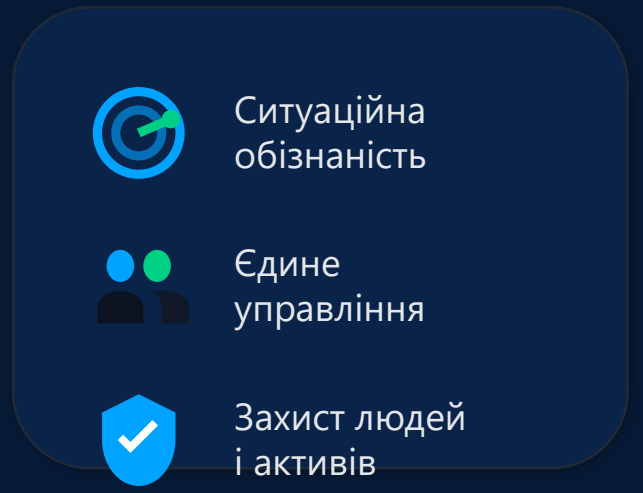
Кризовий штаб компанії під час надзвичайних подій

Хто що робить у перші 30 хвилин • практичний протокол

Руслан ПАПЕНКО

т.моб.: +380633212659



Версія: 1.0

Навіщо кризовий штаб

Коли «всі бігають» — це не управління, це хаос з бейджиками

Мета №1: люди

- зберегти життя і здоров’я
- зняти паніку та забезпечити керованість
- організувати евакуацію/укриття/медичну допомогу

Мета №2: стабілізація

- локалізувати подію й зупинити ескалацію
- підключити відповідні служби
- забезпечити контроль доступу та периметр

Мета №3: стабільність бізнесу

- захистити активи та дані
- зберегти репутацію й комплаєнс
- запустити відновлення роботи

Ключові принципи

- Єдине управління (Incident Commander) — одне джерело рішень
- Швидка комунікація — один канал, один голос назовні
- Фіксація рішень — журнал подій, відповідальні, дедлайни
- Пріоритети: люди → активи/дані → репутація → гроші

Система безпеки компанії

Не “охорона на вході”, а керована модель захисту бізнесу

Компоненти системи

- Люди (ролі, відповідальність, заміни)
- Процеси (SOP, реагування)
- Техніка (СКД, відео, сигналізації, IT-моніторинг)
- Правила (режим, доступи, підрядники, документи)
- Контроль (аудит, KPI, тренування)

Контури безпеки

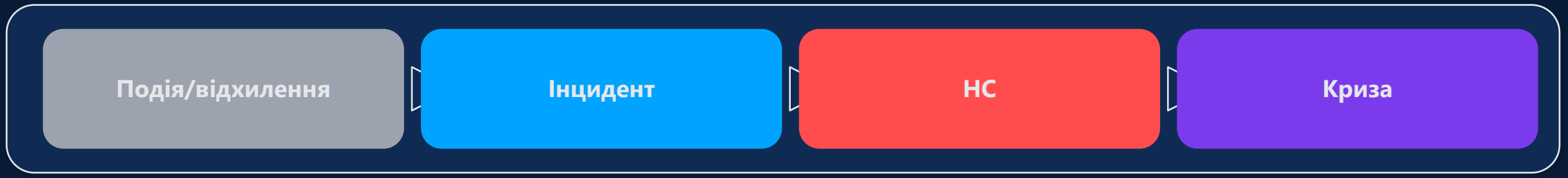
- Фізична: периметр, режимні зони, логістика
- Охорона/чергова служба: 24/7, реагування
- Пожежна/техногенна: евакуація, небезпечні роботи
- Інфо/ТЗІ/діловодство: доступи, носії інформації, переговори
- Кібер: резерви, сегментація, IR-процедури
- Кадрова/антиінсайдер: допуски, перевірки

Роль загальної служби охорони

- Система 24/7: доступ, периметр, тривоги
- Первинна локалізація до прибуття служб/штабу
- Інцидент-репортинг: що/де/коли/хто/дії
- Інтеграція: СКД + відео + тривожні кнопки

Надзвичайні ситуації

Як відрізнити “інцидент” від НС і від кризи



Що таке НС (практично)

