильних і слабких рис безпекових систем ОГС.
15. Формування системи наступних кроків згідно з результатами аудиту (формування реальних і посильних етапів роботи із системами безпеки ОГС).

Після отримання результатів безпекового аудиту зазвичай проводиться ґрунтовна робота з покращення безпекових систем ОГС.

В одному розділі методичного посібника ми точно не зможемо проаналізувати всі види загроз фізичній безпеці громадських активістів/ок, правозахисників/ць і волонтерів/ок, проте принаймні ідентифікуємо та визначимо для себе те, із чим вони стикаються найчастіше, подумаємо, що на це впливає і якими можуть бути алгоритми дій.

Також приклади з нашого детального аналізу, можливо, допоможуть вам аналізувати загрози детальніше.

Напад — це заподіяння фізичної шкоди або небажаного фізичного контакту особі або загроза чи спроба здійснити таку дію.

Потенційні вразливості особи чи організації, яка може постраждати від нападу (перелік необмежений і поданий для прикладу):

- тематика діяльності організації або окремого/ї працівника/ці;
- для працівника/ці: маршрут від дому на роботу або від дому на зустріч, який є завжди однаковим і не змінюється;
- зовнішні ознаки: брендований логотипами організації одяг, що запам'ятовується тощо.

Дії для запобігання наслідкам нападу (перелік необмежений і поданий для прикладу):

- Повідомляти рідним і близьким або колегам про те, куди ви йдете та з ким плануєте зустрітися. Також рідні мають знати, що їм робити, якщо ви не повернетеся в домовлений час.
- Якщо зустріч призначила не відома раніше особа:
  - не зустрічатися вдома;
  - для зустрічі обирати людні місця (кафе, центр міста);

- приходити на зустріч на 30–40 хв раніше, спостерігати, чи буде хтось супроводжувати людину, яка йде на зустріч;
- відмовитися від зустрічей у вечірній і нічний час;
- під час зустрічі телефонувати колегам / родичам, повідомляти геолокацію або тримати геолокацію ввімкненою.

- Не залишати в соціальних мережах інформацію про пересування, відвідування заходів, планів на відпочинок.
- Намагатися якнайменше часу проводити наодинці в публічних місцях або перебувати в безлюдних місцях.
- Проговорити з колегами алгоритм їхніх дій, якщо працівник/ця не виходить на зв'язок певний час.
- Фіксувати коротку інформацію про зустрічі та перемовини. Повідомляти близьких, де та як вони можуть знайти цю інформацію в разі потреби.
- Подумати про безпеку рідних і близьких. Поговорити з родинами відверто про можливі небезпеки, пов'язані з професійною діяльністю, і як їх уникнути.

Ресурси, які можуть допомогти уникнути наслідків нападу (перелік необмежений і поданий для прикладу):


навички самооборони;


навички поводження зі спеціальними засобами захисту;


знання місцевості, де розташований ваш офіс, районів, де відбуваються робочі зустрічі та відрядження;


«тривожна кнопка» у вигляді дармовиса на ключі або програми на смартфоні, яка після натискання викликає приватну службу охорони.

План дій у разі нападу (перелік необмежений і поданий для прикладу):

- Якщо є змога вирватися і втікати, не збільшуючи загрозу собі та своєму життю та здоров'ю, то варто робити це.
- Особисті речі можна кинути в нападників/ць, щоб затримати їх.
- Привертати максимум уваги — використовувати тривожний дармовис, кричати.
- Якщо побиття не уникнути — згрупуватися, закрити руками голову, прийняти позу ембріона.
- Намагатися залишатися на ногах, але якщо все ж таки впали — спробувати «скрутитися», тобто руками закрити голову.
- У разі отримання ножового поранення — сильно притиснути рану рукою та спробувати вирватися від нападників/ць. Якщо переслідування нема — викликати швидку або попросити це зробити перехожих.
- За можливості спробувати запам'ятати прикмети нападників/ць, у що вони були одягнені, у який бік пішли після нападу, яким транспортним засобом користувалися.

Дії після нападу (перелік необмежений і поданий для прикладу):

Звернутися в лікарню. Потрібно здійснити огляд у лікаря для зняття побоїв / визначення характеру ушкодження та зафіксувати ступінь завданих ушкоджень, оскільки це вплине на подальшу кваліфікацію злочину.
Трішки більше про це можна переглянути тут.

Звернутися в поліцію із заявою про те, що скоєно напад, а також про те, що є потреба в охороні.
Зразок заяви можна знайти тут.

Звернутися до адвоката/ки, обговорити, як правильно фіксувати ушкодження та які документи / виписки / чеки зберігати.

Подумати, хто може стояти за нападом, який стався.

Надати ширший розголос події, що може спонукати поліцію активніше займатися розкриттям злочину.

Переглянути заходи безпеки, подумати, чим можна їх підсилити.

Погроза — вид психологічного насильства; залякування, обіцянка заподіяти кому-небудь шкоду, зло. Погроза оприлюднити відомості (істинні або неправдиві) — **шантаж**. Спроба отримання чужого майна шляхом погроз — **вимагання.**

Досить часто все починається з психологічного тиску у вигляді:

- «мовчазних» телефонних дзвінків;
- агресивних повідомлень від ботів у соцмережах;
- sms-повідомлень з невідомих номерів або таких, які неможливо визначити тощо.

