УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

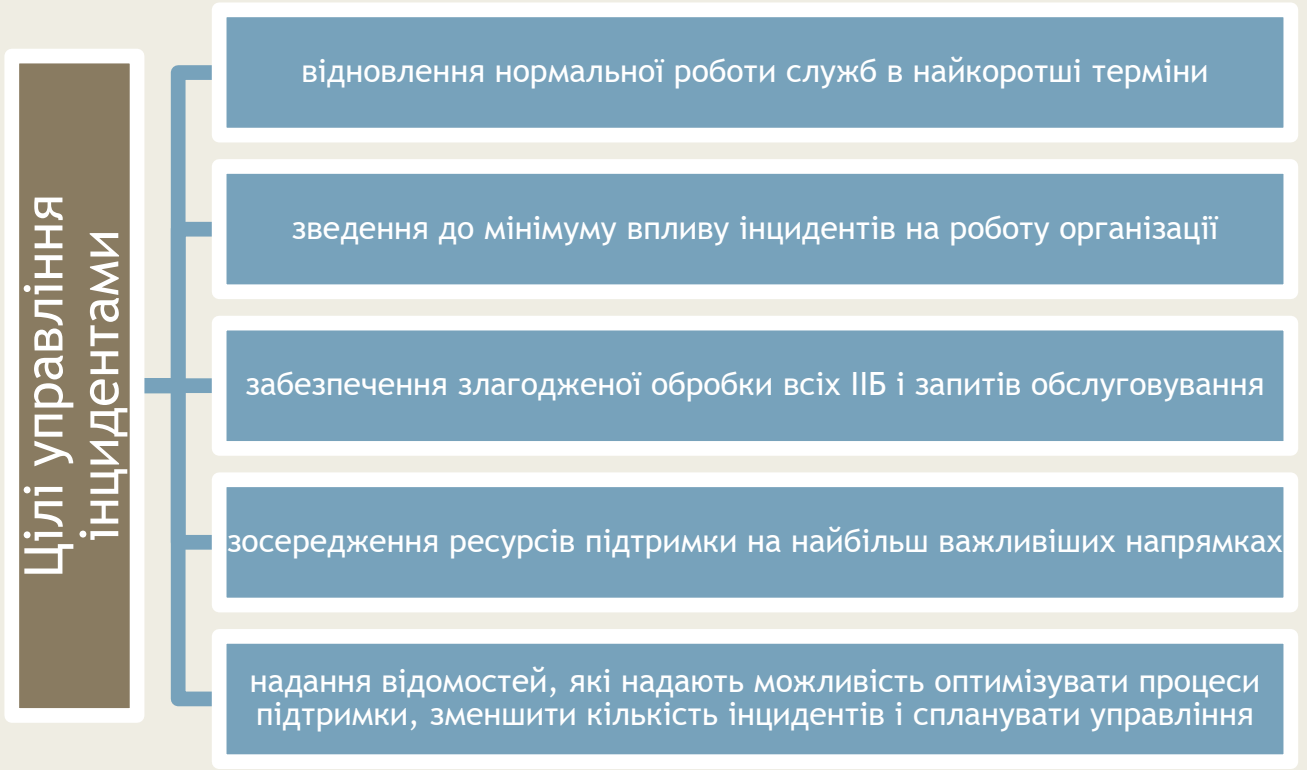
Лекція 14. Управління інцидентами в сфері інформаційної безпеки

1. Основні цілі та задачі управління інцидентами інформаційної безпеки.
2. Аналіз інцидентів інформаційної безпеки.
3. Особливості управління інцидентами інформаційної безпеки.

Управління інцидентами ІБ

Управління інцидентами інформаційної безпеки (УІІБ) є важливим процесом, який забезпечує організацію можливістю своєчасного виявлення інциденту та якомога швидшого реагування на нього за допомогою коректно обраних засобів підтримки.

Основна задача УІІБ – оперативно відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на діяльність організації з метою підтримки якості і доступності служб (сервісів) на максимально можливому рівні.



Основні заходи створення СУІІБ

Завдання, які вирішує СУІІБ

- Оперативний моніторинг стану інформаційної безпеки в межах обраної сфери дії СУІІБ
- Виявлення, облік, реагування, розслідування та аналіз ІІБ
- Інформування вищого керівництва і зацікавлених осіб про поточний стан інформаційної безпеки

Управління інцидентами інформаційної безпеки – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються інформаційних систем, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходи, які необхідно вжити для того, щоб інцидент не повторився у майбутньому.

