ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра комп'ютерної інженерії

Пояснювальна записка

до магістерської роботи
на ступінь вищої освіти магістр

на тему: «**ОПТИМІЗАЦІЯ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ ПЛАТФОРМИ З БЕЗПЕРЕРВНОСТІ БІЗНЕС ПРОЦЕСІВ**»

Виконала: студентка 6 курсу, групи КСДМ-61
спеціальності
123 Комп'ютерна інженерія
(шифр і назва спеціальності)
Касинець Н.В
(прізвище та ініціали)

Керівник Лемешко А. В.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтроль _____
(прізвище та ініціали)

Київ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра – Комп'ютерної інженерії
Ступінь вищої освіти – «Магістр»
Спеціальність – 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної Інженерії
_____ О.М. Ткаченко

"_____" 2021року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Касинець Наталії Василівні
(прізвище, ім'я, по батькові)

1. Тема роботи: Оптимізація функціонування інформаційної платформи з безперервності бізнес процесів.

Керівник роботи: Лемешко Андрій Вікторович, доцент, доктор філософії (PhD)
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом вищого навчального закладу від « __» __20 __року № __.
2. Строк подання студентам роботи _____
3. Вихідні дані до роботи:
   3.1 Вимоги до кваліфікаційної роботи магістра з актуальних завдань спеціальності;
   3.2 Нормативні матеріали (стандарти, Гости);
   3.3 Технічні вимоги;
   3.4 Науково-технічна література з питань, пов'язаних з темою работи.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити).
   1. Галузь BCM,DR та RA.
   2. Дослідження інформаційної платформи Omnitraker з безперервності бізнес та IT-процесів.
   3. Дослідження функціонування інформаційної платформи Omnitraker в компанії «Процесінг».
   4. Оптимізація функціонування інформаційної платформи з безперервності

бізнес процесів.

5.Перелік графічного матеріалу.

Графічна частина роботи представлена на 16 слайдах презентації.

Перелік демонстраційного матеріалу:

1. Тема магістерської кваліфікаційної роботи.
2. Мета, об’єкт та предмет дослідження.
3. Актуальність роботи.
4. Висновки.
5. Дякую за увагу.

6. Дата видачі завдання 2021р

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	10.10.2021	Викон.
2	Розробка першого розділу	14.10.2021	Викон.
3	Розробка другого розділу	20.10.2021	Викон.
	Аналіз інформаційної платорми	05.11.2021	Викон.
	Оптимізація інформаційної платіформи	12.11.2021	Викон.
4	Висновки, реферат	20.11.2021	Викон.
5	Розробка обов’язкових демонстраційних матеріалів	13.12.2021	Викон.
6	Попередній захист роботи	21.12.2021	Викон.
8	Пред'явлення роботи в деканат	24.12.2021	Викон.

Студент _____ Касинець Н.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лемешко А.В.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи 104с., 41рис., 6 таб., 21 джерел.

Об`єкт дослідження – оптимізація функціонування інформаційної платформи з безперервності бізнес процесів..

Предмет дослідження – інформаційна платформа з безперевності бізнес-процессів.

Мета роботи – оптимізація функціонування інформаційної платформи з безперервності бізнес процесів.

Методи дослідження – емпіричні, теоретичні методи дослідження, методи управління

Актуальність роботи полягає в наступних пунктах:

– Галузь управління безперервністю бізнесу та аварійного відновлення – це напрямок, що дуже почав розвиватися зовсім нещодавно, швидко розвивається та набирає популярності серед великих корпорацій;

– Наразі збільшується зацікавленість кожного бізнесу щодо впровадження BCM та DR recovery ,тому всі розробки та дослідження в цій сфері дуже актуальні та затребувані.

Проведено дослідження галузі BCM та інформаційної платформи, що забезпечить налаштувати та запровадити весь життєвий цикл безперервності та аварійного відновлення на підприємствах та організаціях.

В рамках магістерської роботи було вперше досліджено та проаналізовано інформаційну платформу з безперервності бізнес процесів Omnitraker у компанії «Процесінг»,що використовується у роботі компанії.

На основі проведених досліджень визначено ризики, що могли повипливати на саму інформаційну платформу та життя компанії, та запропоновано методи їх вирішення.

Вперше було сформульовано задачу на оптимізацію платформи Omnitraker шляхом мінімізації часу виконання закриття таких об’єктів як «інциденти» та мінімізації часу користувача в роботи з цими об’єктами, також було створено скрипти, що виконують автоматичне закриття інцидентів, що вже мають статус «Виконано» та автоматично створюють інциденти від телекомунікаційного сервісу і обладнання компанії «Процесінг».

Галузь використання – інформаційні технології, управління безперервністю бізнесу, ризиковий менеджмент, аварійне відновлення.

BCM, BCP, BIA, RISK ANALYSIS, ІНФОРМАЦІЙНА ПЛАТФОРМА, БІЗНЕС-ПРОЦЕС, IT – ПРОЦЕСС, PHYTON, VISUALBASIC, КЛАСТЕР

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BC	Business Continuity - безперервністю бізнесу
BCM	Business Continuity Management - Управління безперервністю бізнесу
BCP	Business Continuity Plan -пран з безперрвності бізнесу
BIA	Business impact analysis - Аналіз впливу на бізнес
CSF	Critical success factors - Критичні фактори успіху.
CM	Crisic Management, Change management – Кризовий менеджмент чи управління змінми
DR	Disaster Recovery - Аварійне відновлення
IS	Informational security – інформаційна безпека
IT	Informational technology – інформаційні технології
MBCO	Minimum business continuity objective - Тимчасовий інтервал після збою, протягом якого сервіс має бути доступним на мінімальному рівні.
RA	Risk assessment -
RTO	Recovery time objective (время відновлення)- Часовий інтервал, необхідний для відновлення сервісу у разі його переривання.
RPO	Recovery point objective (момент відновлення)- Часовий інтервал до моменту переривання сервісу, коли дані, необхідні відновлення і роботи сервісу, перебували у цілісному стані.

ВСТУП

Безперервність бізнесу (*англ. Business Continuity, BC*), – це ключова дисципліна, яка забезпечує безперервність діяльності підприємства та підвищує стійкість організації. Безперервність бізнесу вимагає знань і внеску від керівників бізнесу та ІТ для оцінки та управління ризиками, пов'язаними з критичними бізнес-процесами, для розробки плану, який може дозволити організації відновити діяльність. Організації, які мають цілісний підхід до управління ризиками підприємства, можуть краще керувати бізнесовими та технологічними ризиками.

Управління безперервністю бізнесу визначає пріоритети організації та готує рішення для подолання руйнівних загроз. Це розуміння підтримує розробку та реалізацію планів захисту та продовження діяльності організації, що створює цінність у разі будь-яких збоїв. Ефективна програма безперервності бізнесу підтримує стратегічні цілі організації та активно розвиває здатність продовжувати бізнес-операції в разі збою.

У сучасному світі зростає залежність від технологічних ресурсів, що підтверджує необхідність оцінки ділових і технологічних ризиків для забезпечення безперервності бізнесу. Тим не менш, керівництву та керівникам підприємств важко визначити масштаби та вплив ризиків, пов'язаних з діяльністю підприємства. В організаційному контексті планування безперервності бізнесу сприймається як елемент непередбачуваності, а не як можливість для покращення. Крім того, бракує наукової літератури, пов'язаної з організаційною реалізацією плану безперервності бізнесу, оскільки ця галузь доволі нова, але стрімко розвивається в Україні та світі. З цієї причини існує потреба об'єднати управління ризиками підприємства та управління корпоративними ІТ-поглядами, щоб забезпечити інтегрований погляд на бізнес і технологічний ризик у реалізації плану безперервності бізнесу. На допомогу таким задачам вже існує рішення – інформаційні платформи, що допомагають керівникам організацій впроваджувати та підтримувати безперервність бізнесу.

Кінцевою метою роботи є оптимізація функціонування інформаційної платформи з безперервності бізнес процесів.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ

Для подальшого розуміння матеріалу роботи визначимо деякі поняття та процеси.

1.1 Безперервність бізнесу.

Поняття «*безперервність бізнесу*», як і сама дисципліна, (*англ. Business Continuity, BC*), з'явилися досить нещодавно – з 1990-х років, стрімко розвивається з плином часу, і є особливо актуальною. Світ не до кінця оговтався від світової кризи остатнього десятиліття, як почалася хвиля пандемії COVID-19. Людство поступово звикає до нового політичного та економічного порядку у світі, а також намагається впоратися зі зростанням глобальних загроз, починаючи від проблем з енергетикою, безпекою, масовими міграціями, проблемами з екологією, кіберзлочинністю та розгортанням пандемії. Проте, на цьому фоні дисципліна безперевності бізнесу залишається актуальною для основних бізнес та соціальних змін. Безперервність бізнесу актуальна і застосовна до всіх галузей і організацій, незалежно від розміру, складності, типу та розташування.

Дисципліна дуже повязана

Ближче до кінця десятиліття виникла ідея цілісного наскрізного підходу до запровадження Інституту безперевності бізнесу (англ. BCI – Business Continuity Institute), оскільки світ почав змінюватися і стало очевидно, що необхідно забезпечити захист і стійкість, що охоплюють весь бізнес. З відкриттям BC інституту першим кроком було визначено 10 стандартів компетенцій, які б мали мати спеціалісти в цій галузі.

Вважають, що значну роль в розвиту цієї галузі відіграла проблема Millennium Bug («проблема 2000-го року або «проблема Y2K») - проблема можливості неправильної роботи програмного забезпечення у зв'язку з переходом від 1999 до 2000 року. Проблема пов'язана з тим, що розробники програмного забезпечення, випущеного в XX столітті, іноді використовували два знаки для представлення року в датах, перші два неявно вважалися рівними 19. Наприклад 1 січня 1961 року такими програмами зберігалося як 01.01.61. Деякі обчислювальні машини мали апаратну обробку дати, проте також всього два десяткових знаки. При настанні 1 січня 2000 при двозначному поданні року час «закільцьовувався» — після 99 наставав 00 рік, тобто 99+1 = 100, але старший розряд не зберігався і для подальшої роботи використовувалося 00. Це інтерпретувалася багатьма старими програмами як 1900, а це, в свою чергу, могло призвести до серйозних збоїв у роботі критичних додатків, наприклад, систем управління технологічними процесами і фінансових програм[2].

Незважаючи на «надмірний шум» щодо Millennium Bug, була проведена серйозна робота, великими корпораціями в усьому світі. Вона продемонструвала високий рівень залежності від окремих постачальників та інших окремих точок збою. Це мислення вже було інкапсуловано в концепцію BC, вперше

запропоновану багато років тому, але знадобилося більше десяти років, щоб отримати широкомасштабне розуміння. Це зробило такі ініціативи, як BS 25999 та інші національні стандарти BCMS, більш життєздатними, оскільки вони могли б базуватися на міцній концептуальній основі.

У 21 столітті було визначено рішучість кодифікувати BC,і класифікувати його як частину сімейства стандартів систем менеджменту, слідуючи шляху, який вже проробили служби якості, інформаційної безпеки та охорони навколишнього середовища. Це почалося з ряду стандартів керівництва, як-от BS 25999-1 з Великобританії; NFPA 1600 із США та різноманітні довідники з Австралії та Азії. Регуляторні органи, такі як Управління фінансових послуг (FSA) (Великобританія), Австралійське управління пруденційного регулювання (APRA) (Австралія) і Федеральна резервна система (США), також почали активно працювати в цій сфері, особливо після знищення Всесвітнього торгового центру в 2001 р. Нью-Йорк. Офіційні національні стандарти нині існують у ряді країн, а з 2012 р. існують було стандартом вимог ISO (ISO 22301) та окремим стандартом керівництва (ISO 22313).

1.1.1 Міжнародний стандарт ISO 22301

ISO (Міжнародна організація зі стандартизації) — це всесвітня федерація національних органів зі стандартизації (органів-членів ISO). Робота з підготовки міжнародних стандартів зазвичай здійснюється через технічні комітети ISO. Кожен членський орган, зацікавлений у темі, для якої створено технічний комітет, має право бути представленим у цьому комітеті. У роботі також беруть участь міжнародні організації, державні та неурядові, у зв'язку з ISO. ISO тісно співпрацює з Міжнародною електротехнічною комісією (IEC) з усіх питань електротехнічної стандартизації.

Стандарт ISO 22301: 2019 - Security and resilience — Business continuity management systems — (далі - стандарт ISO 22301) обновив вимоги попередньої версії стандарту ISO 22301 до: 2012 - Societal security — Business continuity management systems- Вимоги (він замінив раніше другу частину відомого британского стандарта (Частина 2, BS 25999-2:2007 — Specification for Business Continuity Management) и був створений для сертифікації корпоративних систем управління безперервність бізнесу (англ. Business Continuity Management Systems, BCMS)

Передісторія цього стандарту така. У квітні 2006 року під Флоренцією (Італія) відбулося перше засідання міжнародної організації зі стандартизації (англ. International Organization for Standardization, ISO) з метою виробити єдині вимоги і рекомендації з питань безперервності бізнесу на основі ряду національних стандартів, в тому числі Австралії, Росії, Ізраїлю, Сінгапуру, Японії, Британії і США. В результаті був підготовлений перший загальний документ під назвою ISO / PAS 22399: 2007 - Societal security - Guideline

for incident preparedness and operational continuity management (російський ГОСТ Р 53647.42011 / ISO / PAS 22399: 2007 «Менеджмент безперервності бізнесу. Настанови щодо забезпечення готовності до інцидентів і безперервності діяльності»). Однак більшість країн не прийняли цей стандарт і продовжили використовувати свої локальні нормативні документи в частині менеджменту безперервності бізнесу (англ. Business Continuity Management). Починаючи з 2009 року роботу по створенню єдиних міжнародних стандартів в області менеджменту безперервності бізнесу продовжили три технічних комітети міжнародної організації по стандартизації. У цьому ж році стандарт ISO22301 вже був успішно прийнятий для сертифікації в 120 країнах світу. Над оновленням стандарту працюють і досі, останнє оновлення відбулося у 2019 році. Було оновлено 38 стандартів, в тому числі і стандарт ISO22301. На рисунку 1 можна прослідкувати залежності галузей і становлення стандарту BCM ISO22301.

