ITEZ
IT easy

WHITEPAPER · 2026

СТАБІЛЬНІСТЬ І БЕЗПЕКА БІЗНЕСУ

Бізнес, що працює попри все

Практичний посібник для власників і керівників українських компаній: як зберегти роботу під час блекаутів, ударів по інфраструктурі та кібератак.

Безкоштовно для українського бізнесу

itez.com.ua

ЗМІСТ

Що всередині

Документ розрахований приблизно на годину читання; коротке резюме в розділі 1 — на 3 хвилини. Кожен розділ закінчується конкретними діями, а чек-листи в кінці можна роздрукувати й використовувати окремо.

ЧАСТИНА І

01

Зрозуміти

Компанії зупиняються не через брак генератора, а через механізми, про які не знали.

Які загрози реальні саме для українського бізнесу, чому компанії, що «все зробили правильно», однаково зупиняються, і скільки коштує година простою.

РОЗДІЛ
01
Коротко для керівника

> В Україні стійкість — це вже не IT-проєкт і не «страховка на всяк випадок». Це управлінське рішення, яке визначає, чи працюватиме компанія завтра, коли конкуренти стоятимуть.

1. **Криза — це вже базові умови.** Блекаути, удари по інфраструктурі, кібератаки та втрата людей стали регулярними подіями. Плануйте на «коли», а не на «якщо».
2. **Простій має ціну, і її можна порахувати.** Поки вартість години зупинки не названо в гривнях, інвестиції в стійкість здаються витратами. Коли її порахували, вони стають розрахунком.
3. **Стійкість складається з п'яти шарів:** живлення, зв'язок, дані, інфраструктура, кібербезпека. Бізнес ламається через найслабший із них.
4. **План без тренування не працює.** Перевага не в тому, що у вас є план безперервності, а в тому, що команда відпрацювала його за столом і в реальному перемиканні.
5. **Стійкість стає конкурентною перевагою.** Клієнти, іноземні партнери, банки й страховики дедалі частіше запитують: «Що буде з вашим сервісом, якщо…?»
6. **Криза не закінчиться — будуйте режим, а не аварійну реакцію.** Блекаут чи перемикання на резервний канал мають бути рутинною процедурою, а не приводом скликати штаб. Кризовий план вмикається лише тоді, коли ламається сама рутина. Про це — розділ 10.
7. **Найнебезпечніше — не сама загроза.** Найнебезпечніші — резерв, який падає разом з основною системою, і рішення, яке в кризі нікому ухвалити. Про це — розділи 3 і 5.

ШАР 1 Живлення
Автономність критичних систем і контроль пального

ШАР 2 Зв'язок
Незалежні канали з автоматичним перемиканням

ШАР 3 Дані
Незмінні копії поза зоною ризику

ШАР 4 Інфраструктура
Професійний центр обробки даних (ЦОД) і географічний резерв

ШАР 5 Кібербезпека
MFA, оновлення, контроль доступів

ЯДРО Люди і рішення
Кризовий штаб, намір керівника, тригери

Колесо стійкості: п'ять технологічних шарів працюють лише тоді, коли в центрі є люди, які знають, хто і що вирішує.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Запишіть, хто, крім вас, завтра підпише платіж і звітність (розділ 3.4).
- [ ] Перевірте вхід у пошту й банк без мобільного зв'язку і свого телефона: SMS-коди без зв'язку не приходять (розділ 3.2).
- [ ] Порахуйте вартість години простою для одного процесу (розділ 4).

РОЗДІЛ

02

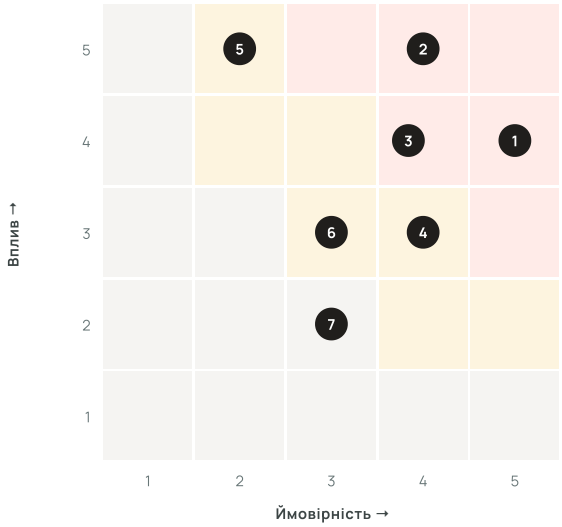
Нова норма: ландшафт загроз для українського бізнесу

> Загрози в Україні комбіновані й одночасні. Удар по енергетиці спричиняє відключення зв'язку, зв'язок впливає на доступ до даних, а все разом б'є по людях. Світові моделі безперервності зазвичай розглядають загрози поодинці. Українська реальність вимагає планувати їхні комбінації.

Карта загроз

Загроза	Як проявляється	Тривалість	Що зупиняється першим	Ризик для МСБ
1 **Енергетичні удари, блекаути**	Графіки, аварійні відключення, багатоденні знеструмлення регіонів	Години — дні	Офіс, серверна, зв'язок операторів	■ Високий
2 **Кібератаки**	Шифрування й знищення даних, витоки, компрометація пошти, атаки через постачальників ПЗ	Дні — тижні	Облікові системи, 1С, пошта, CRM	■ Високий
3 **Кадрові ризики**	Мобілізація, релокація, травми, вигорання	Тижні — постійно	Ключові знання («все знає одна людина»)	■ Високий
4 **Відмова операторів і постачальників**	Збій мобільного оператора, провайдера, SaaS-сервісу	Години — дні	Зв'язок, платежі, логістика	▲ Середній
5 **Удари по ЦОД, вузлах зв'язку, офісах**	Фізичне знищення обладнання, пожежі, заборона доступу	Дні — назавжди	Локальні сервери, документи, обладнання	▲ Середній
6 **Логістика й постачання**	Удари по складах, портах, дорогах	Дні — тижні	Виробництво, торгівля	▲ Середній

Загроза	Як проявляється	Тривалість	Що зупиняється першим	Ризик для МСБ
7 Інформаційні атаки	Фейки про компанію, неправдиві повідомлення про мінування, евакуація відвідувачів	Години — тижні	Торгові зали, офіс, репутація	▲ Середній



Номери точок відповідають рядкам таблиці. Типовий профіль МСБ у центральних регіонах, експертна оцінка ITEZ. Складіть власну матрицю: у прифронтовій громаді чи в компанії без генератора точки зсунуться.

Ланцюгова реакція

Ракетний удар по енергетиці → Блекаут у районі → Базові станції вичерпують батареї → Немає доступу до 1С і хмари → **Зупинка продажів**

Що показали останні роки

У 2025 році CERT-UA опрацювала **5 927 кіберінцидентів**, на 37 % більше, ніж роком раніше.[1] Атаки дедалі частіше йдуть не «в лоб», а через людей і постачальників.

Реєстри Мін'юсту, грудень 2024: угоди зупинилися по всій країні

19 грудня 2024 року кібератака, яку СБУ пов'язує з ГРУ РФ, вивела з ладу близько 60 державних реєстрів. Нотаріуси не могли посвідчувати угоди, зупинилися реєстрація компаній та операції з нерухомістю. Дані вціліли: реєстри відновили з холодних резервних копій, що зберігалися в кількох локаціях. Але повне відновлення тривало місяць, до 20 січня 2025 року.[2]

Урок: копія, недосяжна для зловмисника, рятує дані, а швидкість повернення визначає лише перевірене відновлення. І ваш бізнес залежить від державних реєстрів так само, як від власних серверів (плейбук — у розділі 9).

«Укрзалізниця», березень 2025: робота на папері

Після масштабної кібератаки 23 березня 2025 року онлайн-продаж квитків не працював майже чотири доби. Потяги курсували за графіком: компанія перейшла на резервні протоколи, підготовлені після попередніх атак, і продавала квитки в касах. Вантажні перевезення перейшли на паперові документи.[3]

Урок: заздалегідь підготовлений ручний режим тримає бізнес, поки IT відновлюється. Але все, що зроблено на папері, потім доведеться внести в систему.

«Київстар», грудень 2023: оператор як єдина точка відмови

Кібератака на найбільшого мобільного оператора країни (близько 24 млн абонентів) залишила мільйони людей і компаній без зв'язку та мобільного інтернету. За даними СБУ, зловмисники перебували в мережі оператора щонайменше з травня 2023 року.[4]

Урок: залежність від одного оператора зв'язку — це єдина точка відмови вашого бізнесу.

Блекаути: вплив на 80 % компаній

За опитуванням Європейської Бізнес Асоціації (січень 2026), відключення електроенергії вплинули на роботу 80 % компаній. Найчастіші наслідки: зростання собівартості (61 %), зміна графіків роботи (58 %), падіння обсягів виробництва чи послуг (50 %) і простої (48 %).[5]

Уроки інших країн

Естонія у 2017 році створила першу у світі «цифрову амбасаду»: копії ключових державних реєстрів зберігаються у ЦОД у Люксембурзі.[6] Україна за тиждень до вторгнення ухвалила закон про хмарні послуги,[7] і в перші дні війни понад 10 ПБ даних міністерств, реєстрів і компаній перенесли в хмари за кордоном.[8] **Урок:** критичні дані мають копію поза зоною ризику, а швидкі рішення можливі, якщо заздалегідь відомо, що рятувати.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Проведіть 60-хвилинну сесію з керівниками: складіть власну карту загроз і оцініть кожну за шкалою від 1 до 5 (ймовірність × вплив).
- [ ] Позначте 3 комбіновані сценарії, наприклад «блекаут 48 год + збій мобільного оператора».

РОЗДІЛ

03

Невидима частина айсберга

> Більшість компаній, які «все зробили правильно» (генератор, Starlink, хмарний бекап), падають не через брак заходів. Вони падають через механізми, про існування яких не підозрювали. Цей розділ — про питання, які навіть не спадає на думку поставити.

3.1 Чотири приховані концепції

1. Корельовані відмови: резерв, який падає разом з основною системою

Резерв має сенс, лише коли він не відмовляє одночасно з основною системою. Інженери називають це відмовою зі спільної причини (common-mode failure). Популярні поради кажуть «майте резерв», але рідко додають: «перевірте, що резерв незалежний». Типові приклади фальшивого резервування:

- Starlink і оптичний роутер живляться від одного інвертора;

- два «різні» провайдери заходять у будинок одним кабельним колектором;
- основний і «резервний» SaaS працюють в одному регіоні одного хмарного провайдера.

Найглибша спільна точка відмови — **облікові записи**. Один скомпрометований акаунт адміністратора відкриває і робочі системи, і всі резервні копії. Саме так програми-вимагачі знищують бекапи ще до шифрування.

> ■ ІНСТРУМЕНТ
>
> **Аудит спільних залежностей.** Для кожної пари «основна система + резерв» запитайте: що в них спільного? Живлення, кабель, будівля, місто, обліковий запис, постачальник, людина, яка знає, як це працює. Кожна спільна відповідь — прихована єдина точка відмови.

2. Нормалізація відхилень і дрейф до відмови

Діана Воган, досліджуючи катастрофу шатла «Челленджер», описала **нормалізацію відхилень**: організація звикає до маленьких порушень, бо «минулого разу нічого не сталося». Сідні Деккер назвав це **дрейфом до відмови**. На п'ятому році великої війни це головний невидимий ризик українського бізнесу. «Тимчасові» рішення 2022 року стали постійними, генератор працює без ТО, бо «ще тягне», тест відновлення відкладають. «Адмін знає, як», але адмін уже інший. Кожне відхилення окремо нешкідливе, але разом вони роблять реальну стійкість значно нижчою за ту, яку бачить керівник.

> ■ ІНСТРУМЕНТИ
>
> Журнал тимчасових рішень (у кожного обхідного шляху є власник і дата, коли його прибирають або узаконюють); метрика «днів від останнього реального тесту» для кожної критичної системи; погляд «свіжими очима» щонайменше раз на рік.

3. Прихований хвіст відновлення

Час відновлення зазвичай міряють до моменту, коли сервер знову працює. Але бізнес повертається до норми пізніше: треба звірити дані, що розійшлися, обробити накопичені замовлення й платежі, повторно ввести документи і відновити довіру клієнтів. До того ж **повернення — найризикованіша фаза кризи**:

- одночасне ввімкнення всього обладнання після блекауту спричиняє перевантаження й пошкодження дисків;
- бекап, створений після проникнення зловмисника, відновлює і його: медіанний час прихованої присутності атакувальника у 2025 році — 14 днів;[9]
- команда виснажена, тож помилки найімовірніші саме зараз.

> ■ ІНСТРУМЕНТИ
>
> Плейбук повернення з черговістю ввімкнення систем; «карантинне» відновлення (спершу в ізольоване середовище); метрика **«час до повної бізнес-норми»** на додачу до технічного часу відновлення.