Побудова процесу управління ІІБ

1. отримання інформації про інцидент
2. отримання додаткової інформації, пов'язаної з виявленим порушенням
3. аналіз ситуації, локалізація порушення і оперативне застосування контрзаходів
4. встановлення причин, через які стало можливим порушення, що трапилося, і, можливо, визначення відповідальних осіб
5. проведення профілактичних заходів, розробка і впровадження заходів з недопущення повторного порушення

Ефективність процесу управління інцидентами

СУІБ надає можливість:

- консолідувати всю інформацію про інциденти в єдиному сховищі;
- створити єдиний центр УІІБ з метою забезпечення контролю і координації дій з локалізації і розслідування;
- підвищити швидкість реагування і оперативність виявлення причин інциденту;
- підвищити достовірність одержуваних результатів з виявлення причин інциденту, відповідальних осіб і визначення необхідних дій, усунення наслідків інциденту і застосування контрзаходів;
- формувати статистику інцидентів ІБ, виявляти тенденції її змін і аналізувати динаміку цих змін;
- автоматизувати застосування контрзаходів для зниження ризику ІБ з виявлення типових інцидентів.

Ознаки інциденту інформаційної безпеки

Можливі порушення вимог конфіденційності

- інциденти, через які отримано несанкціонований доступ до інформації;
- втрата носіїв інформації за межами приміщення;
- втрата або крадіжка ноутбука;
- спроби персоналу організації отримати доступ вище наданого рівня;
- спроби зсередини або ззовні отримати доступ до систем (злам).

Можливі порушення вимог цілісності

- втрата даних або незавершені транзакції;
- віруси, «троянські коні» (зловмисне ПЗ);
- пошкоджені сектори на жорстких дисках, помилки парності і пам'яті;
- невірні контрольні суми або значення хеш-функцій.

Можливі порушення вимог доступності

- зупинка роботи протягом неприйнятного періоду часу;
- віруси, «троянські коні»;
- крадіжка ноутбуків, комплектуючих або носіїв інформації.

Аналіз інцидентів інформаційної безпеки

Повідомлення про події інформаційної безпеки

- Ці повідомлення повинні якомога швидше поширюватися належними управлінськими каналами.

Повідомлення про уразливості захисту

- Необхідно зобов'язати всіх співробітників, підрядчиків і користувачів із сторонніх організацій, що використовують інформаційні системи та сервіси, відмічати і повідомляти про всі спостережувані або передбачувані уразливості захисту систем або сервісів.

Відповідальність і процедури

- Необхідно встановити відповідальність керівників та визначені процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки.

Навчання інцидентам ІБ

- Повинні бути реалізовані механізми, які надають можливість виміряти та відстежувати типи, об'єми і вартість ІІБ.

Збір доказів

- Якщо в результаті аналізу ІІБ встановлено, що дії осіб потребують правової кваліфікації, то необхідно зібрати, зберегти та надати докази такої протиправної діяльності у встановленому правовою системою певної країни порядку.

