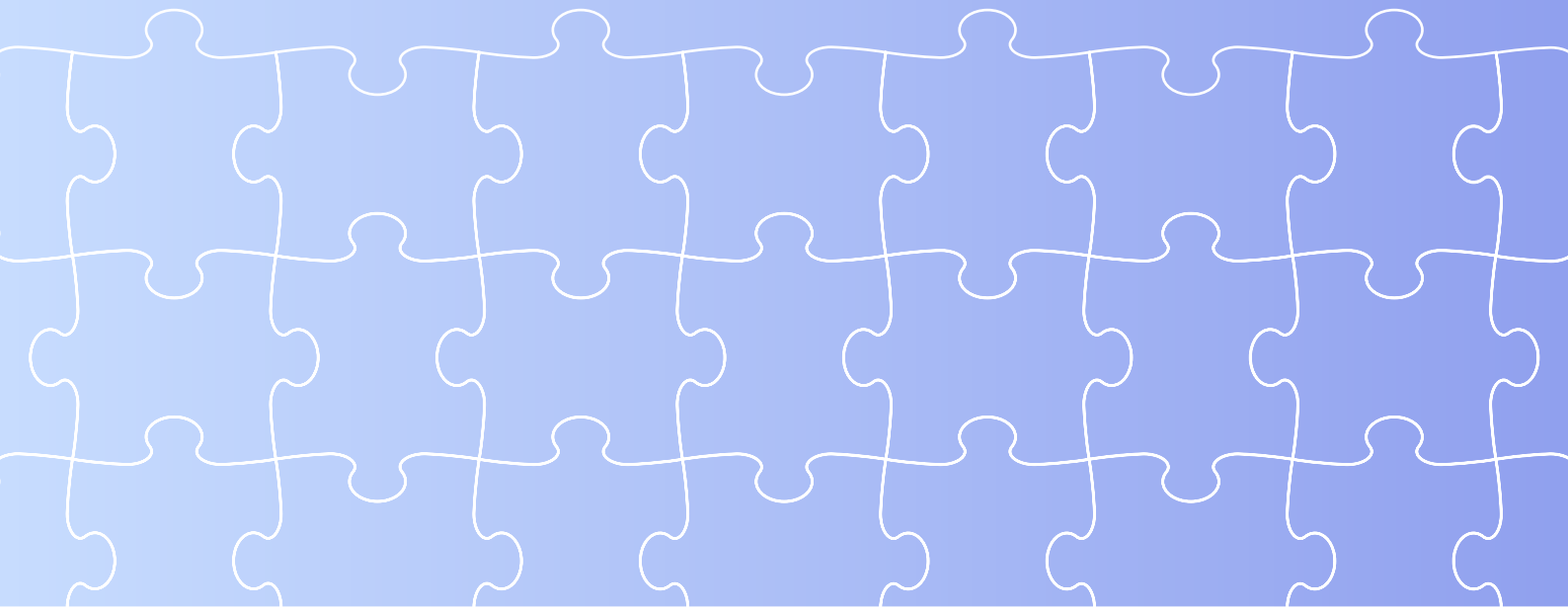
ПРОЦЕДУРА УПРАВЛІННЯ РИЗИКАМИ



м. Київ – 2025

ЗМІСТ

1 Сфера застосування

Ця процедура визначає підхід до оцінки ризиків діяльності громадської організації. Оцінка інформаційного ризику - це метод систематичного, задокументованого виявлення, аналізу, оцінки та контролю ризиків операційної діяльності та проектів. Він використовується для визначення їх впливу, а також для визначення та застосування контролів, які відповідають ризикам.

Організація проводить оцінку ризику з запланованими інтервалами або коли пропонуються чи відбулися значні зміни. Організація зберігає документально підтверджену інформацію про результати оцінок ризику.

2 Терміни та визначення

прийнятний ризик (acceptable risk) - ризик, знижений до рівня, який організація може допустити, враховуючи свої правові зобов'язання

небезпека, небезпечний чинник (hazard) - джерело, ситуація або дія, які потенційно можуть завдати шкоди організації, або їх комбінація

ідентифікація небезпеки (hazard identification) - процес розпізнавання наявності небезпеки та визначення її характеристик

ризик (risk) - поєднання ймовірності виникнення небезпечної події чи впливу(-ів) та істотності травми чи погіршання здоров'я, які може бути зумовлено такою подією чи впливом(-ами)

оцінювання ризику (risk assessment) - процес оцінювання ризику, що виникає від небезпеки, з урахуванням адекватності наявних засобів управління та прийняття рішення стосовно прийнятності чи неприйнятності ризику

3 Порядок оцінки ризиків

Процес оцінки ризиків включає систематичне визначення, оцінку та моніторинг ризиків та діяльність з управління ризиками.

