Назва ЗОЗ **Процедура планування відновлення після аварій**	
Назва: Планування відновлення після аварій	**ЗОЗ 1,2 категорії**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Затверджено: ПІБ Назва ЗОЗ**

ПРОЦЕДУРА ПЛАНУВАННЯ ВІДНОВЛЕННЯ ПІСЛЯ АВАРІЙ ЗАКЛАДУ ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ



ЗМІСТ

стр.

1. ВСТУП 3
2. ВИЗНАЧЕННЯ 3
3. ВІДПОВІДАЛЬНІСТЬ 4
4. ПЛАНУВАННЯ ВІДНОВЛЕННЯ ПІСЛЯ АВАРІЙ 5
   - 4.1. Визначення критичності 5
   - 4.2. Проведення оцінки ризиків 6
   - 4.3. Визначення можливостей для планування відновлення 6
   - 4.4. Визначення цільового часу відновлення та цільових точок відновлення 6
   - 4.5. Визначення команд з відновлення 7
   - 4.6. Визначення необхідних дій для відновлення 7
   - 4.7. Розробка критеріїв оцінки ПВПА та проведення тестування плану 8
   - 4.8. Перегляд та оновлення 8

Додаток А. Приклад ПВПА для ЗОЗ 1 категорії. 9

Додаток Б. Приклад ПВПА для ЗОЗ 2 категорії. 11

1. ВСТУП

Цей документ містить порядок дій з планування відновлення інформаційної інфраструктури та складання плану відновлення після аварій (далі – ПВПА) для ЗОЗ.

Мета діяльності з планування відновлення полягає в тому, щоб визначити послідовність необхідних заходів, які необхідно вжити до, під час і після аварії і забезпечити можливість виконання цих заходів.

Планування відновлення є частиною діяльності з безперервності бізнесу. ЗОЗ які хочуть використовувати повний цикл вимог до планування безперервності, мають керуватись настановами що викладені у стандартах ISO 22301 та ISO 22313.

2. ВИЗНАЧЕННЯ

Аварійне відновлення – це стратегія реагування на природну або техногенну катастрофу.

Аварія – значне пошкодження або вихід з ладу обладнання або елементів інформаційної інфраструктури, що супроводжується тривалим порушенням роботи ЗОЗ або його частини.

ВІБ – відповідальний за інформаційну безпеку, призначена особа, яка відповідає за впровадження та дотримання Політики інформаційної безпеки в закладі охорони здоров'я. Уразі неможливості призначити окремого відповідального за інформаційну безпеку, його функцію виконує керівник ЗОЗ.

Елемент інфраструктури – частина інформаційної інфраструктури, яка має окремі межі та має правила взаємодії (напр. – комутатор, сховище даних, поштовий сервер, сервер друку тощо). До елементів інфраструктури також відносяться застосунки, які розміщуються на серверах, мають відокремлене середовище та правила взаємодії (наприклад, ПЗ для обліку кадрів, ПЗ для бухгалтерського обліку, електронна система діловодства).

ІБ - Інформаційна безпека, це процес, який забезпечує збереження визначених Політикою безпеки властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи.

Інформаційна інфраструктура – інфраструктура, яка обробляє інформацію ЗОЗ. До неї відносяться (не виключно) – мережі, включаючи пристрої комутації та управління, сервери, сховища даних (включаючи хмарні), пристрої друку (принтери, МФУ), медичне обладнання, яке має мережеве підключення та/або зберігає дані.

Керівник – керівник закладу охорони здоров'я (ЗОЗ).

Користувач - Будь-яка особа зі складу персоналу ЗОЗ, уповноважена на доступ до певного інформаційного ресурсу.

Надзвичайна ситуація (НС) – порушення нормальних умов діяльності ЗОЗ, що призвели або можуть призвести до втрат.

ПВПА – план відновлення після аварій, це документ який описує, як слід реагувати на незаплановані інциденти, які порушують нормальну роботу ЗОЗ. ПВПА повинен розглядати як техногенні катастрофи, так навмисні (наприклад, діяльність терористичних організацій, хакерів, злочинців) або випадкові дії (наприклад, відмова обладнання).

ПІБ – Політика інформаційної безпеки, це центральний, програмний документ, який визначає основні засади забезпечення належного рівня інформаційної безпеки закладу охорони здоров'я.

Персонал – всі працівники ЗОЗ, які використовують інформаційні ресурси закладу, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до своїх посадових обов'язків.

Цільовий час відновлення (ЦЧВ) – це показник відновлення, який визначає прийнятний час, через який система або елемент інфраструктури має повернутись у працездатний стан. протягом якого критичні програми можуть вийти з ладу. Наприклад, якщо ЦЧВ дорівнює 1 годину, це значить, що збитки для діяльності після простою системи більше 1 години є неприйнятними.