До таких випадків потрібно ставитися максимально серйозно і в жодному разі не ігнорувати їх.

Що робити у випадку погроз (перелік необмежений і поданий для прикладу):

- Якщо погрози надходять анонімно, спробувати дізнатися більше інформації. Така інформація буде корисна для подання заяви до поліції.
- Не відповідати образами на образи й не погрожувати у відповідь.
- Не зволікати і відразу звернутися до поліції з повідомленням про те, що вам погрожують.
- Звертатися можна усно, написавши паперову заяву й подавши в найближчий відділ поліції за місцем проживання; також можна надіслати електронною поштою. Зразок заяви можна знайти тут.
- Подзвонити в поліцію, дізнатися, за яким номером Єдиного реєстру досудових розслідувань (ЄРДР) зареєстрували заяву про кримінальне правопорушення та хто його виконавець/иця. Також запитати контактний номер телефону виконавця/иці. Зв'язатися з виконавцем/ицею.
- Відвідати відділ поліції, докласти всіх зусиль для особистого спілкування з працівниками/цями органу правопорядку, які відповідають за розслідування справи.
- Фіксувати ПІБ, посаду / звання, контакти правоохоронців/иць з приводу заяви.
- Якщо виконавець/иця не виходить на зв'язок або ігнорує, написати скаргу керівнику/ці призначеного виконавця/иці.
- Якщо погрози повторюються, звернутися до поліції із заявою про надання охорони.
- У разі відмови в реєстрації кримінального правопорушення звернутися до адвоката/ки для звернення до суду, щоб зобов'язати орган правопорядку внести відомості про кримінальне правопорушення до ЄРДР.

Що робити, якщо погрози надходять від правоохоронців або інших зловмисників?

- Навіть якщо погроза була усною чи сказаною мимохідь, не варто її ігнорувати.
- Усі подібні випадки слід описати, а інформацію направити у вигляді заяви (можна на електронну адресу) до Державного бюро розслідувань (ДБР).
- Надати розголос цій події (написати про цей випадок у соцмережах; сконтактувати із журналістами, розказати їм про те, що сталося; звернутися до місцевих правозахисних організацій).
- Повідомити про ситуацію, яка склалася, представника Уповноваженого Верховної Ради України з прав людини та Управління забезпечення прав людини Національної поліції України (якщо погрози надходили від поліцейських).

Обшук — це слідча дія, що полягає в примусовому обстеженні приміщень, споруд, ділянок місцевості та інших об'єктів, які перебувають у віданні певних осіб, з метою знайдення та вилучення предметів та/чи документів.

Вразливості особи чи організації, яка потенційно може постраждати від обшуку (перелік не обмежений і поданий для прикладу):

- тематика діяльності (наприклад, антикорупційна діяльність або захист вразливих груп тощо);
- необмежений доступ до офісу (наприклад, двері не зачиняються на замок, коли заходять відвідувачі);
- розташування офісу (перший поверх з прямим виходом на вулицю без чорного ходу);
- незапаролені та незашифровані пристрої (ноутбуки, комп'ютери, телефони);

- сервер з даними зберігається в офісі;
- паролі на стікерах на моніторах;
- відсутність адвоката.

Неповний, але пропонований перелік ресурсів, які можуть допомогти уникнути наслідків обшуку (перелік необмежений і поданий для прикладу):

- адвокат/ка;
- план дій на випадок обшуку (з описаними безпековими ролями, які закріплені за всіма членами/кинями команди);
- повнодискове шифрування та встановлені паролі на гаджетах;
- наявність віддаленого сервера (використання хмарних сховищ);
- розташування офісу (наприклад, високий поверх в офісному центрі із чорним виходом);
- дружні стосунки з охороною офісного центру;
- система відеоспостереження в офісі;
- план дій під час обшуку з детальним розподілом ролей: хто і що робить у момент, коли дізналися про прибуття спецслужб, хто затягує час і не впускає, хто видаляє дані, хто вимикає комп'ютери, хто може вийти з офісу через чорний хід із флешками, жорсткими дисками тощо.
- Окрема стратегія для фізичного зберігання чутливої чи конфіденційної інформації, особливо такої, що містить персональні дані активістів/ок чи журналістів/ок.

План дій у разі обшуку (перелік необмежений і поданий для прикладу):

- за можливості зберігайте спокій;
- спробуйте зупинити спецслужби на вході до виклику адвоката;
- не піддавайтеся на переконування: «Вам же нема чого приховувати, просто впустіть нас!»;
- поки спецслужби чекають, переконайтеся, що вся техніка зашифрована та запаролена, після чого вимкніть усі комп'ютери та ноутбуки;
- якщо щось потрібно зберегти і це ніяк не можна видаляти, збережіть це на флешках і покладіть ці флешки у свої кишені. Обшук найчастіше санкціонований саме для офісу і він не передбачає особистий огляд усіх, хто в ньому перебуває;
- у випадку, якщо частина з них не зашифрована, видаліть усі сенситивні дані за допомогою спеціального програмного забезпечення для 100 % видалення даних (CCleaner, Eraser, etc.);
- фіксуйте на відео все, що відбувається під час обшуку, за можливості ведіть онлайн-трансляцію в соцмережі.