Процес управління ризиками реалізується за допомогою таких процедур:

- ідентифікація критичного робочого простору / процесів та збору даних;

- ідентифікація та оцінка ризиків;
- моніторинг та контроль ризиків.

Визначення критичного робочого простору / процесів та збору даних.

З метою підготовки до ідентифікації ризику відповідальні особи підрозділів (за організаційною структурою) визначають критичну робочу зону та збирають дані про потенційні загрози в діяльності.

Відповідальний працівник (або група працівників) повинен дослідити робоче місце / процеси / обладнання / проекти та виявити потенційні загрози.

Назва підрозділу	Критична робоча область / процеси
Відділ персоналу	Сейф
Відділ системних адміністраторів	Серверна
	Склад

Ідентифікація та оцінка ризиків

Оцінка ризику проводиться один раз на рік. Протягом року керівники підрозділів надсилають таблицю ризику службовцю з інформаційної безпеки, яка містить:

Джерела загроз, які заносяться до реєстру ризиків (додаток 1 до цієї процедури). Наступний перелік загроз використовується для заповнення регістра ризиків.

№	Назва небезпеки
1	Пожежа
3	Крадіжка
5	Збої електроживлення
6	Відмова телекомунікаційного обладнання
9	Розкриття/продаж інформації працівниками
10	Помилка/недбалість персоналу
11	Зловживання працівником
12	Компрометація паролів доступу
15	Хакерські дії
16	Фальсифікація та підробка даних

На підставі інформації про загрози відповідальна особа аналізує загрози та визначає ризики та значення ризиків. Він записує інформацію про ризик у форму _ Реєстр ризиків (додаток 1).

Важкість ризику розраховується відповідальним працівником у таблиці обчислення ризику за формулою:

Рівень ризику = Ймовірність x Наслідок = (2) X (4) = 8

Шкала ймовірності та ризик ризику були спрощені та визначені наступним чином:

Масштаб Фактор ризику	5	4	3	2	1
Ймовірність виникнення	1 раз на день	1 раз на тиждень	1 раз на місяць	1 раз в квартал	1 раз на рік (або більше року)
Наслідки ризику	Призводить до зупинки Процесу / проекту і порушує законодавство Призводить до зупинки процесу/ проекту на тривалий час, який перевищує максимально допустимий час простою)	Призводить до великих фінансових втрат (визначити суму), має значний вплив на репутацію і може призвести до зупинки роботи процесу або проекту	Призводить до значних фінансових втрат (визначити суму) та має значний вплив на репутацію	Призводить до незначних фінансових втрат (визначити суму) та має незначний вплив на репутацію	Практично не призводить до наслідків з фінансовими втратами, та не впливає на процеси / проекти

Після обчислення рівня ризику слід використовувати наступну матрицю ризику для визначення пріоритетності кожної задачі; де, більш високим завданням по контролю ризиків слід надавати більший пріоритет і швидше вирішувати їх.

Ймовірність	Матриця ризиків				
5	B	A	A	A	A
4	B	B	A	A	A
3	B	B	B	A	A
2	C	B	B	A	A
1	C	C	B	B	B
	1	2	3	4	5
	Наслідки				

RPN		
Ризик<2		Допустимий ризик
3<Ризик=<4		Помірний ризик
Ризик=>6		Недопустимий ризик

Частота оцінки ризику

Початковий ризик	Оцінка ризику на початок звітного періоду або перед початком проекту
Залишковий ризик	Після завершення звітного періоду (наприклад 1 рік) або після закінчення проекту

Контроль ризиків

За результатами оцінки ризику їх подальший моніторинг та контроль.

Рівень ризику	Дії з ризиком
Прийнятний ризик - С	Приймаємо
Помірний ризик - В	Моніторинг
Неприйнятний ризик - А	Контроль

Не рідше 1 разу на рік необхідно проводити аналіз ризиків та готувати звіт по результатах мінімізації ризиків.

5 Відповідальність

Відповідальним за розробку цієї процедури є _____
Відповідальним за моніторинг відповідності цієї процедури є _____

Додаток
Форма оцінки ризиків

Територія, виробничий процес/ обладнання	Небезпека	Опис ризиків інформаційної безпеки	Важкість наслідків	Ймовірність виникнення	Базовий рівень ризику	Заходи по контролю за ризиками (технічний захист, адміністративний захист)