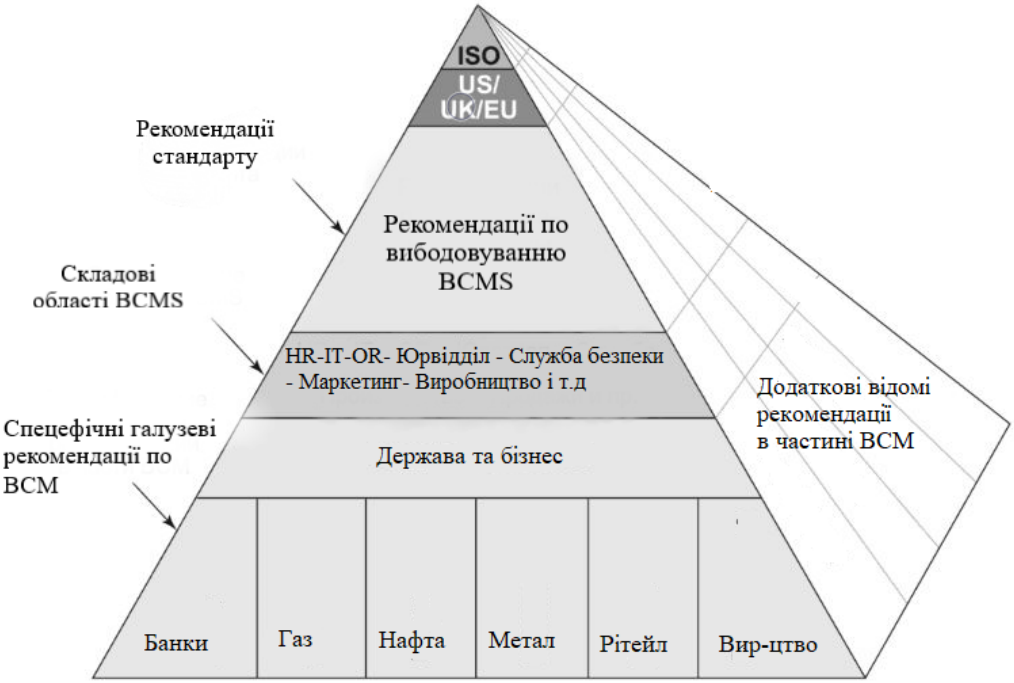


Рисунок 1.1 – Роль та місце стандарту ISO22301

Сам стандарт визначає структуру та вимоги до впровадження та підтримки системи управління безперервністю бізнесу (BCMS), яка розвиває безперервність бізнесу відповідно до величини та типу впливу, з яким організація може впоратися чи ні. Результати підтримки BCMS визначаються правовими, нормативними, організаційними та галузевими вимогами організації, наданими продуктами та послугами, використовуваними процесами, розміром і структурою організації, а також вимогами її зацікавлених сторін.

Стандарт ISO22301 застосовується до організацій усіх типів і розмірів, які:

— впроваджують, підтримують та покращують BCMS;

— прагнуть забезпечити відповідність заявленій політиці безперервної діяльності;

— мають можливість продовжувати постачати продукти та послуги з прийнятною попередньо визначеною потужністю під час збою;

— прагнуть підвищити свою стійкість шляхом ефективного застосування BCMS.

Також стандарт можна використовувати для оцінки здатності організації задовольняти власні потреби та зобов'язання щодо безперервності бізнесу[4].

1.1.2 Міжнародний стандарт ISO 22316

Стандарт ISO 22316 містить рекомендації щодо підвищення стійкості організації для будь-якого розміру або типу організації. Він не є специфічним для будь-якої галузі чи сектору, а також може застосовуватися протягом усього життя організації.

В додаток стандарт не сприяє однаковості підходу в усіх організаціях, оскільки конкретні цілі та ініціативи пристосовані до потреб окремої організації.

В стандарті зазначене визначення ***стійкості організації (англ. Business Resilience)*** як – «здатність організації поглинати й адаптуватися у мінливому середовищі, щоб дати змогу їй достягати своїх цілей, виживати, процвітати»[5].

Стандарт встановлює принципи стійкості організації. Він визначає атрибути та види діяльності, які підтримують організацію у підвищенні її стійкості.

ISO 22316 включає:

— принципи, що створюють основу для підвищення стійкості організації;

— атрибути, що описують характеристики організації, що дозволяють прийняти принципи;

— діяльність, спрямована на використання, оцінку та покращення атрибутів.

1.1.3 Стійкість бізнесу (Business Resilience)

Раніше було поширене уявлення про те, що безперервність бізнесу – це лише боротьба з подіями з великим впливом і низькою ймовірністю. Зараз більш загально оцінюється, що безперервність бізнесу може підвищити стійкість організації. Ці концепції також можна застосувати до вирішення нефізичних подій, таких як збій постачальників і бізнес-кризи, що виникають через несприятливу увагу ЗМІ.

Успішне застосування BC підвищує стійкість організації, що, у свою чергу, сприяє вищій корпоративній ефективності.

Поняття безперервність бізнесу є ключовим для більш загального поняття

«*стійкість бізнесу*»

Стійкість бізнесу (англ. *Business Resilience*) широко визначається як здатність організації, співробітників, систем, мереж, активностей чи процесів поглинати вплив заподіяний збоями, перериваннями чи втратами, відновлюватися після них та реагувати на них.

На стійкість організації впливає унікальна взаємодія та поєднання стратегічних та оперативних факторів. Організації можуть бути лише більш-менш стійкими; немає абсолютної міри чи остаточної мети.

Прихильність до підвищення стійкості організації сприяє:

— покращена здатність передбачати й усувати ризики та вразливі місця;

— посилення координації та інтеграції управлінських дисциплін для покращення узгодженості та продуктивності;

— краще розуміння зацікавлених сторін і залежностей, які підтримують стратегічні цілі та завдання.

Більш стійкі організації можуть передбачати та реагувати на загрози та можливості, що виникають внаслідок раптових або поступових змін у їхньому внутрішньому та зовнішньому середовищі. Підвищення стійкості може бути стратегічною метою організації та є результатом належної ділової практики та ефективного управління ризиками.

Стійкість бізнесу – це розробка та впровадження надійної інфраструктури із технічними стратегіями та рішеннями відновлення, які ефективно забезпечують безперервність послуг організації з будь-якої сфери. Сьогодні фокус концепції стійкості і безперервності бізнесу зміщується на організацію в цілому, критично важливі для бізнесу процеси (основні і забезпечуючі), розширюючи горизонти колишнього розгляду проблеми за межі інформаційних систем і IT-сервісів, незважаючи на їх важливість для сучасних цифрових підприємств.

На Рисунку 1.2 відображені основні поняття, що впливають на визначення *Business Resilience.*

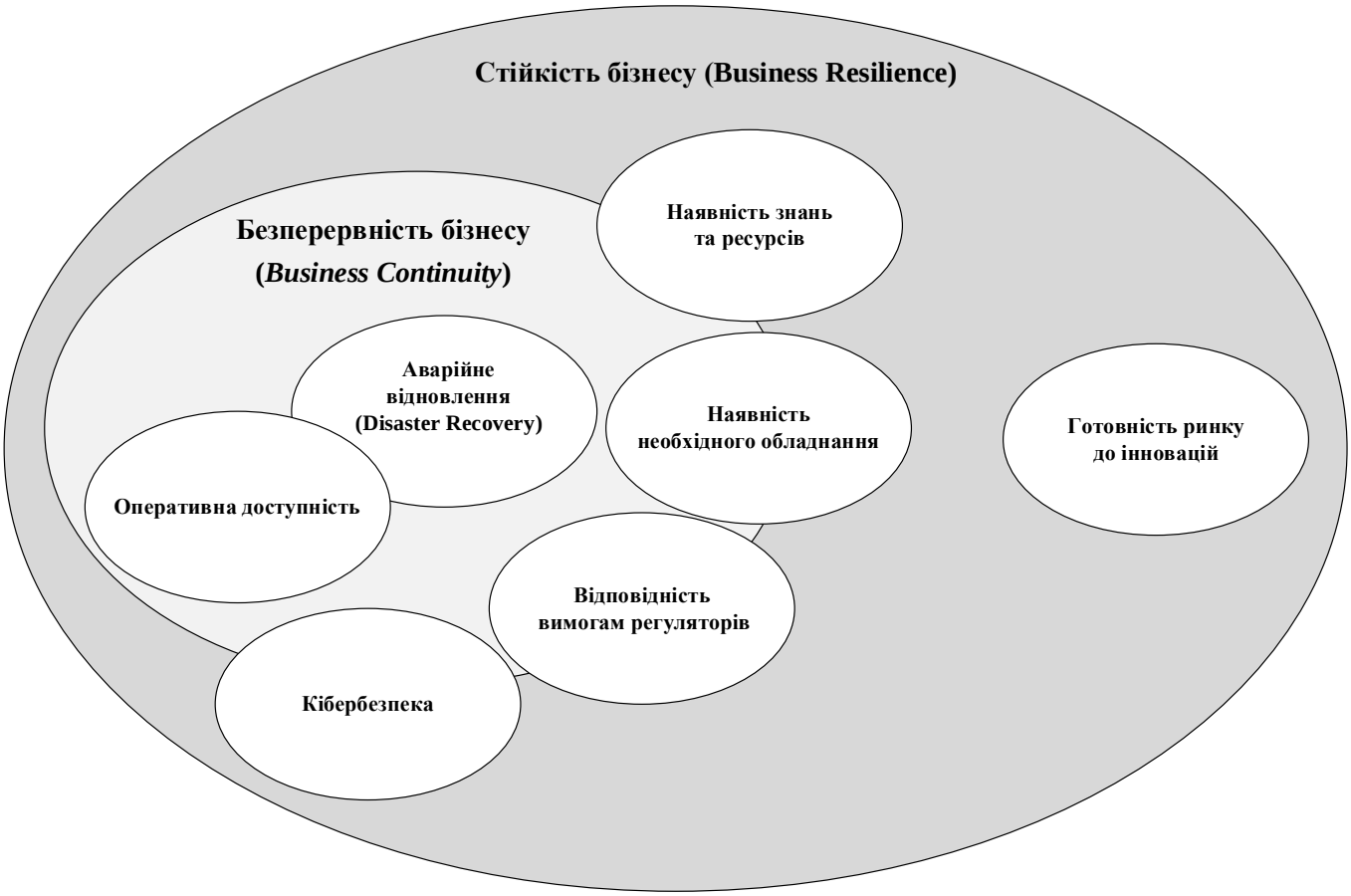


Рисунок 1.2 - основні поняття, що впливають на визначення *стійкості бізнесу.*

Існують принципи, що забезпечують основу, на якій можна розробити, впровадити та оцінити структуру та стратегію досягнення підвищеного стану організаційної стійкості.

Стійкість організації:

— покращується, коли поведінка узгоджується зі спільним баченням і метою;

— спирається на сучасне розуміння контексту організації;

— покладається на здатність поглинати, адаптуватися та ефективно реагувати на зміни;

— покладається на належне врядування та управління;

— підтримується різноманітними навичками, лідерством, знаннями та досвідом;

— покращується координацією між дисциплінами управління та внеском технічних та наукових галузей знань;

— покладається на ефективне управління ризиком.

Стійкість організації підвищується завдяки чітко сформульованим і зрозумілим цілям, баченням і цінностям, щоб забезпечити ясність прийняття рішень на всіх

рівнях організації.

Організація повинна визначити пріоритети та виділити такі види діяльності:

— сформулювати своє бачення, мету та основні цінності всім зацікавленим сторонам, щоб забезпечити стратегічний напрям, узгодженість та ясність у прийнятті всіх рішень;

— забезпечити відповідність індивідуальних цілей і завдань цілям, баченню та цінностям організації та їх відданість;

— контролювати та регулярно переглядати відповідність стратегій організації та їх узгодженість із метою, баченням, основними цінностями та цілями;

— визнати необхідність обміркувати та, якщо необхідно, переглянути мету, бачення та основні цінності організації у відповідь на зовнішні та внутрішні зміни;

— шукати та просувати нові та інноваційні ідеї для досягнення та розвитку своїх стратегічних цілей.

Для підвищення стійкості бізнесу не існує єдиного підходу, про це також згадує стандарт ISO 22316, але поєднання наступних двох пунктів є результатом такого підходу:

— Взаємозв’язки і взаємодії атрибутів і діяльності.

— Внески з інших дисциплін управління, таких як відновлення після катастроф, управління кризою та безперервність бізнесу, які самі по собі недостатні для забезпечення стійкості.

Для побудови організаційної стійкості існує таке поняття як управління безперервністю бізнесу (англ. Business Continuity Management, BCM).

1.1.4 Управління безперервністю бізнесу (Business Continuity Management)

Управління безперервністю бізнесу (англ. Business Continuity Management, BCM) ґрунтується на принципі, що ключовою відповідальністю директорів організації є забезпечення продовження її бізнес-операцій у будь-який час.

BCM - Цілісний процес управління, який визначає потенційні загрози для організації та вплив на бізнес-операції, які ці загрози можуть спричинити, якщо вони реалізовані, і який забезпечує основу для формування стійкості організації зі здатністю ефективного реагування, що захищає інтереси її ключових зацікавлених сторін. , репутація, бренд і діяльність зі створення цінності[4].

Управління безперервністю бізнесу (BCM) об'єднує дисципліни реагування на надзвичайні ситуації(Emergency Response), управління кризами (Crisis Management), аварійне відновлення (Disaster Recovery -безперервність технологій) і безперервність бізнесу (Business Continuity - організаційне/оперативне переміщення).

Управління безперервністю бізнесу (BCM) перетворилося на процес, який визначає, що організація піддається внутрішнім і зовнішнім загрозам,

забезпечуючи ефективне запобігання та відновлення. Це виникло через потребу в механізмі для демонстрації зрілості організації – безперервного управління. Будь-який інцидент, який погіршує здатність підприємства функціонувати, може негативно вплинути на організацію ще довго після відновлення нормальної діяльності. Інтеграція системи управління безперервністю бізнесу в організацію демонструє діловим партнерам і клієнтам, що організація прагне надавати найкращі послуги в будь-який час, незалежно від перерв.

Критичні фактори успіху(CSF) для запровадження управління безперевності бізнесу.

Критичні фактори успіху (CSF) спочатку мають бути визначені та адаптовані до організації – це конкретні цілі, бізнес, менеджери, середовище, в якому працює організація, та стратегії, які вона. Таким чином, з точки зору реалізації BCM, CSF – це ті умови, які повинні бути виконані, щоб його впровадження відбулося успішно.

Відповідно до стандарту ISO 22301 відповідне планування робочої сили в організації є важливим аспектом мобілізації організаційних ресурсів і є критичним фактором успіху управління безперервністю бізнесу, що в подальшому призводить до позитивних результатів діяльності організації. Ефективна діяльність організації є результатом стійкої конкурентної переваги. Така ефективність випливає з унікальних, цінних і незамінних ресурсів, які позитивно впливають на безперервність бізнесу.

За даними Всесвітнього секретаріату ACI , для того, щоб розробити або впровадити BCM, потрібні цілеспрямовані зусилля, керовані командою вищого керівництва, щоб визначити структуру BCM та контроль за її виконанням. Галлахер [7] підкреслив, що для того, щоб BCM працював, він повинен бути керований і отримати чітку і недвозначну підтримку зверху. Автор додав, що найбільший вплив, який визначає стан або умови плану, або всього процесу BCM, — це ступінь прихильності до нього з боку вищого керівництва. У таблиці 1.1 наведено важливі стратегічні та тактичні фактори успіху, важливі для успішного впровадження BCM.

Таблиця 1.1 - стратегічні та тактичні фактори успіху

Критичні стратегічні фактори успіху	**Тактичні критичні фактори успіху**
Відданість та підтримка вищого керівництва	Використання фінансів та бюджету
Орієнтованість на галузь	Ефективна комунікація,
Ключові зацікавлені сторони	Навчання та тренінги BCM
Людські ресурси	Законодавча база
Культурні зміни	Участь обладнання та персоналу
Право власності	BCP комітети
Організація BCM	Кампанія обізнаності
	Лідерство
	Введення програми BCM

1.1.5 Практика BCI інституту

У 1994 року у Великобританії була заснована некомерційна організація Інститут безперервності бізнесу — Business Continuity Institute (BCI) Сьогодні BCI об'єднує понад 8,5 тисячі сертифікованих фахівців в області області забезпечення безперервності бізнесу з більш ніж 100 країн світу. До основним напрямів діяльності Британського інституту BCI належать поширення і просування найкращих практик управління безперервністю бізнесу і аварійного відновлення в разі непередбачуваних ситуацій.