Цільова точка відновлення (ЦТВ) – це прийнятний обсяг даних (вимірюється часом), який ЗОЗ готовий втратити в разі інциденту.

3. ВІДПОВІДАЛЬНІСТЬ

Відповідальність за виконання цього документу несе керівник ЗОЗ та ВІБ.

Відповідальність за підтримку ПВПА в актуальному стані та виконання дій, що визначені ПВПА несуть власники процесів/об'єктів інфраструктури.

4. ПЛАНУВАННЯ ВІДНОВЛЕННЯ ПІСЛЯ АВАРІЙ

Діяльність з планування відновлення складається з таких етапів:

1. Визначення критичності процесів, обладнання та інформації в діяльності ЗОЗ.
2. Проведення оцінки ризиків щодо критичних об'єктів інформаційної інфраструктури ЗОЗ.
3. Визначення можливостей для планування відновлення та вибір систем, щодо яких буде проводитись діяльність з відновлення.
4. Визначення цільового часу відновлення та цільових точок відновлення.
5. Створення команд з відновлення, визначення обов'язків, інформування та взаємодію учасників.
6. Визначення необхідних дій для відновлення та порядку їх виконання.
7. Розробка критеріїв перевірки ПВПА та проведення тестування плану.
8. Регулярний перегляд актуальності та оновлення (за необхідності) плану.

ПВПА, за задумом, дуже гнучкі, тому роботи можуть бути імпровізовані та адаптовані до несподіваних подій. Це важливо, оскільки будь-яке небезпечне явище є нестабільним за своєю природою, і фактори, які впливають на його прогресування, ніколи не можуть бути точно передбачені.

Приклади ПВПА наведено у Додатках А та Б.

4.1. Визначення критичності

На цьому етапі визначаються критичні для ЗОЗ активи та/або елементи інформаційної інфраструктури, встановлюються пріоритети для відновлення та визначається перелік надзвичайних ситуацій (сценаріїв), які можуть призвести до аварій інформаційної інфраструктури та унеможливлення діяльності ЗОЗ.
Розподіл ІКС ЗОЗ на елементи має відповідати складності інфрастуктури ЗОЗ.
Для ЗОЗ 1 категорії прикладами елементів є:

- Медична інформаційна система (МІС) та пристрій, на якому вона встановлена або з якого здійснюється робота з МІС.
- Засоби для обробки та зберігання персональних даних пацієнтів (у випадку, якщо оброблення та/або зберігання здійснюється поза межами МІС).
- Засоби обробки та зберігання інформації про кадровий склад ЗОЗ.
- Засоби обробки та зберігання іншої інформації, яка є критичною для ЗОЗ.
- Сервер (скринька) електронної пошти, яка використовується для комунікацій ЗОЗ.

Для ЗОЗ 2 категорії, прикладами елементів є:

- Поштовий сервер.

- Система діловодства.
- Медична інформаційна система (МІС).
- Внутрішнє сховище даних.
- Сервери бухгалтерського та кадрового ПЗ.
- Мережеві пристрої.
- Енергозабезпечення інфраструктури (засоби безперебійного, резервного та автономного живлення).

При визначенні критичності враховується думка всіх підрозділів/структурних елементів ЗОЗ.

Під час проведення цього етапу розглядаються, щонайменше, такі елементи, які у якості можливих наслідків можуть мати такі можливі наслідки:

- Неможливість продовження діяльності ЗОЗ;
- Неможливість надання частини послуг ЗОЗ;
- Притягнення до відповідальності посадових осіб ЗОЗ через невиконання вимог законодавства;
- Фінансові збитки ЗОЗ.

Всі елементи інфраструктури які визначені як критичні, є обєктами для відновлення і мають бути враховані в ПВПА.

4.2. Проведення оцінки ризиків

На цьому етапі аналізуються всі функції ЗОЗ, щоб визначити та оцінити можливі наслідки від різних сценаріїв та їх відношення до обраного рівня прийнятних ризиків. ЗОЗ 1 категорії на цьому етапі варто визначити щонайменше 2 сценарії – половина та найгірший випадок розвитку аварії (часткова та повна відмова елементу інфраструктури).

Оцінка ризиків проводиться відповідно до «Політики управління ризиками інформаційної безпеки ЗОЗ».