- Подія створює загрозу життю/здоров’ю або значні збитки
- Є ризик швидкої ескалації або ситуація “неясна”
- Потрібні невідкладні скоординовані дії та/або зовнішні служби
- Зупиняються критичні процеси (виробництво, склад, IT, логістика)

Ознаки, що час активувати штаб

- Є/може бути шкода людям
- Подія виходить за межі одного підрозділу
- Необхідна евакуація/укриття/локдаун
- Є медійність або контакт з регуляторами/органами
- Багато чуток, мало фактів

Тероризм і терористичні загрози для бізнесу

Ціль — не лише шкода, а й резонанс, страх і хаос

Базові поняття

- Тероризм: насильство/загроза насильства для залякування
- Ефект: страх + медійність + тиск на рішення
- Для бізнесу важлива дисципліна протоколів і комунікацій

Як виглядає загроза

- Погроза вибуху / мінування (в т.ч. фейки)
- Диверсії: підпал, саботаж, псування інфраструктури
- Напади на персонал/керівництво
- Кібер як елемент гібридної дії (шок + зупинка)

Принципи протидії

- Контроль доступу + режим
- Навчання персоналу: ознаки й алгоритми
- Журналювання інцидентів і збереження даних
- Один голос назовні, мінімум деталей
- Чіткі тригери активації штабу

Безпековий аудит

Профілактика НС: дешевше, ніж “героїчно гасити”

Що це таке

- Системна перевірка ризиків, вразливостей і готовності
- Оцінка: люди • процеси • техніка • документи
- Результат — пріоритети та план змін, а не “папка для полички”

Що перевіряємо (ядро)

- Фізична безпека: периметр, доступ, логістика, транспорт
- Техніка: СКД/відео/, резервування
- Кібер/ТЗІ: доступи, сегментація, бекапи, логи
- Персонал: допуски, перевірки, антиінсайдер

Вихід аудиту для керівника

- Карта ризиків + Top-10 “дір” із бізнес-впливом
- План 30/60/90 днів: відповідальні, бюджет, швидкі перемоги
- KPI готовності: час реагування, покриття камер, дисципліна доступів, тренування
- Оновлені SOP/чеклісти + сценарні навчання

Тригери активації кризового штабу

Коли “пора”, а не “може завтра”

Активуємо штаб, якщо…

- Є загроза людям (травми, пожежа, напад, евакуація)
- Зупинка критичного процесу (виробництво/логістика/IT)
- Підозра на витік даних / кібератаку / блокування
- Потрібні зовнішні служби або масове управління людьми
- Є медійний резонанс або ризик для репутації
- Є регулятори/органи/обшуки/перевірки

Поріг рішення

- Якщо ціна помилки висока — активуємо швидко
- Краще “зайвий” запуск, ніж пропущена ескалація
- Після стабілізації — зняли режим і повернулись у норму

Правило достовірності

- 1 джерело = чутка
- 2+ незалежних джерела = робочий факт
- Кожен факт має: час • місце • джерело • підтвердження

Склад кризового штабу (мінімальний “скелет”)

Коротко: хто має бути “на лінії” у перші хвилини

Керівник інциденту (Incident Commander)

Безпека / охорона

Операції / виробництво

IT / кібер

HR (персонал)

Юрист

PR / комунікації

Фінанси / закупівлі

Правило

- Кожна роль має мати заміну

Ролі й відповідальність (RACI-логіка)

Щоб не було “я думав, це робить IT/охорона/юрист”

Позначення: R — виконує • A — затверджує • C — консультує • I — інформується

Функція	R	A	C	I
Захист людей (евакуація/укриття/медицина)	Охорона	IC	Пол/ДСНС	Всі
Локалізація події / периметр / доступ	Охорона	IC	///////	PR
Кібер / збереження логів	IT	IC	Юрист	Операції
Комунікація назовні (медіа/партнери)	PR	IC	Юрист	Всі
Рішення про зупинку/перезапуск процесів	////////	IC	Безпека/IT	Фін
Документація / журнал подій / докази	Офіцер штабу	IC	Юрист	Всі

Перші 30 хвилин: 0–5

0–5

хв

Ключові дії

- Призначити керівника інциденту (IC) — одразу
- Підтвердити факт: що/де/хто/ризики
- Захист людей: укриття/евакуація/медична допомога
- Запуск штабу: канал зв’язку, учасники, місце/онлайн
- Перше повідомлення персоналу: коротко, фактами