BCI побудований за принципом професіоналізації практики безперервності бізнесу і продовжує залишатися авторитетним і надійним джерелом інформації з усіх аспектів теорії та практики безперервності бізнесу для професіоналів, а також пропонує безліч онлайн-ресурсів на сайті www.thebci.org. Рекомендації з належної практики були переглянуті як частина процесу BCI щодо постійного вдосконалення та постійного розвитку наших знань, щоб залишатися актуальними для професіоналів у всьому світі..

Також BCI є учасником та організатором таких заходів:

— BCI International Symposium - міжнародний форум спеціалістів в об ласті управління неперервністю бізнесу, на якому відбувається обмін ідеями по актуальним питання і намету;

— Business Continuity EXPO - велика міжнародна виставка, на якій системні інтегратори, виробники програмного і апаратного забезпечення, а також консалтингові компанії щорічно представляють свої досягнення і діляться передовим досвідом в області BCM (одночасно з виставкою проводяться тематичні конференції з питань BCM);

— Business Continuity Awareness Weeks - регулярно проводяться по всьому світу заходи, в ході яких через сайт інституту вільно розповсюджуються презентації, методичні рекомендації та довідкова література з питань BCM для залучення уваги фахівців і керівників державних і комерційних організацій;

— Busines Continuity Awards - щорічний урочистий захід, на якому за декільком номінаціям відзначаються визначні досягнення ня в області BCM і тд.

До основних результатів діяльності BCI належать:

— розробка та покращення документації, що містить у собі кращі практики по управлінню безперервністю бізнесу - Good Practice Guidelines books;

— участь у розробці стандартів в галузі BCM, як для Великобританії так і для світу;

— методична допомога для Автарілії, Нової Зеландії, США, Китаю та Сингапуру;

— організація і проведення навчання та сертифікації для спеціалістів в галузі BCM.

Існує 4 рівня підготовки спеціалістів у галузі BCM:

— AMBCI – починаючий спеціаліст, який тільки знайомиться з стандартами та компетенціями BCM.

— CBCI – спеціаліст з досвідом не менше 2х років, який користується принаймні хоча б 4-ма стандартами та компетенціями.

— MBCI – практикуючий спеціаліст з досвідом не менше 2х років в галузі BCM, який користується всіма 10-стандартами і компетенціями.

— FBCI – практикуючий спеціаліст, який працює в галузі не менше 5 років на керівних посадах, який знає та користується на практиці всі 10 стандартів.

На Рисунку 1.3 вказано всі сфери діяльності інституту BCI, з якими знайомляться і вивчають всі члени інституту

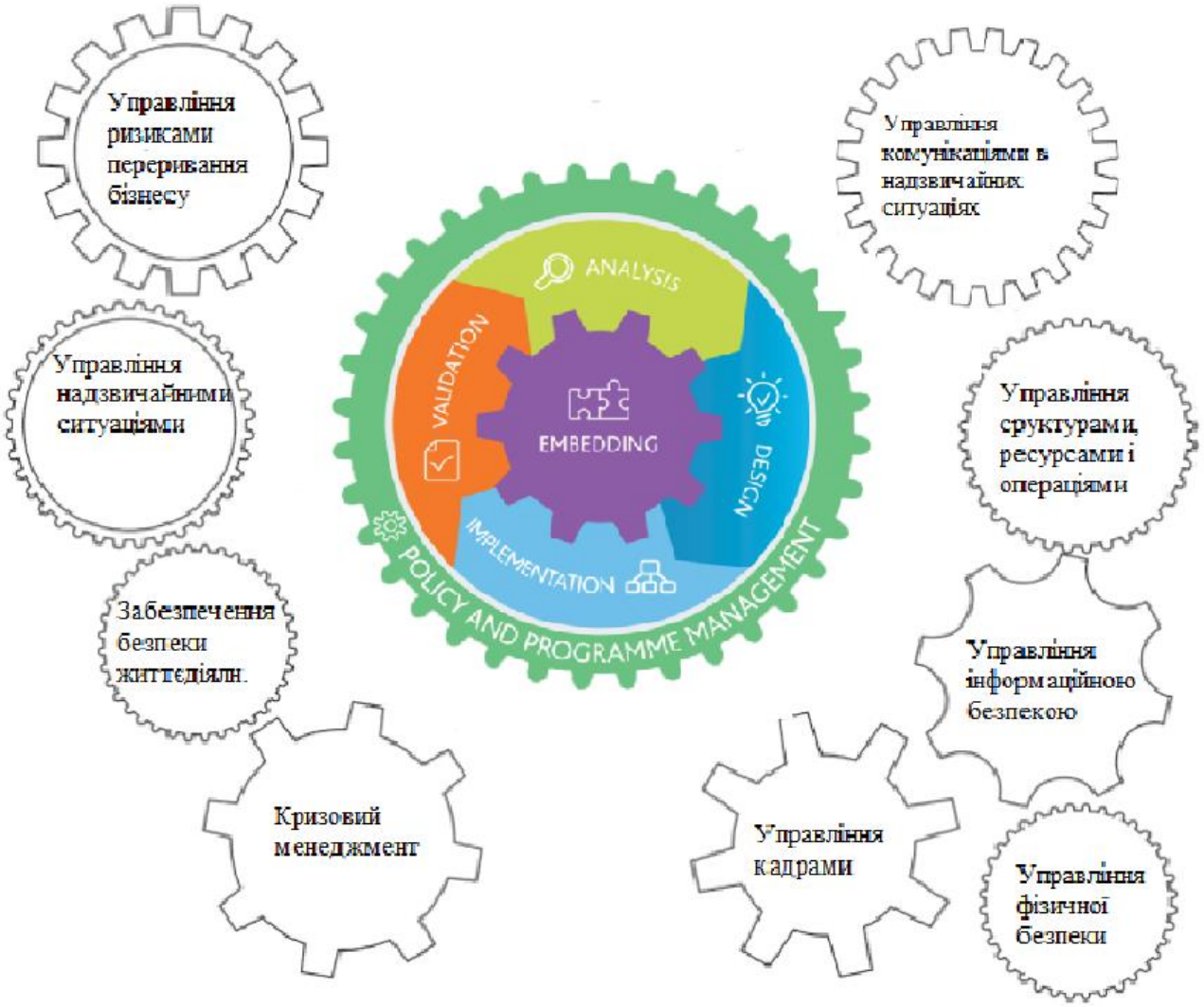


Рисунок 1.3 – Сфери діяльності BCI[9]

1.1.6 Практика DRII інституту

У 1988 році при Вашингтонському університеті була створена некомерційна організація - Міжнародний інститут аварійного відновлення (Disaster Recovery Institute International, DRII) в склад якого входять три базових філії: DRI Canada (Toronto), DRI Asia (Singapore) і DRI Japan (Tokyo). Сьогодні DRI об'єднує понад 15 тисяч сертифікованих фахівців у сфері сфері забезпечення безперервності бізнесу більше ніж в 100 країнах.

Напрями діяльності інституту DRII:

— підготовка і поширення так назывного загального зводу знань для управління безперервністю бізнесу;

— початкове навчання спеціалістів у сфері забезпечення безперебійної діяльності організації у випадку аварійного відновлення;

— підвищення кваліфікації фахівців в області аварійного відновлення;

— експертиза відповідних стандартів і нормативних документів в області аварійного відновлення.

Важливо зазначити, що інститут DRII підтримує робочі звязки з інститутом BCI, Загальний звід знань DRII — Professional Practices for Business Continuity Management (2017) корелює кращими практиками управління безперервністю бізнесу - BCI — Good Practice Guidelines 2018 Edition. У нього ввійшли теми, аналогічні Certification Standards for Business Business Continuity Professionals В BCM практиці практики з інституту DRII використовуються так само часто. В моделі DRII та BCI по плануванню дій в надзвичайних ситуаціях виділені наступні етапи, вказані на рисунку 1.4.

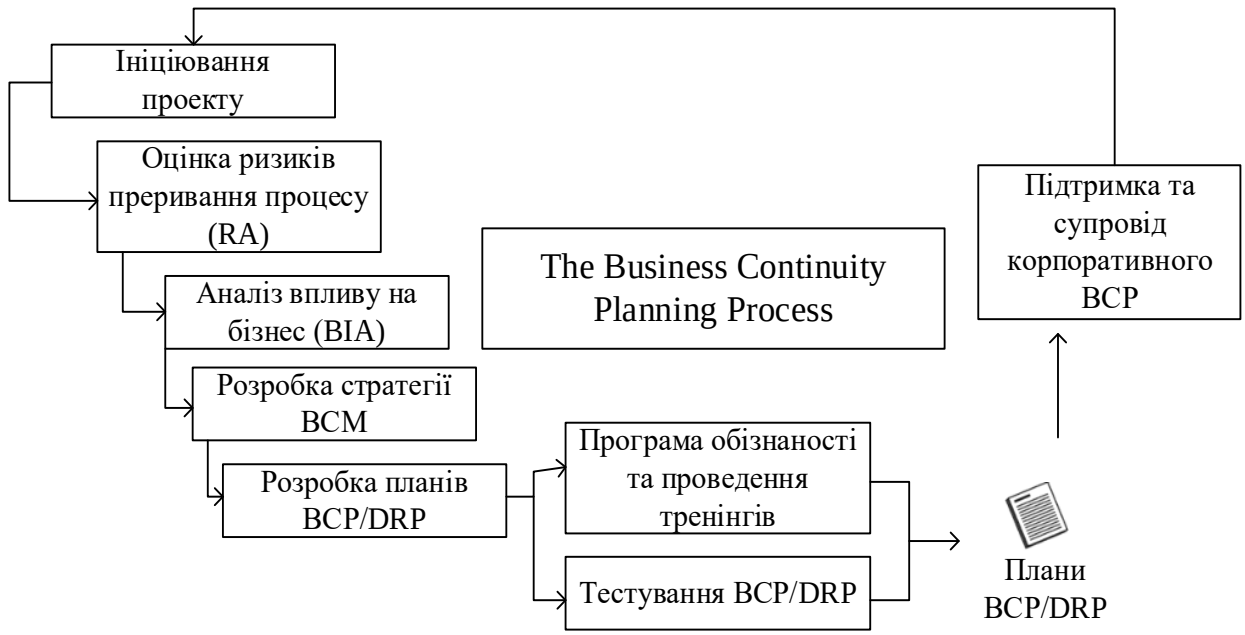


Рисунок 1.4 – Етапи розробки BCP/DRP

1. Ініціювання проекту Project Initiation Phase:
   - уточнення проблеми;
   - визначення мети і завдань. Аналіз вимог;
   - визначення допущень і використовуваних термінів;
   - визначення рамок і вартості проекту;
   - створення керуючого комітету проекту;
   - визначення політик безперервності бізнесу.
2. Аналіз вимог— Functional Requirements Phase:
   - оцінка і управління ризиками, RA;
   - оцінка впливу на бізнес, BIA;
   - розробка альтернативних стратегій BC;
   - вартісний аналіз (ABC) стратегій BC;
   - визначення бюджету програми з управління безперервністю бізнесу.
3. Розробка плану BCP & DRP — Design and Development Phase:
   - визначення мети і завдання плану;
   - уточнення мети і завдання відновлення;
   - визначення складу і структури плану;
   - розробка плану і вироблення необхідних сценаріїв дій;
   - порядок приведення плану на дії;
   - створення резервного офісу;
   - програма управління персоналом;
   - розрахунок допустимих втрат даних;
   - адміністрування плану.
4. Впровадження плану BCP & DRP — Implementation Phase:
   - визначення першочергових дій в надзвичайних ситуаціях;
   - визначення регламенту роботи антикризового центру;
   - розподіл повноваження і відповідальності;
   - перевірка ефективності управління безперервністю бізнесу;
   - деталізація процедур дій в надзвичайних ситуаціях;
   - уточнення необхідних ресурсів;
   - перевірка контрактних зобов'язань постачальників.
5. Тестування плану BCP & DRP — Testing and Exercising Phase:
   - визначення мети і завдання тестування;
   - розробка необхідних сценаріїв тестування;
   - оцінка адекватності планів тестування.;
   - навчання і реалізація програми обізнаності за питань BCM.
6. Супровід і підтримка плану BCP & DRP — Maintenance and Updating Phase:
   - планування термінів і потрібного бюджету;
   - супровід необхідного програмного забезпечення;
   - перегляд критеріїв забезпечення безперервності бізнесу;

— аудит плану BCP & DRP;
— організація ознайомлення з згаданим планом.

7. Введення плану в дія — Execution Phase

1.1.7 План та програма безперервності бізнесу

Організація може реалізувати програму та план безперервності бізнесу (англ. Business Continuity plan, and Business Continuity Program, BCP), а також план аварійного відновленняb(Disaster Recovery Plan) в результаті низки подій або потенційних катастроф, які викликають кризи. Деякі з цих подій, які можуть порушити всі операції, можуть бути стихійними лихами, ненавмисними катастрофами, такими як проблеми з програмним забезпеченням або збій живлення. Інші можуть бути навмисними діями, такими як хакери, терористи, повідомлення про замінування та правопорушення серед працівників. Ці потенційні катастрофи чи події в кінцевому підсумку мають негативний вплив на організації, наприклад, втрату доходів, репутації, інформації, доступу до засобів та персоналу. Керівництво має турбуватися про вплив цих катастроф, щоб задовольнити потреби своїх клієнтів за цих обставин. Тому організаціям стає обов’язково планувати продовження критичних операцій функцій робочого процесу, незважаючи на негаразди та втрату систем підтримки, шляхом впровадження хороших BCP/DRP .

Ініціатором процесу по забезпеченню безперервності бізнесу може виступати і служба безпеки. Проте вона, за рідким винятком, поки рідко розглядає даний напрямок як невід’ємну частину системи безпеки. Найчастіше на питання безперервності бізнесу першим звертає увагу IT-залежний бізнес. Зрозуміло, що забезпечення безперервності бізнесу не є виключно завданням IT.

Основні мотиви організації щодо розробки та впровадження BCP/DRP

Мотив 1. Усвідомлення впровадження та розробки BCP/DRP шляхом аналізу

Усвідомлення керівництвом компанії необхідності забезпечення безперервності бізнесу як зобов'язання перед партнерами і клієнтами — найбільш правильний, еволюційний шлях. При цьому розуміється важливість впровадження кращих практик по забезпечення безперервності бізнесу, розробки і впровадження для цього корпоративної програми управління. Виконуючи вимоги керівництва, бізнес-одиниці компанії приймають на себе відповідальність за створення і оновлення відповідних планів, а також процедур по забезпеченню з Будучи найбільш правильним, цей шлях є дуже вимогливим.Привести до усвідомлення необхідності впровадження всього спектра заходів щодо забезпечення безперервності без будь-яких зовнішніх дій може тільки керівництво, що володіє високою управлінською культурою і здатністю до адекватного прогнозування в середньо- і довго терміновій перспективі. У цілому якість розробки і впровадження

корпоративної програми безперервності бізнесу та планів BCP/DRP нерозривно пов'язано з рівнем зрілості управлінської діяльності в області управління ризиками.
Мотив 2. Усвідомлення впровадження та розробки BCP/DRP через інцидент.