Нормативні документи з УІІБ

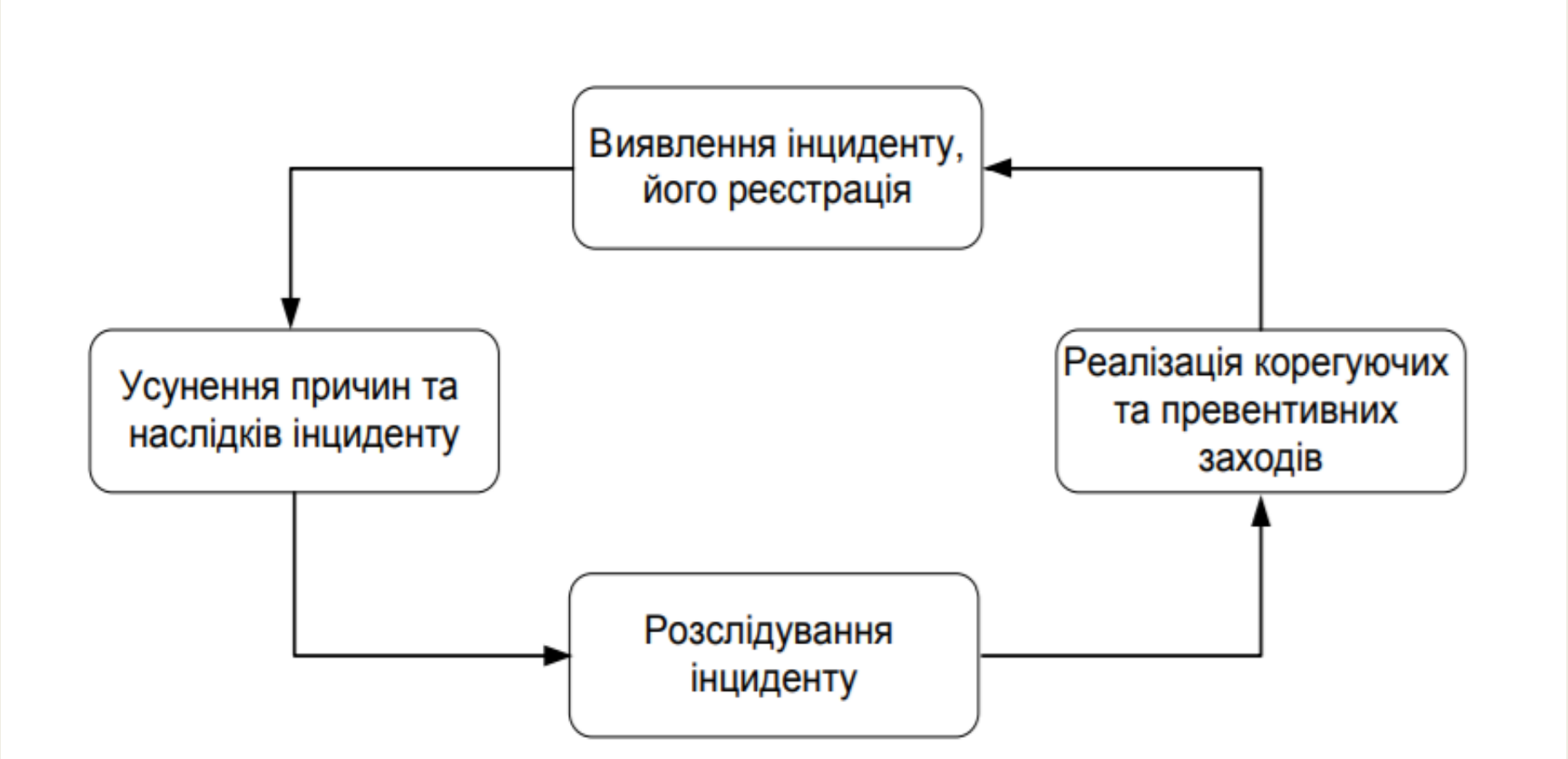
Мають описувати:	визначення ІІБ, перелік подій, що є інцидентами (які є інцидентом саме в цій компанії);
	порядок оповіщення відповідальних осіб про виникнення інциденту (необхідно визначити формат оповіщення, а також відобразити контактну інформацію осіб, яких треба оповіщати про інцидент);
	порядок усунення наслідків і причин ІІБ;
	порядок розслідування ІІБ (визначення причин інциденту, винних у виникненні інциденту, порядок збору та збереження доказів);
	накладання дисциплінарних стягнень;
	реалізацію необхідних корегувальних і превентивних заходів.

Приклади інцидентів ІБ

- відмова в обслуговуванні сервісів, засобів обробки інформації, обладнання
- порушення конфіденційності та цілісності цінної інформації
- недотримання вимог інформаційної безпеки, прийнятих в компанії
- незаконний моніторинг інформаційної системи
- виявлення шкідливих програм
- компрометація інформаційної системи
- неавторизована зміна даних на сайті компанії
- залишення комп'ютера незаблокованим без нагляду
- пересилання конфіденційної інформації за допомогою корпоративної або особистої пошти

Етапи формування СУІІБ відповідно до моделі PDCA

Модель життєвого циклу процесу УІІБ



Особливості управління інцидентами відповідно до ITIL

Управління інцидентами відповідно до ITIL – один з процесів, який відповідає за управління життєвим циклом усіх інцидентів. Підхід ITIL визначає, що основна мета управління інцидентами – якнайшвидше відновлення послуги для користувачів.

Управління інцидентами призначено для максимально швидкого відновлення нормальної експлуатації послуг та мінімізації несприятливого впливу на бізнес у разі виникнення інциденту.