Арешт — це різновид кримінального покарання, за якого суд може позбавити особу права вільно переміщатися в просторі, що має на меті встановити перебування засудженої особи в ізольованому від зовнішнього світу приміщенні.

Вразливості особи, яка потенційно може постраждати від арешту (перелік необмежений і поданий для прикладу):

- тема вашої роботи торкається інтересів представників/ць влади, представників/ць недоброчесного бізнесу чи органів правопорядку;
- ви працюєте із засекреченою інформацією;
- відсутній адвокат/ка

Ресурси, які можуть допомогти уникнути наслідків арешту (перелік необмежений і поданий для прикладу):

- адвокат/ка;
- ваші знання кримінального та процесуального законодавства.

План дій щодо запобігання арешту (перелік необмежений і поданий для прикладу):

- дізнатися про свої права на випадок обшуку, затримання, арешту;
- обговорити ризики з рідними й домовитися про те, що ваш/а партнер/ка чи батьки робитимуть у разі арешту: кому дзвонити, що говорити тощо;
- у період підвищеного ризику дітей (за наявності) варто відправити до родичів;
- встановити приховане відеоспостереження в будинку: це допоможе зняти процес арешту та можливі порушення процедури;
- не зберігати вдома секретну інформацію;
- на випадок обшуку під час арешту подбати про безпеку своїх пристроїв: зашифрувати їх і встановити пароль на вхід.

План дій щодо запобігання арешту (перелік необмежений і поданий для прикладу):

- коли до вас постукали, видаліть особливо секретну інформацію, яку встигнете видалити, і вимкніть ноутбук / комп'ютер;
- повідомте адвоката/ку своєї організації про те, що сталося;
- не чиніть опору співробітникам/цям поліції — це може обернутися проти вас;

- якщо ви стали свідком свавілля поліції, передайте цю інформацію колегам та адвокату/ці й готуйте заяву до ДБР;
- вимагайте дотримання всіх процедур.

Ми також хочемо нагадати про такі загрози, як викрадення, підпал, знищення чи пошкодження майна, а також ті загрози, які несе із собою війна. У таких випадках краще звернутися до експертів/ок з безпеки для аналізу кожної конкретної ситуації.

РОЗДІЛ 2. ОЦІНЮВАННЯ РИЗИКІВ ФІЗИЧНОЇ БЕЗПЕКИ І ЯК ЙОГО ПРОВОДИТИ. ПЛАНИ БЕЗПЕКИ

Загрози та ризики — це поняття, якими ми зазвичай послуговуємося під час аналізу безпекової ситуації та ризиків настання негативних наслідків.

Загрози — це зовнішні ознаки, які свідчать про небезпеку або чийсь намір заподіяти шкоду. Наприклад, ми чуємо постріли або сигнал повітряної тривоги, нас зупиняють на блокпосту й кудись ведуть чи пересаджують в іншу машину, ми читаємо новини про те, що до міста заходять ворожі війська тощо. Також до загроз відносять отримання повідомлень з погрозами чи шантажем.

Ризик — це ймовірність того, що щось погане з вами може трапитися.

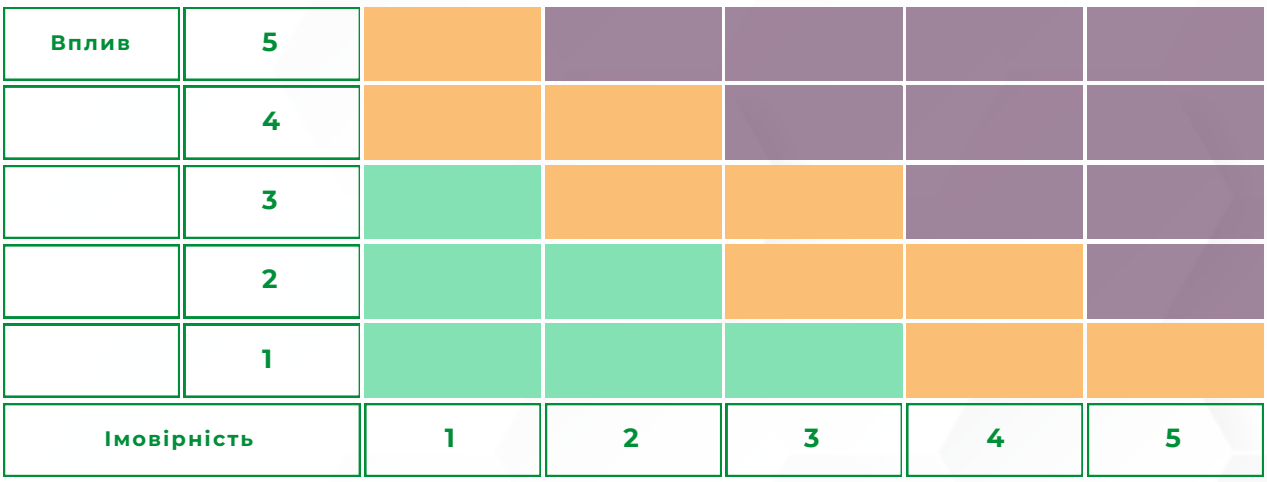
Класична матриця оцінювання ризиків враховує два основні вектори — рівень впливу шкоди та ймовірність її настання.