4. Прихована деградація резерву

Генератори, інвертори й акумулятори, які врятували компанію минулої зими, вважають перевіреними. Насправді вони розраховані на епізодичну роботу, а не на тижні щоденних циклів. Тому новий багатоденний блекаут часто починається з каскадної відмови «перевіреного» заліза.

- Дизель-генератору потрібна заміна мастила й фільтрів приблизно кожні 250 мотогодин або раз на рік. Щоденний блекаут-сезон вичерпує цей інтервал за кілька тижнів.[10]
- Якісні LiFePO4-акумулятори витримують кілька тисяч циклів при розряді на 80 %, дешевші — помітно менше.[11] Зима з щоденними відключеннями — це сотні циклів.

■ ІНСТРУМЕНТ

Життєвий цикл резерву. Журнал для кожного вузла: дата встановлення, мотогодини або цикли, дата ТО, результат навантажувального тесту, планова дата заміни. Бюджет на заміну **до** відмови і тест під реальним навантаженням перед кожним сезоном. Шаблон — чек-лист 3 у розділі 14.

3.2 Сліпі зони: пастки, про які не підозрюють

Ці помилки виникають не через недбалість, а через те, що людина не знає про існування механізму, правила чи інструменту.

Сліпа зона	Механізм, про який не знають	Що зробити
КЕП і право підпису	Директор мобілізований, поранений або поза зв'язком, і ніхто не може підписати платіжки, податкову звітність, договори. Бізнес «живий», але юридично паралізований	Друга особа з правом підпису, довіреності, КЕП заступника в банку й податковій, перевірка статуту
Війна як виключення в страхуванні	З 2023 року ринок Lloyd's вимагає, щоб поліси кіберстрахування містили чіткі виключення для кібератак, пов'язаних з державами. З 2025 року покриття таких атак можливе лише окремим, прямо прописаним продуктом.[12] Майнові поліси часто не покривають збитки від обстрілів	Прочитати розділ «Виключення» в кожному полісі, окремо з'ясувати покриття воєнних ризиків
Форс-мажор не спрацьовує автоматично	Посилання на «війну» саме по собі не звільняє від відповідальності: треба довести зв'язок з конкретним зобов'язанням і вчасно повідомити контрагента. SLA з вашими клієнтами часто взагалі не мають винятків	Переглянути договори: форс-мажорні застереження, SLA, строки й порядок повідомлення
MFA проти кризи	SMS-коди не приходять без мобільного зв'язку. Другий фактор прив'язаний до телефона працівника, який звільнився чи мобілізований. Захист блокує самих власників	Апаратні ключі або застосунки-автентифікатори, коди відновлення в сейфі, 1–2 аварійні акаунти
Домен і DNS	Домен зареєстровано на особисту пошту колишнього працівника чи підрядника, а продовження прив'язане до неактивної картки. Втрата домену означає втрату пошти, сайту і входу в усі сервіси	Реєстр цифрових активів: хто власник домену, акаунта реєстратора, DNS, хмар, Starlink
Блокування SaaS	Картка не пройшла, акаунт заблоковано за підозрілу активність: сервіс зупиняється, а дані з часом видаляються. Microsoft 365 і Google Workspace працюють за моделлю спільної відповідальності й не є повноцінним бекапом	Незалежний бекап SaaS-даних, резервна картка, моніторинг оплат
Ключі від бекапів	Бекап зашифровано правильно, але ключ лежить на тому самому сервері, який зашифрували зловмисники, або його знає одна людина	Ключі й паролі від бекапів зберігаються окремо: офлайн і в двох довірених осіб
Фізика автономного живлення	Дизель без стабілізатора зберігає якість приблизно 6–12 місяців.[13] Генератор, що довго працює з навантаженням менше 30 %, «замулюється» (wet stacking).'[14] LiFePO4-акумулятори не можна заряджати нижче 0 °C.'[15]	Ротація пального, ТО і навантажувальні тести генератора, акумулятори в опалюваному приміщенні

3.3 Контрінтуїтивна правда

Парадокс 1. Більше резервування може знизити надійність

Кожен новий елемент додає складності, а складність сама стає джерелом аварій. Про це писали Чарльз Перроу («Normal Accidents») і Річард Кук («How Complex Systems Fail»). У бізнесі це виглядає так. Автоматичне перемикання, яке ніколи не тестували, створює дві «головні» копії системи з різними даними. «Розумний» роутер постійно перемикає канали й рве з'єднання з обліковою системою. П'ять видів бекапу, у яких ніхто не розбирається, гірші за один зрозумілий. Ручне перемикання, яке команда виконує за 10 хвилин навіть уночі під час тривоги, надійніше за автоматику, якої ніхто не розуміє.

Не додавайте резерв, який не будете регулярно тестувати.

Парадокс 2. Неефективність — це актив

Поставки «точно вчасно» і 100 % завантаження людей роблять бізнес дешевшим у мирний час і крихким у кризі (Том ДеМарко, «Slack»). Команда без вільної години не має часу на кризу, склад без запасу не переживе тиждень зупинки логістики, бюджет без резерву не дозволить за день купити генератор. Стійкі компанії свідомо тримають запас часу, товарів і грошей як **ціну опціону на виживання**.

Висновок: плануйте наслідки, а не сценарії. Не треба вгадувати, що станеться. Досить плану на п'ять наслідків, до яких зводиться будь-яка криза: **втрата приміщення, людей, IT, ключового постачальника, грошей.** Такий план працює навіть для загроз, яких ще не існує.

3.4 Питання, яке ви мали поставити

«Що саме я готовий втратити, і хто ухвалить це рішення, якщо мене не буде поруч?»

Більшість керівників питають, як захистити все. Досвідчені кризові менеджери питають, що вони свідомо віддадуть, щоб зберегти головне, і як компанія ухвалюватиме рішення без них.

Стійкість — це заздалегідь вирішене сортування

У справжній кризі ресурсів не вистачить на все: пального, людей, уваги, грошей, годин роботи інженерів. Компанії, які виживають, у спокійний час затверджують:

- **Ієрархію пріоритетів:** люди → критичні дані → ключові клієнти й контракти → грошовий потік → усе інше.
- **Стоп-лист:** продукти, напрями, проєкти й витрати, які зупиняються першими, щоб звільнити ресурси.
- **Мінімально життєздатну операцію:** з яким найменшим набором функцій компанія ще заробляє.

Без цього в кризі все здається пріоритетом, ресурс розмазується, і компанія втрачає головне, рятуючи другорядне.

Тригери замість нарад

У кризі рішення найгірше ухвалювати саме тоді, коли його треба ухвалити: тиск, брак інформації та втома спотворюють судження. Тому стійкі організації ухвалюють рішення заздалегідь і прив'язують їх до вимірюваних порогів. Це «договір Одіссея»: герой наказав прив'язати себе до щогли, поки ще мав ясну голову.

Поріг	Рішення, що вмикається автоматично	Хто виконує
Відключення світла понад 6 год	Офіс переходить у скорочений режим, персонал працює вдома або в «пунктах незламності»	Операційний директор
Зв'язку з керівником немає понад 4 год	Заступник отримує повноваження кризового лідера	Заступник
Резерву менше ніж на 8 тижнів (до 10 людей — 4, понад 50 — 12 тижнів)	Інвестиції за списком заморожуються, вмикається стоп-лист	Фінансовий директор
Підтверджено злам акаунта адміністратора	Ізоляція систем без погодження, дзвінок IT-партнеру	Відповідальний за IT
Основна система недоступна довше за допустимий час	Перемикання на резервний майданчик	IT + операційний директор

Тригери долають три головні когнітивні пастки кризи: **параліч аналізу** («ще трохи почекаємо на інформацію»), **ефект невиправданих витрат** («ми вже стільки вклали в основний офіс») і **звикання до поступового погіршення** (синдром «жаби в окропі»). Крім того, вони дають людям на місцях право діяти без керівника, а отже, рішення ухвалюють швидше, ніж розвивається криза.

Наступність влади — фізично, а не на папері

Питання «хто ухвалить рішення» в Україні буквальне. Мобілізація, поранення, відсутність зв'язку — реальні сценарії для власника бізнесу.

> ● ПИТАННЯ-ТЕСТ
>
> «Якщо мене не буде 30 днів без зв'язку, чи отримають люди зарплату, чи отримають клієнти сервіс і чи не зупиниться компанія юридично?» Якщо відповідь «не впевнений», це і є найважливіша точка входу в стійкість, важливіша за будь-який генератор.

Мінімальний набір входить у кроки на 30 днів (розділ 13). Це заступник з реальними повноваженнями, друга особа з КЕП і доступом до банку, реєстр цифрових активів і «лист на випадок моєї відсутності».

3.5 Коли падає екосистема

Найпідступніші сценарії — ті, де вся ваша інфраструктура ціла: світло є, сервери працюють. Але ключові клієнти, які дають 80 % виручки, до блекауту не готові. Вони зупиняються й припиняють платити. Або зупиняється єдиний перевізник, здатний возити ваш вантаж, або державний реєстр, без якого не закрити угоду. Або платформа-посередник: маркетплейс блокує акаунт, служба доставки стоїть, платіжний провайдер заморожує виплати. Ви інвестували в автономність, але компанія гине, бо не вижила екосистема навколо неї.

Карта залежностей: колір показує типовий рівень ризику для МСБ. Для своєї компанії позначте кожен вузол за двома питаннями: скільки у вас альтернатив і чи є в цього партнера план безперервності.

Стійкість ваших клієнтів — це стійкість вашої виручки. Проте плани безперервності її майже ніколи не враховують.

▲ ЯК ПІДГОТУВАТИСЯ

Рахуйте частку трьох найбільших клієнтів у виручці та встановіть для себе поріг концентрації; перед підписанням річних контрактів питайте ключових клієнтів і перевізників про їхній план безперервності; для клієнтів з низькою стійкістю — передоплата, гарантії або коротші строки оплати; альтернативні перевізники з договором заздалегідь; якщо продаєте через платформи — другий канал продажів і доставки, власна база клієнтів і резерв на час заморожених виплат; географічна диверсифікація клієнтів, зокрема експорт.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Проведіть аудит спільних залежностей для трьох найважливіших пар «основна система + резерв».
- [ ] Заведіть журнал тимчасових рішень і журнал життєвого циклу резерву.
- [ ] Затвердьте стоп-лист, тригери рішень і заступника з реальними повноваженнями.

РОЗДІЛ

04

Ціна простою: мова грошей для керівника

Інвестиції в стійкість обґрунтовуються не страхом, а арифметикою. Вартість години простою — перша цифра, яку має знати власник.

Прямі втрати
Втрачена виручка, штрафи за SLA, зіпсована продукція, оплата понаднормових.

Непрямі втрати
Зарплата працівників, які простоюють, відтік клієнтів, штрафи регуляторів.

Відкладені втрати
Репутація, втрата тендерів і партнерів, дорожче фінансування та страхування.

Приховані втрати
Вони зазвичай у рази перевищують видимі: аварійні закупівлі, переробка, повторне введення даних.[16]

Проста формула для МСБ

Вартість години простою = (річна виручка ÷ робочі години на рік) × частка виручки, яка зупиняється (через IT, світло чи доступ до приміщення)
+ кількість працівників, що простоюють × середня вартість години праці
+ запаси, що псуються або втрачають цінність, за годину
+ прямі штрафи й витрати на відновлення за годину

Приклад: компанія на 35 людей

Складова	Розрахунок	грн за годину
Виручка, яка зупиняється без облікової системи	42 млн ÷ 2 000 год × 60 %	12 600
Працівники, що простоюють	20 осіб × 220 грн	4 400
Запаси, що псуються	у цієї компанії немає	0
Штрафи, понаднормові, відновлення	оцінка	2 000
Разом		**19 000**

60 % — продажі через облікову систему; 220 грн — година праці з ЄСВ. У магазині чи кав'ярні в рядку «запаси» буде товар, що псується без світла.

Три робочі дні простою (24 год) коштують 456 000 грн, а якщо такий збій імовірний двічі на рік — близько 0,9 млн грн на рік. Захід, що запобігає збою й коштує менше, окупається (розділ 10).

Простої дорожчають. Компанії Global 2000 втрачають від них $600 млрд на рік, на 50 % більше, ніж два роки тому,[17] а компанії до 250 працівників через кіберінциденти — ~$52 000 і ~32 год простою на рік.[18]

Аналіз впливу на бізнес за 2 години

1. Перелічіть 10–15 бізнес-процесів: продажі, відвантаження, бухгалтерія, підтримка тощо.
2. Для кожного визначте допустимий час простою (**RTO**), допустимі втрати даних (**RPO**) і вартість години зупинки.
3. Розподіліть процеси на критичні (години), важливі (дні) й відкладені (тижні).
4. Знайдіть залежності кожного критичного процесу: IT, світло, приміщення, постачальники.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Порахуйте вартість години простою для трьох ключових процесів за прикладом вище і порівняйте її з річним бюджетом на стійкість. Детальніше — у статті «Вартість простою бізнесу за годину».