Контрольні точки

- Ситуація під контролем керівника
- Є базова картина події
- Люди та процеси у безпечному режимі
- Штаб активований і працює
- Внутрішня паніка не масштабується

Перші 30 хвилин: 5–15

5–15

хв

Ключові дії

- Оцінити масштаб і сценарій ескалації
- Ізолювати зону: периметр, доступ, маршрути
- Виклик екстрених служб через одного відповідального
- ІТ: збереження логів (за потреби)
- Визначити перший бізнес-пріоритет (що зупиняємо/захищаємо)

Контрольні точки

- Зона контролюється
- Зовнішні служби в дорозі/на зв’язку
- Ризики ескалації зафіксовані
- Дані/докази не “випаровуються”
- Є фокус, а не 20 задач одночасно

Перші 30 хвилин: 15–30

Рішення → комунікація → ресурси (і все це під запис)

Ситуаційний звіт, 10 рядків

- Що сталося (1 речення)
- Де/коли/масштаб
- Люди: постраждалі/евакуація/ризики
- Статус процесів: що стоїть/що працює
- Що робимо далі (2–3 кроки)

Рішення штабу (мінімум)

- Рішення №1: зупинка/продовження критичних процесів
- Рішення №2: хто і що говорить назовні (один голос)
- Рішення №3: ресурси (охорона/підрядники/резервні майданчики)
- Все — з відповідальними і дедлайнами

Матриця пріоритетів рішень

1) Люди (життя/здоров’я) — без компромісів
2) Зупинка ескалації (вогонь/вода/агресор/витік)
3) Активи й дані (критичні системи, документи)
4) Репутація та комплаєнс (правда, але дозовано)
5) Гроші (витрати/втрати) — останні у черзі

Після 30 хвилин

Стабілізація → відновлення → розбір польотів (AAR)

Стабілізація (1–4 год)

- План дій по сценаріях (що якщо погіршиться)
- Ротація людей, ресурсів, чергування
- Безпека периметра і контроль доступу
- Підтримка персоналу (стрес/медицина/логістика)

Відновлення роботи

- План дій: резервні майданчики, процеси, IT
- Оцінка збитків і пріоритети відновлення
- Комунікація з клієнтами/партнерами (вихід у “стабільність”)
- Контроль ризиків повторної події

Висновки

- Що спрацювало / що ні
- Де була затримка і чому
- Оновити SOP і чеклісти
- План дій на 30 днів
- Навчання на кейсі

Комунікації та ситуаційна обізнаність

Один голос + якісні дані = контроль (а не чутки)

Один голос (PR/IC)

- Внутрішньо: коротко, фактами, без “версій”
- Зовні: медіа/партнери/регулятори — централізовано
- Заборона самодіяльних коментарів і постів
- Повідомлення: що відомо • що робимо • що не коментуємо

Дані (джерела) і якість

- Черговий/охорона: відео, СКД, датчики, IT-логи
- Очевидці: тільки через збір фактів (час/місце/джерело)
- Оновлення інформації кожні 15–30 хв або по події
- Ніяких “припущень” у зовнішніх комунікаціях

Журнал подій

- Хронологія: час → подія → рішення → відповідальний → статус
- Фіксуємо дзвінки, накази, доступи, дії систем (логування)
- Докази: відео/фото/логи зберігаємо, не “чистимо”
- Журнал = захист від хаосу + основа для розбору і юридичних питань

Готовність ДО інциденту

Кризу не обирають. Обирають готовність.

Обов’язкові артефакти

- Положення про кризовий штаб + контакти 24/7
- Чеклісти за типами НП (пожежа, мінування, напад, кібер, аварія)
- Мапи евакуації/укриття, точки збору, доступи
- Шаблони повідомлень

Тренування

- Постійні та позапланові навчання та тренінги
- Навчання охорони/чергових: реагування + журнал
- Перевірка комунікацій: канали, резерви, дисципліна
- Актуалізація контактів і замін ролей

Мінімальний кризовий набір

- Резервні телефони/ноутбуки, powerbank, SIM/зв’язок
- Доступи до систем (за принципом мінімально необхідного)
- Ключі/карти доступу, ліхтарі, аптечка, радіостанції
- Контакти підрядників і служб, шаблони документів

Тезис для керівника: швидкість = процедура + тренування + дисципліна.