Менш вдалий варіант, але має більший рушійний потенціальний шлях усвідомлення керівництвом необхідності заходів по безперервності бізнесу, на жаль, полягає в проходженні через інцидент її порушення. У кращому випадку цим інцидентом є невдалий досвід – компаній-партнерів, сусідів, конкурентів, у найгіршому – підприємстві.

Причини, що здатні привести до різного роду не передбачених обставин:

- перебої електроживлення;
- відмови і збої апаратного і програмного забезпечення;
- помилки в комунікаціях;
- недоступність господарських обєктів()
- людський фактор;
- вплив зовнішнього середовища (затоплення, пожежі, природні явища);
- епиідемії, інфекційні захворювання;
- інциденти фізичної та кібербезпеки;
- і т.д

Мотив 3. Виконання вимог стандартів та законодавства

Забезпечення безперервністю бізнесу зазвичай може виконуватись через використання локальних чи міжнародних стандартів чи рекомендацій або ж радом законодавчих норм. Бувають ситуації, в яких організації впроваджують BC навіть якщо тереторіально не знаходяться в країні де зареєстрована компанія, оскільки на відділи в інших країнах також будуть діяти міжнародні стандарти чи організаційна політика щодо BCM/DR.

Мотив 4. Підготовка до сертифікації

Для відповідності стандартам та відповідності найкращим практикам по BCM – організації можуть пройти аудит на відповідність стандарту ISO 22301: 2019, який в свою чергу підтвердить зрілість Системи управляння безперевністю бізнесом та забезпечить стабільність та стійкість критично-важливих бізнес-процесів чи сервісів.

Мотив 5. Усунення зауважень аудиторів

Будь-яка зовнішня аудиторська перевірка звертає увагу на необхідність розробки і впровадження корпоративної програми управління безперервністю бізнесу. Акцент робиться на Плані безперервності бізнесу (BCP), Плані антикризового управління (CMP) і Планах аварійного відновлення (DRP). При підготовці до перевірки аудиторами рекомендується використовувати вимоги і рекомендації стандартів ISO 22301:2019 та нормативних заходів чи законів уряду.

Доцільність розробки та впровадження BCP

Правильно розроблена і впроваджена програма BCP дозволяє збільшити час доступності і коефіцієнт готовності бізнес-процесів і IT сервісів організації.
Таким чином, збільшується загальна стійкість бізнесу (Business Resilience) і забезпечується її конкурентна перевага в діловому співтоваристві. Зауважимо, що

60–80% зусиль на забезпечення безперервності бізнесу повинні бути направлені на організаційні заходи та розробку відповідної програми.
Програма і плани BCP/DRP можуть одночасно являтися як найдешевшим, так і найбільш ефективним способом, а решта 20–40% зусиль організації на забезпечення безперервності бізнесу витрачаються на вибір і впровадження технічних рішень, які потрібно обгунтовувати і економічному ключі.

Коефіцієнт готовності

Коефіцієнт готовності це «ймовірність того, що об’єкт виявиться в працездатному стані в виробничий момент часу, крім планованих періодів, під час яких застосування об’єкта за призначенням не передбачається»[8].

Коефіцієнт готовності важливий показник, який дозволяє зрівняти два і більше варіантів реалізації IT-інфраструктури. Зрівняння двох варіантів, наприклад, за вартість володіння, буде некоректним за різним коефіцієнтом готовності.

У свою чергу, робочий стан - це «стан об'єкта, при якому значення всіх параметрів, характеризуючих здатність виконувати задані функції, відповідають вимогам нормативно-технічної та (або) конструкторської (проектної) документації»[8].

При визначенні потрібного коефіцієнта готовності враховуються наступні дані:

— обсяги прямих фінансових втрат при зупинці в роботі бізнес-застосунків;

— непрямі втрати, спричинені непрацездатністю бізнес-додатків (зниження рівня довіри, перехід клієнтів до конкурентів або відмова від сервісів та ін.).

Виходячи з цих показників можна говорити про максимально допустимий час простої всієї IT-інфраструктури та окремих сервісів.
У загальному випадку коефіцієнт готовності можна записати таким чином:

$$К_г = \frac{t_p}{t_p + t_b} = \frac{\text{MTBF}}{\text{MTBF+MTTR}} \qquad (1.1)$$

$К_г$ - коефіцієнт готовності системы (Кг)

t_p- MTBF (Mean Time Between Failure) - суммарний час нахождения об'єкта в працездатному стані

t_b – MTTR (Mean Time To Repair)- суммарний час відновлення обєкту.

Для знаходження потрібних параметрів, потрібно зробити наступні кроки:

1. Скласти архітектурну схему системи.
2. Перетворити її на логічну.

3. Розбити на модулі з послідовним/паралельним з'єднанням компонентів.
4. Виконати розрахунок готовності за модулями.
5. Виконати розрахунок готовності для системи загалом.

Головне, що при розрахунку враховується, ЯК усередині системи пов'язані -об'єкти (обладнання). Для послідовного чи паралельного з'єднання, коефіцієнт готовності розраховується по-різному, що у результаті істотно позначається остаточному результаті для всієї системи.

Імовірність безвідмовної роботи системи розраховується як:

Для послідовного з'єднання $\mathrm{A} = \prod_{i=1}^{k} a_i$ (1.2)

Для паралельного з'єднання $\mathrm{A} = 1 - \prod_{i=1}^{k} a_i \, [1 - a_i]$ (1.3)

Наприклад припустимо, що коефіцієнт готовності окремого сервера дорівнює 0,99. У разі кластера коефіцієнт готовності системи, згідно з формулами, становитиме 0,9999:

$$\mathrm{К_г} = 1 - (1 - 0.99) * (1 - 0.99) = \ 1 - 0.0001 = 0.9999 \quad (1.4)$$

Слід зазначити, що готовність підвищилася не у 2 рази, а в 2 порядки, тобто - стала кращою у 100 разів.

Переваги для впровадження програми BCP

1. Зниження впливу інциденту на діяльність організації

Головними підставами для зменшення шкоди через переривання бізнесу при наявності розробленої та впровадженої програми BCP є:

— мінімізація часу прийняття рішень у випадках надзвичайної ситуації;
— зниження риску людської помилки в стресової ситуації;
— забезпеченість персоналу засобами (в том числі комунікацій) як для ліквідації інциденту, так і для виконання деякій часті службових обов'язків;
— наявність у персоналу досвіду і навичок дій в надзвичайних ситуаціях.
— У тому числі отриманих в ході регулярних тренінгів та проведення тестувань як BCM процедур, DR процедур так і процедур з безпеки.

Важливо зазначити, що програма ECP може принести віддачу, навіть перевищую витрати на окремі захисні заходи по кожному напрямку (DRP)

Програма BCP націлена на відновлення працездатності організації в випадках великих негативних впливів, зазвичай тих, що можуть зачепити кілька об'єктів і напрямків інфраструктури При таких впливах окремі плани DRP, часто розроблені структурними підрозділами і ізольовано і засновані на припущеннях про працездатності інших сервісів, не здатні відображувати які заходи для відновленяя потрібні. Тільки комплексна програма, враховує різні сценарії і що охоплюють різні напрямки, може формувати оптимальну стратегію поведінки.

2. Зниження ризику перед клієнтами

Впровадження заходів за забезпечення безперервності бізнесу дозволяє уникнути або значно зменшити вагомий для багатьох організацій ризик юридичної

відповідальності перед клієнтами і замовниками, і як слід — зменшити обсяги страхових виплат, штрафів і т. д.

3. Зниження ризику нанесення шкоди репутації

Ризик того, що буде нанесено шкоду репутації, тісно пов'язаний інцидентами по порушенню працездатності організації і при цьому відноситься до числа незастрахованих. Тому впровадження плану BCM і его відповідне технічне забезпечення — одне з небагатьох засобів управління даним ризиком.

4. Документування процесів

В організаціях, які раніше не проводили одноманітну інвентаризацію своїх бізнес-процесів та IT-сервісів з точки зору впливу на працездатність, розробка програми BCP в якості додаткового результату формує детальний і, що особливо важливо, бізнес-орієнтований пакет документації про компанію. Даний матеріал буде корисний і топ-менеджерам, та середній управлінській ланці, і новоспеченим працівникам (наприклад, з метою швидкого та адресного ознайомлення з принципами функціонування бізнес-процесів і обслуговуючих їх систем).

Перспективи розвитку BCP

Ключове завдання, яке сьогодні намагаються вирішити фахівці, - перехід від формулювання загальних вимог і постановки завдань до вироблення кількісних показників, метрик і заходів нової практики стійкості організації, наприклад, з урахуванням рекомендацій NIST SP 80034. Interrelationship of Emergency Action Plans. У цій спеціальній публікації Інституту станів дартів США дано типові рекомендації. Проте документ не містить зміст опису кількісних показників – мова йде, в кращому випадку, про процентному співвідношенні. Відсутність чітких кількісних оцінок не можна порівняти, не оптимізувати процеси, не прийняти адекватні заходи для переходу з стану в стан систем, що буде відповідати стандартам. Тому цікавий досвід, організацій, що роблять спроби побудувати системи кількісних показників. Наприклад, розрахунок основі абсолютних часу активації резервних площ, відновлення процесів ня критично важливою інформаційної інфраструктури, відновлення критичних бізнес-процесів та IT-сервісів та ін. і відносних значень (відсоток і кількість постійно готових резервних робочих місць, кількість проведених навчань по відновленню критичних бізнес процесів і IT-сервісів і т.д.).

Загальні підходи впровадження технологій відмовостійкості і аварійного відновлення

Перед впровадженням технічних заходів за забезпечення безперервності бізнесу слід належним чином класифікувати технічні рішення і співвіднести їх з поставленими задачами.

Класифікація за рівнем використання

До критерій класифікації за рівнем використання можна віднести:

— кількість і склад користувачів системи;
— ступінь агрегації інформації;
— спосіб зберігання і обробки даних;
— особливості розв'язуваних завдань;
— рівень складності і т. д

Класифікація за рівнем безперервності

Можлива наступна класифікація IT-систем:

1. *Critical* — системи, працюючі в «бойовому» режимі (RTO, RPO близькі до «нуля»). До таких систем відносяться:

— критично важливі для бізнесу і навколишнього середовища системи і програмні програми;

— центри управління (моніторингу, безпеки, адміністрування) мережею;

— технологічні додатки, працюючі в режимі реального часу.

Вихід з ладу згаданих систем тягне за собою втрати для бізнесу, несе загрозу життю і здоров'ю співробітників. Для таких систем повинні використовуватися спеціалізовані серверні платформи і інфраструктурні рівні з багаторазовим резервуванням компонентів, в тому числі використанням резервних дата центрів.

2. *Business Critical* — системи, критично важливі для бізнесу, з режимом роботи 24 × 7 × 365. Рекомендований час аварійного відновлення подібних систем – більше двох годин. Тут мають використовуватися кластерні рішення і інфраструктурні рівні з частковим резервування застосовуваних компонентів.
3. Business Operational — звичайні бізнес-додатки — системи з режимом роботи 8 × 5. Рекомендований час їх аварійного відновлення — не більше 8-ми годин. Для таких систем рекомендується використовувати резервування збереження даних і електроживлення.
4. Office Production — додатки, не критичні для ведення бізнесу. Їхній вихід з ладу не впливає на динаміку ключових показників ефективності підприємства. Рекомендований час аварійного відновлення подібних систем — 24 години.

Способи забезпечення безперервності

До основних способів забезпечення неперервності бізнесу в області інформаційних технологій можна віднести:

— консолідацію IT-ресурсів;

— віртуалізацію IT-ресурсів;

— технології відмовостійкості і аварійного відновлення.

Консолідація ресурсів

До основних видів консолідації IT-ресурсів відносяться:

— Централізація (Centralization) — консолідація географічно розподілених серверів в одному або декількох дата центрах.

— Консолідація даних (Data Consolidation) — консолідація баз даних і/або пристроїв зберігання для досягнення більш високої доступності і керованості даними.

— Фізична консолідація (Physical Consolidation) — об'єднання серверів під управлінням одної операційної системи і з подібними додатками на більше потужних системах.

— Консолідація додатків і сховищ даних (Application Consolidation) — розміщення різних додатків на «великих» серверах з розподілом розділами .

Віртуалізація ресурсів

Можливі варіанти віртуалізації IT-ресурсів залежать від мети і платформ, для яких вона застосовується. Основні засоби віртуалізації для Windows-платформ - віртуальні машини або емулятори операційних середовищ. Доповненням до них є технології кластеризації і технології міграції віртуальних машин: P2V (PhysicaltoVirtual), V2P (Virtualto Physical) і V2V (міграція). При цьому технології віртуалізації для серверів класу enterprise і операційних систем high availability відрізняються у різних виробників серверів даного го класу і розрізняються Технологія апаратних і програмних розділів (partitioning) дозволяє віртуалізувати апаратні ресурси і зробити їх доступними для великої кількості незалежних операційних середовищ. Спочатку розроблена для mainframe, вона дозволяє розділити один сервер на кілька незалежних апаратних або програмних віртуальних серверів.

Вихід з ладу конкретного фізичного об'єкта не призводить до серйозних і довготривалих простоїв системи: віртуальний об'єкт передається на фізичний хост, який на даний момент має резерви ресурсів і продовжує функціонувати з мінімальними простоями. Крім того, впровадження даного механізму забезпечує більш вищий рівень вимірювання процесів, в першу чергу их вимог к ресурсам, і як слід Технологія partitioning разом з планами аварійного відновлення (DRP — Disaster Recovery Plan) для двох окремих дата центрів (основного і резервного) створює базу аварійного відновлення IT-іфраструктури.

Резервне копіювання даних

Резервне копіювання даних повинно здійснюватись в відповідності з спеціальною методикою, містить опис процесів резервного копіювання різних інформаційних систем і регламенту виконання

Для резервного копіювання даних рекомендується наступний підхід:

— локальне резервне копіювання даних для их швидкого відновлення лення;

— віддалене резервне копіювання даних для забезпечення катастрофо стійкості.

Локальне резервне копіювання даних має виконуватися на мобільний носій із сервера резервного копіювання, який також є проміжним обладнанням, що має зменшити вікно резервного копіювання шляхом попереднього подвоєння даних на швидку дискову систему SATA, розташовану в мережі SAN.

Повинен бути ухвалений і затверджений порядок резервного копіювання, в якому необхідно регулювати періоди і вікна даного процесу для повного і часткового резервного копіювання. Способи такого слід вибирати, виходячи з наступних параметрів:

— RTO – цільовий час відновлення, необхідний для відновлення даних.

— RPO — цільова точка відновлення, момент, до треба потрібно відновити дані або, іншими словами, фактично допустимий обсяг втрачених даних

Найбільш поширені сьогодні технології резервного копіювання:

— загальне (консолідоване) резервне копіювання. Зазвичай здійснюється на стрічки або диски великої ємності. Найменш дороге рішення, максимальне

значення RTO і RPO;

— періодична реплікація змін. Зазвичай виконується по кана лам зв'язку на віддалений майданчик (інше місто) без гарантій часу відповіді. Менше значення RTO, чим у консолідованого резервного копіювання, однак RPO – не нульове, знаходиться в межах періоду виконання реплікації;

— асинхронна реплікація. Підтримує RPO в межах декількох секунд/хвилин і при цьому не знижує швидкість системи в випадку значної затримки на лініях передачі між основною і резервними копіями.

— синхронна реплікація. Виконується по високошвидкісним лініям зв'язку з мінімальними затримками (ця величина прямо впливає на швидкодію робочої системи у цілому) RPO = 0.