Оцінювання ризиків

Оцінювання ризиків — це процес визначення ймовірності виникнення факторів ризику, тобто певних подій або ситуацій, здатних негативно вплинути на розвиток подій і досягнення запланованих результатів.

Тому варто аналізувати негативні події з огляду на їх ймовірність і розставляти пріоритети (до уникнення чогось ми докладаємо більше зусиль, а ймовірність чогось просто приймаємо, продовжуючи роботу).

Один з варіантів — розподілити ризики на зелені (прийнятні), жовті (критичний вплив) і червоні (понад критичний вплив).



Робота з кожним ризиком для різних працівників/ць та кожної окремої команди є дуже індивідуальним явищем. На кожен випадок потрібно звертати окрему увагу. Варто почати з опрацювання ризиків із червоної зони, бо вони можуть завдати найбільшої шкоди вашій діяльності чи команді.

Для кращого розуміння розглянемо випадок небезпеки та проаналізуємо його.

Небезпека (до прикладу): **руйнування теплової електростанції у вашому місті / селищі під час чергового обстрілу або ракетної атаки.**

Крок 1. Визначаємо для себе ймовірність настання цієї небезпеки:

1. Імовірність близька до нуля (проаналізувати контексти: як часто за статистикою відбувалися будь-які обстріли вашого міста за останній рік; яких пошкоджень вони завдавали; яким було реагування тощо).

2. Імовірність існує, але вона невелика.

3. Імовірність помітна, її не можна відкидати.

4. Висока ймовірність.

5. Імовірність майже гарантована, і після оцінювання рівня завданої шкоди потрібен чіткий план дій.

Крок 2. Визначаємо для себе впливи настання такої небезпечної ситуації:

- **Впливу майже немає або він непомітний** (не було жодного прильоту за останній рік; теплова електростанція розташована далеко від вашого дому чи офісу; кожну повітряну тривогу ви та ваша родина або ви та ваша команда перебуваєте в укритті).
- **Несуттєвий вплив** (від наслідків атаки ймовірні перебої в теплопостачанні, електропостачанні).
- **Помітний вплив, який не можна ігнорувати** (може бути пошкоджене ваше майно, житло внаслідок віддаленого удару, помітні перебої у водопостачанні, газопостачанні, електроживленні).
- **Суттєвий вплив** (потенційна травматизація вас або ваших близьких. Часткове знищення майна, житла. Загроза евакуації).
- **Катастрофічний вплив** (потенційне каліцтво вас або ваших близьких, колег, потенційна загибель. Повне знищення майна, житла без можливості його відновити).

Крок 3. Розміщуємо ймовірність і вплив у таблиці (приклад):

Вплив	5					
	4					
	3			+		
	2					
	1					
Імовірність		1	2	3	4	5

Пояснення: ми індивідуально (бо це залежить від контексту) визначили для себе середню ймовірність настання цієї небезпечної ситуації і що вплив настання такої ситуації може бути дуже помітним для нас.

Примітка: аналізуючи ймовірність і впливи, ми робимо розгорнутий аналіз усіх додаткових факторів: де розташована ТЕЦ, у якому вона стані на цей момент; які райони вона обслуговує, де розташований найближчий підрозділ ДСНС, як швидко в разі загрози життю зазвичай прибуває швидка медична допомога тощо. Тільки на основі цього ми робимо висновки.

Висновок: після проведеного аналізу та оцінювання ризиків ви маєте сформувати план безпеки для такої ситуації, означити безпекові ролі для вас і членів/кинь вашої команди, подбати про матеріально-технічне забезпечення офісу на випадок настання відповідної небезпечної ситуації, наявність екстрених контактів тощо.

Дуже важливо присвятити час і зусилля проведенню комплексного оцінювання ризиків, а вже потім формуванню планів безпеки для ОГС, ініціативних груп чи індивідуальних активістів/ок, волонтерів/ок.

План безпеки — це порядок простих і зрозумілих дій, які допоможуть захистити себе, рідних, команду в критичній ситуації. План треба створювати із залученням всіх членів/кинь команди, а також за допомогою безпекового менеджера/ки та/або експерта/ки з безпеки.

ГОЛОВНА МЕТА СТВОРЕННЯ ПЛАНУ БЕЗПЕКИ — ефективно керувати надзвичайною ситуацією в разі її виникнення. Розроблення такого документа дає змогу проаналізувати небезпеки, які можуть погіршити перебіг кризової ситуації, і вжити заходів для їх усунення. Процес аналізу та оцінювання допоможе виявити недоліки, наприклад брак ресурсів (обладнання, навченого персоналу, матеріалів), які можна ліквідувати до настання шкоди.

ВАЖЛИВО!

План безпеки — це неформальний сталий документ, який напрацьовується залежно від умов, у яких перебуває та працює організація чи ініціативна група. Максимально важливим є розподіл безпекових ролей і спроможність членів/кинь команди виконувати ці ролі. Також під час роботи над планом потрібно визначити потреби та сфери для навчання та покращення.

Етапи роботи з планом безпеки:

- аналіз контексту;
- виявлення джерела й причини ризику;
- оцінювання кожного ризику й рівня завданої шкоди;
- визначення допустимого рівня ризику;
- робота з вразливостями та слабкими сторонами ОГС;
- розроблення заходів зі зниження ймовірності або впливу на недопущення настання ризику;
- розроблення алгоритму дій під час настання ризику (наприклад, дії під час викрадення, арешту або обшуку).