ЧАСТИНА II

02

Підготуватися

Технології купують час. Бізнес рятують люди, які знають, хто вирішує.

Хто і як ухвалює рішення, коли зв'язку немає. П'ять технологічних шарів. План безперервності на кілька сторінок. Гроші, право і держава у воєнний час.

РОЗДІЛ

05

Кризове управління: люди і рішення

> Технології лише купують час. Бізнес рятують люди, які знають, хто ухвалює рішення, як зв'язатися одне з одним і що робити в перші години.

Кризовий штаб

- **Склад:** керівник (лідер кризи), операційний директор, фінансист, відповідальний за IT (внутрішній або аутсорс), відповідальний за комунікації, HR.
- **Правило заміщення:** у кожної ролі є дублер. Якщо лідер недоступний понад визначений час, повноваження автоматично переходять до заступника.
- **Делеговані повноваження:** заздалегідь визначені ліміти рішень без погодження, наприклад витрати на пальне, оренду чи обладнання, перемикання на резервний ЦОД.
- **Коли скликається:** лише на рівні «криза» за шкалою серйозності (розділ 10). Штаб — не постійний орган управління.
- **Точки збору:** основна, резервна й віртуальна (месенджер поза корпоративною інфраструктурою).

Хто за що відповідає в штабі

Рішення	Лідер кризи	Операційний директор	Фінансист	IT	Комунікації	HR
Скликати штаб, оголосити рівень кризи	A	R	I	C	I	I
Безпека людей, укриття, евакуація	A	R	I	I	C	R
Ізоляція систем, перехід на резерв	A	C	I	R	I	–
Витрати понад делегований ліміт	A	C	R	C	–	–
Повідомлення клієнтам і публічні заяви	A	C	–	C	R	I
Графік змін, віддалена робота, підтримка людей	I	A	C	C	I	R

A ухвалює і відповідає (один на рядок) · R виконує · C радиться · I отримує інформацію

Зв'язок, коли все лежить

- Дерево оповіщення: хто кого повідомляє, яким каналом і в який строк, окремо — люди в дорозі, на виїзді чи на відкритих ділянках (розділ 11).
- **План PACE** з військового зв'язку: *основний*, *альтернативний*, *резервний* і *аварійний* канали, які не залежать один від одного. Наприклад: корпоративний месенджер → мобільний зв'язок іншого оператора → супутниковий зв'язок штабу → заздалегідь визначене місце й час зустрічі. Кожен знає, коли переходити на наступний рівень.[19]

- Роздрукований список контактів (працівники, постачальники, IT-підрядник, банк, страховик) у кожного члена штабу.
- Правило «тиші»: якщо зв'язку немає довше за визначений час, кожен діє за заздалегідь узгодженим сценарієм.

Перші 72 години

0–1 год	1–4 год	4–24 год	24–72 год	72+ год
Безпека людей Укриття, перевірка стану працівників, зупинка небезпечних процесів.	**Оцінка ситуації** Що не працює і що під загрозою, скликання штабу, перше повідомлення команді.	**Стабілізація** Активація планів безперервності й відновлення, перехід на резервні ресурси, повідомлення клієнтам.	**Мінімально життєздатна операція** Робота критичних процесів, контроль ліквідності, регулярні оновлення стану.	**Режим «норми воєнного часу»** Перехід до рутинних процедур, розбір уроків, оновлення планів. Штаб розпускається за правилом деескалації (розділ 10).

Намір керівника: компас замість інструкції

Гельмут фон Мольтке-старший зауважив, що жоден план не можна розрахувати далі першого зіткнення з противником.[20] Для бізнесу це означає: найкращий плейбук стає марним, якщо в перші хвилини блекауту чи атаки зник зв'язок із керівником. Тому армії використовують **намір командира** (commander's intent): коротке формулювання мети, яке дозволяє діяти без додаткових наказів, навіть коли все йде не за планом.[21] Власник заздалегідь доносить до команди три речі:

1 · МЕТА	2 · ЧЕРВОНІ ЛІНІЇ	3 · СВОБОДА ДІЙ
Що для нас перемога? *Не «відновіть сервери за інструкцією», а «10 ключових клієнтів зі списку А отримали замовлення до кінця дня».*	**Чого не можна робити?** *Не платимо викуп хакерам; не ризикуємо людьми заради обладнання; не вимикаємо автентифікацію навіть заради швидкості.*	**Що можна без мене?** *До 100 000 грн з рахунку компанії на оренду генераторів, транспорту чи потужностей у ЦОД без погоджень.*

Основна система впала, резервний план не спрацював, керівника немає на зв'язку. Відповідальний за IT чи керівник складу не чекає: він знає намір. Він орендує чужий сервер, переводить операції в ручний режим або наймає сторонніх кур'єрів — у межах червоних ліній і заради головного: мінімально життєздатної операції. Порожній бланк — шаблон И у розділі 14.

Завдання лідера — не написати ідеальну інструкцію для хаосу, а дати команді компас і повноваження діяти без нього.

Практики екстремальних галузей

Армія, авіація, медицина катастроф, атомна енергетика й біржі десятиліттями вчаться ухвалювати рішення там, де помилка коштує життів або мільярдів. Жодна з їхніх практик не вимагає бюджету.

- **Дії з пам'яті (авіація).** Перші дії в аварії пілоти виконують без чек-листа.[22] Для бізнесу: 3 дії першої хвилини інциденту, які кожен знає напам'ять, — ізолювати пристрій, повідомити за деревом оповіщення, зафіксувати час.

- **Довіра до експертизи (атомна енергетика, авіаносці).** У кризі рішення ухвалює той, хто найбільше знає про проблему, а не найвищий за посадою.[23] Для бізнесу: інженер, який бачить аварію, ізолює систему сам у межах наміру керівника.
- **Автоматичні вимикачі (біржі).** Якщо S&P 500 за день падає на 7 %, 13 % або 20 %, торги зупиняються автоматично.[24] Для бізнесу: фінансові тригери на кшталт «резерв нижче 8 тижнів → стоп-лист» (розділ 3.4).
- **Розбір після дій (армія).** Без пошуку винних: що мало статися, що сталося, чому є різниця, що робимо наступного разу.[25] Для бізнесу: 30 хвилин після кожного інциденту рівня 1 і вище.

Тріаж процесів: чотири кольори

Коли постраждалих більше, ніж рятувальників, медики катастроф за кількома ознаками відносять кожного до однієї з чотирьох категорій і рятують тих, кого можна врятувати зараз.[26] Бізнесу варто розподілити процеси так само — заздалегідь.

Червоний
Рятуємо негайно: без цього компанія втрачає гроші чи клієнтів за години. Продажі, відвантаження, розрахунки.

Жовтий
Можна відкласти на дні без критичних втрат. Бухгалтерія поза звітним періодом, закупівлі.

Зелений
Почекає тижні. Маркетинг, внутрішні проєкти, навчання.

Чорний
Свідомо зупиняємо, щоб звільнити людей і ресурси. Це і є стоп-лист.

Люди як критична інфраструктура

- **«Все знає одна людина»:** знайдіть знання, які має лише один працівник (паролі, доступи, «як працює 1С»), і задокументуйте їх. Мета — щонайменше двоє людей на кожну критичну функцію.
- **Розподілена команда:** віддалена робота як стандартний режим, співробітники в різних районах або містах; сценарії релокації (часткова, повна, тимчасова) з бюджетом (розділ 11).
- **Психологічна стійкість:** реалістичні очікування щодо продуктивності й ротація в кризових ролях, щоб запобігти вигоранню.

Кадри у війні: бронювання, мобілізовані, ветерани

Брак людей став головною перешкодою для бізнесу: у серпні 2026 року на нього скаржилися 69 % підприємств, а наймати в найближчі місяці планують лише 2,6 %.[27] Для малої компанії мобілізація одного ключового фахівця може зупинити цілий напрям.

- **Бронювання доступне лише критичним підприємствам.** Держава ставить поріг зарплати і для забронюваного працівника, і для середньої зарплати на підприємстві, обмежує частку військовозобов'язаних, яких можна забронювати, і вимагає періодично підтверджувати статус критичності. Пороги й строки — у додатку.
- **За мобілізованим працівником зберігаються місце роботи й посада,** але з 19 липня 2022 року роботодавець не зобов'язаний зберігати йому середній заробіток. Виняток — поранені на лікуванні, полонені та зниклі безвісти: за ними середній заробіток зберігається.[28]
- **Ветерани — кадровий резерв, який держава допомагає наймати.** За працевлаштування учасника бойових дій через центр зайнятості роботодавець отримує часткову компенсацію зарплати, якщо не звільнить працівника раніше визначеного строку (умови — у додатку).

▲ ЯК ПІДГОТУВАТИСЯ

Перевірте, чи відповідає компанія критеріям критичності, і подайте документи через «Дію» заздалегідь, а не після повістки; ведіть облік військовозобов'язаних і строків їхніх відстрочок; для кожної ключової ролі визначте, хто її підхопить; оформлюйте найм ветеранів через центр зайнятості, щоб отримати компенсацію. Звіряйте норми з юристом.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Призначте склад кризового штабу і дублера для кожної ролі.
- [ ] Напишіть намір керівника на одну сторінку (шаблон И у розділі 14) і обговоріть його з командою.
- [ ] Розподіліть процеси за чотирма кольорами тріажу і погодьте план зв'язку PACE.

РОЗДІЛ

06

Технологічна стійкість: п'ять шарів

> Бізнес зупиняється через найслабший шар. Немає сенсу купувати Starlink, якщо дані зберігаються на одному сервері в офісі, і навпаки.

ПИТАННЯ-ТЕСТ ДЛЯ КОЖНОГО ШАРУ

ШАР 5	Кібербезпека	Чи ввімкнено MFA для всіх, хто має доступ до пошти й фінансів? Так чи ні?
ШАР 4	Інфраструктура	Якщо офіс стане недоступним сьогодні, звідки й за скільки годин запрацюють критичні системи?
ШАР 3	Дані	Коли ми востаннє повністю відновлювали критичну систему з бекапу, і скільки це зайняло?
ШАР 2	Зв'язок	Якщо зникне основний провайдер, скільки хвилин мине до відновлення роботи, і хто про це дізнається?
ШАР 1	Живлення	Скільки годин наш бізнес працює без міської мережі, і хто це перевіряв востаннє?

Відповідь без числа або імені — сигнал, що шар не перевірено.

Шар 1. Живлення

- Розділіть навантаження на три групи: критичне (сервери, мережа, каса), важливе (робочі місця), комфорт.
- Для офісу: гібридні інвертори й LiFePO4-акумулятори, для тривалих відключень — генератор.
- Генератор підбирають з урахуванням пускових струмів і запасу потужності, але без хронічного недовантаження.

- Пальне: запас на кілька діб, ротація, договір з постачальником. Для заправлення генератора дозволено зберігати до 2 000 л на кожному об'єкті без ліцензії, понад цей обсяг подається декларація.[29]
- **Принцип:** замість того щоб живити весь офіс, винесіть критичні системи туди, де живлення — профільна задача, тобто в ЦОД з резервуванням або в хмару.
- **Тепло — окремий ризик.** У січні 2026 року після атак на енергосистему в Києві без опалення лишалося до 6 тис. будинків, і відновлення тривало тижнями.[30] У холодному приміщенні рвуться труби, на техніці з'являється конденсат, а люди не можуть працювати. Домовтеся з власником будівлі, хто зливає воду з системи опалення під час тривалої аварії; для серверної чи складу передбачте резервний обігрів, розрахований на ваш генератор, і датчик температури з оповіщенням.

Читайте детальніше: Як підготувати бізнес до відключень світла та інтернету

Шар 2. Зв'язок

- Щонайменше два канали різної фізичної природи: оптика (бажано GPON, яка менше залежить від живлення проміжних вузлів) і супутник або мобільний зв'язок.
- Автоматичне перемикання з перевіркою доступності реальних сервісів, а не лише наявності з'єднання.
- Базові станції мобільних операторів мають обмежену автономність, тому мобільний інтернет не є надійним резервом під час тривалого блекауту.
- Для віддаленого доступу до офісу через супутник чи мобільний зв'язок потрібна окрема архітектура, наприклад VPN через хмарний вузол.
- Моніторинг каналів і сповіщення відповідальним.