Місце процесу управління інцидентами серед усіх процесів ITIL

Модель інцидентів ITIL

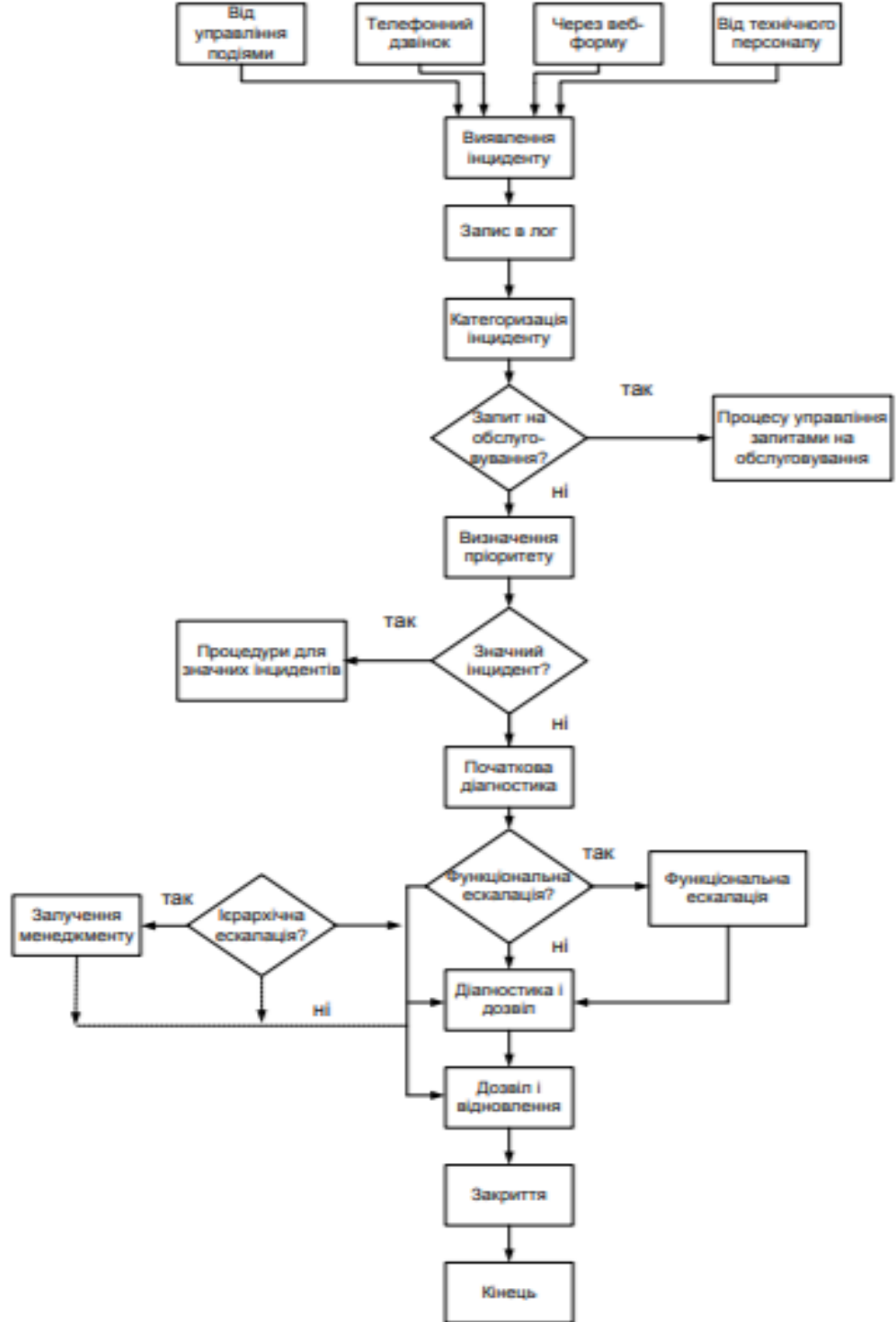
Модель містить:	кроки, які необхідно вжити для того, щоб вирішити інцидент;
	хронологічний порядок кроків;
	розподіл відповідальності - хто і що робить;
	часові рамки і порогові величини для завершення кожної дії;
	питання того, з ким необхідно пов'язати і на якому етапі.