Можна використовувати таблиці або інші зручні для вас формати ведення планів безпеки.

Ризик	Серйозність наслідків	Імовірність того, що це станеться	Заходи запобігання та пом'якшення наслідків (для прикладу, перелік не обмежений)
Напад	Межові негативні наслідки як для особи, так і команди організації, оскільки впливають на життя та здоров'я	Висока, пов'язана з напрямами роботи	Урізноманітнювати свої маршрути: щоразу ходити не так, як учора, це дозволить уникнути засідки на маршруті. Користуватися особистим транспортом або таксі. Ходити разом з колегами та родичами. Застрахувати своє життя та здоров'я, так у разі нападу ви отримаєте компенсацію за шкоду, завдану здоров'ю. Укласти ко нтракт з адвокатом/кою, який/а згодом притягне до відповідальності нападників/ць.

Ризик	Напад
Імовірність	Висока, пов’язана з напрямами роботи
Вплив	Межовий негативний як на особу, так і команду організації
Оцінювання загроз	• Чи нападали на вас чи ваших колег раніше? • Чи отримували ви погрози про те, що на вас готується напад? • Чи помічали ви за собою стеження?
Вразливості	• Тематика вашої діяльності • Маршрут від дому на роботу та назад завжди однаковий • На маршруті від дому до роботи є неосвітлені ділянки, пустирі • Ваш зовнішній вигляд (яскравий одяг, що запам'ятовується)
Наявні ресурси	• Навички самооборони • Навички вміння користуватися спеціальними засобами, наприклад газовим балончиком або електрошокером (зверніть увагу на законодавство у сфері використання спецзасобів для самозахисту, їх використання може бути регламентовано або заборонено) • Знання місцевості
Необхідні ресурси	• «Тривожна кнопка» у вигляді дармовиса на ключі або програми на смартфоні, яка після натискання викликає приватну службу охорони • «Тривожний брелок», який видає оглушливий писк, привертаючи увагу всіх навколо у великому радіусі
Необхідні дії для запобігання ризику	• Урізноманітнювати свої маршрути: щоразу ходити не так, як учора, це дозволить уникнути засідки на маршруті. • Користуватися особистим транспортом або таксі. • Ходити разом з колегами та родичами. • Застрахувати своє життя та здоров’я, так у разі нападу ви отримаєте компенсацію за шкоду, завдану здоров’ю. • Укласти контракт з адвокатом/кою, який/а згодом притягне до відповідальності нападників/ць.
Дії в разі настання ризику (для прикладу, перелік не обмежений)	Тікати, якщо є така змога • Особисті речі можна кинути в нападників/ць, щоб затримати їх, адже здоров’я і життя дорожчі за будь-які речі • Привертати максимум уваги: використовувати «тривожний брелок», кричати (причому кричати варто не «Допоможіть», а щось інше, що приверне увагу, наприклад «Пожежа»)
Час	Подбати про превентивні дії — негайно
Відповідальна особа	• Безпековий/а спеціаліст/ка, що забезпечить базове навчання для команди ОГС • Охорона офісу

РОЗДІЛ 3. СВІТЛОФОР БЕЗПЕКИ ДЛЯ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Повномасштабна війна в Україні змусила ОГС приділяти дедалі більше уваги безпеці — захисту членів/кинь команди, службової інформації, персональних даних тощо. Так, системна робота із цими темами допоможе організаціям діяти на випередження й запобігати ризикам.

Щоб полегшити організаціям роботу з власною безпекою, Центр демократії та верховенства права в межах проєкту «Ініціатива секторальної підтримки громадянського суспільства України» у співпраці з безпековою експерткою, тренеркою та юристкою Анною Литвиновою розробили «Світлофор безпеки» — інструмент самооцінювання рівнів безпеки у форматі тесту. Він дасть змогу громадській або благодійній організації оцінити, наскільки вона захищена від зовнішніх загроз і ризиків, пов'язаних із фізичною, правовою та цифровою безпекою, під час роботи. Світлофор безпеки для ОГС можна знайти за посиланням.

Розробити цей інструмент організаторів спонукав, зокрема, і запит ОГС, які розуміють: безпекові аудити — важливі.

Світлофор безпеки побудований як поблоковий опитувальник з варіантами відповідей, кількість і зміст яких визначає рівні небезпеки. Далі система вираховує кількість балів і вказує зелений, жовтий або червоний рівень небезпеки для кожного з розділів.