Читайте детальніше: Резервний інтернет для офісу: Multi-WAN і Starlink

Шар 3. Дані

- Синхронізація (Google Drive, OneDrive) не є бекапом: зашифровані чи видалені файли синхронізуються так само, як і звичайні.
- Правило **3-2-1-1-0**: три копії, два типи носіїв, одна за межами офісу чи країни, одна незмінна або ізольована, нуль помилок під час тестового відновлення.
- Частоту копіювання визначає допустимий обсяг втрат даних (RPO), а швидкість відновлення — допустимий час простою (RTO).
- Регулярне тестове відновлення — єдиний доказ того, що бекап справді існує.
- **Особливо чутливі дані** — про здоров'я, фінанси клієнтів, дітей, біометрію — є в будь-якій компанії: у кадрах, бухгалтерії, клієнтській базі. Зберігайте їх окремо, зашифрованими й з мінімальним колом доступу; заздалегідь визначте, хто діє при витоку і кого повідомляє. Вимоги до повідомлення уточніть з юристом, для партнерів з ЄС діє GDPR.

Читайте детальніше: Резервне копіювання даних: посібник з кібербезпеки

Шар 4. Інфраструктура та географія

- Серверна в офісі — найвразливіший варіант: живлення, фізичний доступ, удари, вилучення обладнання.
- **Гібридна модель:** робочі системи в професійному ЦОД в Україні (мала затримка, оплата в гривні, українська юрисдикція) і резервні копії або репліка в ЄС.
- Не тримайте основну систему й резерв в одному місті або енергорайоні.
- Шифрування дисків захищає дані на випадок фізичного вилучення або крадіжки обладнання.

- Відновлення як сервіс (DRaaS) дає «резервний офіс для IT» без власних капітальних витрат.
- Читайте SLA в годинах: 99,9 % — це до 8 год 46 хв простою на рік, 99,99 % — до 53 хв.

Все в офісі

Стійкість

Капітальні витрати
Високі: сервери, ДБЖ, генератор

Відновлення після втрати офісу
Тижні, якщо копії теж в офісі

ЦОД в Україні

Стійкість

Капітальні витрати
Низькі: оренда або колокація

Відновлення після втрати офісу
Години: працівники підключаються з будь-якого місця

Лише хмарні сервіси

Стійкість

Капітальні витрати
Мінімальні: підписки на SaaS

Відновлення після втрати офісу
Години, якщо є незалежний бекап SaaS-даних (розділ 3.2)

Гібрид Україна + ЄС

Стійкість

Капітальні витрати
Низькі, операційні — помірні

Відновлення після втрати ЦОД
Від хвилин до годин, залежно від реплікації

Шкала стійкості — експертна оцінка ITEZ за трьома ознаками: чи переживуть системи втрату офісу, чи є копія в іншому місті чи країні, як швидко можна відновитися.

Читайте детальніше: Сервери в Україні чи в Європі: де дані безпечніші

Шар 5. Кібербезпека

- **Базова гігієна, що закриває більшість атак:** багатофакторна автентифікація (MFA) скрізь, менеджер паролів, автоматичні оновлення, захист кінцевих пристроїв (EDR).
- Принцип найменших привілеїв: бухгалтер не має прав адміністратора, адміністратор має окремий обліковий запис для щоденної роботи.
- Навчання працівників розпізнавати фішинг, регулярні тренувальні розсилки.
- Контроль постачальників: хто з підрядників має віддалений доступ і як його відкликати. Атаки дедалі частіше заходять саме через підрядників і оновлення стороннього ПЗ.
- Сегментація мережі: гостьовий Wi-Fi, камери та «розумні» пристрої відокремлені від облікових систем.
- Журнали подій зберігаються поза досяжністю зловмисника.

Читайте детальніше: Як захистити малий бізнес від кібератак

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Дайте відповідь на питання-тест кожного з п'яти шарів і запишіть найслабший.
- [ ] Перевірте, що резервний канал зв'язку не має спільних точок відмови з основним.
- [ ] Відновіть одну критичну систему з бекапу і заміряйте, скільки це зайняло.

РОЗДІЛ

07

Плани безперервності без бюрократії

> План на 200 сторінок ніхто не прочитає під час обстрілу. План на 5 сторінок, відпрацьований двічі на рік, врятує компанію.

BCP — план безперервності бізнесу

Відповідає на питання, як бізнес продовжує працювати: процеси, люди, клієнти.

DRP — план відновлення IT

Відповідає на питання, як відновити сервери, дані й доступи. DRP — частина BCP, а не його заміна.

Шість кроків до робочого плану

1. Призначте власника плану з керівництва, а не з IT.
2. Проведіть аналіз впливу на бізнес і оцінку ризиків (розділи 2 і 4).
3. Оберіть стратегію відновлення для кожного критичного процесу.
4. Напишіть плейбуки на одну сторінку для кожного сценарію.
5. Навчіть людей і протестуйте план.
6. Переглядайте щонайменше раз на рік і після кожного інциденту.

Стратегії відновлення IT

Стратегія	Час відновлення	Вартість	Кому підходить
Холодний резерв	Дні	Низька	Некритичні системи: є бекапи, обладнання готують за потреби
Теплий резерв	Години	Середня	Більшість МСБ для 1С, CRM і файлів: інфраструктура підготовлена, дані синхронізуються періодично
Гарячий резерв	Хвилини	Висока	Інтернет-магазини, фінанси, сервіси 24/7: реплікація в реальному часі й автоматичне перемикання
DRaaS (відновлення як сервіс)	Від хвилин до годин	Підписка	МСБ без власного резервного майданчика

Тестування: сходинки зрілості

1. **Паперовий огляд:** чи актуальні контакти, паролі, схеми.
2. **Настільна вправа:** 2 години, штаб розбирає сценарій «блекаут 48 год + атака на пошту».
3. **Технічний тест:** відновлення системи з бекапу на окремій інфраструктурі.
4. **Повне перемикання:** реальна робота з резервного майданчика.

Правило доступності плану

- План зберігається офлайн: роздруківка в штабі, копія на захищеному носії, копія в хмарі поза корпоративною інфраструктурою.
- Паролі аварійного доступу лежать у запечатаному конверті в сейфі або в менеджері паролів з функцією аварійного доступу.

Читайте детальніше: План безперервності бізнесу (BCP) · План відновлення IT-систем (DRP)

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Складіть план безперервності на одну сторінку (шаблон Д у розділі 14).
- [ ] Проведіть 90-хвилинну настільну вправу за одним сценарієм.
- [ ] Покладіть друковану копію плану й аварійні паролі туди, де вони доступні без офісу й мережі.

РОЗДІЛ

08

Гроші, право і держава

> Компанія може мати ідеальне IT, але зупинитися через брак грошей, одного постачальника, новий податок чи правило, про яке власник не знав. У воєнний час держава — не лише регулятор, а й окремий фактор ризику і джерело можливостей.

Фінансова стійкість

- Резерв ліквідності на кілька місяців фіксованих витрат. Поріг, нижче якого вмикається стоп-лист, визначте заздалегідь (див. розділ 3.4).
- Рахунки щонайменше у двох банках різних груп і мобільний банкінг на кількох пристроях, щоб платити без офісного інтернету.
- Кредитні лінії відкривайте заздалегідь, а не під час кризи.
- Критичні платежі (ЦОД, зв'язок, оренда) — авансом на 1–3 місяці; договір з постачальником пального з пріоритетом відвантаження.
- Генератор можна купити за пільговим кредитом: держава компенсує відсотки малому й середньому бізнесу (умови — у додатку).

- Перевірте, що саме покривають ваші страхові поліси на випадок воєнних дій і кібератак (див. розділ 3.2).

Курс, інфляція і податки

НБУ прогнозує інфляцію 10 % у 2026 році.[31] Довгий договір у гривнях без механізму перегляду ціни поступово стає збитковим. Закон дозволяє прив'язати ціну до валютного еквівалента з оплатою в гривні за курсом на день платежу (ст. 524 і 533 Цивільного кодексу), і Верховний Суд цей підхід підтверджує.'[32] Податки теж змінюються раптово: військовий збір 5 % і збір для ФОП ухвалили восени 2024 року, а діяти вони почали вже з 1 грудня 2024 року.'[33]

▲ ЯК ПІДГОТУВАТИСЯ

У договорах на строк понад 3 місяці — валютне застереження або індексація; у бюджеті — сценарій «+20 % до курсу»; податковий резерв на 1–2 місяці; хтось у компанії або бухгалтер стежить за законопроєктами, що стосуються вашої системи оподаткування.

Майно у воєнний час

Під час воєнного стану військове командування може примусово відчужити або вилучити майно для потреб оборони: автомобілі, пальне, генератори. Рішення погоджує військова чи цивільна адміністрація, а в районах бойових дій командування ухвалює його самостійно. Власник має отримати акт з описом майна і висновок про його вартість. Повну компенсацію держава виплачує протягом п'яти бюджетних періодів після скасування воєнного стану, і тільки за наявності цих документів.[34]

▲ ЯК ПІДГОТУВАТИСЯ

Тримайте реєстр цінного майна з документами на право власності й фото поза офісом; поясніть водіям і керівникам складу, що в разі вилучення треба вимагати акт з підписом і копію висновку про вартість.

Фіксація збитків: компенсацію отримає той, хто підготувався

З 10 вересня 2026 року юридичні особи можуть подавати заяви до міжнародного Реєстру збитків для України (RD4U) в усіх категоріях. Це пошкоджене майно, упущена вигода, втрата активів, евакуація й релокація, інші економічні втрати і гуманітарні витрати на підтримку працівників. Заяву подає керівник з власним КЕП або представник за електронною довіреністю через портал «Дія»; збитки мають бути завдані з 24.02.2022.[35] Для податкового обліку знищеного майна потрібні акт ДСНС, витяг з ЄРДР і акт інвентаризації, а про втрату первинних документів треба повідомити ДПС протягом 5 днів.'[36] Сертифікат ТПП про форс-мажор допомагає, але сам не звільняє від відповідальності за договорами: суди вимагають довести вплив на конкретне зобов'язання.'[37]

▲ ЯК ПІДГОТУВАТИСЯ

Уже зараз зробіть фото й відео приміщень, обладнання та запасів з датою й геолокацією і збережіть їх у хмарі; тримайте реєстр основних засобів з інвентарними номерами і скани документів поза офісом; пропишіть порядок дій після удару (ДСНС і поліція, акт, ЄРДР, інвентаризація, повідомлення ДПС); призначте відповідального за подання до Реєстру збитків і перевірте, що в нього є КЕП.

Власник за кордоном

Керувати бізнесом дистанційно можна, але з'являються ризики, про які рідко думають заздалегідь. Після 183 днів перебування країна проживання може вважати власника своїм податковим резидентом, і тоді його доходи можуть оподаткувати двічі.[38] Дані про закордонні рахунки українців ДПС отримує автоматично: перший обмін за стандартом CRS відбувся у вересні 2024 року.'[39] Прострочений паспорт чи КЕП блокує банк і звітність, а консульські послуги чоловікам 18–60 років надають лише з військово-обліковим документом.'[40]

▲ ЯК ПІДГОТУВАТИСЯ

Податкова консультація щодо резидентства до виїзду, а не після; довіреність і друге право підпису на людину в Україні; два КЕП (хмарний і резервний) з контролем строків дії; вчасне оновлення паспорта й військово-облікових даних.

Можливості: гранти й пільгові кредити

Держава й міжнародні партнери фінансують відновлення й розвиток малого бізнесу. За програмою «єРобота» видано гранти загальною сумою близько 12 млрд грн.[41] Гранти дають на старт, масштабування, переробку й відновлення потужностей, пошкоджених війною; окремо є програма для ветеранів. Розмір гранту залежить від кількості створених робочих місць, тож план найму — частина заявки. ЄБРР і ЄІБ через українські банки дають кредити МСБ під гарантії ЄС зі зниженими вимогами до застави.'[42] Суми й умови програм — у додатку.

▲ ЯК ПІДГОТУВАТИСЯ

Прозора звітність і чиста податкова історія, бо без них не дадуть ні гранту, ні кредиту; готовий бізнес-план на 3 роки; запланована власна частка співфінансування; питання до свого банку про програми з гарантіями ЄС.

Ланцюги постачання

- Складіть карту критичних постачальників, включно з IT: провайдер, хостинг, SaaS, підрядник з обслуговування.
- Для кожного критичного постачальника потрібна альтернатива або стратегічний запас.
- Запитайте своїх IT-постачальників: «Який у вас план безперервності?» Відповідь багато скаже про ризик.
- Знайте постачальників своїх постачальників: Toyota склала таку карту після землетрусу 2011 року.[43]
- Рахуйте концентрацію клієнтів: яку частку виручки дають три найбільші клієнти і наскільки вони самі готові до кризи (див. розділ 3.5).

ЩО ЗРОБИТИ КЕРІВНИКУ

- ☐ Сфотографуйте й опишіть основні засоби вже цього тижня і збережіть архів поза офісом.
- ☐ Перегляньте три найбільші договори: чи є в них валютне застереження, форс-мажор і строки повідомлення.
- ☐ Якщо ви за кордоном або плануєте виїзд, отримайте консультацію щодо податкового резидентства і друге право підпису в Україні.

ЧАСТИНА III

03 Діяти

Коли криза триває роками, стійкість — це режим роботи, а не надзвичайна подія.

