

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо проведення аналізу впливу порушення безперервності виконання робочих
процесів (бізнес-процесів) та пов'язаних з ними засобів інформатизації
(інформаційних та інформаційно-комунікаційних систем)

1. Загальні положення

Проведення аналізу впливу порушення безперервності виконання робочих процесів (бізнес-процесів) та пов'язаних з ними засобів інформатизації (далі — аналіз впливу) є складовою системного управління безперервністю діяльності та дає змогу визначити, які робочі процеси є критичними або важливими для виконання завдань і функцій державного органу, які наслідки може спричинити їх припинення, а також які вимоги до резервування, відновлення та захисту інформаційних ресурсів необхідні для забезпечення їх безперервності.

При проведенні аналізу рекомендується враховувати положення національних стандартів, гармонізованих з міжнародними стандартами у сфері управління безперервністю, зокрема ДСТУ EN ISO 22301:2021 Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT) — щодо побудови системи управління безперервністю, визначення потреб та вимог до безперервності, планування заходів реагування та відновлення; ДСТУ EN ISO 22313:2021 Безпека та стабільність. Системи управління неперервністю бізнесу. Настанови щодо застосування ISO 22301 (EN ISO 22313:2020, IDT; ISO 22313:2020, IDT) — щодо практичного застосування вимог та принципів управління безперервністю діяльності, зокрема планування реагування, забезпечення безперервності та відновлення діяльності; ДСТУ ISO/TS 22317:2023 Безпека та стабільність. Системи управління неперервністю бізнесу. Настанови щодо аналізування впливу на бізнес (ISO/TS 22317:2021, IDT) — щодо проведення аналізу впливу на діяльність замовника, визначення наслідків порушення діяльності, пріоритетності діяльності та процесів, а також визначення вимог щодо забезпечення їх безперервності та відновлення; ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу (ISO/IEC 27031:2011, IDT) — щодо забезпечення готовності інформаційно-комунікаційних технологій до підтримання безперервності діяльності, визначення вимог до ІКТ-послуг та інфраструктури, необхідних для підтримання критичних робочих процесів, планування їх відновлення та оцінювання готовності ІКТ до функціонування в умовах порушень.

Метою проведення аналізу впливу є визначення:

- 1) робочих процесів (бізнес-процесів), безперервність виконання яких є необхідною для виконання завдань і функцій замовника;
- 2) наслідків порушення або припинення виконання таких процесів;
- 3) залежностей від інформаційних, технологічних, комунікаційних, інфраструктурних та організаційних ресурсів;
- 4) необхідних строків відновлення виконання робочих процесів (бізнес-процесів) та пов'язаних з ними засобів інформатизації;
- 5) вимог до резервування, аварійного відновлення та забезпечення безперервності функціонування;
- 6) основних ризиків, проблем та потреб замовника щодо забезпечення безперервності.

Аналіз впливу проводиться замовником з урахуванням особливостей його діяльності, структури, повноважень, залежностей від інших органів державної влади, державних інформаційних ресурсів, постачальників послуг та інших зовнішніх і внутрішніх ресурсів.

Під час проведення аналізу впливу необхідно враховувати наслідки порушення функціонування засобів інформатизації внаслідок, зокрема, технічних відмов, відмов

електроживлення або телекомунікацій, кібератак, компрометації інформації, знищення або пошкодження обладнання, недоступності персоналу, надзвичайних ситуацій, воєнних ризиків та інших подій, які можуть призвести до порушення безперервності виконання робочих процесів.

Результати аналізу впливу повинні ґрунтуватися на фактичному стані організації та її інформаційно-комунікаційної інфраструктури. Не рекомендується зазначати як реалізовані заходи, які перебувають на етапі планування або впровадження.

2. Загальні вимоги до заповнення форми

Звіт заповнюється для кожного засобу інформатизації, щодо якого відповідно до законодавства проводиться аналіз впливу.

Усі показники та відомості зазначаються станом на дату проведення аналізу впливу або іншу дату, визначену у формі.

У разі відсутності відповідної інформації зазначається «відсутня», «не визначено» або «не застосовується» із зазначенням причини, якщо це необхідно для розуміння результатів аналізу.

Значення показників часу зазначаються в годинах або хвилинах із достатньою точністю для оцінки їхньої відповідності встановленим вимогам.

3. Визначення робочих процесів (бізнес-процесів)

Для кожного робочого процесу зазначаються його найменування, відповідальний структурний підрозділ або посадова особа, основне призначення та пов'язані із ним засоби інформатизації.

Під час визначення процесів необхідно враховувати не лише безпосередню діяльність замовника, а й процеси, безперервність яких необхідна для:

- виконання визначених законодавством завдань і функцій;
- надання публічних послуг;
- забезпечення міжвідомчої взаємодії;
- виконання обов'язкових процедур та строків;
- збереження та використання інформації.

Наслідки переривання робочого процесу (бізнес-процесу) оцінюються для кожного процесу окремо.

4. Визначення MTPD, RTO та RPO

Для кожного критичного або важливого робочого процесу визначаються показники максимально допустимого періоду порушення функціонування (MTPD), цільового часу відновлення (RTO) та цільової точки відновлення (RPO).