4.3. Визначення можливостей для планування відновлення

При складанні ПВПА враховуються наявні ресурси ЗОЗ або можливість долучення ресурсів, які можуть бути наявними у підрядників (наприклад, вибір хостинг-провайдеру з переліку тих, який має опцію захисту від DDoS атак). Заходи для виконання яких у ЗОЗ відсутні ресурси або ресурс є суворо обмеженим не розглядаються. Відновлення може вимагатись непередбачувано, і наявність необхідних ресурсів є важливим чинником успішного виконання відновлення.

4.4. Визначення цільового часу відновлення та цільових точок відновлення

Для кожного елементу інфраструктури, який обрано для планування відновлення, визначаються параметри ЦЧВ та ЦТВ. При визначенні цих показників, думка бізнес-власника є основною.
Цільовий час відновлення визначається як максимальний час простою, який не призводить до неприйнятних наслідків.
При визначенні ЦЧВ враховуються обмеження та можливості персоналу щодо відновлення. Чим менше цей показник, тим критичніші вимоги щодо часу відновлення та способу резервування.
При визначенні ЦТВ слід враховувати, що цей показник напряму впливає на процес резервного копіювання, та може призвести до зросту витрат на резервне копіювання та збільшити навантаження.
Ці показники можна попередньо визначити на етапах визначення критичності та оцінки ризиків та уточнити їх в подальшому з командою з відновлення.

4.5. Визначення команд з відновлення

Склад команд з відновлення включає в себе учасників, що виконують такі ролі:

- Керівник команди.
- Технічний фахівець.
- Власник бізнес-процесу (за необхідності).

Керівник команди відновлення виконує такі функції:

- Організує діяльність команди та забезпечення необхідними для відновлення ресурсами.
- Приймає рішення про початок відновлення.
- Організовує пошук та усунення причин виникнення аварії (за необхідності).
- Проводить періодичний перегляд планів відновлення та інформує команду про зміни.
- Слідкує за достатністю компетенцій учасників команди з відновлення запланованим діям.
- Звітує про результати діяльності вищому керівництву.

Технічний фахівець (фахівці) мають володіти всіма необхідними знаннями та вміннями, які потрібні для виконання дій з відновлення, включаючи створення передумов.
Власник бізнес-процесу залучається для інформування про стан відновлення, а також для проведення перевірки після відновлення.
Учасники команди з відновлення приймають участь у визначенні причин аварій, оцінки дій з відновлення, а також подають пропозиції щодо прискорення та покращення відновлення.

Склад команди відновлення:

Функція	ПІБ	Контакти для екстреного зв’язку
Керівник команди відновлення		
Технічний фахівець		
Власник бізнес-процесу		

4.6. Визначення необхідних дій для відновлення

На цьому етапі плануються необхідні дії та їх послідовність для відновлення та порядок взаємодії і комунікації учасників команд відновлення.
Після визначення необхідних дій, визначаються необхідні передумови для відновлення. Необхідні передумови – це інші елементи інфраструктури, які необхідні для відновлення. До необхідних передумов може входити – необхідне ПЗ або операційна система, наявність фізичного доступу до обладнання, права та облікові дані для віддаленого доступу, наявність конкретних налаштувань на мережевих пристроях та інше.

Всі дії та передумови відновлення мають бути внесені в ПВПА (Додаток А, Додаток Б). ПВПА має бути затверджений керівником ЗОЗ та доведений до відома всіх зацікавлених сторін.

4.7. Розробка критеріїв оцінки ПВПА та проведення тестування плану

Критерії перевірки та процедури тестування є важливою частиною процесу відновлення, за допомогою яких визначається його результативність та ефективність. Критерії та процедури тестування визначаються на підставі критичності елементу інфраструктури, що відновлюється та наявних можливостей. Критерії перевірки та процедури тестування містять опис методу перевірки та частоту проведення перевірок. Факти поведення перевірок ПВПА мають бути відображені в окремих звітах, які містять результати із причинно-наслідковим аналізом невідповідностей.
Щонайменше 1 раз на 3 роки слід проводити сценарний тест на відмову та відновлення зігдно плану. Проведення тесту на відмову не повинно обмежувати діяльність ЗОЗ.
Приклад плану тестування наведено у Додатку В.

4.8. Перегляд та оновлення

ПВПА переглядається та оновлюється щонайменше 1 раз на рік. Позапланове оновлення відбувається при наявності таких подій:

- Змінились умови щодо елементу інфраструктури (критичність, зв’язки з іншими елементами, правила роботи або вимоги щодо інформації, яку обробляє елемент).

- Змінились наявні ресурси (переглядається їх достатність для виконання відновлення).
- При перевірках та тестуванні виявляються недоліки ПВПА.
- Негативні результати тестування на відновлення, та заходи по виправленню.

Оновлені ПВПА затверджуються та доводяться до відома команд з відновлення та бізнес-власників.