Що робити в перші години інциденту, як не вигоріти, коли криза стає нормою, і як діяти, коли під загрозою сама територія.

РОЗДІЛ

09

Інцидент стався: плейбуки

> У кризі люди не думають — вони виконують те, що відпрацювали. Плейбуки — це заздалегідь ухвалені рішення.

Кібератака: шифрувальник або знищення даних

1. **Ізолюйте, але не вимикайте.** Відключіть уражені пристрої від мережі, але не вимикайте живлення: в оперативній пам'яті лишаються сліди.
2. **Перейдіть на незалежний канал зв'язку.** Корпоративна пошта може бути скомпрометована.
3. **Зберіть докази:** журнали, скриншоти, час виявлення.
4. **Повідомте** CERT-UA, кіберполіцію, страховика та європейських партнерів, якщо на них поширюються вимоги NIS2 чи GDPR.
5. **Викуп — не рішення за замовчуванням.** Платіж не гарантує повернення даних і може порушувати санкційне законодавство. Рішення ухвалює штаб разом з юристом.
6. **Відновлюйте з чистих копій** лише після того, як закрито точку входу.
7. **Розберіть уроки** й оновіть план.

Читайте детальніше: Що робити після кібератаки: покроковий план

Удар по офісу або втрата доступу до приміщення

1. Проведіть перекличку працівників через дерево оповіщення.
2. Оцініть, що фізично втрачено: обладнання, документи, сервери.
3. Перейдіть на віддалену роботу або в резервну локацію.
4. Відновіть IT з ЦОД чи хмари. Якщо критичних систем не було в офісі, цей крок займає години, а не тижні.
5. Зафіксуйте збитки: виклик ДСНС і поліції, акт, витяг з ЄРДР, інвентаризація, повідомлення ДПС про втрату документів протягом 5 днів, заява до Реєстру збитків (розділ 8).

Багатоденний блекаут

1. Перейдіть на автономне живлення за пріоритетами навантаження.
2. Увімкніть резервні канали зв'язку, стежте за пальним і зарядом.
3. Перейдіть у скорочений режим: лише мінімально життєздатна операція.
4. Переведіть касу в офлайн-режим ПРРО: базовий ліміт — 36 годин поспіль і 168 годин на календарний місяць. Під час воєнного стану ці ліміти можна перевищувати, але це не підстава працювати офлайн щодня.[44]
5. Складіть графік змін і визначте «пункти незламності» для працівників.

Платежі не проходять

1. **Каса:** ПРРО в офлайн-режим (ліміти — у плейбуку вище).
2. **Картки:** термінал з резервним каналом зв'язку (SIM іншого оператора, резервний інтернет) або другий термінал від іншого банку.
3. **Готівка:** розмінна готівка на початок зміни, правила зберігання, якщо інкасація не приїхала.
4. **Клієнту:** поруч — готівка; онлайн — другий платіжний провайдер або оплата при отриманні; бізнес-клієнту — рахунок.
5. **Вихідні платежі:** банк на двох пристроях і двох каналах зв'язку, другий банк, заздалегідь складений список платежів, які не можна пропустити.
6. **Після відновлення:** звірка каси, терміналів і банку.

Державна система недоступна

Реєстри, податкова, митниця чи «Дія» можуть не працювати днями, як реєстри Мін'юсту в грудні 2024 року (розділ 2).

1. **Заздалегідь:** список процесів, які зупиняються без кожної державної системи.
2. **Ручний режим:** що можна зробити на папері чи відкласти, а що — ні.
3. **Облік «на потім»:** хто веде перелік документів, які треба внести чи подати після відновлення, і в які строки.
4. **Фіксація збою:** скриншоти й офіційні повідомлення знадобляться, якщо строк пропущено. Наслідки для звітності уточнюйте з бухгалтером.
5. **Клієнтам і контрагентам:** повідомлення про затримку з посиланням на збій.

Неправдиве «мінування»

30 березня 2026 року поліція за кілька годин отримала понад 1 200 анонімних листів про замінування, зокрема підприємств і банків; жоден не підтвердився.[45] Мета таких атак — зупинити роботу й посіяти хаос. Кожна евакуація — це години простою, зірвані зустрічі й відвантаження. Ігнорувати повідомлення не можна, тому реакцію треба відпрацювати заздалегідь.

1. Той, хто отримав повідомлення, одразу телефонує 102 і повідомляє відповідального за безпеку.
2. Евакуація за заздалегідь визначеним маршрутом до точки збору; відповідальний перевіряє, що вийшли всі.
3. Критичні процеси продовжуються дистанційно за процедурою «втрата доступу до приміщення».
4. Лист чи повідомлення з погрозою зберігається повністю, із заголовками, для поліції.

Кризова комунікація

Принципи: швидко, чесно, регулярно. Одна людина говорить від імені компанії, одна версія фактів, жодних здогадок про те, хто стоїть за атакою. Криза, яку добре пояснили, зміцнює довіру клієнтів.

До 1 год

Працівники

Що сталося, що робити, коли наступне оновлення.

1–2 год

Ключові клієнти

«Ми знаємо, працюємо, наступне оновлення о 15:00», навіть якщо більше нічого сказати.

2–6 год

Партнери, постачальники, банк, страховик

Вплив на зобов'язання, строки, контактна особа.

6–24 год

Публічні канали

Статус сервісу, очікуваний час відновлення, регулярні оновлення.

Після

Підсумок

Що сталося, що зроблено, що змінено, щоб це не повторилося.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Роздрукуйте плейбуки для трьох найімовірніших інцидентів і роздайте членам штабу.
- [ ] Підготуйте шаблони першого повідомлення для команди, клієнтів і партнерів.
- [ ] Визначте, хто говорить від імені компанії, і його дублера.

РОЗДІЛ

10

Хронічна криза: коли норма не повертається

> Класичні плани безперервності розраховані на шок і повернення до норми. На п'ятому році війни норми немає: блекаути, тривоги й атаки стали фоном. Якщо щоразу вмикати аварійний режим, компанія вигорить раніше, ніж закінчиться криза.

Три пастки хронічної кризи

Марафон у темпі спринту

Кожен блекаут запускається як надзвичайна подія, і команда працює на адреналіні. За кілька місяців адреналін закінчується, приходять апатія й падіння продуктивності, які не компенсує жодна інструкція.

Штаб, що замінив управління

Кризовий штаб стає постійною паралельною структурою. Керівники «гасять пожежі» щодня і втрачають час на стратегію, продукти й нові ринки. Компанія виживає сьогодні, але втрачає завтра.

Стійкість, яку не можна оплатити

Резерви, дублювання функцій і обслуговування обладнання коштують грошей. За низької маржі виникає питання: як довго компанія зможе платити за свою стійкість, коли конкурент цього не робить?

Вихід — перестати ставитися до повторюваних подій як до інцидентів. Робота на генераторі чи перемикання на резервний ЦОД мають бути такою ж рутиною, як прибирання офісу. Кризовий план вмикається лише тоді, коли ламається сам механізм рутинного виживання.

Шкала серйозності: де закінчується рутина і починається криза

Межу визначають вимірювані критерії, а не відчуття. Шкала побудована за логікою рівнів пріоритету інцидентів, звичною для IT-служб, і адаптована до умов війни.

0
Норма воєнного часу

ПРИКЛАД
Блекаут за графіком, перемикання на генератор чи резервний канал, тривога

ХТО ДІЄ
Працівники за стандартною процедурою

ЕСКАЛАЦІЯ
Немає, лише запис у журнал

1
Інцидент

ПРИКЛАД
Процедура частково не спрацювала: генератор не запустився, один сервіс недоступний

ХТО ДІЄ
Операційний менеджер у межах бюджету й повноважень

ЕСКАЛАЦІЯ
Звіт у кінці дня

2
Серйозний інцидент

ПРИКЛАД
Критичний процес стоїть довше за допустимий час простою або збитки перевищили поріг

ХТО ДІЄ
Керівник напряму та IT-партнер

ЕСКАЛАЦІЯ
Повідомлення власнику

3
Криза

ПРИКЛАД
Кілька критичних процесів одночасно, загроза людям або існуванню компанії: гроші, юридичний статус, репутація

ХТО ДІЄ
Кризовий штаб і власник, плейбуки

ЕСКАЛАЦІЯ
Скликається штаб

> **ПРАВИЛО ДЕЕСКАЛАЦІЇ**
> Штаб розпускається, щойно ситуація повертається на рівень 1, а не тоді, коли «все заспокоїться». Інакше надзвичайний режим стає постійним.

Норма воєнного часу: рутина з контролем

- Кожна повторювана подія отримує стандартну процедуру на одну сторінку: блекаут за графіком, перемикання каналу, тривога, збій мобільного зв'язку.
- Процедури виконують працівники без ескалації і без участі керівника.
- Але рутина без контролю перетворюється на нормалізацію відхилень (розділ 3.1). Коли блекаут стає «як прибирання», генератор перестають обслуговувати, а тести відкладають, бо «все ж працює».
- Тому до кожної процедури додаються журнал виконання, 2–3 метрики, щомісячна перевірка й квартальний тест.

Процедуру, яку ніхто не перевіряв три місяці, вважайте непрацездатною.

Два контури управління

Операційний контур
Менеджери й процедури рівнів 0–2. Завдання — утримувати компанію в режимі «норми воєнного часу» без участі власника.

Стратегічний контур
Власник і керівники. Щотижнева стратегічна сесія, яку не скасовують події рівнів 0–2, і квартальний перегляд ринків, продуктів і клієнтів.

Дослідники менеджменту Чарльз О'Райлі та Майкл Тушман називають це **організаційною амбідекстрією**: здатністю одночасно ефективно керувати поточним бізнесом і шукати нові можливості. У хронічній кризі саме стратегічний контур першим приносять у жертву, і саме його треба захищати.

Виснаження — це метрика, а не настрій

Показник	Сигнал тривоги
Ескалації рівня 1 і вище на тиждень	Ростуть кілька тижнів поспіль: процедури перестали працювати
Понаднормові години	Стали постійними, а не епізодичними
Ротація чергувань і кризових ролей	Ті самі люди чергують місяцями
Рішення, які може ухвалити лише власник	Їхня кількість зростає, заступники не вирішують самостійно

Якщо ці показники погіршуються два місяці поспіль, це криза рівня 2–3, навіть коли сервери працюють. Найчастіше першим вигорає не команда, а власник, який роками єдиний ухвалює всі рішення. Практики, що працюють: ротація чергувань, обов'язкові відпустки, «тихі» години без операційних питань, заступники, які реально ухвалюють рішення, і тиждень, коли власника заміщують повністю.

Економіка стійкості

- **Бюджет визначає аналіз впливу, а не відчуття.** Захід виправданий, якщо його річна вартість менша за очікувані річні втрати, яких він запобігає: ймовірність події × вартість години простою × тривалість (розділ 4).
- **Почніть з дешевих заходів з найбільшим ефектом:** MFA, друга особа з правом підпису, тригери рішень, список відкликання доступів, тест відновлення. Вони коштують часу, а не грошей.
- **Переводьте капітальні витрати в операційні:** ЦОД, хмарні сервіси, бекап і відновлення як сервіс замість власного заліза, яке треба купувати, обслуговувати й замінювати.
- **Монетизуйте стійкість:** SLA з гарантіями доступності можна продавати дорожче; питання про безперервність є в тендерах і анкетах європейських партнерів, адже NIS2 вимагає від компаній контролювати безпеку свого ланцюга постачання.[46]

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Затвердіть шкалу серйозності з критеріями для вашої компанії і правило деескалації.
- [ ] Складіть процедури «норми воєнного часу» для 3–5 найчастіших подій і призначте, хто їх перевіряє.
- [ ] Внесіть у календар щотижневу стратегічну сесію, яку не можна скасувати через події рівнів 0–2.

РОЗДІЛ

11

Коли під загрозою територія

> Для компаній у прифронтових і прикордонних регіонах фізична загроза — щоденна реальність. Але втратити доступ до офісу, складу чи серверної може будь-яка компанія в будь-якому місті: через удар, уламки, пожежу або перекриття району.

Укриття і робота під час тривоги

Від укриття тепер залежить, чи працюватиме бізнес під час тривоги. Постанова КМУ № 1092 від 04.09.2026 ділить тривоги на «жовті» (загроза дронів) і «червоні» (ракети або масована атака). Під час «жовтої» працювати можна лише за наявності укриття або «безпечного простору», тобто найзахищенішої частини ваших приміщень, яку визначає власник. Без нього працювати дозволено тимчасово, за погодженням з трудовим колективом і до облаштування укриття (строк — у додатку). Під час «червоної» тривоги роботу зупиняють.[47] З 1 лютого 2025 року за недопуск до укриття або його неготовність передбачено штрафи, а якщо порушення призвели до загибелі людей, — кримінальну відповідальність.'[48]

● СТРОК — 04.12.2026

Працювати під час «жовтої» тривоги без укриття за згодою колективу можна лише до цієї дати. Після неї без укриття чи безпечного простору робота під час «жовтої» тривоги зупиняється так само, як під час «червоної». Якщо укриття немає, облаштуйте його вже зараз.