Основні етапи управління інцидентами відповідно до ITIL

Для того щоб вирішити інцидент, його необхідно спочатку виявити, тобто *ідентифікувати*. Усі ключові компоненти повинні контролюватися, щоб своєчасно виявляти збої або можливості їх виникнення.

Після того, як інцидент виявлений, інформацію про нього необхідно *занести в бланк*. Запис про інцидент є основою для вирішення останнього відповідною командою техпідтримки.

Терміновість (Urgency) – показник того, наскільки швидко з моменту свого прояву інцидент, проблема або зміна набуде істотного вплив на бізнес.



Запис про інцидент повинен містити:

- унікальний ідентифікатор інциденту
- категорію інциденту
- терміновість інциденту
- вплив інциденту
- пріоритет інциденту
- дата і час запису
- ім'я/ID людини або групи, що зробила запис про інцидент
- метод повідомлення
- ім'я/відділ/номер/розташування користувача
- метод зворотного зв'язку

Запис про інцидент повинен містити:

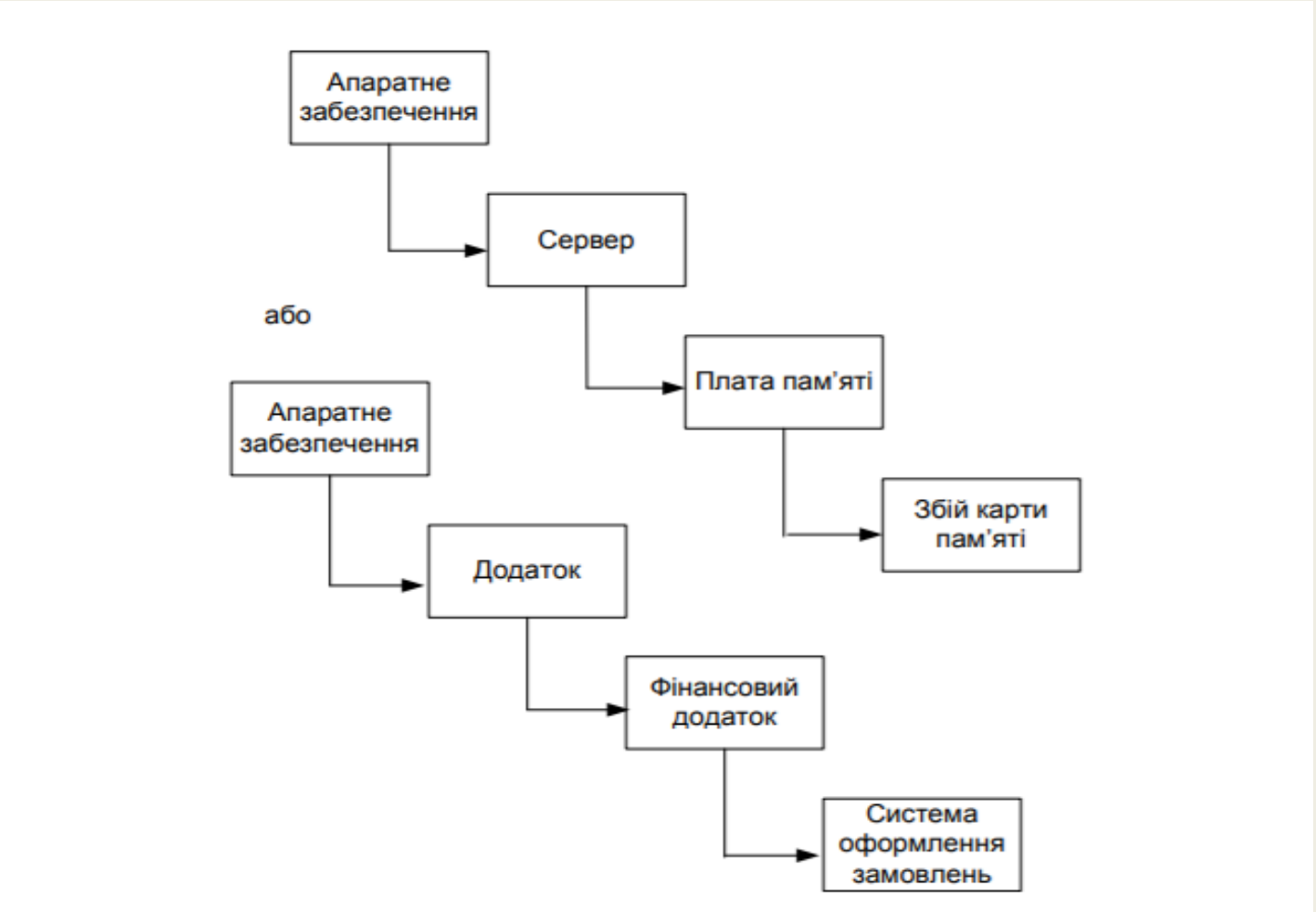
- опис симптомів (ознак)
- статус інциденту
- пов'язані конфігураційні одиниці
- група підтримки/ співробітник, якому переадресовано інцидент
- пов'язана з інцидентом проблема/відома помилка
- заходи, вжиті для вирішення інциденту
- час і дата вирішення інциденту
- категорія закриття
- час і дата закриття