MTPD визначається як максимальний час, протягом якого порушення виконання відповідного робочого процесу не призводить до неприйнятних наслідків для діяльності замовника.

RTO визначається з урахуванням MTPD та встановлює час, протягом якого має бути відновлено функціонування відповідного засобу інформатизації на рівні, необхідному для продовження виконання робочого процесу.

RPO визначається з урахуванням допустимого обсягу втрати або неактуальності даних, який замовник може прийняти без виникнення неприйнятних наслідків.

Значення MTPD, RTO та RPO мають бути взаємопов'язаними. Як правило:

$$\mathbf{RPO \leq RTO < MTPD.}$$

Визначені значення RTO та RPO не повинні перевищувати граничних значень, установлених для відповідної категорії засобу інформатизації, якщо інше не передбачено законодавством.

5. Визначення категорії засобу інформатизації

Категорія засобу інформатизації визначається замовником за результатами аналізу впливу з урахуванням масштабу можливих наслідків порушення його функціонування та потреб у забезпеченні безперервності виконання робочих процесів (бізнес-процесів).

Під час визначення категорії не рекомендується використовувати лише технічні характеристики системи, її розмір, кількість користувачів або вартість.

Основним критерієм є вплив порушення функціонування засобу інформатизації на діяльність замовника та пов'язані з нею робочі процеси.

Якщо засіб інформатизації забезпечує декілька робочих процесів із різними показниками MTPD, RTO або RPO, під час визначення вимог до безперервності враховують найбільш вимогливі показники серед відповідних процесів.

6. Залежності та ресурси

У формі зазначаються основні ресурси та залежності, необхідні для функціонування робочих процесів і засобу інформатизації.

Доцільно враховувати:

- державні інформаційні ресурси та реєстри;
- системи електронної взаємодії;
- системи електронної ідентифікації;
- електронні комунікаційні мережі;
- центри обробки даних;
- електроживлення;
- хмарні послуги;
- резервні майданчики;
- резервні копії;
- програмне та апаратне забезпечення;
- персонал;
- постачальників послуг;
- експлуатаційну та технічну документацію.

Для кожної суттєвої залежності зазначаються її власник, тип залежності, рівень залежності, наявність договірних або інших зобов'язань щодо забезпечення доступності та відновлення, а також наслідки її недоступності.

У разі наявності відповідних зобов'язань зазначаються конкретні показники SLA, RTO та/або інші встановлені показники доступності та відновлення.

7. Оцінка стану резервування та відновлення

Під час заповнення форми необхідно відображати фактично реалізовані механізми резервування та відновлення.

Для кожного критичного ресурсу доцільно зазначати:

- що саме резервується;
- де розміщується резерв;
- спосіб резервування або реплікації;
- періодичність резервування;
- строк зберігання резервних копій;
- наявність географічно відокремленої копії;
- застосування immutable або інших механізмів захисту від зміни чи знищення резервних копій;
- спосіб переключення на резервне середовище;
- відповідальну особу.

Необхідно окремо зазначати випадки, коли резервування формально передбачене документацією, але фактично не реалізоване або не перевірене.

У формі зазначаються результати фактично проведених тестувань.

Доцільно враховувати такі сценарії:

- відновлення окремого сервісу;

- відновлення даних із резервної копії;
- відновлення після відмови обладнання;
- переключення на резервне середовище;
- відновлення після втрати основного майданчика;
- відновлення після кіберінциденту;
- комплексне відновлення функціонування засобу інформатизації.

За результатами тестування зазначаються фактичний час відновлення, фактично досягнутий RPO, виявлені проблеми та невиконані дії.

Якщо встановлений RTO не досягнуто, у формі зазначаються причина, вплив та запланований захід щодо усунення невідповідності.

8. Перевірка та актуалізація результатів

До затвердження звіту результати аналізу впливу перевіряються відповідальними посадовими особами структурних підрозділів, які є власниками відповідних робочих процесів, засобів інформатизації та ресурсів.

Результати аналізу впливу переглядаються з періодичністю, визначеною замовником, але не рідше одного разу на рік, а також у разі змін робочих процесів (бізнес-процесів), архітектури засобу інформатизації, його залежностей або інших змін, що можуть вплинути на результати аналізу.

Під час повторного проведення аналізу доцільно порівнювати отримані результати з попередніми для визначення:

- зміни категорії засобу інформатизації;
- зміни MTPD, RTO та RPO;
- зміни рівня резервування;
- виконання запланованих заходів;
- нових ризиків та залежностей;
- фактичного прогресу у забезпеченні безперервності.

Результати аналізу впливу використовуються замовником для планування заходів із забезпечення безперервності функціонування, розвитку резервної інфраструктури, удосконалення резервного копіювання та аварійного відновлення, планування ресурсів і проведення тестувань.

Додаток: Зразок заповнення аналізу впливу порушення безперервності виконання робочих процесів (бізнес-процесів) та оцінювання пов'язаних з ними засобів інформатизації, на 30 арк. в 1 прим.