▲ ЯК ПІДГОТУВАТИСЯ

Визначте й позначте укриття або безпечний простір (в орендованому приміщенні — письмово з власником будівлі); оформіть протокол згоди колективу, якщо укриття поки немає; налаштуйте власне оповіщення працівників і таблички. Правила змінюються: звіряйте їх з рішеннями своєї обласної військової адміністрації.

Люди й процеси під час тривоги

Сторонні й нові люди

- Відвідувачі, працівники підрядників і новачки не знають, де укриття: хто на кожній зміні веде їх туди.
- Таблички зі шляхом до укриття; допомога людям з обмеженою мобільністю.
- Новачку в перший день — 5 хвилин: де укриття, хто старший, що робити.

Люди поза приміщенням

- Водії, виїзні працівники, кур'єри: де сховатися; продовжувати роботу — за рішенням керівника.
- Маршрут і час повернення відомі керівнику.
- Вихід на зв'язок після тривоги; хто діє, якщо людина мовчить.

Безпечна зупинка

- Піч, котельню, лінію, процедуру чи розрахунок з клієнтом за секунду не зупиниш.
- Для кожного процесу: хто, за скільки хвилин і в якій послідовності доводить його до безпечного стану.

Рівні загрози і тригери

Як і в розділі 3.4, рішення ухвалюються заздалегідь і прив'язуються до ознак, а не до відчуттів. Офіційні рішення військових адміністрацій та ДСНС завжди мають пріоритет.

1
Спостереження

ОЗНАКИ

Частішають удари по району, з'являються офіційні попередження, евакуація в сусідніх громадах

ЩО РОБИМО

Оновлюємо списки людей і контактів, перевіряємо, що на місці немає локальних даних і бекапів, збираємо «тривожну валізу», визначаємо місце релокації

2
Підготовка

ОЗНАКИ

Регулярні удари по місту, загроза логістиці, рекомендована евакуація

ЩО РОБИМО

Переводимо людей на віддалену роботу, вивозимо документи й резервні носії, переносимо критичні системи в ЦОД чи хмару, домовляємося про приміщення й житло на новому місці

3
Евакуація

ОЗНАКИ

Обов'язкова евакуація або пряма загроза об'єкту

ЩО РОБИМО

Люди виїжджають першими; беремо «тривожну валізу»; відкликаємо доступи з обладнання, що лишається, і віддалено стираємо його; фіксуємо, що саме залишено

Порядок пріоритетів

Люди → Доступи й дані → КЕП-носії, печатки, установчі документи → Гроші й платіжні засоби → Обладнання

Обладнання — останнє в списку. Якщо дані й доступи живуть у ЦОД чи хмарі, втрата ноутбуків і серверів у приміщенні — це витрати, а не катастрофа. Інша справа, коли гроші приносить саме обладнання: верстати, техніка, транспорт. Для нього потрібен окремий план захисту або вивезення, який вмикається на рівні загрози 2.

Захист даних на обладнанні, яке може залишитися

Ризик не лише у втраті обладнання. Дані про працівників, клієнтів і контрагентів можуть потрапити до ворога й бути використані проти людей, зокрема для тиску на них чи їхніх рідних.

- **Повне шифрування дисків** на всіх ноутбуках, серверах і телефонах. Без ключа вилучений пристрій — лише залізо.
- **Централізоване керування пристроями (MDM)** з віддаленим блокуванням і стиранням.
- **Політика «на пристрої нічого немає»:** робота через ЦОД чи хмару і термінальний доступ замість локальних файлів.
- **Список відкликання для кожної локації:** які акаунти, VPN-ключі, сертифікати й паролі треба відкликати, якщо об'єкт втрачено, і хто це робить.
- **Мінімум паперу з персональними даними** і заздалегідь визначений порядок його знищення.
- **Жодних резервних копій на тому самому об'єкті,** що й основні дані.

Ізоляція вцілілого об'єкта

Офіс або власна серверна цілі, пальне є. Але район оточили військові, ДСНС чи поліція через нерозірваний боєприпас, уламки або хімічну загрозу, і доступу немає днями чи тижнями. Хто перезапустить зависле обладнання, заправить генератор або забере первинну документацію?

- Жоден критичний бізнес-процес не має бути прив'язаний до конкретного приміщення. Найпростіше рішення — професійний ЦОД, де фізичний доступ і живлення забезпечує оператор.
- **Керування «поза смугою»:** IP-KVM, керовані розетки PDU, віддалене ввімкнення серверів, щоб перезапустити обладнання без виїзду.
- **Послуга «віддалених рук»** у ЦОД: інженер оператора виконає фізичні дії за вашою заявкою.
- **Дубль ключів і доступів** у людей, які живуть в іншому кінці міста або в іншому місті.
- **Електронний документообіг** замість паперових первинних документів в офісі.

Техногенні загрози: вода

Удар може зупинити не ваш об'єкт, а ресурс, від якого він залежить. Після підриву Каховської ГЕС у червні 2023 року частина міст Дніпропетровщини лишилася без централізованого водопостачання, а великі підприємства регіону зупиняли або скорочували виробництво.[49] Якщо ваш процес залежить від води (харчове виробництво, мийки, медицина, охолодження), тримайте запас і контакти постачальників технічної води, а в плані безперервності передбачте сценарій «немає води тиждень».

Якщо ви в прифронтовій громаді

Правила для бізнесу залежать від статусу громади в державному Переліку територій бойових дій (наказ Мінрозвитку № 987, чинний з 05.06.2026, зі змінами). Від нього залежать податкові пільги й доступ до програм підтримки: наприклад, на територіях активних бойових дій не нараховують плату за землю.[50] Комендантську годину й обмеження встановлює обласна військова адміністрація, тож у кожному регіоні вони свої. Статус громади може змінитися за тиждень.

> ▲ ЯК ПІДГОТУВАТИСЯ
>
> Раз на місяць перевіряйте статус громад, де у вас офіс, склад чи орендована земля; зміну статусу одразу передавайте бухгалтеру; підпишіться на канали своєї обласної військової адміністрації; тримайте готовий пакет документів для грантів і страхування воєнних ризиків.

Релокація і філії в регіонах ризику

- **Філії:** мінімум локальних даних (облік, склад і CRM через ЦОД чи хмару), ротація персоналу, чіткий порядок, хто і за якої умови ухвалює рішення на місці.
- **Рішення:** часткова (частина людей чи функцій), повна чи тимчасова; хто ухвалює і за яким рівнем загрози.
- **Люди:** хто їде, житло, транспорт, виплати на переїзд; хто лишається і на яких умовах.
- **Активи:** що вивозимо першим (за порядком пріоритетів вище), що консервуємо, що списуємо; документи на вивезене.
- **Запуск:** приміщення, підключення, зміна адреси в реєстрах і податковій, повідомлення клієнтів і контрагентів.
- **Бюджет:** оцінений заздалегідь і закладений у грошовий резерв.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Для кожної локації визначте три рівні загрози й дії на кожному з них.
- [ ] Зберіть «тривожну валізу» компанії (чек-лист Ж у розділі 14) і складіть список відкликання доступів.

ЧАСТИНА IV

04 Інструменти

Почніть з того, що коштує часу керівника, а не грошей.

Де ваша компанія зараз, що робити в найближчі 30, 90 і 180 днів, чек-листи й шаблони для друку, а також чесно про межі цього документа.

РОЗДІЛ

12

Модель зрілості та самооцінка

> Кожна компанія десь на цій драбині. Реалістична мета — піднятися на один рівень за 6 місяців.

1
Реактивний
«Розберемося, коли станеться». Сервер в офісі, бекап на зовнішньому диску або його немає, все знає один адміністратор.

2
Базовий
Є ДБЖ або генератор, другий канал інтернету, хмарний бекап, MFA на пошті. Плану немає або його не тестували.

3
Керований
Визначено критичні процеси й допустимий простій, системи в ЦОД чи хмарі, правило 3-2-1-1-0, плани тестуються щороку, є кризовий штаб.

4
Антикрихкий
Резерв в Україні та ЄС, регулярні навчання, відпрацьоване перемикання, тригери рішень. Кожен інцидент покращує систему.

Самооцінка: 20 питань

Відповідайте «так» лише тоді, коли можете це показати. Кожне «так» — 1 бал. 0–5: реактивний рівень, 6–11: базовий, 12–16: керований, 17–20: антикрихкий.

Люди і рішення

- [ ] Знаємо вартість години простою для ключових процесів.
- [ ] Визначено склад кризового штабу і заступників.
- [ ] Компанія не зупиниться юридично без власника чи директора: є друга особа з правом підпису.
- [ ] Затверджено тригери рішень, стоп-лист і «лист на випадок відсутності» у форматі наміру керівника.

Живлення, зв'язок, тривоги

- [ ] Процеси, що приносять гроші, працюють 72 год без міської мережі.
- [ ] Генератор проходив навантажувальний тест за останні 3 місяці.
- [ ] Є два канали інтернету різної фізичної природи з автоматичним перемиканням.
- [ ] Є процедура на час тривоги: сторонні люди, люди поза приміщенням, безпечна зупинка.

Дані

- [ ] Є незмінна або ізольована копія даних поза офісом.
- [ ] Відновлювали систему з бекапу за останні 6 місяців.
- [ ] Бекапи не можна видалити з акаунта, яким керують робочими системами.
- [ ] Ключі від бекапів знають щонайменше двоє людей.

Інфраструктура

- [ ] Критичні системи працюють поза офісом: у ЦОД або в хмарі.
- [ ] Є копія або репліка критичних даних в іншому місті чи країні.
- [ ] Знаємо, хто власник домену й акаунтів реєстратора та DNS.
- [ ] Жоден процес не залежить від фізичного доступу до одного приміщення.

Кібербезпека

- [ ] MFA ввімкнено для всіх, хто має доступ до пошти й фінансів.
- [ ] Є аварійні акаунти й коди відновлення в сейфі.
- [ ] Знаємо, хто з підрядників має віддалений доступ, і вміємо його відкликати.
- [ ] Проводили навчання з фішингу за останній рік.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Пройдіть самооцінку разом з 2–3 керівниками: розбіжності в оцінках самі є знахідкою.
- [ ] Оберіть рівень, якого хочете досягти за рік, і три кроки до нього.
- [ ] Повторіть самооцінку через 6 місяців.

РОЗДІЛ

13

Дорожня карта: 30 / 90 / 180 днів

> Почніть з того, що не потребує великих бюджетів, але закриває найбільші ризики.

Мінімум за розміром компанії

Орієнтир, а не норматив. Почніть з колонки свого розміру і лише потім переходьте до наступної.

	До 10 працівників	10–50 працівників	50–250 працівників
Штаб і ролі	Власник і заступник з правом підпису, IT-партнер на аутсорсі	Штаб із 3–4 ролей, у кожної є дублер	Повний штаб із 6 ролей, тригери затверджено наказом
Живлення	ДБЖ для роутера й каси; серверів в офісі немає	Інвертор і генератор для критичного навантаження, журнал ТО	Резервування офісу й складу, договір на пальне, навантажувальні тести
Зв'язок	Два канали: оптика + мобільний зв'язок або Starlink	Автоматичне перемикання між каналами, моніторинг	Два оптичні провайдери різними трасами + супутник
Дані	Хмарний бекап з незмінною копією, бекап пошти й SaaS	Правило 3-2-1-1-0, тест відновлення щокварталу	3-2-1-1-0 + реплікація критичних систем, тест щомісяця
Інфраструктура	Облікова система в хмарі або ЦОД	1С і CRM у ЦОД, копія в ЄС	Теплий чи гарячий резерв або DRaaS, гібрид Україна + ЄС
Кібербезпека	MFA, менеджер паролів, автооновлення	+ захист пристроїв (EDR), окремі адмін-акаунти, навчання	+ сегментація мережі, централізовані журнали, реагування 24/7
Фінанси	Резерв на 1–2 місяці, два банки, фото й реєстр майна	Резерв на 2–3 місяці, фінансові тригери	Резерв на 3+ місяці, кредитна лінія, страхування з перевіркою виключень
Навчання	Одна настільна вправа на рік	Дві вправи на рік і тест відновлення	Щоквартальні вправи, повне перемикання раз на рік

30 / 90 / 180 днів

30 ДНІВ

Знати й закрити найочевидніше

- [ ] **Наступність власника: друга особа з правом підпису, КЕП, довіреності від компанії, статут**
- [ ] **MFA скрізь (не лише SMS), менеджер паролів, перевірка доступів підрядників**
- [ ] **Вартість години простою для 3 процесів**
- [ ] Карта загроз і аналіз впливу для топ-3 процесів
- [ ] Перевірка бекапів і тестове відновлення
- [ ] Кризовий штаб, дерево оповіщення, друкований список контактів
- [ ] Реєстр цифрових активів: домен, DNS, хмари, Starlink
- [ ] Аудит спільних залежностей резервів
- [ ] Укриття або безпечний простір, власне оповіщення
- [ ] Фото й реєстр основних засобів поза офісом

90 ДНІВ

Побудувати фундамент

- [ ] Аналіз впливу для решти процесів (топ-10)
- [ ] Перенесення облікових систем і файлів з офісу в ЦОД або хмару
- [ ] Бекап за правилом 3-2-1-1-0 з копією в ЄС
- [ ] Другий канал зв'язку з автоматичним перемиканням
- [ ] План безперервності на 5 сторінок, перша настільна вправа
- [ ] Перші 5 тригерів рішень і намір керівника на випадок відсутності
- [ ] Бронювання ключових працівників, якщо компанія критична
- [ ] Навчання працівників з фішингу
- [ ] Паливний договір, авансові платежі, валютні застереження в договорах
- [ ] Шкала серйозності і процедури «норми воєнного часу»
- [ ] Журнал життєвого циклу резерву

180 ДНІВ

Стати стійким

- [ ] Теплий чи гарячий резерв або DRaaS для критичних систем
- [ ] Технічний тест відновлення з вимірюванням реального часу
- [ ] Плейбук повернення і метрика «час до повної бізнес-норми»
- [ ] Крос-навчання ключових ролей, документування знань
- [ ] Журнал тимчасових рішень переглянуто
- [ ] Рівні загрози й «тривожна валіза» для кожної локації
- [ ] Повторна самооцінка й план на наступний рік

СКІЛЬКИ ЦЕ КОШТУЄ

Бюджет залежить від кількості працівників, критичних систем і поточного рівня зрілості. Почніть з кроків на 30 днів: більшість із них потребує часу керівника, а не грошей.