Розробники поклали в основу тесту три розділи:

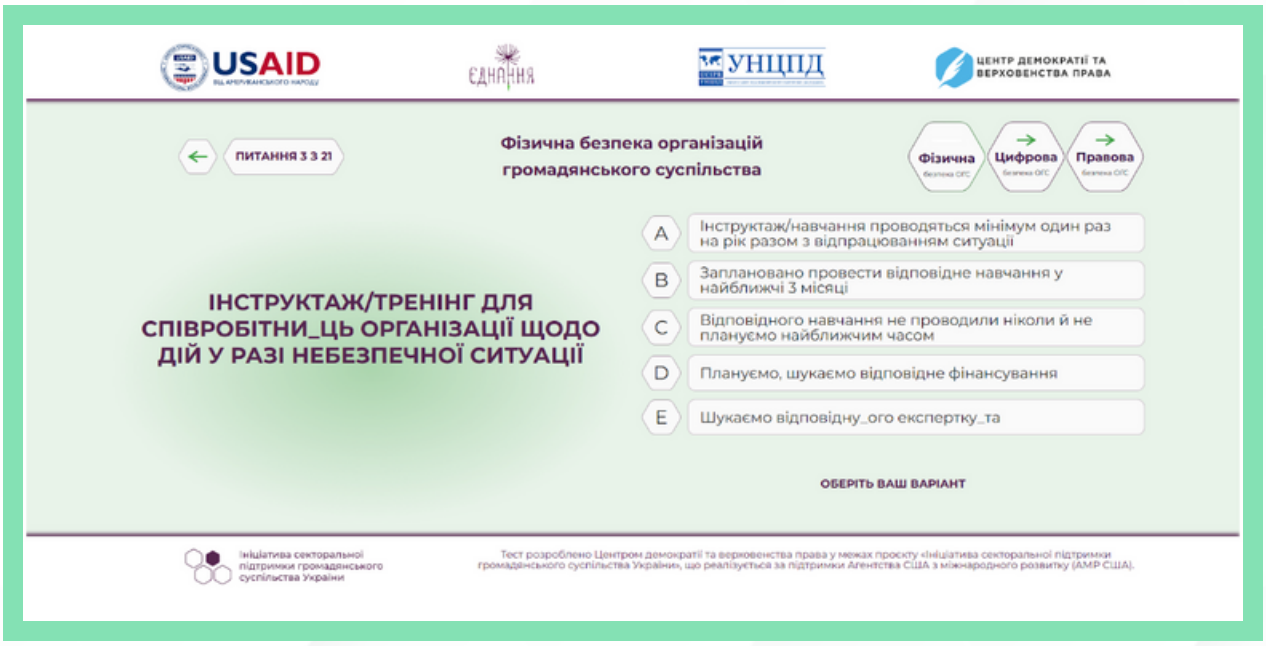
- Фізична безпека ОГС — заходи, покликані захистити організацію, її майно, співробітників/ць і бенефіціарів/ок від навмисних чи випадкових загроз.
- Цифрова безпека — технічні та цифрові інструменти, IT-рішення, які захищають цифрові активи, службову інформацію й персональні дані членів/кинь і бенефіціарів/ок ОГС.
- Правова безпека — захист організації від юридичних ризиків через внутрішні неузгодженості або зовнішні впливи.

Ще один важливий компонент інструменту — короткі методичні рекомендації, які генерує система залежно від рівня небезпеки в кожному розділі. Завдяки цим порадам ОГС зможе змінити своє становище на краще.

Інструмент покликаний зміцнити спроможність і стійкість та спонукати розвиток культури безпеки ОГС — і не лише тих, хто постійно стикається з ризиками (наприклад, працюючи у прифронтовій зоні), але й решти громадського сектору.

На думку розробників, важливо пройти всі три розділи тесту, щоб мати повноцінний безпековий скринінг для організації. У кожному блоці — 15–20 питань з декількома варіантами відповідей. Орієнтовний час на проходження опитувальника — 20 хвилин.

Тут подано приклад одного з питань у Світлофорі безпеки:



Цей інструмент рекомендовано пройти керівникам/цям і заступникам/цям керівників/ць громадських або благодійних організацій, безпековим менеджерам/кам, директорам/кам з програмного чи стратегічного розвитку, фінансовим директорам/кам.

РОЗДІЛ 4. ПРО ПОЛІТИКИ ТА ПРОЦЕДУРИ ІЗ ФІЗИЧНОЇ БЕЗПЕКИ

Внутрішні політики та процедури є дуже важливою складовою життєдіяльності організації. Навіть коли команда лише планує створювати громадське об'єднання, ідеї однодумців/иць і початкові записи — це вже перші внутрішні стратегічні документи.

Політики й процедури для ОГС — це майже завжди зафіксовані документально набори внутрішніх правил, які допомагають організаціям працювати ефективно, дотримуючись визначених цілей і цінностей. Політики встановлюють основні принципи та напрями діяльності, тоді як процедури визначають конкретні кроки та послідовність дій для виконання завдань.

В ОГС такі політики та процедури можуть охоплювати різноманітні аспекти, такі як фінансове управління, робота з волонтерами/ками, спілкування з громадськістю, захист персональних даних співробітників/ць та учасників/ць освітніх / тренінгових заходів, безпека тощо. Вони допомагають створити структуру та порядок у діяльності організації, забезпечуючи її стабільність і відповідність визначеним цілям.

Причини розроблення стратегічних документів — політик, процедур, планів, протоколів та алгоритмів:

1. Прагнення прозорості, підзвітності та дотримання законів (процедури допомагають гарантувати, що діяльність організації відбувається відкрито та прозоро).

2. Ефективне управління (процедури встановлюють основні принципи та цінності, які визначають напрям діяльності. Процедури визначають конкретні кроки та стандарти для виконання завдань, що сприяє ефективному управлінню ресурсами).

3. Фінансовий менеджмент ОГС (регулюють управління бюджетами, забезпечуючи ефективне використання ресурсів й уникнення фінансових ризиків).