1.2 BCM lifecycle

Програма безперервності бізнесу – це постійний *цикл заходів*, що реалізують політику. Ці дії здійснюються шляхом дотримання життєвого циклу управління безперервністю бізнесу.

У той час як програма безперервності бізнесу впроваджується та вбудовується в звичайну діяльність, важливо, щоб організація мала певні можливості для управління інцидентом або кризою. Якщо при впровадженні програми безперервності бізнесу вперше немає такої можливості, слід створити проміжну структуру та план, щоб організація могла реагувати на інцидент.

Цей життєвий цикл BCM — етапи діяльності, які організація проходить і повторює кожен рік з загальною метою підвищення стійкості організації. Сам цикл складається з 6 пактик 2-ох практик управління та 4-ох технічних практик (англ. Management Practices і Technical Practices). На Рисунку 1.5 відображений життєвий цикл BCM (BCM lifecycle)[9].

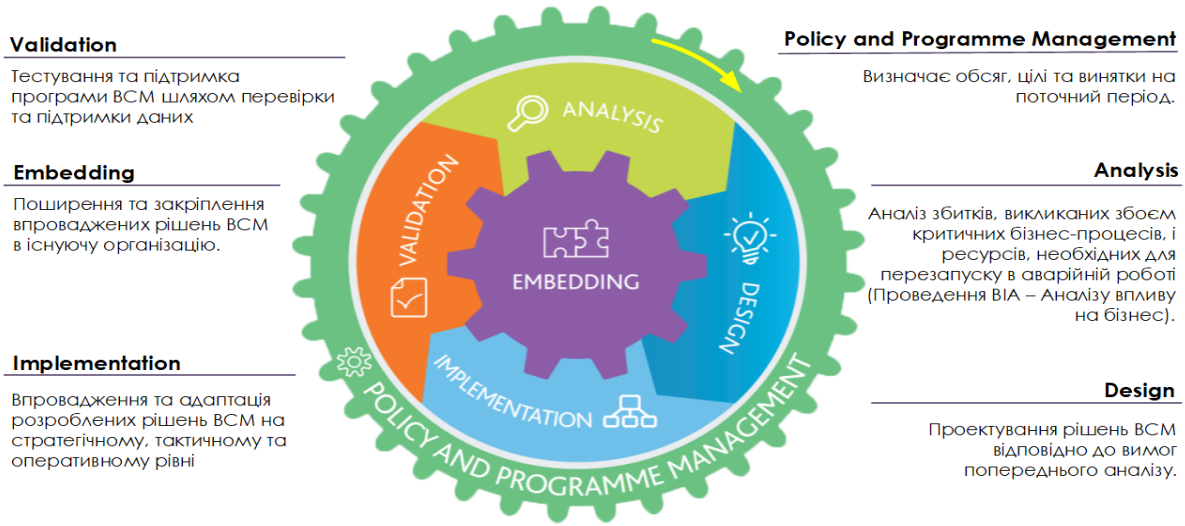


Рисунок 1.5 - BCM lifecycle [9]

Management Practices (Практики управління)

1. *Управління політикою та програмою (англ. Policy and Programme Management (PP1))* (знаходиться на початку життєвого циклу управління безперервністю бізнесу (BCM). Саме професійна практика визначає організаційну політику щодо забезпечення безперервності бізнесу (BC), а також те, як ця політика буде впроваджена, контрольована та підтверджена за допомогою програми BCM.
2. *Вибудовування безперервності бізнесу (англ. Embedding BC (PP2))* – це професійна практика, яка постійно прагне інтегрувати BC у повсякденну бізнес-діяльність та організаційну культуру.

Technical Practices (Технічні практики)

3. *Аналіз (англ. Analysis (PP3))* – це професійна практика в рамках життєвого циклу BCM, яка розглядає та оцінює організацію з точки зору її цілей, як вона функціонує та обмежень середовища, в якій вона працює.
4. *Розробка (англ. Design (PP4))* – це професійна практика в рамках життєвого циклу BCM, яка визначає та вибирає відповідні стратегії та тактики, щоб визначити, як буде досягнуто безперервності та відновлення після інциденту.

5. *Впровадження (англ. Implementation (PP5))* – це професійна практика в рамках життєвого циклу управління безперервністю бізнесу (BCM), яка виконує узгоджені стратегії та тактики в процесі розробки Плану безперервності бізнесу (BCP).
6. *Перевірка (англ. Validation (PP6))* – це професійна практика в рамках життєвого циклу BCM, яка підтверджує, що Програма BCM відповідає цілям, встановленим у Політиці BC, і що BCP організації відповідає цілям[9].

1.2.1 Практика управління політикою та програмою (англ. Policy and Programme Management (PP1))

Професійна практика управління політикою та програмою – це перша професійна практика життевого циклу BCM, яка встановлює політику організації щодо безперервності бізнесу. Вона визначає, як ця політика має реалізовуватися через постійний цикл заходів у рамках програми безперервності бізнесу.

Цей етап життєвого циклу управління безперервністю бізнесу вимагає дій вищого керівництва, підтримки та зобов'язань щодо створення, розробки та перегляду політики щодо безперервності бізнесу та програми, яка використовується для її впровадження.

Політика безперервності бізнесу є ключовим документом, який визначає мету, контекст, обсяг та управління програмою безперервності бізнесу.

Програма безперервності бізнесу – це постійний цикл заходів, що реалізують політику. Ці дії здійснюються шляхом дотримання життєвого циклу управління безперервністю бізнесу.

У той час як програма безперервності бізнесу впроваджується та вбудовується в звичайну діяльність, важливо, щоб організація мала певні можливості для управління інцидентом або кризою. Якщо під час першого впровадження програми безперервності бізнесу такої можливості немає, слід створити проміжну структуру та план, щоб організація могла реагувати на інцидент.

Перша професійна практика складається з наступних етапів:

1. Встановлення політики безперервності бізнесу

Політика «забезпечує наміри та напрямок діяльності організації, офіційно виражені її вищим керівництвом»[4]. Політика безперервності бізнесу встановлює межі та вимоги до програми безперервності бізнесу та вказує причини, чому вона впроваджується. Політика визначає керівні принципи, яким дотримується організація, і оцінює свою ефективність, а також визначає, як організація повинна будувати та підтримувати ВС програму, щоб продовжувати надавати продукти та послуги в разі інциденту.

Політика безперервності бізнесу забезпечує керівні принципи, на основі яких розробляється та будується програма безперервності бізнесу. Політика діє як заява, щоб донести принципи організації до зацікавлених сторін. Оскільки його основна мета – спілкування, воно повинно бути коротким, чітким, точним і по суті**.** Процес створення ефективної ВС політики відображений на Рисунку 1.6.

Рисунок 1.6 - Процес створення ефективної BC політики

2. Визначення обсягу BC програми

Політика безперервності бізнесу повинна чітко визначати сферу застосування програми безперервної діяльності. Визначення обсягу включає розгляд продуктів і послуг організації, які мають бути включені або виключені з програми. Етап аналізу має визначити вимоги до безперервності бізнесу та може допомогти змінити обсяг програми.

Чітко визначені рамки програми безперервності бізнесу, які можуть бути підтверджені для забезпечення досягнення цілей політики безперервності бізнесу. Обсяг програми забезпечення безперервності бізнесу повинен регулярно переглядатися через заздалегідь узгоджені проміжки часу або після істотних змін, як це визначено в політиці безперервної діяльності. Процес створення обсягу BC програми відображено на Рисунку 1.7.

Рисунок 1.7 - Процес створення обсягу BC програми

3. Встановлення контролю та керівництва

Діяльність з контролю має включати моніторинг та вимірювання прогресу за ключовими показниками ефективності, щоб підтвердити, що політика та програма безперервності бізнесу ефективно впроваджуються та узгоджуються з цілями та стратегією організації.

Існує кілька джерел рекомендацій для професіоналів щодо того, як розробити, керувати, впроваджувати та переглядати програму безперервності бізнесу. Вищезгаданий міжнародний стандарт управління безперервністю бізнесу ISO 22301[4] визначає процеси управління та управління для роботи, моніторингу, перегляду та постійного вдосконалення системи управління безперервністю бізнесу. Вимоги щодо управління безперервністю бізнесу також передбачені в національних або міжнародних стандартах, законодавстві, нормативно-правових актах або інструкціях для конкретних галузевих секторів. Норми в деяких секторах можуть вимагати офіційної демонстрації ефективного управління безперервністю бізнесу вищому керівництву організації.

Визначаючи контролювання та управління під час встановлення політики безперервності бізнесу, вище керівництво має бути повністю залучено та відповідати за результативність та ефективність програми безперервної діяльності з самого початку.

Найвище керівництво повинно забезпечити, щоб політика безперервності бізнесу вказувала, які заходи необхідні для забезпечення ефективної програми

безперервності бізнесу. Відповідні методи є частиною етапу перевірки життєвого циклу управління безперервністю бізнесу і включені в програму забезпечення безперервності бізнесу.

Рисунок 1.8 – Процес встановлення контролю над BC

4. Розподіл ролей та повноважень

Ефективна програма безперервності бізнесу залежить від раннього визначення чітко визначених ролей і пов'язаних з ними обов'язків і повноважень для управління програмою. Це буде визначено в політиці безперервності бізнесу. Метою розподілу ролей та відповідальності є забезпечення того, щоб завдання, необхідні для впровадження та підтримки програми безперервності бізнесу, розподілялися між конкретними компетентними особами, чию роботу можна оцінити та де можна визначити потреби в подальшому навчанні. Вимоги до підготовки та компетентності для професійної та ширшої програми безперервності бізнесу висвітлені в PP2.

5. Створення BC програми.

Програма безперервності бізнесу встановлюється для реалізації політики безперервності бізнесу, коли визначено обсяг, управління, ролі та обвязки . Важливою частиною програми є керування документацією для підтримки впровадження. Методологія управління проектами є корисним підходом під час реалізації програми безперервності бізнесу. Ефективне управління проектом має збільшити шанси на успішне виконання загальної програми в узгоджені терміни та бюджети. Впровадження та управління програмою передбачає управління багатьма взаємопов'язаними завданнями для досягнення цілей, зазначених у політиці. Ці задання описані на Рисунку 1.9 нижче.

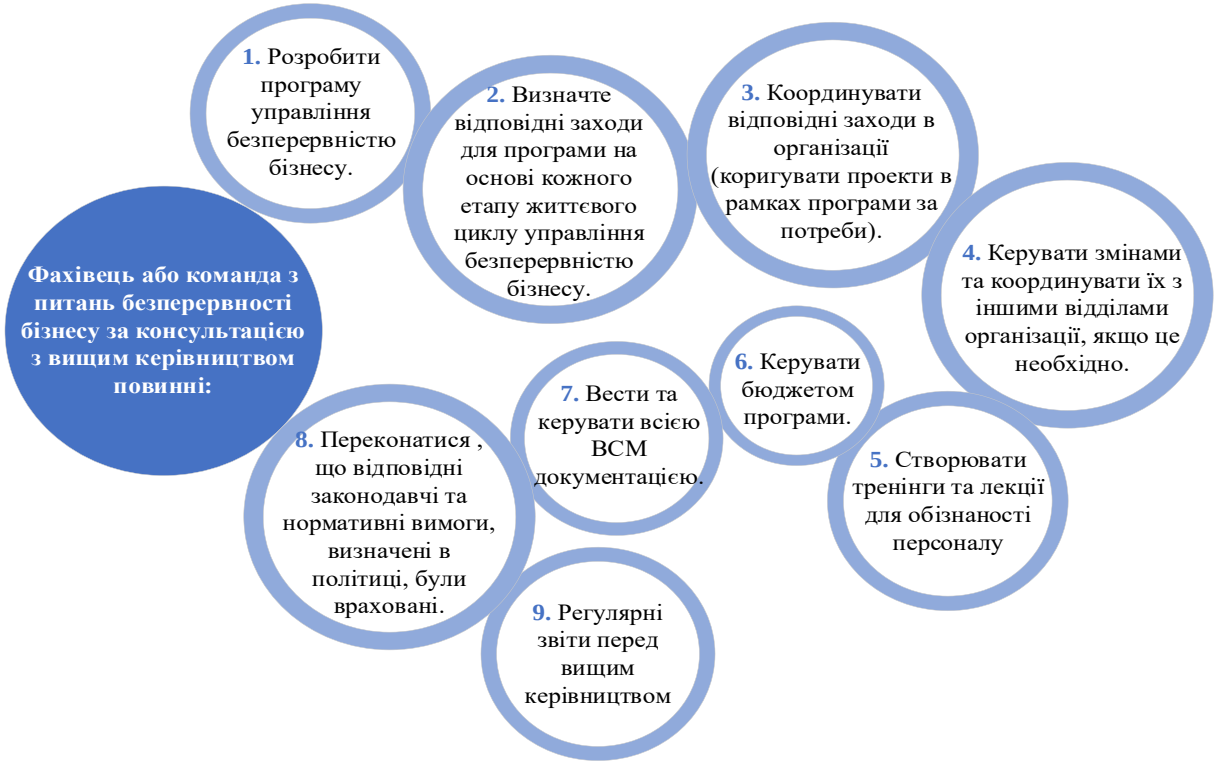


Рисунок 1.9 - Впровадження та управління BC програмою

1.2.2 Практика Вибудовування безперервності бізнесу(англ. Embedding BC, PP2)

Вибудовування безперервності бізнесу — це професійна практика, яка визначає, як інтегрувати знання про безперервність бізнесу та практикичні навичка в звичайну діяльність та організаційну культуру. Впровадження безперервності бізнесу має бути спільним підходом між суміжними дисциплінами управління для підвищення загальної стійкості організації.

Вибудовування безперервності бізнесу включає:

- Підвищення обізнаності про безперервність бізнесу через спілкування.
- Заохочення залучення зацікавлених сторін.
- Забезпечення наявності необхідних компетенцій та навичок.
- Забезпечення належної підготовки та можливостей навчання.

Успішне впровадження безперервності бізнесу вимагає спільного підходу вищого керівництва та спеціаліста з безперервності бізнесу.

Метою впровадження безперервності бізнесу є забезпечення того, щоб вона стала частиною звичайного бізнесу в організації.

Впровадження заходів щодо безперервності бізнесу має відповідати стратегічним

цілям і культурі організації. Безперервність бізнесу також слід враховувати та інтегрувати в практику управління проектами та змінами, де це доречно. Навички та компетенції, необхідні для реалізації політики та програми безперервності бізнесу, включають як загальні управлінські, так і технічні навички.

Залежно від зрілості програми забезпечення безперервності бізнесу організації існує кілька ефективних методи впровадження:

— Зміна ставлення та поведінки. Може бути корисно визначити наслідки дії (або бездіяльності) і зробити їх відповідними короткостроковим бізнес-цілям або добробуту особи. Наприклад, якщо організація подібного типу в схожому місці зазнала зриву або значних змін і діяла таким чином, що продемонструвала високий рівень стійкості, уроки можна засвоїти та поділитися ними. Так само, якщо організація подібного типу в аналогічному місці не спрацювала, це також може надати можливості для навчання.

— Забезпечення врахування безперервності бізнесу вищим керівництвом під час розробки або перегляду стратегічного плану організації.

— Включення безперервності бізнесу до порядку денного відповідних зустрічей.