ЩО ЗРОБИТИ КЕРІВНИКУ

- [ ] Внесіть кроки на 30 днів у календар з відповідальним і датою для кожного.
- [ ] Призначте одну людину, яка раз на тиждень звітує про прогрес.
- [ ] Через 30 днів перегляньте план на 90 днів з урахуванням того, що дізналися.

РОЗДІЛ

14

Чек-листи, шаблони й глосарій

Роздрукуйте й тримайте поруч із планом безперервності.

А. Блекаут 72 години

- [ ] Навантаження розподілено за пріоритетами
- [ ] Автономність критичних систем ≥ 72 год або їх винесено в ЦОД чи хмару
- [ ] Запас пального, ротація й договір на постачання
- [ ] Резервний канал зв'язку живиться від автономного джерела
- [ ] ПРРО готовий до роботи офлайн
- [ ] Графік змін і правила для працівників
- [ ] Раз на квартал: тест вимкнення живлення офісу на 2 год

Б. Кібератака: перші 24 години

- [ ] Уражені пристрої ізольовано від мережі, але не вимкнено
- [ ] Штаб перейшов на незалежний канал зв'язку
- [ ] Докази зафіксовано
- [ ] Повідомлено CERT-UA, кіберполіцію, страховика, партнерів
- [ ] Паролі критичних акаунтів змінено з чистого пристрою
- [ ] Перше повідомлення команді й ключовим клієнтам
- [ ] Рішення щодо відновлення ухвалено штабом

В. Щоквартальна перевірка

- [ ] Тестове відновлення однієї системи з бекапу
- [ ] Тест перемикання інтернет-каналів
- [ ] Актуалізація контактів і дерева оповіщення
- [ ] Перегляд доступів звільнених працівників і підрядників
- [ ] Перевірка генератора, акумуляторів, пального
- [ ] Короткий звіт для керівника

Г. Сліпі зони за 15 хвилин

- [ ] Хто, крім директора, завтра підпише платіж?
- [ ] На чию пошту зареєстровано домен?
- [ ] Чи увійдемо в пошту й банк без мобільного зв'язку?
- [ ] Що спільного між основним і резервним каналом?
- [ ] Чи можна видалити бекапи з робочого адмін-акаунта?
- [ ] Що кажуть наші поліси про воєнні дії?
- [ ] Скільки днів від останнього реального тесту?
- [ ] Де фото й документи на майно, якщо офісу не стане?
- [ ] Чи можемо працювати під час «жовтої» тривоги?

Д. План безперервності на одній сторінці

КРИТИЧНІ ПРОЦЕСИ, ДОПУСТИМИЙ ПРОСТІЙ І ВТРАТИ ДАНИХ

СКЛАД ШТАБУ ТА ЗАСТУПНИКИ

КАНАЛИ ЗВ'ЯЗКУ: ОСНОВНИЙ, РЕЗЕРВНИЙ, АВАРІЙНИЙ

ТОЧКИ ЗБОРУ; ХТО ВІДПОВІДАЄ ЗА СТОРОННІХ ЛЮДЕЙ І ЛЮДЕЙ ПОЗА ПРИМІЩЕННЯМ

ПРОЦЕСИ, ЩО ПОТРЕБУЮТЬ БЕЗПЕЧНОЇ ЗУПИНКИ, І ХТО ЇХ ЗУПИНЯЄ

ДЕ ЛЕЖАТЬ БЕКАПИ І ХТО ВМІЄ ВІДНОВЛЮВАТИ

КОНТАКТИ: ІТ-ПІДРЯДНИК, ЦОД, ПРОВАЙДЕРИ, БАНК, СТРАХОВИК, CERT-UA

ЛІМІТИ ДЕЛЕГОВАНИХ ПОВНОВАЖЕНЬ

ТРИГЕРИ РІШЕНЬ І СТОП-ЛИСТ

Компанія: _____ Затвердив: _____

Дата: _____ Наступний перегляд: _____

Е. Реєстр тригерів рішень

#	Поріг (вимірюваний)	Рішення	Хто виконує	Хто заміщує	Кого повідомити
1					
2					
3					
4					
5					

Ж. «Тривожна валіза» компанії

- ☐ КЕП-носії (паролі до них — окремо)
- ☐ Печатки, установчі документи або їхні копії
- ☐ Зашифровані резервні носії
- ☐ Ноутбуки з повним шифруванням дисків
- ☐ Друкований план безперервності і список контактів
- ☐ Архів фото й відео майна, реєстр основних засобів
- ☐ Ключі, картки доступу, список відкликання доступів
- ☐ Павербанки й зарядні станції

З. Життєвий цикл резерву

- ☐ Генератор: мотогодини, дата ТО, дата навантажувального тесту
- ☐ Акумулятори: дата встановлення, кількість циклів, тест ємності
- ☐ Інвертори й ДБЖ: вік, дата перевірки, плановий строк заміни
- ☐ Пальне: дата закупівлі, ротація, стабілізатор
- ☐ Мережеве обладнання резервного каналу: вік, прошивка
- ☐ План заміни до відмови і бюджет на рік

И. Намір керівника на випадок моєї відсутності

Заповніть, роздрукуйте й зберігайте разом із планом безперервності. Переглядайте раз на квартал.

1 · МЕТА	2 · ЧЕРВОНІ ЛІНІЇ	3 · СВОБОДА ДІЙ
Що для нас перемога?	**Чого не можна робити?**	**Що можна без мене?**
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Хто заміщує мене першим: _____ · другим: _____ · Дата: _____

Глосарій

BCP	план безперервності бізнесу: як компанія працює під час і після збою	**DRP**	план відновлення IT-систем, частина BCP
RTO	допустимий час простою процесу чи системи	**RPO**	допустимі втрати даних, виміряні в часі роботи
MFA	вхід з паролем і ще одним підтвердженням	**EDR**	захист пристроїв, що виявляє й зупиняє підозрілі дії
SaaS	програма як онлайн-сервіс за підпискою	**DRaaS**	резервний майданчик для IT за підпискою
ЦОД	центр обробки даних з резервованим живленням і зв'язком	**GPON**	оптична мережа, що менше залежить від живлення проміжних вузлів
MDM	централізоване керування пристроями, зокрема віддалене стирання	**IP-KVM**	віддалене керування сервером, ніби ви поруч
PDU	блок розеток у стійці; керований вмикає обладнання віддалено	**SOC**	служба цілодобового моніторингу й реагування на атаки
КЕП	кваліфікований електронний підпис	**ПРРО**	програмний реєстратор розрахункових операцій

РОЗДІЛ

15

Межі документа і методологія

> Чого документ свідомо не охоплює і на що спирається. Тема потрапляла в документ, якщо вона може зупинити МСБ в Україні, механізм підтверджено законом, регулятором чи дослідженням і власник може щось зробити заздалегідь.

15.1 Чого цей документ не охоплює

- **Галузеві особливості.** Медицина, харчова промисловість, логістика й торгівля мають власні критичні процеси та регуляторні вимоги. Документ описує спільне для всіх, зокрема сторонніх людей на об'єкті, людей поза приміщенням і процеси без миттєвої зупинки.
- **Виявлення атак і кіберуправління (NIST Detect, Govern).** Ми описуємо, хто в керівництві відповідає за кібербезпеку і що перевірити, але не моніторинг подій безпеки: для МСБ це робота IT-партнера або сервісу SOC.
- **Транспорт, вода й продовольство.** Вони описані як зовнішні залежності (розділи 3.5 і 11), без окремих плейбуків. Для логістичних і харчових компаній цього недостатньо.
- **Теми, для яких поки бракує надійних даних:** інсайдерські загрози, дезінформація проти конкретної компанії, взаємодопомога бізнесів, ризики сценарію «після війни», оборонні закупівлі для МСБ. Вони в черзі на наступні видання.
- **Юридична й податкова консультація.** Норми й програми наведено станом на 26.09.2026 і зібрано в додатку. Кожен юридичний крок узгоджуйте з юристом.

15.2 Рамки, на які спирається документ, і що взяти з них за тиждень

- **ISO 22301:2019**[51] — список критичних процесів і допустимий час простою для кожного.
- **NIST CSF 2.0**[52] — функція Govern робить кібербезпеку відповідальністю керівництва: призначте відповідального на цьому рівні й складіть перелік IT-активів.
- **NIST SP 800-61 Rev. 3**[53] — базовий плейбук реагування на інциденти (розділ 9).
- **Базові вимоги НАТО**[54] — чек-лист залежностей: що станеться, якщо відмовить енергія, зв'язок, транспорт, вода.
- **Фінська модель**[55] — домовленості про взаємодопомогу з сусідами, партнерами, галузевою асоціацією.
- **NIS2, DORA, GDPR**[46,56,57] — якщо ви підрядник європейської компанії чи банку, підготуйте «пакет стійкості» для партнерів.

15.3 Журнал змін

- **Четверте видання:** три дії на сьогодні, приклад розрахунку простою, нові плейбуки, люди й процеси під час тривоги, релокація, глосарій.
- **Третє видання:** фактчек, додаток актуальних норм, редагування, нові схеми, бланки й обкладинка.
- **Друге видання:** право, податки, кадри, укриття, намір керівника, практики екстремальних галузей.
- **Перше видання:** загрози, п'ять шарів технологічної стійкості, плейбуки, чек-листи.

ДОДАТОК

Актуальні норми й програми

> Суми, пороги й строки змінюються кілька разів на рік, тому зібрані тут, а не в тексті розділів. Станом на 26.09.2026. Цю сторінку ми оновлюємо кожні 6 місяців; перед рішенням звіряйте норму з першоджерелом і юристом.