Варіанти категорування інцидентів відповідно до ITIL

Наступний етап вирішення інциденту – *категорування*. Воно необхідне для подальших заходів, зокрема, пошуку відомих помилок і проблем, які могли стати причиною виникнення інциденту.

Зазвичай використовується три, чотири рівня категорування.

Немає стандартних методів для категорування інцидентів. Кожна організація сама визначає, які категорії буде використовувати.



Оцінка впливу ІІБ

Пріоритет інциденту визначається залежно від терміновості і впливу. *Вплив* інцидентів найчастіше визначається кількістю користувачів, діяльності яких він торкається.

Тим не менш, цей показник не завжди є об'єктивним. У деяких випадках вплив інциденту навіть на одного єдиного користувача може мати значний негативний вплив на бізнес в цілому.

Матриці для визначення пріоритетів інциденту та часу, за який його необхідно вирішити

Визначення пріоритету залежно від впливу та терміновості інциденту

		Вплив		
		Високий	Середній	Низький
Терміновість	Висока	1	2	3
	Середня	2	3	4
	Низька	3	4	5

Визначення часу для вирішення інциденту залежно від пріоритету

Пріоритет	Характеристика	Час вирішення
1	Критичний	1 год
2	Високий	8 год
3	Середній	24 год
4	Низький	48 год
5	Планується	Запланувати

Основні етапи управління інцидентами відповідно до ITIL

Етап початкової діагностики стосується інцидентів, які надійшли до Service Desk. Фахівець повинен спробувати вирішити інцидент і закрити його. Якщо це неможливо, він повідомляє користувачеві ідентифікаційний номер інциденту.

Якщо Service Desk не може вирішити інцидент або терміни першого ступеня вирішення інцидентів минули, інцидент має бути негайно переданий іншим фахівцям. Тобто у такому випадку застосовується ескалація.

Ескалація (Escalation) – діяльність, спрямована на отримання додаткових ресурсів, коли це необхідно для досягнення цільових показників рівня послуги або очікувань замовників.

Функціональна ескалація

- передача інциденту в групу підтримки з більш високою кваліфікацією і компетенцією;
- відповідальність за інформування користувача про стан вирішення інциденту покладається на Service Desk.