4. Взаємодія з волонтерами та працівниками ОГС (встановлюють стандарти роботи з волонтерами/ками та персоналом, визначаючи права та обов'язки всіх учасників/ць організації).

5. Збільшення довіри громадськості до ОГС.

6. Захист прав та інтересів (встановлені політики й процедури дозволяють організаціям боротися за права та інтереси, які вони визначають як свою місію).

7. Адаптація до змін (чіткі процедури допомагають легше адаптуватися до змін у внутрішньому та зовнішньому середовищі).

8. Виконання зовнішніх вимог донорів і партнерів заради залучення, наприклад, додаткового фінансування (одна з найпоширеніших причин появи стратегічних документів).

Питання безпеки в ОГС є надзвичайно важливим, і політики та процедури відіграють ключову роль у забезпеченні цілісності, захисту учасників/ць та ефективного управління ризиками.

Аспекти важливості політик і процедур з безпеки для ОГС

- Політики визначають стандарти та правила, які спрямовані на **захист учасників/ць організації, таких як волонтери/ки, працівники/ки та клієнти/ки.**
- Процедури встановлюють конкретні кроки **для уникнення, зменшення та управління різними видами ризиків,** включаючи фінансові, організаційні та інші.
- Політики можуть містити плани **кризового управління,** що визначають дії та відповіді організації на непередбачені події або екстремальні ситуації.
- З урахуванням розвитку технологій **політики з кібербезпеки** стають усе важливішим елементом для захисту інформації та даних організації.
- Багато ОГС працюють у сферах, де існують конкретні **правила та нормативи.** Політики допомагають забезпечити дотримання цих правил організацією та донорами.
- Захист від непорозумінь, скандалів та інцидентів сприяє **збереженню довіри громадськості та доброї репутації організації.**
- Забезпечення **безпеки інформації** є ключовим аспектом, особливо якщо організація працює із чутливими даними клієнтів/ок, партнерів/ок або фінансовою інформацією.

Створення політик і процедур з безпеки для ОГС — це важливий крок у забезпеченні стійкої та ефективної діяльності.

Декілька порад для ОГС, які готуються до створення або покращення наявних безпекових політик і процедур:

- Оцініть потенційні небезпеки, з якими може стикатися ваша організація. Це може стосуватися фізичної, цифрової, правової та психологічної безпеки.
- Врахуйте думки та досвід різних представників/ць вашої організації при створенні політик і процедур.
- Забезпечте чітке розуміння політик і процедур серед усіх членів/кинь організації. Проведіть потрібне навчання та надайте вдосталь інформації про важливість безпеки.
- Уважно вивчіть і впроваджуйте заходи з кібербезпеки, зокрема стосовно захисту інформації та даних.
- Чітко визначте безпекові ролі й межі безпекової відповідальності за виконання політик і процедур. Кожен/на член/киня організації має знати свої обов'язки.
- Змінюйте та оновлюйте політики та процедури з безпеки відповідно до змін у загальному середовищі й контексті та внутрішніх потреб.
- Регулярно проводьте аудити безпеки, щоб перевірити ефективність ваших заходів і виявити можливі слабкі місця.
- У випадку потреби залучайте експертів/ок з безпеки для консультацій та аудитів.
- Розробіть плани кризового управління для ефективної реакції на непередбачені події чи кризові ситуації.
- Забезпечте прозору комунікацію щодо політик і процедур з безпеки серед усіх учасників/ць.

Пам'ятайте, що безпека — це неперервний процес, і важливо регулярно переглядати та оновлювати ваші заходи забезпечення безпеки для відповідності новим викликам і ризикам.

Корисні джерела для отримання інформації від розробників посібника

Перелік організацій, які займаються питаннями безпеки, а також корисні освітні матеріали (перелік рекомендований і невичерпний):

Міжнародні організації:

- Freedom House
- Frontline Defenders
- People in Need

Українські організації, які можуть надати інформацію чи підтримку у випадку переслідування (перелік невичерпний):

- ZMINA
- Інститут масової інформації (медіа)
- Українська Гельсінська спілка з прав людини
- Інсайт (фем і ЛГБТІ+ активізм)
- Наш світ (ЛГБТІ+ активізм)
- Екодія (екологічний активізм)

Підбірка великої кількості матеріалів за напрямом «Безпека ОГС, активістів/ок, волонтерів/ок» від ЦЕДЕМ

РОЗДІЛ 5. ШАБЛОНИ ДОКУМЕНТІВ

ДОДАТОК № 1

Політика безпеки (назва організації)

Остання редакція: (день, місяць, рік)

Зміст

Принципи захисту та безпеки (ця частина має містити коротку інформацію про важливість формування культури безпеки в організації, мету політики, яка актуальна саме для вашої ОГС, та її функції)

Стратегія безпеки (про важливість принципів неупередженості та нейтральності, якими керуються більшість ОГС, про підходи до прийняття та розуміння в ОГС)

Розроблення та впровадження політики безпеки (про те, що політика та протоколи безпеки розробляються безпековим/ою менеджером/кою у співпраці зі співробітниками/цями організації. Однак фізична безпека та піклування про себе має бути пріоритетом кожного/ї в команді, а не лише керівника/ці організації чи безпекового/ї менеджера/ки. Політика та протоколи переглядаються й оновлюються щопівроку. Зворотний зв'язок та пропозиції щодо внесення змін до політики слід направляти безпековому/ій менеджеру/ці)