— Включення планів безперервності бізнесу до стандартних операційних процедур.

— Включаючи проінформованість про безперервність бізнесу як частину індукційних процесів.

— Планування заходів, тренувань тестів щодо безперервності бізнесу, щоб збігатися з запланованими зупинками або сповільненими часами.

— Забезпечення будь-яких нових продуктів або послуг враховує безперервність бізнесу на етапі планування.

Компетенції та навички

Фахівець із забезпечення безперервності та стійкості бізнесу, а також усі особи, які мають ролі та відповідальність за безперервність бізнесу, повинні мати відповідну освіту, підготовку та досвід, необхідні для розробки та впровадження політики та програми безперервності бізнесу, як визначено в PP1.

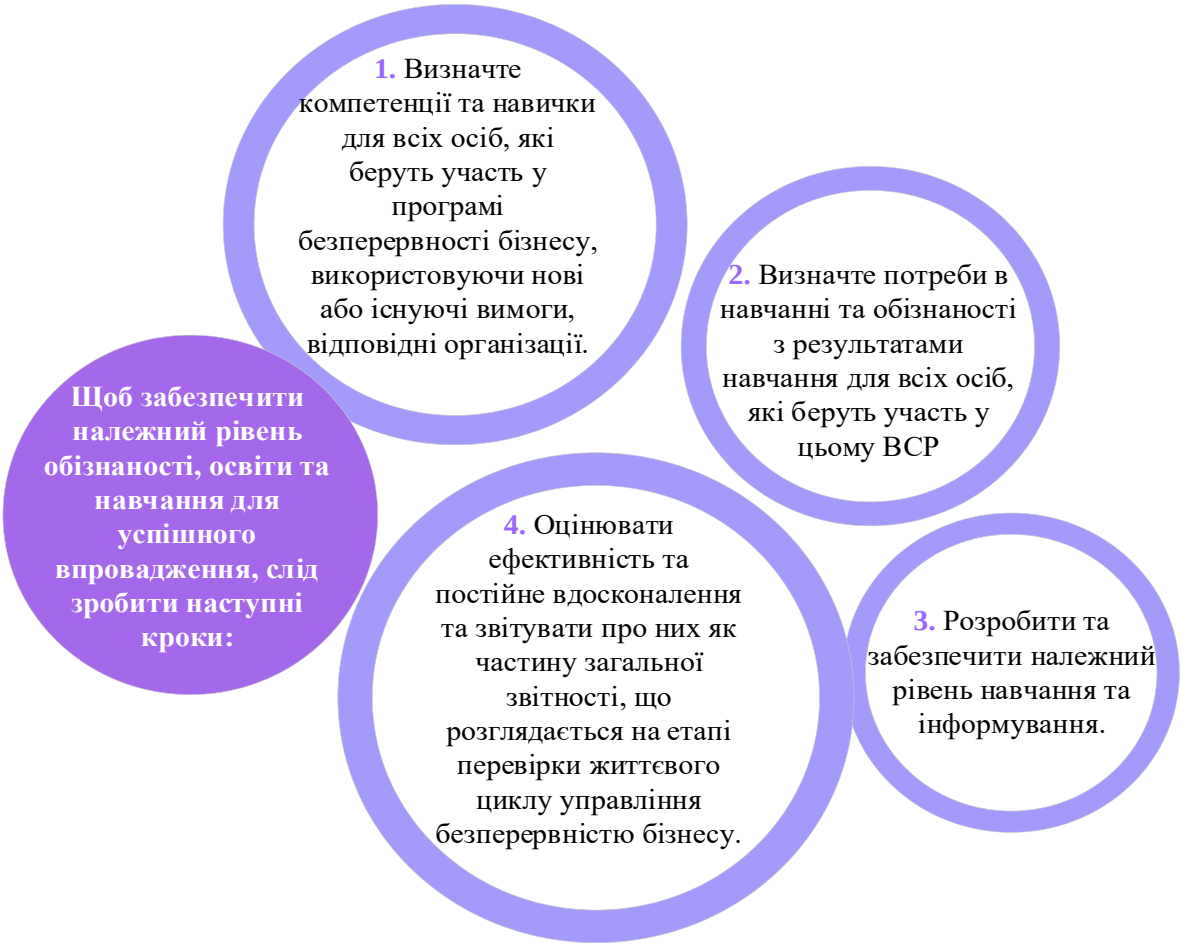


Рисунок 1.10 – кроки для успішного впровадження PP2.

1.2.3 Практика Аналізу BC (англ. Analysis. PP3)

Аналіз – це професійна практика в рамках життєвого циклу управління безперервністю бізнесу, яка переглядає та оцінює організацію для визначення її цілей, того, як вона функціонує та обмежень її операційного середовища.

Основним методом, який використовується для аналізу організації з метою безперервності бізнесу, є аналіз впливу на бізнес (BIA). Фахівець з безперервності бізнесу використовує BIA для визначення вимог організації до безперервності бізнесу.

Існує чотири типи BIA:

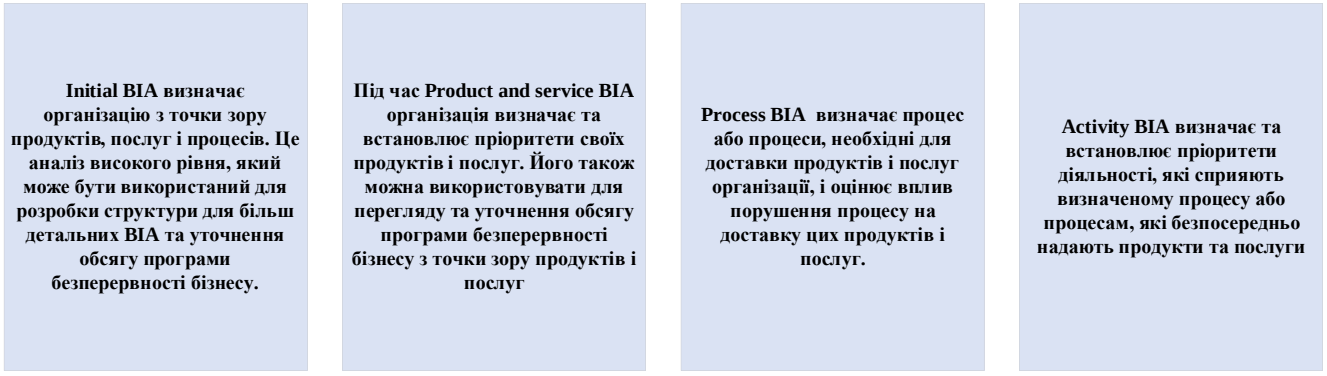
— An initial BIA.
— A product and service BIA.
— A process BIA.
— An activity BIA.

Існує багато підходів до проведення BIA. Не є обов’язкjовим виконувати всі чотири типи BIA. Комбінація деяких типів BIA іноді є найбільш прийнятним підходом

залежно від розміру, складності та типу організації, а також обсягу програми забезпечення безперервності бізнесу.

На цьому етапі слід провести оцінку ризику, щоб потім можна було визначити заходи з пом'якшення(mitigation measures) на етапі проектування життєвого циклу управління безперервністю бізнесу.

Досконале розуміння організації, використання цих методів аналізу часто може висвітлити неефективність та області, які необхідно покращити для вищого керівництва.



BIA розглядає як продукти та послуги, які надає організація, так і процеси, дії та залежності, які забезпечують доставку цих продуктів і послуг.

— ***Продукти та послуги*** визначаються як «вигідні результати, надані організацією своїм клієнтам, одержувачам та зацікавленим сторонам»[4].

— ***Процес*** описується як «набір взаємопов'язаних або взаємодіючих дій, які перетворюють вхідні дані у вихідні» [4]. Процес можна розділити на кілька видів діяльності. Наприклад, процесом може бути виробництво (від отримання товарів до доставки), управління інвестиціями або збір відходів.

— ***Діяльність/активність (англ.* activity*)*** визначається як одне або кілька завдань, які виконуються організацією або для неї, яка виробляє або підтримує доставку одного або кількох продуктів і послуг. Наприклад, контроль якості, відвідування дому, виставлення рахунків і відповіді на дзвінки через службу допомоги.

Рівень деталізації діяльності, яку необхідно проаналізувати, може залежати від їх складності та від того, чи можна визначити їх максимальний допустимий період збою (англ. MTPD - maximum tolerable period of disruption), максимально допустимий відключення (англ. MAO- maximum acceptable outage) та цілі часу відновлення (англ. RTO - recovery time objectives). Подібні види діяльності можна згрупувати.

Терміни «максимально допустимий період збою» або «максимально допустимий час відключення» використовуються для опису «часу, необхідного для того, щоб негативні впливи, які можуть виникнути в результаті ненадання продукту/послуги або виконання діяльності, стали неприйнятними »[4].

Параметр RTO – (англ. recovery time objective)- «Ціль часу відновлення» визначається як «період часу після інциденту, протягом якого продукт або послуга

має бути відновлено, або діяльність має бути відновлена, або ресурси повинні бути відновлені».

Рисунок 1.11 – Кроки для створення BIA.

Для збору інформації можна використовувати такі методи:

— анкети -опитувальники;
— інтерв’ю;
— нарди по обміну досвідом, майстер-класи.

Оцінка впливу для визначення MTPD та RTO

Зібрана інформація BIA включатиме ідентифікацію всіх продуктів і послуг, процесів і заходів, пріоритет яких визначається шляхом визначення максимально допустимого періоду збою (MTPD).

Параметр MTPD буде досягнуто, коли прийнятні рівні збитків будуть перевищені і збій організації неминучий.

Основними факторами, які слід враховувати під час оцінки MTPD збоїв у доставці продукції або послуг, є:

— Пошкодження фінансової вартості або життєздатності (короткострокові чи довгострокові).
— Пошкодження репутації або довіри зацікавлених сторін.
— Порушення юридичних або нормативних зобов'язань.
— Недосягнення стратегічних цілей організації.

У BIA не робиться жодних спроб кількісно оцінити вплив на зацікавлені сторони, спричинений порушенням. Замість цього він оцінює вплив, який може бути накладений на організацію у відповідь, наприклад, фінансові санкції або погана відгуки у ЗМІ.

Важливо враховувати часові рамки при визначенні впливу збою на доставку продуктів і послуг. Вищий менеджмент має вирішувати, що є неприйнятним для організації на основі впливу з часом

The Initial BIA

Initial BIA визначає організацію з точки зору продуктів, послуг і процесів. Це аналіз високого рівня, який може бути використаний для розробки структури для більш детальних BIA та уточнення обсягу програми безперервності бізнесу.

Зазвичай це потрібно, коли організація вперше проводить BIA. Однак може бути корисно повторити початковий BIA після істотної зміни в організації або якщо з моменту останнього BIA минуло кілька років. Початковий BIA підтримує вимогу постійного вдосконалення системи або програми управління безперервністю бізнесу, і є технікою, яка постійно покращує та вдосконалює результати BIA, поки вона не задовольняє цілі організації.

Мінімальна мета початкового BIA – визначити продукти, послуги та процеси в організаційній структурі. MTPD можна оцінити пізніше. Для забезпечення успішної реалізації програми безперервності бізнесу своєчасне надання початкового BIA може бути важливішим, ніж надання детального BIA, якщо воно приносить користь організації.

Рисунок 1.12 – Процес Initial BIA

Product and service BIA

У Product and service BIA організація визначає та визначає пріоритети своїх продуктів і послуг. Його також можна використовувати для перегляду та уточнення обсягу програми безперервності бізнесу з точки зору продуктів і послуг.

BIA продукту та послуги можна використовувати для визначення впливу збою перед впровадженням значних організаційних змін.

Результати Product and service BIA

— роз'яснення або зміна обсягу програми забезпечення безперервності бізнесу;

— список пріоритетних продуктів і послуг організації;

— оцінка впливів у часі.

Рисунок 1.13 – Процес Product and service BIA

The Process BIA

Обсяг Process BIA може бути пов'язаний із сферою BIA продукту та послуги, яка вивчає вплив зриву на одну або кілька груп продуктів і послуг.

Організація може вирішити обмежити обсяг Process BIA процесами, що стосуються продуктів і послуг вищого пріоритету.

Process BIA буде ґрунтуватися на результатах Product and service BIA. Він надає вказівки щодо визначення значних часових рамок, які можна використовувати для підсумовування впливів для кожного процесу. Process BIA також повинен допомогти перевірити результати Product and service BIA.

Розглядаючи вплив у часі, часові рамки можна згрупувати в діапазони для спрощення аналізу, наприклад, від 1 до 4 годин, від 12 до 4 годин тощо. Кількість груп та їх точні значення будуть відрізнятися в різних галузях промисловості. У деяких секторах вплив може досягати неприйнятного рівня протягом декількох хвилин, тоді як в інших організаціях може не відчувати неприйнятних впливів протягом кількох днів після збою.

The Activity BIA

Activity BIA визначає та встановлює пріоритети діяльностей/активностей, які сприяють визначеному процесу або процесам, які безпосередньо надають продукти та послуги.

Під час Activity BIA організація збирає детальну інформацію про ресурси, необхідні для продовження діяльності, яка підтримує стратегічні цілі організації.

На цьому рівні при визначенні вимог до ресурсів можна визначити залежність від зовнішніх постачальників і постачальників послуг, які залучаються на аутсорсинг. Зазвичай доцільно визначити загальні залежності, наприклад, комунальні послуги (енергія, вода, телекомунікації тощо) на рівні діяльності, оскільки вони впливають на більшість процесів.

Під час діяльності BIA повинна бути зібрана така інформація:

— Процеси, які підтримує діяльність (де це доречно).
— Операційні методи діяльності.
— Тривалість або час виконання діяльності.
— Коливання попиту або час пікової роботи.
— Фактори, які ще не виявлені, які можуть вплинути на визначення вимог безперервності бізнесу, наприклад, відставання в роботі або законодавчі та нормативні вимоги цієї діяльності.

Детальна інформація про ресурси, необхідні для продовження діяльності, поділяється на такі категорії:

— «Люди.
— Інформація та дані.
— Будинки, робоче середовище та супутні комунікації.
— Обладнання, обладнання та витратні матеріали.
— системи ІКТ.
— Транспорт.
— Фінанси.
— Партнери та постачальники» [4].

Часто передбачається, що ресурсів необхідних після збоїв буде менше, ніж тоді, коли вони використовуються під час звичайної діяльності, принаймні на певний період. Однак у деяких випадках кількість ресурсів на ранніх етапах може знадобитися бути більшою, ніж зазвичай, щоб впоратися з відставаннями.

Крім того, організація повинна визначити відповідні RECOVERY POINT OBJECTIVE (RPO), щоб зрозуміти, як втрата даних може вплинути на відновлення, а також доступність записів на паперових копіях (за потреби).

«Ціль точки відновлення (RPO) — це точка, до якої необхідно відновити інформацію, що використовується для діяльності, щоб дати можливість діяльності працювати після відновлення. RPO також можна назвати «максимальною втратою даних»»[4].

Рисунок 1.13 – Процес Activity BIA

Оцінка ризиків і загроз

Управління безперервністю бізнесу визначається як «цілісний процес управління, який визначає потенційні загрози для організації та вплив на бізнес-операції, ці загрози, якщо вони реалізовані, можуть спричинити…» [4]. BIA оцінює впливи з часом, пов'язані з до збою в доставці продуктів і послуг після збою та визначає вимоги безперервності бізнесу.