Ієрархічна ескалація

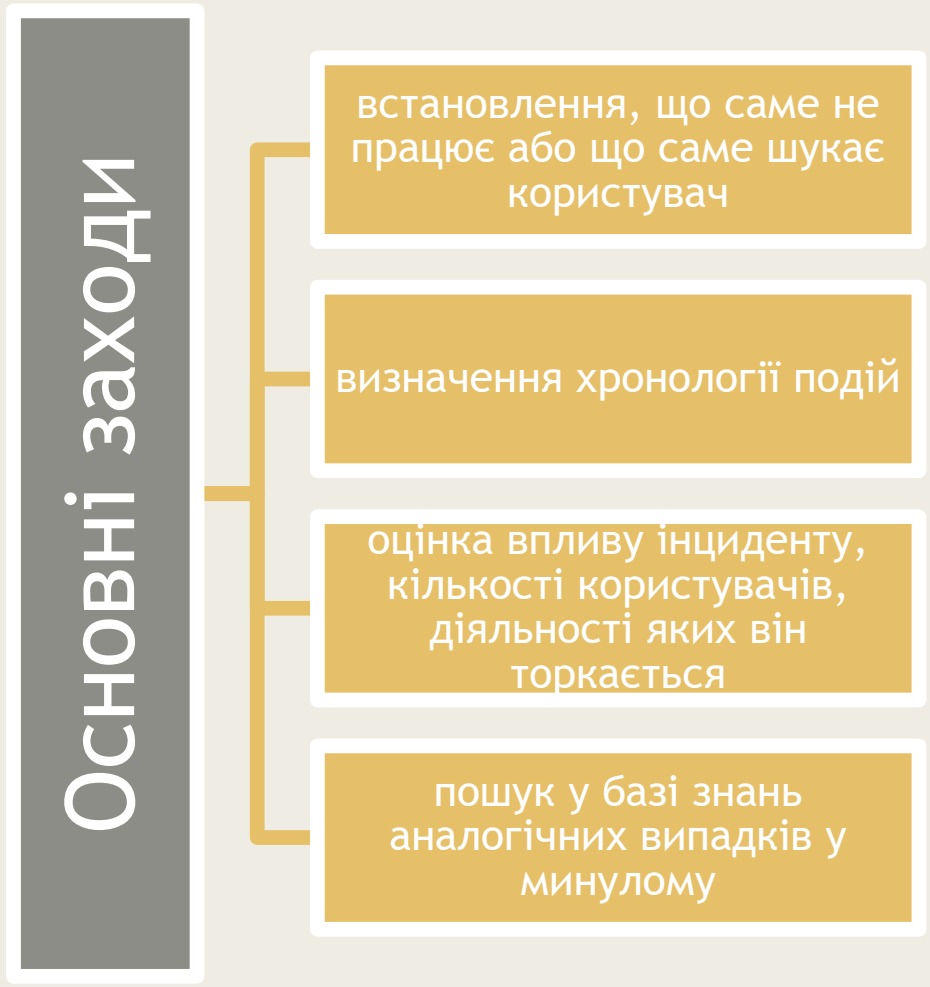
- передбачає залучення або просто інформування керівників вищого рівня про виникнення інциденту;
- сприяє своєчасному прийняттю рішень про виділення додаткових ресурсів і залучення зовнішніх організацій у процес вирішення інциденту.

Основні етапи управління інцидентами відповідно до ITIL

Наступний етап вирішення інцидентів - *дослідження та діагностика.*

У випадках, коли користувачі звертаються тільки для пошуку інформації, Service Desk повинен надати її у найкоротший проміжок часу. Але якщо користувач повідомляє про технічну проблему, це потребує вжиття заходів для з'ясування та діагностики інциденту.

Вирішення інциденту закінчується *закриттям*. Service Desk перевіряє, що всі дії, необхідні для вирішення інциденту, виконані, користувачі задоволені і згодні закрити інцидент.



Процедура закриття інциденту передбачає

- Закриття категорування
- Опитування задоволеності користувачів
- Перевірка повноти запису про інцидент
- Визначення причини інциденту, є вона постійною або періодично повторюється
- Формальне закриття інциденту

Метрики ефективності процесу управління

Загальна кількість інцидентів
Кількість інцидентів, що знаходяться на різних стадіях
Розмір поточного логу про інциденти
Кількість значних інцидентів
Середній час вирішення інцидентів
Відсоток інцидентів, вирішених в установлений час

Метрики ефективності процесу управління

Середні витрати на інцидент

Кількість повторно відкритих інцидентів і їх відсоткове співвідношення до загальної кількості інцидентів

Кількість інцидентів, неправильно направлених у команди підтримки

Кількість інцидентів, для яких були неправильно визначені категорії

Кількість віддалено вирішених інцидентів

Кількість інцидентів, вирішених з використанням кожної моделі інцидентів

Для ефективного управління інцидентами необхідно забезпечити:

- здатність виявляти інциденти якомога раніше;
- переконати персонал у тому, що всі інциденти мають бути занесені в журнал;
- доступність інформації про відомі проблеми і помилки, завдяки чому персонал зможе використовувати досвід попередніх інцидентів;
- взаємодія з CMS (Configuration Management System) для визначення взаємозв'язків конфігураційних одиниць та звернення до їх історії з метою підтримки першого рівня;
- взаємодія з SLM (Service Level Management) для коректної оцінки інцидентів, розстановки пріоритетів і виконання процедур ескалації.