Норма або програма	Що передбачає	Суми, пороги, строки	Розділ
Постанови КМУ № 1092 від 04.09.2026 і № 1128 від 15.09.2026	Жовтий (дрони) і червоний (ракети) рівні тривоги. На жовтому працювати можна за наявності укриття або облаштованого безпечного простору на об'єкті (уточнення постанови № 1128, чинне з 18.09.2026); на червоному роботу зупиняють[47]	Без укриття — за згодою колективу, не довше 3 місяців: до 04.12.2026	11
Постанова КМУ № 692 від 30.05.2026 (зміни до № 76)	Бронювання працівників критичних підприємств[58]	З 01.09.2026 зарплата — від 3 МЗП (25 941 грн), на прифронтових територіях — від 2,5 МЗП (21 617,50 грн); бронювати до 50 % військовозобов'язаних	5
КЗпП, ст. 119	За мобілізованим зберігаються місце роботи й посада; середній заробіток — лише за пораненими на лікуванні, полоненими, зниклими безвісти[28]	Діє з 19.07.2022	5
Компенсація за найм ветеранів	Через центр зайнятості[59]	50 % витрат на оплату праці, не більше МЗП; працевлаштування щонайменше на рік	5
Зберігання пального для генераторів	Без ліцензії на час воєнного стану і 30 днів після нього[29]	До 2 000 л на об'єкті — без повідомлень; понад — безоплатна декларація в ДПС	6
ПРРО в офлайн-режимі	Робота каси без зв'язку з фіскальним сервером[44]	36 год поспіль і 168 год на місяць; під час воєнного стану ліміти можна перевищувати	9
«Енергокредит» (програма «Доступні кредити 5-7-9 %»)	Кредит МСБ на генератори: дизельні, бензинові, газові, газопоршневі[60]	До 10 млн грн під 0 % до 3 років; бізнес працює щонайменше 12 місяців	8
«Власна справа» (з 01.09.2026)	Гранти на старт і масштабування[61]	Старт — до 500 тис. грн, масштабування — до 2,5 млн грн (залежить від робочих місць і регіону)	8
Гранти для ветеранів і їхніх сімей	Окрема програма, постанова КМУ № 1401 від 29.10.2025	До 1 млн грн	8
Гранти для переробних підприємств	Розвиток і відновлення пошкоджених потужностей[61]	До 8 млн грн (від 5 нових робочих місць); до 16 млн грн на відновлення, не більше підтверджених збитків	8
Реєстр збитків для України (RD4U)	Заяви юросіб через «Дію»: майно, упущена вигода, активи, евакуація, інші економічні й гуманітарні витрати[35]	Усі категорії відкрито з 10.09.2026; збитки з 24.02.2022	8
Перелік територій бойових дій (наказ Мінрозвитку № 987, зі змінами)	Від статусу громади залежать податкові пільги й програми підтримки	Новий формат переліку з 05.06.2026; статус перевіряйте щомісяця	11

ДЖЕРЕЛА

Джерела

Посилання перевірено у вересні 2026 року. Правові норми наведено станом на 26.09.2026.

1. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів. Держспецзв'язку. cip.gov.ua
2. Відновлено функціонування Єдиних та Державних реєстрів. Міністерство юстиції України, 20.01.2025; Кібератака на державні реєстри. Українська правда, 23.12.2024; УНІАН, 20.01.2025. minjust.gov.ua; pravda.com.ua; unian.ua
3. Збій у роботі «Укрзалізниці». Економічна правда, 03.2025; Інтерфакс-Україна, 04.2025. epravda.com.ua; interfax.com.ua
4. SBU: Russian GRU hackers behind Kyivstar cyberattack. The Kyiv Independent. kyivindependent.com
5. Вплив відключень електроенергії відчули 80 % компаній — опитування ЄБА. Forbes.ua, 21.01.2026. forbes.ua
6. Diplomatic immunity for data: Estonia creates a virtual embassy. Microsoft EU Policy Blog, 2017. blogs.microsoft.com
7. Закон України «Про хмарні послуги» № 2075-IX від 17.02.2022. zakon.rada.gov.ua
8. Safeguarding Ukraine's data to preserve its present and build its future. Amazon. aboutamazon.com
9. Mandiant M-Trends 2026: global median dwell time 14 days in 2025. Help Net Security, 24.03.2026. helpnetsecurity.com
10. Industrial Generator Maintenance Schedule & Checklist. PowerGen Enterprises, 2026. powergenenterprises.com
11. LiFePO4 Battery Cycle Life & Durability. EcoTree Lithium. ecotreelithium.co.uk
12. Lloyd's Market Bulletins Y5381 (08.2022) і Y5433 (state backed cyber-attack exclusions). Lloyd's. lloyds.com
13. Guidelines for Long-Term Fuel Storage of Diesel. Bell Performance. bellperformance.com
14. What is Wet Stacking and how do Load Banks prevent it? Avtron Power Solutions. avtronpower.com
15. Why you should not charge a lithium battery below 0°C. REDARC Electronics. redarcelectronics.com
16. The True Cost of Downtime 2024 (Siemens): a comprehensive analysis. AEMT. theaemt.com
17. The $600 Billion Wake-up Call: New Splunk Research Reveals Downtime is a Systemic Business Crisis. Cisco Newsroom, 05.2026. newsroom.cisco.com
18. Hiscox: cyber attacks cost small firms USD $52,000. IT Brief. itbrief.co.uk
19. Leveraging the PACE Plan into the Emergency Communications Ecosystem. CISA, 2024. cisa.gov
20. H. von Moltke. Über Strategie, 1871; англ. переклад: D. Hughes (ed.). Moltke on the Art of War: Selected Writings. Presidio, 1993. Походження цитати: quoteinvestigator.com
21. ADP 6-0. Mission Command: Command and Control of Army Forces. Headquarters, Department of the Army, 07.2019. armypubs.army.mil
22. Checklist Memory Items. EASA Research Project 2013.01, Final Report; Checklists — Purpose and Use. SKYbrary. easa.europa.eu; skybrary.aero
23. K. Weick, K. Sutcliffe. Managing the Unexpected: Sustained Performance in a Complex World. 3rd ed. Wiley, 2015.
24. Stock Market Circuit Breakers. Investor.gov, U.S. SEC. investor.gov
25. TC 25-20. A Leader's Guide to After-Action Reviews. Headquarters, Department of the Army, 09.1993. hsdl.org
26. START Adult Triage Algorithm. CHEMM, U.S. Department of Health and Human Services. chemm.hhs.gov
27. Дефіцит кадрів турбує 69 % підприємств — опитування ІЕД. Forbes.ua, 21.09.2026. forbes.ua
28. Кодекс законів про працю України, ст. 119 (у редакції з 19.07.2022); Гарантії трудових прав працівників, призваних на військову службу. WikiLegalAid; Kadroland. kadroland.com
29. Який об'єм палива юрособа зберігає без ліцензії та реєстрації акцизного складу. 7eminar. 7eminar.ua
30. Як змінювалася кількість будинків без тепла в столиці в січні–лютому 2026 року. Слово і Діло, 16.02.2026. slovoidilo.ua
31. Інфляційний звіт, липень 2026 року. Національний банк України. bank.gov.ua
32. Постанова КЦС ВС щодо зобов'язань у валютному еквіваленті; Цивільний кодекс України, ст. 524, 533. Верховний Суд. supreme.court.gov.ua
33. 2026 рік для ФОП: ставки єдиного податку та військового збору. ДПС України. tax.gov.ua
34. Закон України «Про передачу, примусове відчуження або вилучення майна в умовах правового режиму воєнного чи надзвичайного стану» № 4765-VI; Примусове відчуження або вилучення майна в умовах воєнного стану. Система безоплатної правничої допомоги. legalaid.gov.ua
35. Реєстр збитків відкрив усі категорії заяв для юридичних осіб. Київська ОВА, 09.2026; Register of Damage for Ukraine: launch of claims categories for legal entities. RD4U, Council of Europe, 04.2026; Європейська правда, 10.09.2026. koda.gov.ua; rd4u.coe.int; eurointegration.com.ua
36. Майно знищене внаслідок обстрілу: перелік документів від ДСНС, Нацполіції, ТПП та покрокова інструкція. DTKT. news.dtkt.ua
37. Форс-мажорні обставини в умовах воєнного стану (огляд практики). Верховний Суд, 14.10.2024. court.gov.ua
38. Податкове резидентство: як українцям платити податки за кордоном. Уповноважений Верховної Ради з прав людини. ombudsman.gov.ua
39. Україна успішно здійснила перший міжнародний автоматичний обмін інформацією про фінансові рахунки. Кабінет Міністрів України, 04.10.2024. kmu.gov.ua
40. Консульські послуги для осіб призовного віку 18–60 років. МЗС України. mfa.gov.ua
41. єРобота: 12 млрд грн інвестувала держава в розвиток малого й середнього бізнесу через гранти. Міністерство економіки України. me.gov.ua
42. EBRD and EU provide further support to MSMEs in Ukraine. EBRD, 2026; EIB Group provides EU-backed guarantees to expand finance for war-affected businesses in Ukraine. EIB, 14.01.2026. ebrd.com; eib.org
43. Toyota, citing lessons learned from 2011 earthquake, expects no major semiconductor impact. Supply Chain Dive. supplychaindive.com
44. Порядок застосування ПРРО, наказ Мінфіну № 317 від 23.06.2020, розд. V; ПРРО: режим офлайн під час воєнного стану (Закон № 2120-IX). ДПС. tax.gov.ua
45. Нацполіція: понад 1200 повідомлень про мінування. Радіо Свобода, 30.03.2026. radiosvoboda.org

46. Directive (EU) 2022/2555 (NIS2), Article 23. eur-lex.europa.eu
47. Постанова КМУ № 1092 від 04.09.2026; Червоний та жовтий рівень загрози за Постановою № 1092. DTKT. news.dtkt.ua; Бізнесу дали три місяці: нові правила роботи під час тривог. Мінфін, 22.09.2026; Робота компаній без укриття допускається лише за погодженням з трудовим колективом. ЛІГА:ЗАКОН, 09.2026. minfin.com.ua; ligazakon.net
48. Закон України № 4200-IX (чинний з 01.02.2025): КУпАП ст. 175-3, ККУ ст. 270-2. За необлаштування та недопуск до укриттів запроваджено адміністративну та кримінальну відповідальність. ЛІГА:ЗАКОН. ligazakon.net
49. Кривий Ріг, Марганець, Покров і Нікополь мають проблеми з водою. Радіо Свобода, 06.2023. radiosvoboda.org; Міста, фермери, промисловість: хто залишився без води після підриву Каховської греблі. Тексти.org.ua, 03.07.2023. texty.org.ua
50. Наказ Мінрозвитку № 987 від 26.05.2026. zakon.rada.gov.ua; Мінрозвитку затвердило новий Перелік територій бойових дій та ТОТ. Донецька ОДА, 09.06.2026; пільги з плати за землю. ДПС у Київській області. dn.gov.ua; tax.gov.ua
51. ISO 22301:2019 Security and resilience — Business continuity management systems. iso.org
52. NIST Releases Version 2.0 of Landmark Cybersecurity Framework, 26.02.2024. nist.gov
53. NIST Revises SP 800-61: Incident Response Recommendations and Considerations, 04.2025. nist.gov
54. Resilience, civil preparedness and Article 3. NATO. nato.int
55. Security of supply: overview. National Emergency Supply Agency (Huoltovarmuuskeskus), Finland. huoltovarmuuskeskus.fi
56. Regulation (EU) 2022/2554 (DORA). eur-lex.europa.eu
57. Regulation (EU) 2016/679 (GDPR), Article 33. eur-lex.europa.eu
58. Постанова КМУ № 692 від 30.05.2026. Перегляд критичності роботодавців до 1 вересня 2026 р. та інші зміни у бронюванні: аналіз постанови КМУ № 692. DTKT; Зарплатні вимоги для бронювання з 1 вересня 2026. 7eminar, 25.09.2026. news.dtkt.ua; 7eminar.ua
59. Роботодавці можуть отримати кошти за працевлаштування ветеранів. Дніпропетровський обласний центр зайнятості. dcz.gov.ua
60. Енергокредит для бізнесу — кредит під 0 % на енергообладнання. Фонд розвитку підприємництва. energycredit.bdf.gov.ua
61. «Власна справа 2.0»: гранти на відкриття та масштабування бізнесу за новими правилами. Дія.Бізнес; Грант на виробництво переробної промисловості. Дія. business.diia.gov.ua; diia.gov.ua

Рекомендована література

- C. Perrow. *Normal Accidents: Living with High-Risk Technologies.* 1984.
- R. Cook. *How Complex Systems Fail.* 1998. how.complexsystems.fail
- D. Vaughan. *The Challenger Launch Decision.* 1996.
- S. Dekker. *Drift into Failure.* 2011.
- T. DeMarco. *Slack: Getting Past Burnout, Busywork, and the Myth of Total Efficiency.* 2001.
- C. Heath, D. Heath. *Decisive: How to Make Better Choices in Life and Work.* 2013.
- G. Klein. *Sources of Power: How People Make Decisions.* 1998.
- N. N. Taleb. *Antifragile: Things That Gain from Disorder.* 2012.
- C. O'Reilly, M. Tushman. *Lead and Disrupt: How to Solve the Innovator's Dilemma.* 2016.
- K. Weick, K. Sutcliffe. *Managing the Unexpected.* 2015.

ITEZ
IT easy

ПРО ITEZ

ITEЗ — українська IT-компанія зі Львова, працює з 2018 року. IT-аутсорсинг і технічна підтримка, хмарні сервіси, розміщення обладнання в дата-центрі, монтаж IT-інфраструктури для бізнесу.

ТЕЛЕФОН +38 (098) 220 97 25

E-MAIL office@itez.com.ua

САЙТ itez.com.ua

Вересень 2026

Наступний перегляд — березень 2027. Правові норми наведено станом на вересень 2026.

Як цитувати

ITEZ. Бізнес, що працює попри все: практичний посібник зі стійкості бізнесу. Львів, 2026. itez.com.ua.

Застереження

Документ має інформаційний характер і не є юридичною, податковою чи фінансовою консультацією. Кожен юридичний крок узгоджуйте з фахівцем.