Фахівець з безперервності бізнесу використовує методи оцінки ризиків, щоб визначити неприйнятні рівні ризику та окремі точки збою. Інформація та методи оцінки ризиків для оцінки загрози зриву дозволяють розробити ефективні рішення щодо безперервності бізнесу та заходів щодо їх пом'якшення.

На етапі Analysis, як правило, спочатку проводиться BIA, щоб оцінка ризиків і загроз і заходи з їх пом'якшення могли бути зосереджені на пріоритетній діяльності організації та допоміжних ресурсах. Це може максимізувати вигоду від будь-яких інвестицій і зменшити частоту або вплив збоїв.

Ризик визначається як «вплив невизначеності на цілі»

Загроза визначається як «потенційна причина небажаного інциденту, який може призвести до шкоди особам, системі чи організації»[4].

Оцінка ризиків, як правило, включає методи виявлення, аналізу та оцінки низки ризиків, що мають відношення до організації. Для обчислення оцінки ризику використовується формула, заснована на ймовірності та впливі. Оцінка ризику визначається як «загальний процес ідентифікації ризику, аналізу ризику та оцінки ризику» [9].

Методи оцінки ризиків можуть бути ефективними під час аналізу відомих і очікуваних ризиків, однак фахівець з безперервності бізнесу повинен знати про деякі обмеження методів оцінки ризиків, коли вони використовуються для оцінки загроз і причин збоїв. Значні збої, як правило, трапляються нечасто, тобто оцінки, засновані на ймовірності виникнення загрози, базуються на обмежених наборах даних та історичній інформації, а також на періоді часу, який розглядається.

Оцінка ризику як частина програми безперервності бізнесу враховує ризик зриву через різні загрози. Фахівець з безперервної діяльності отримає загальне розуміння управління ризиками, і він повинен використовувати свої знання організації та її операційного середовища, щоб вирішити, скільки часу витрачати на оцінку ризиків і загроз, а також рівень деталізації, який підходить для організація. На рисунку нижче можна прослідкувати за необхідними кроками при оцінці ризиків та загроз.

Рисунок 1.14 – процес оцінки ризиків та зпгроз

1.2.4 Практика Розробка ВС рішень (англ. Design, PP4)

Design — це професійна практика в рамках життєвого циклу управління безперервністю бізнесу, яка визначає та вибирає відповідні рішення, щоб визначити, як можна досягти безперервності в разі інциденту. Етап аналізу визначає вимоги до безперервності бізнесу, а етап проектування визначає рішення, які потім слід реалізувати для найкращого досягнення цих вимог.

На цьому етапі життєвого циклу управління безперервністю бізнесу фахівець із забезпечення безперервності бізнесу повинен розробити рішення, які дозволять організації реагувати на інцидент і продовжувати виконувати пріоритетні види діяльності.

Визначаються вимоги, які підтримують впровадження для кожного запропонованого рішення для безперервності бізнесу, а найбільш підходящі вибираються за консультацією з вищим керівництвом. Деякі рішення залежатимуть від постачальників, їхніх ланцюгів поставок та сторонніх постачальників послуг. Важливою частиною цього етапу життєвого циклу управління безперервністю бізнесу є консолідація вибраних рішень, щоб забезпечити врахування можливостей співпраці в масштабах організації перед переходом до етапу впровадження. Проактивні заходи з пом'якшення покликані подолати ризики та загрози, виявлені на етапі Аналізу. Заходи пом’якшення можуть бути реалізовані для захисту організації та зменшення впливу зриву на пріоритетні види діяльності.

Розробка ВС рішень

Розробка рішень щодо того, як організація буде продовжувати роботу після збою, базується на вимогах безперервності бізнесу, визначених BIA, та результатах оцінки ризиків і загроз.

Переглядаються вимоги щодо безперервності бізнесу та результати оцінки ризиків і загроз і розроблено відповідні рішення щодо безперервності бізнесу.

Після того, як рішення розроблені, вище керівництво повинно узгодити найбільш відповідні рішення, і не слід розпочинати проекти для впровадження цих рішень.

Ціна та продуктивність, ціна та вигода часто використовуються вищим керівництвом при узгодженні найбільш відповідних рішень

Розробка рішень щодо того, як організація буде продовжувати роботу після збою, базується на вимогах безперервності бізнесу, визначених BIA, та результатах оцінки ризиків і загроз. Організації, які вже мають програму безперервності бізнесу, можуть мати рішення, які були розроблені та впроваджені, але більше не актуальні через мінливі загрози. Для будь-якого рішення, яке розробляється, мають бути дотримані не лише вимоги безперервності бізнесу, але й слід враховувати будь-які виявлені взаємозалежності, особливо коли рішення покладаються на постачальників та їхні ланцюги поставок.

Наприклад, постачальник, чиє обладнання стає недоступним, може більше не виконувати існуючі RTO або надавати послуги.

Без угоди про рівень обслуговування ця недоступність не може бути виявлена, доки не буде запущено план безперервності бізнесу.

Існує 5 рішень для забезпечення безперервності бізнесу, які можна використовувати в організації.
Цими рішеннями є:

- ***Diversification;***
- ***Replication;***
- ***Standby;***
- ***Post-incident acquisition;***
- ***Do nothing;***

Diversification: розділення діяльності та ресурсів і проведення активних заходів у двох або більше місцях, щоб у разі збою в одному місці діяльність могла продовжитися в іншому місці. Це рішення може бути дорогим і не захистити організацію, якщо збій не обмежується одним місцем або областю. При розробці цього рішення слід звернути увагу на те, щоб у разі збою в одному місці, альтернативне розташування могло впоратися з будь-яким додатковим робочим навантаженням, яке було переміщено з пошкодженої ділянки. Це може включати призупинення виконання несуттєвих операцій в альтернативному місці, доки пошкоджене місце не відновиться. Це рішення може бути доречним, *коли RTO вимірюється в секундах, хвилинах або годинах,* а не днях.

Replication: дублювання ресурсів для швидкого відновлення діяльності є різновидом диверсифікації. Відтворений сайт підтримується у високому стані готовності з усіма необхідними ресурсами. Він не починає функціонувати, доки йому не буде потрібно взяти на себе будь-яку порушену діяльність, переміщену з місця інциденту. Це рішення для забезпечення безперервності бізнесу може бути придатним, коли *RTO в рамках від кількох годин до кількох днів*, якщо персонал може бути переміщений в інше місце в межах своєї діяльності. Однак це покладається на те, що персонал може і хоче працювати далеко від свого основного місця протягом невідомого періоду часу.

Standby: якщо *RTO дозволяє довший час реагування, що вимірюється днями, а не годинами*, відповідним рішенням може бути наявність резервного засобу, який можна ввести в експлуатацію в межах RTO. Це рішення можна назвати «теплим сайтом» і особливо підходить для тих випадків, коли організація має доступ до об’єкта, який був тимчасово закритий, але його можна відновити та почати працювати в найкоротші терміни. Це рішення покладається на те, що персонал може і хоче працювати далеко від свого основного місця протягом невідомого періоду часу.

Post-incident acquisition: коли пріоритетні види діяльності мають *RTO, які вимірюються днями або тижнями,* організації можуть розглянути рішення для безперервності бізнесу, коли необхідні ресурси придбаваються після збою. Це рішення покладається на те, що організація має заздалегідь визначений і пріоритетний список вимог до ресурсів. Це також залежить від здатності постачальників забезпечити ресурси належної якості та кількості в прийнятні

терміни. Це не буде відповідним рішенням безперервності, якщо є потреба в спеціалізованих ресурсах, наприклад, обладнання, засоби, матеріали чи навички, які може бути важко отримати або які мають тривалий час виконання, що перевищує визначені МРД.

Do nothing: це рішення передбачає очікування після інциденту, щоб вирішити, що робити. Це може бути відповідним рішенням, коли RTO вимірюється тижнями або місяцями, або коли неможливо, занадто складно або занадто дорого надати альтернативні засоби або ресурси до того, як станеться інцидент. Фахівець із забезпечення безперервності бізнесу завжди повинен документувати причини, чому вибране рішення є бездіяльністю, щоб уникнути суперечок чи конфліктів у разі виникнення інциденту.Для більш чіткого уявлення нижче будуть наведені прикладие у Таблицях 1.2-1.4

Таблиця 1.2 - ВС рішення для будівель та робочого середовища

Варіант рішення для безперервності бізнесу	**Розташування офісу**	**Віддалена робоча локація**
Diversification	Окремі приміщення, де однакова діяльність відбувається паралельно.	Діяльність відділу повністю віддалена або існує комбінація персоналу, що працює віддалено та в офісі.
Replication	Окремі приміщення, які мають усі необхідні для здійснення діяльності, але наразі не використовуються.	Дистанційна робота доступна і готова в будь-який час з наявністю офісного обладнання та ІКТ, хоча наразі вони не використовуються.
Standby	Окремі приміщення, які мають деякі засоби, необхідні для здійснення діяльності, але додаткові приміщення будуть потрібні, перш ніж можна буде здійснювати діяльність.	Віддалену роботу можна підготувати після простого налаштування або часткового придбання.
Post-incident acquisition	Можна придбати відповідні приміщення, які можуть мати чи не мати приміщень, необхідних для здійснення діяльності.	Віддалена робота, як правило, не готова, але її можна підготувати, придбавши офісне обладнання та ІКТ.

Таблиця 1.3 - BC рішення для персоналу під час криз чи збоїв

Diversification	Персонал знаходяться в різних місцях, які одночасно здійснюють ту саму діяльність.
Replication	Персонал знаходяться в різних місцях, які мають досвід і здатні виконувати ту саму діяльність, але ще не роблять цього.
Standby	Персонал знаходяться в різних місцях, які пройшли навчання для виконання такої ж діяльності, але ще не мають досвіду та потребують керівництва.
Post-incident acquisition	Зовнішній персонал, кваліфіковані у здійсненні діяльності, яку можна найняти, або внутрішній персонал, який може бути навчений для здійснення діяльності

Таблиця 1.4 - BC рішення для інформаційних та комунікаційних технологій під час криз чи збоїв

Diversification	BCI копії системи та її дані в окремих місцях, які зберігаються синхронізовано та працюють.
Replication	Оперативна копія системи та її даних, що зберігаються в окремому місці, яке періодично синхронізується з поточною версією та потребує перемикання, щоб перейти в дію.
Standby	Робоча копія системи, що зберігається в окремому місці, і резервна копія її даних, які потрібно завантажити та протестувати з ручним перемиканням, щоб запустити його в режимі реального часу
Post-incident acquisition	Резервні копії системи та її даних, які необхідно встановити на обладнання, придбане після інциденту.

Таблиця 1.4 - ВС рішення для обладнання під час криз чи збоїв

Diversification	Обладнання задубльоване та утримується в окремому місці, з автоматичним переміщенням з одного на інший
Replication	Точна непрацююча копія обладнання, що зберігається в окремому місці, яку можна швидко ввести в експлуатацію. синхронізується з поточною версією та потребує перемикання, щоб перейти в дію.
Standby	Обладнання, що буде заміняти те, що вийшло з ладу знаходиться в окремому місці, але ще не працю, його потрібно буде ввести в дію.
Post-incident acquisition	Обладнання, яке можна придбати у постачальника після збою і прийняття рішення.

Консолідація

Зазвичай є можливість об'єднати певні елементи процесу 4-ї практики Design, щоб усунути дублювання і в кінцевому підсумку зробити дизайн більш ефективним.

Наведені нижче приклади підкреслюють концепцію консолідації:

Лідери закупівлі: якщо відома загальна потреба в ресурсах відновлення, то організація, швидше за все, отримає кращі умови від свого постачальника, ніж якщо кожна окрема вимога обговорюється окремо. Цей консолідований підхід повинен застосовуватися персоналом, який має досвід у сфері закупівель і переговорів за контрактами.

Логістика: логістику для поетапної доставки та прийняття консолідованих ресурсів кількома відділами також можна оптимізувати за допомогою консолідованих закупівель і доставки.

Конфлікт: дві або більше територій тодішньої організації можуть планувати використовувати один і той самий ресурс як частину свого вирішення безперервності, і тому будуть конфліктувати під час інциденту, наприклад, кімнати для нарад в іншому офісі.

Оптимізація: для двох або більше видів діяльності може знадобитися ресурс, наприклад, принтер, ксерокс або проектор, але можна поділитися ним з іншими. Консолідація може оптимізувати використання ресурсів шляхом визначення можливостей для спільного використання.

Послідовність: підхід до рішень безперервності може бути непослідовним усередині організації, наприклад, впровадження інформаційної безпеки. Консолідація може виділити додаткові ресурси, необхідні для забезпечення узгодженості.

Можливості: при застосуванні по всій організації рішення безперервності, наприклад, віддалена робота, може бути недосяжним за допомогою існуючої інфраструктури. Це може спрацювати, коли лише кілька людей працюють віддалено, але не тоді, коли всі в організації, які мають можливості, намагаються зробити це одночасно. Консолідація може визначити додаткові потреби в ресурсах для підтримки таких ситуацій.

Заходи щодо зменшення ризиків і загроз

Необхідно визначити та впровадити заходи зі зменшення наслідків, щоб зменшити вплив зриву на пріоритетних діяльностей чи сервісів організації.

Фахівець із забезпечення безперервності бізнесу повинен співпрацювати з фахівцями з ризиків, фізичної безпеки та інформаційної безпеки для розробки та впровадження заходів щодо зменшення наслідків. Стійкість організації можна підвищити, якщо відповідні дисципліни менеджменту координуються не тільки всередині організації, а й з постачальниками та іншими зацікавленими сторонами.

Вибрані заходи повинні бути спрямовані на неприйнятні рівні ризику, будь-які окремі точки збою та основні загрози пріоритетної діяльності організації. Усі вони визначаються на етапі аналізу життєвого циклу управління безперервністю бізнесу.

При визначенні найбільш відповідних заходів слід враховувати очікування зацікавлених сторін і договірні угоди з постачальниками. Відповідальність за виконання вимог організації безперервності бізнесу залишається на організації незалежно від будь-якого ризику чи загрози, виявлених у ланцюжку поставок.

Розробка заходів з пом’якшення наслідків передбачає, що вигоди від запропонованих заходів можна оцінити. Розуміння переваг покладається на знання ймовірності реалізації загрози, яка в багатьох випадках ґрунтується на історичній інформації або ймовірності.

Також може існувати юридична або нормативна вимога щодо забезпечення належних заходів зменшення ризиків чи загоз. Для пріоритетних видів діяльності, які передані стороннім виконавцям або залежать від постачальників, слід розглянути заходи та провести аналіз витрат і результатів як частину оцінки. При залученні сторонніх постачальників послуг можуть виникнути додаткові витрати.

Процес оцінки заходів щодо зменшення загроз та ризиків показаний на Рисунку 1.15.

Рисунок 1.15 – Процес під час оцінки заходів щодо зменшення ризиків та загроз.

Методи для створення заходів по зменшенню ризиків та загроз

Аналіз витрат і вигод: аналіз витрат і вигод може використовуватися для оцінки заходів з пом'якшення наслідків шляхом порівняння вартості заходу з ймовірною вигодою, яку можна отримати. При проведенні аналізу витрат і результатів необхідно визначити часові рамки, протягом яких рішення або захід мають бути ефективними, і ймовірність реалізації загрози в цей період часу.