Основні ризики для процесу управління інцидентами

- Велика кількість інцидентів, які не можуть бути вирішені у встановлені терміни у зв'язку з недостатністю ресурсів або їх недостатньою підготовкою
- Призупинення вирішення інцидентів через некоректну роботу засобів підтримки
- Недостатність або несвоєчасність інформації через некоректну роботу засобів підтримки або погану взаємодію з іншими процесами
- Недотримання контрактів та угод внаслідок їх недостатнього опрацювання та не реалістичність узгоджених цільових показників

Управління інцидентами ІБ

Обов’язки і процедури

- Повинна бути встановлена відповідальність і процедури, щоб гарантувати швидку, результативну і належну відповідь на інциденти інформаційної безпеки.

Сповіщення про події інформаційної безпеки

- Інформація про події, пов'язані з безпекою, повинна доводитись до керівництва через відповідні канали якнайшвидше.

Повідомлення про вразливості в інформаційної безпеки

- Від співробітників, які працюють за контрактом, використовують інформаційні системи і сервіси організації, необхідно вимагати фіксувати і доповідати про будь-які виявлені або передбачувані вразливості в ІБ систем і сервісів.

Оцінка і рішення про події інформаційної безпеки

- Події, пов'язані з інформаційною безпекою, повинні оцінюватися і потім прийматися рішення, чи слід їх класифікувати як інцидент інформаційної безпеки.

Управління інцидентами ІБ

Відповідь на інцидент інформаційної безпеки

- Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до документально оформлених методик.

Облік досвіду інцидентів інформаційної безпеки

- Знання, отримані з аналізу та дозволу інцидентів інформаційної безпеки, повинні використовуватися для зменшення ймовірності інцидентів в майбутньому або їх впливу.

Збір доказів

- Організація повинна визначити і застосовувати процедури для ідентифікації, збирання, одержання і збереження інформації, яка може служити в як докази.

Обов’язки і процедури

Рекомендації для встановлення обов'язків керівництва і процедур, пов'язаних з управлінням інцидентами інформаційної безпеки

Повинні бути встановлені обов'язки керівництва, щоб гарантувати, що такі процедури розроблені та організація відповідним чином про них сповіщена:

- процедури планування та підготовки реакції на інцидент;
- процедури моніторингу, виявлення, аналізу та інформування про події та інциденти інформаційної безпеки;
- процедури реєстрації дій з управління інцидентами;
- процедури управління свідоцтвами для суду.

Встановлена процедура повинна гарантувати, що:

- проблеми, пов'язані з інцидентами інформаційної безпеки, вирішує компетентний персонал;
- контактний центр з питань виявлення та інформування про інциденти безпеки діє;
- відповідні контакти з повноважними органами, зовнішніми зацікавленими групами або форумами, які присвячені питанням, пов'язаним з інцидентами інформаційної безпеки, підтримуються.

Процедури звітності повинні включати в себе:

- розробку форм звітності про події інформаційної безпеки;
- процедуру, яка повинна бути виконана, якщо відбулася подія інформаційної безпеки;
- посилання на офіційно встановлений процес прийняття дисциплінарних заходів до співробітникам, котрі допустили порушення безпеки;
- працездатні процеси зворотного зв'язку.

Сповіщення про події, пов'язані з інформаційною безпекою

Ситуації, які передбачають передачу повідомлення про подію інформаційної безпеки, включають в себе:

- нерезультативний контроль безпеки;
- порушення очікуваного рівня цілісності, конфіденційності або можливості застосування інформації;
- людські помилки;
- невідповідності політикам та інструкціям;
- порушення заходів фізичної безпеки;
- неконтрольовані зміна систем;
- збої в роботі програмного забезпечення або технічних засобів;

Відповідні заходи на інциденти інформаційної безпеки

Відповідні заходи повинні включати наступне:

- якомога швидший збір свідчень того, що сталося;
- проведення ретроспективного аналізу, якщо потрібно;
- передача рішення на більш високий рівень, якщо це необхідно;
- забезпечення того, що всі виконувані дії у відповідь відповідним чином зареєстровані для подальшого аналізу;
- сповіщення про те, що виявлено інцидент інформаційної безпеки іншим особам, які мають про це знати в силу службової необхідності, як в самій організації, так і в інших організаціях;
- усунення вразливості інформаційної безпеки, що викликала чи яка сприяла виникненню інциденту;
- офіційне закриття та документування інциденту, після того, як він був успішно відпрацьований.

Процедури збору доказів повинні брати до уваги:

- порядок передачі та зберігання
- збереження свідчень
- безпеку персоналу
- ролі та обов'язки задіяного персоналу
- компетентність персоналу
- документацію
- інструктаж