Комунікаційна стратегія як складова політики (про те, хто кому яку інформацію передає, як збирається інформація про потенційні загрози та ризики, як опрацьовується, хто що робить у випадку кризи тощо)

Безпекові ролі та обов'язки:

- **в офісі**
- **під час виїздів і відряджень**
- **під час надзвичайних ситуацій**

Відповідність і масштаби політики та протоколів безпеки (про те, на кого розповсюджуються ці політики і хто береться за виконання безпекових ролей згідно з розподілом в алгоритмах)

Характер політики (від працівників/иць, підрядників/иць і членів/кинь виїзних груп вимагається дотримання політики та протоколів безпеки. Тільки в ситуаціях, що загрожують життю, менеджери/ки мають певні повноваження нехтувати ними)

Протоколи:

- **протоколи для окремих ситуацій** (наприклад, протокол відряджень, відряджень у сіру зону, відряджень за кордон; протокол проведення заходів тощо)
- **інструктажі**
- **стратегії безпечної комунікації** (офіс, відрядження та поїздки; надзвичайні ситуації)
- **управління кризовими ситуаціями**
- **звітування про надзвичайні ситуації**

Додаткова необхідна документація (плани евакуації з офісу, перелік екстрених контактів тощо)

ДОДАТОК № 2

Таблиця-матриця оцінювання ризиків безпеки

Вплив	5					
	4					
	3					
	2					
	1					
Імовірність		1	2	3	4	5

ДОДАТОК № 3

Таблиця-матриця оцінювання ризиків безпеки

Ризик	
Імовірність	
Вплив	
Оцінювання загроз	
Вразливості	
Наявні ресурси	
Необхідні ресурси	
Необхідні дії для запобігання ризику	
Дії в разі настання ризику (для прикладу, перелік не обмежений)	
Час	
Відповідальна особа	

ДОДАТОК № 4

Інший варіант плану безпеки для певної ситуації у вигляді таблиці

Ризик	Серйозність наслідків	Імовірність того, що це станеться	Заходи запобігання та пом'якшення наслідків (для прикладу, перелік не обмежений)

ДОДАТОК № 5

Приклад безпекового протоколу

ВАЖЛИВО!

Інформація, яку містить протокол, є рекомендованою, ви або члени/кині вашої команди можете та/або повинні доповнити її.

Протокол дій під час виїзду в прифронтову зону та на деокуповані території для працівників/ць (назва організації)

Затверджено: (день, місяць, рік)

Рекомендований план дій під час підготовчого етапу (у цьому розділі йдеться про пропрацювання ризиків і загроз; вивчення інформації про локацію; види зброї, яка застосовується на цих територіях; необхідність вивчити різницю між одностроями, іншу підготовчу інформацію).

Під час поїздки (у цьому розділі йдеться про місця для сну та їди; зберігання обладнання; координати місцевих і військових закладів швидкої допомоги та як їх дістатися; розташування стратегічних об'єктів; план евакуації; налагодження контактів з активістами/ками та волонтерами/ками, які також працюють на цій ділянці; потребу дбати про своє здоров'я тощо).

Зауваження до добору персоналу (важливо подумати про те, чи репутація, стать, етнічна належність або сексуальна орієнтація особи не роблять її потенційною мішенню для вороже налаштованих учасників/ць; про достатній рівень фізичної підготовки, щоб швидко реагувати на виникнення небезпеки та швидко переміщатися; про роботу в парі та місце зустрічі на випадок непередбачуваних обставин тощо).

Основи комунікаційної стратегії (про графік виходу на зв'язок з колегами; протокол екстреного зв'язку на випадок надзвичайної ситуації; контактну особу, яка перебуває в інших умовах та на іншій території).

Одяг та спорядження (про зручність одягу та взуття; уникнення елементів, за які вас можна схопити (ланцюжків, шарфів, нашийних шнурків для аксесуарів, зачісок на кшталт «кінський хвіст»), а також легкозаймистих матеріалів (на кшталт нейлону); про потребу в захисних окулярах, респіраторах, масках, захисному жилеті; про зарядки та електростанції; воду та їжу).

Транспорт (планування переміщень з урахуванням перекриття доріг чи інших перепон; інструктування з мінної безпеки; паркування вашого транспорту; що можна залишати в транспорті тощо).

МЕТОДИЧНИЙ ПОСІБНИК

ІЗ ФІЗИЧНОЇ БЕЗПЕКИ

ДЛЯ ОРГАНІЗАЦІЙ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА, АКТИВІСТІВ/ОК І ВОЛОНТЕРІВ/ОК

Цей методичний посібник створений ЦЕДЕМ у межах проєкту «Ініціатива секторальної підтримки громадянського суспільства», що реалізується ІСАР Єднання у консорціумі з Українським незалежним центром політичних досліджень (УНЦПД) та Центром демократії та верховенства права (ЦЕДЕМ) завдяки щирій підтримці американського народу, наданій через Агентство США з міжнародного розвитку. ІСАР Єднання несе повну відповідальність за зміст, який може не відображати поглядів АМР США або Уряду Сполучених Штатів Америки.