Додаток А. Приклад ПВПА для ЗОЗ 1 категорії.

Елемент відновлення	ЦЧВ	ЦТВ	Вимоги до резервування	Необхідні ресурси та передумови	Команда відновлення	Порядок відновлення	Періодичність та тип перевірки
Доступ до медичної інформаційної системи з робочого місця медпрацівника	2 год	-	Резервування не вимагається	1. ПК або ноутбук з встановленою ОС Windows 2. Наявність підключення до Інтернет	ВІБ – керівник команди відновлення IT адміністратор – учасник команди відновлення	1. Завантажити дистрибутив МІС за адресою ftp://MIS.COMPANY Пароль та логін підключення вказано в договорі з провайдером. 2. Встановити МІС з дистрибутиву 3. Налаштувати згідно з вимогами інструкції про налаштування МІС.	Щорічно, шляхом перевірки доступності МІС за вказаною адресою та окремою перевіркою актуальності інструкції з налаштування МІС.
Доступ до електрнної пошти ЗОЗ@ukr.net	4 год	1 день	Окреме резервування не вимагається.	1. Функція відновлення паролю до скриньки у провайдера 2. Доступ до номеру телефону, на який проведено реєстрацію.	ВІБ – керівник команди відновлення IT адміністратор – учасник команди відновлення	1. Впевнитись, що доступ втрачено. 2. Скористуватись опцією «відновлення паролю». 3. Очікувати код підтвердження на номер, який вказано при реєстрації (+380001234567) та ввести його в поле підтвердження. 4. Ввести новий пароль з урахуванням вимог щодо складності.	2 рази на рік проводити перевірку процедури відновлення паролю та перевіряти наявність всіх складників для відновлення (номер телефону, таємні питання тощо).

Живлення критичних компонентів ІКС електричним струмом	0,5 год	-	Наявність генератора та засобів перемикання	Генератор електроенергії 40 літрів дизельного палива для генератора Засоби перемикання джерел живлення	ВІБ – керівник команди відновлення Електрик.	1. Відключити ЗОЗ від енергомережі міста. 2. Завести генератор. 3. Подати електрику з генератора на мережі ЗОЗ. 4. Після відновлення енергопостачання від міста – відключити генератор та переключити мережі ЗОЗ на мережі міста.	Щомісячно перевіряти працездатність генератора шляхом йог о ввімкнення на 5 хвилин та перевіряти наявність і кількість запасу дизельного палива.

Додаток Б. Приклад ПВПА для ЗОЗ 2 категорії.

Елемент відновлення	**ЦЧВ**	**ЦТВ**	**Вимоги до резервування**	**Необхідні ресурси та передумови**	**Команда відновлення**	**Порядок відновлення**	**Періодичність та тип перевірки**
Доступ до медичної інформаційної системи з робочого місця медпрацівника	1 год	-	Резервування не вимагається	1. ПК або ноутбук з встановленою ОС Windows 2. Наявність підключення до Інтернет	ВІБ – керівник команди відновлення ІТ адміністратор – учасник команди відновлення	1. Завантажити дистрибутив МІС за адресою ftp://MIS.COMPANY Пароль та логін підключення вказано в договорі з провайдером. 2. Встановити МІС з дистрибутиву 3. Налаштувати згідно з вимогами інструкції про налаштування МІС.	Щорічно, шляхом перевірки доступності МІС за вказаною адресою та окремою перевіркою актуальності інструкції з налаштування МІС.
Поштовий сервер	2 год	24 год	Створення щоденних резервних копій	1. Доступ до місця зберігання резернвих копій 2. Віртуальне середовище із ОС Windows. 3. Виконати процедуру відновлення	ВІБ – керівник команди відновлення Поштовий адміністратор – учасник команди Адміністратор віртуальної інфраструктури – учасник команди	1. Отримати розпорядження на початок відновлення. 2. Перевірити доступність та характристики віртуального середовища. 3.	

Додаток В. Приклад плану тестування ПВПА

Критерій перевірки	Процедура тестування	Місяць											
		1	2	3	4	5	6	7	8	9	10	11	12
Відновлення МІС на робочих станціях	Перевірка наявності доступу до офіційного джерела розповсюдження дистрибутивів МІС. Перевірка чинності логіну/паролю.		x										
Відновлення доступу до електронної пошти ЗОЗ	Перевірити в налаштуваннях наявність другого фактору, на який зареєстровано поштову адресу.		x						x				
Відновлення електропостачання	Запуск генератора без підключення до енергомережі ЗОЗ. Перевірка кількості палива.	x	x	x	x	x	x	x	x	x	x	x	x