Для заходів, *які знижують ймовірність*, вигода розраховується шляхом оцінки зменшення ймовірності реалізації загрози після того, як захід зниження ризику було введено в дію, і множення її на вплив на організацію, якщо загроза була реалізована, з точки зору вартості.

Для заходів, *які зменшують вплив*, вигода розраховується шляхом оцінки зменшення впливу загрози на організацію з точки зору витрат після того, як захід пом’якшення було введено в дію, та множення його на ймовірність виникнення загрози.

Управління ризиками ланцюга поставок: загроза порушення роботи продуктів і послуг організації, спричинена збоями в роботі постачальників та їхніх ланцюгів поставок, може бути зменшена, якщо постачальники мають ефективні та адекватні механізми безперервності бізнесу. Цього можна досягти за допомогою:

— включення вимог щодо безперервності бізнесу в контрактах на постачання;

— пошук доказів відповідності визнаному стандарту безперервності бізнесу;

— перегляд програми забезпечення безперервності бізнесу кожного постачальника, щоб переконатися, що вона ефективна та адекватна;

— проведення спільних навчань з постачальниками сервісів чи послуг;

— узгодження реалістичних рівнів обслуговування у разі перебоїв у постачанні.

1.2.5 Практика Впровадження ВС рішень (англ. Implementation, PP5)

Implementation — це професійна практика в рамках життєвого циклу управління безперервністю бізнесу, яка реалізує рішення, узгоджені на стадії проектування(Design). Реалізація досягається шляхом розробки планів безперервності бізнесу для задоволення узгоджених вимог організації безперервності бізнесу та рішень, визначених на етапі аналізу та проектування життєвого циклу. Етап впровадження також включає розробку структури реагування, яка визначає необхідні ролі, повноваження та навички, необхідні для управління інцидентом.

Мета полягає в тому, щоб визначити та задокументувати пріоритети, процедури, відповідальність та ресурси, які підтримають організацію під час управління інцидентом. Це повинно забезпечити безперервність пріоритетних заходів і забезпечити відновлення порушеної діяльності до попередньо визначеного рівня обслуговування (мінімальна ціль безперервності бізнесу) протягом запланованих термінів.

Термін «план безперервності бізнесу» (BCP) передбачає єдиний документ. Однак на будь-якому організаційному рівні можуть існувати різноманітні плани. Фактично BCP може включати кілька документів. Він може охоплювати всю організацію або частину організації і може бути структурований відповідно до розміру, складності та типу, наприклад, за продуктами, послугами, розташуванням, підрозділами чи відділами.

Основними вимогами до впровадження ефективного плану безперервності бізнесу є:

— Здатність розпізнавати й оцінювати існуючі та потенційні загрози, коли вони виникають, і визначати відповідну відповідь.

— Створена структура реагування для активації, ескалації та контролю реагування організації.

— Персонал, який має повноваження та компетенцію для впровадження узгоджених рішень та заходів.

— Здатність ефективно спілкуватися між внутрішніми та зовнішні зацікавлені сторони.

— Доступ до достатніх ресурсів для підтримки узгоджених рішень безперервності.

Плани безперервності бізнесу не призначені для охоплення всіх випадків, оскільки всі інциденти різні. Плани мають бути достатньо гнучкими, щоб бути адаптованими до конкретного інциденту, який стався, і можливостей, які він міг створити. Однак за деяких обставин для подолання значної загрози чи ризику доречні плани, що стосуються інцидентів, наприклад, план боротьби з пандемією чи план відкликання продукції.

У багатьох організаціях можуть бути наявні процедури, які стосуються реагування на різні типи збоїв.

Наприклад, плани евакуації, охорони здоров'я та безпеки, безперервності послуг ІКТ, фізичної безпеки, кризового зв'язку та інформаційної безпеки.

Багато збоїв будуть мати широкий вплив на організації і вимагатимуть активації кількох планів реагування для ефективної боротьби з тим самим інцидентом. Ефективні можливості організаційного реагування можуть бути досягнуті, якщо професіонали з безперервності бізнесу співпрацюють з іншими професіоналами, які відповідають за управління реагуванням у відповідних дисциплінах управління.

Структура ревгування

Метою створення структури реагування є забезпечення того, що організація має чітко задокументований і добре зрозумілий механізм реагування на інцидент, незалежно від його причини. Структура реагування встановлює системи командування, контролю та зв'язку, щоб допомогти організації керувати інцидентом та мінімізувати вплив зриву.

Ефективна структура реагування включає механізми, які дозволяють швидко та точно передавати інформацію відповідним особам і командам у всій організації. Вона також повинен визнавати та включати зовнішніх постачальників, які мають відношення до пріоритетної діяльності.

Структура реагування організації повинна бути гнучкою і здатною впоратися з багатьма типами збоїв. Існує два основних типи порушення:

— ***Інцидент***, який визначається як «ситуація, яка може бути або може призвести до збою, втрати, надзвичайної ситуації чи кризи»[10].

— ***Криза***, яка визначається як «ситуація з високим рівнем невизначеності, яка порушує основну діяльність та/або довіру до організації та вимагає невідкладних заходів» [10].

Інциденти та кризи пов'язані між собою, але чітко відрізняються один від одного і тому вимагають іншого рівня реагування.

Управління організацією інциденту, ймовірно, буде вирішено за допомогою встановлених планів і процедур.

Криза – це непередбачувана ситуація, яка виходить за межі очікуваних і вимагає гнучкого, креативного та стратегічного реагування. Існуюча структура реагування, інформація та процедури в плані безперервності бізнесу повинні бути побудовані та адаптовані під час реагування на кризу, якщо це необхідно.

Перебої можуть бути негайними та очевидними, але також можуть розвиватися повільно з плином часу. Структура відповіді повинна включати

механізм для окремих осіб та команд, щоб негайно визначити інцидент, щоб ситуація була оцінена досвідченим та уповноваженим персоналом та відповідною відповіддю.

Основні вимоги до ефективної структури реагування є:

— здатність розпізнавати та оцінювати загрози, коли вони виникають;

— зрозумілі процедури ескалації, коли відбулося порушення або скоро відбувається;

— особи та команди з повноваженнями та можливостями розробляти та вибирати відповідну відповідь на інцидент;

— чітко зрозумілі процедури для активації та контролю над реакцією на інцидент або кризу;

— відповідальний персонал з повноваженням та здатністю здійснити узгоджені рішення безперервності бізнесу, як визначено в рамках планів організації;

— здатність ефективно спілкуватися з внутрішніми та зовнішніми зацікавленими сторонами;

— доступ до достатніх ресурсів для підтримки реалізації рішення безперервності;

— можливість розпізнавання, коли основні зовнішні постачальники повинні бути повідомлені та включені до реалізації рішення безперервності;

— узгоджений бюджет для підтримки структури відповіді.

У деяких організаціях може бути доцільним мати до трьох рівнів команд у структурі відповіді. Стратегічні, тактичні та операційні команди у структурі відповіді здійснюють різні заходи наступним чином, як зображено на Рисунку 1.16.

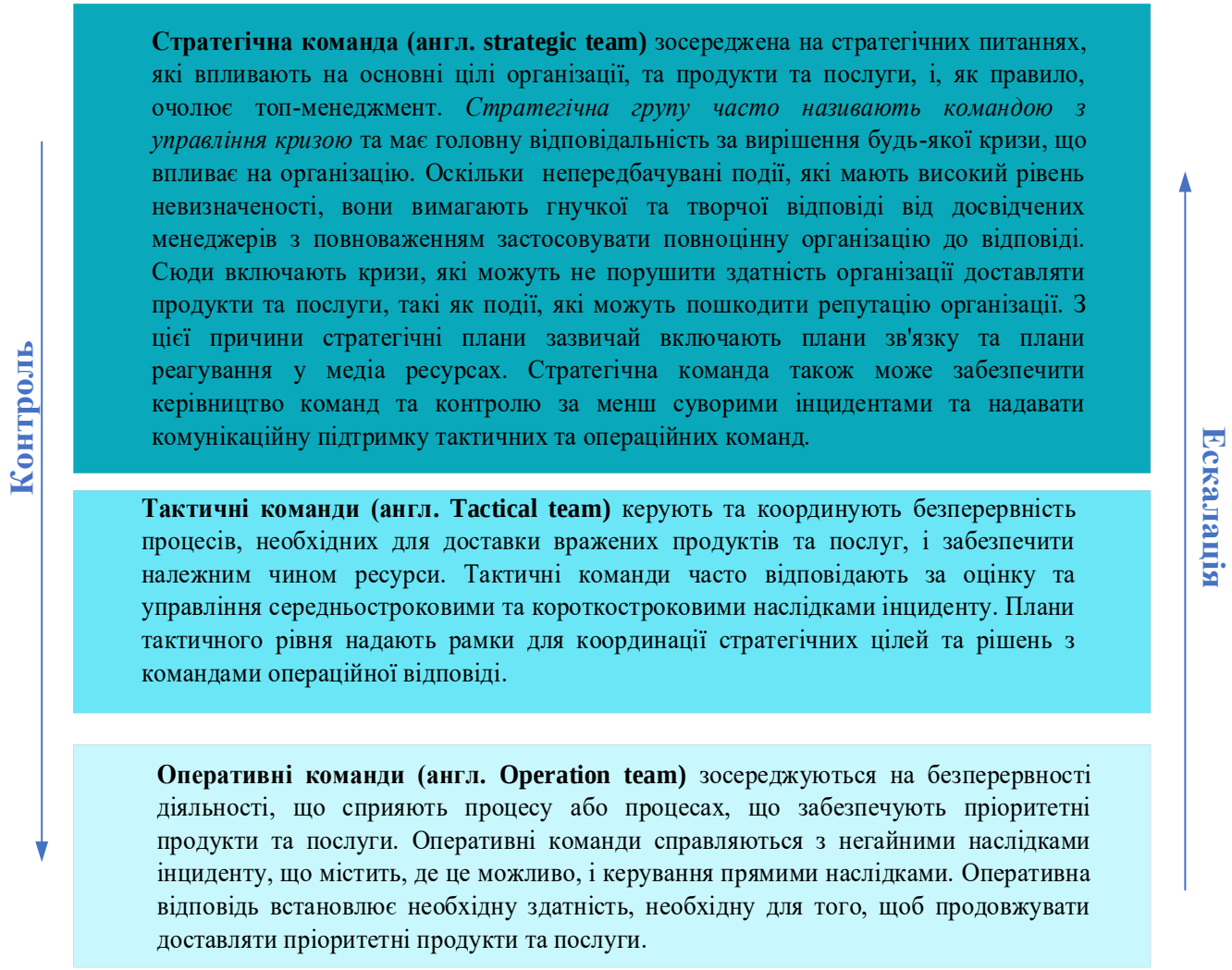


Рисунок 1.16 – Рівні команд та їх управління

Структура відповіді потребує включення всіх команд та окремих осіб, які ідентифікуються в політиці та програму "Бізнес-політику організації". Ці команди та особи повинні охоплювати всі аспекти надзвичайної ситуації, управління безперервністю бізнесу та управління кризовими ситуаціями. Структура відповіді повинна розглянути, яка з цих команд та окремих людей є компетентними, щоб здійснити стратегічні, тактичні та операційні ролі.

Слід розглянути наступне:

— існуючу структура управління;
— Навички, компетенції та повноваження команд та фізичних осіб;
— процес зв'язку та процес ескалації;
— Розмір організації, складність та тип, а також технологічна інфраструктура;
— узгоджені рішення безперервності.

Розробка та управління планами

Плани безперервності бізнесу можуть бути створені для вирішення стратегічних, тактичних та експлуатаційних вимог організації. Кількість та тип планів, які будуть встановлені, повинні бути визначені структурою відповіді та

рішеннями безперервності бізнесу, узгодженими на етапі проектування життєвого циклу. Це має відображати існуючу структуру управління, а також розмір, складність та тип організації.

Загальні принципи

Плани призначені для використання у високому тиску, часових обмежених ситуаціях. Для користувачів повинен бути стислий та легко читати. Плани не повідомляють і не повинні містити непотрібну інформацію, яка не потрібна під час інциденту.

Щоб зробити план зосередженим, специфічним та простим у використанні, він повинен бути:

— прямий; забезпечення чіткого, орієнтованого на дію та напрямок часу. Він повинен забезпечити швидкий доступ до життєвої інформації;

— адаптований; Увімкнення організації реагувати на широкий спектр інцидентів, у тому числі ті, що організація може не передбачити;

— короткі; що містить лише керівництво, інформацію та інструменти, які, ймовірно, будуть використовуватися командою в інциденті. Нічого іншого є непотрібним;

— актуальні; Надання інформації, яка є поточною та корисною команді, використовуючи план.

План безперервності бізнесу повинен бути оновлений та задокументований таким чином, що дозволяє персоналу швидко отримати доступ до інформації.

Тактичні та Операційні плани можуть містити інформацію про процедури, які можуть бути розроблені лише після того, як рішення щодо безперервності були узгоджені на етапі проектування.

Навпаки, план *стратегічного рівня* не містить такої детальної процедурної інформації. Як наслідок, вони можуть бути реалізовані на початку процесу безперервності бізнесу, щоб забезпечити початкові можливості відповіді до розробки інших планів. Який тип плану розробляється, його не слід робити в ізоляції. Для досягнення успішного результату необхідно залучити користувачів планів, включаючи керівництво, у процесі розробки та впровадження.

Управління планом

Хоча деякі плани можуть належати конкретними відділам, вони є частиною загальної програми безперервності організації.

Копії всіх документів безперервності бізнесу повинні зберігатися та підтримуватися централізовано, щоб полегшити спостереження за планом перегляду та технічного обслуговування.

Всі плани повинні проводитись у відомих та безпечних місцях, доступних для всіх членів команди. Якщо плани проводяться в електронному вигляді, організація повинна забезпечити також, щоб вони також доступні у жорсткій копії під час порушення.

Ролі та обов'язки

Персонал, призначений для членів команди відповіді, повинен мати необхідну повноваження та здатність реагувати на інцидент на відповідному рівні. Заступник повинен існувати для кожної ролі.

Активація та мобілізація

План повинен документувати умови або обставини, за яких план повинен бути активований, і команда мобілізується.

Не всі інциденти трапляються раптово. Деякі ескалації відбуваються в повільному темпі, перш ніж вони визнаються як інцидент.

Наприклад, загрози промислових заходів, медичних проблем та порушення ланцюга постачання або дефіцит через екологічні чи економічні наслідки.

Отже, план повинен включати інформацію про неприйнятний рівень порушень. Ця інформація може підтримувати оцінку інциденту та забезпечити своєчасне прийняття рішень та ескалації відповідними членами організації.

Добробут персоналу

Організації несуть відповідальність за охорону здоров'я, безпеку та добробут свого персоналу, підрядників, відвідувачів та клієнтів (це юридична вимога в деяких галузевих секторах). План безперервності бізнесу повинен вирішувати питання персоналу та добробуту. Персонал організації, швидше за все, підтримує додаткові вимоги, розміщені на них у інциденті, якщо їхні потреби добробуту виконуються.

Нижче наведені питання повинні бути включені до спеціального плану добробуту або бути включені в організм більш загального плану безперервності бізнесу.

Під час інциденту, і де відповідним, одна або декілька членів команди повинні бути призначені відповідальність за:

— Перевірка результатів евакуації сайту.
— Облік персоналу та відвідувачів організації.
— спілкування з персоналом та іншими на місці.
— спілкування з надзвичайними послугами.
— Налаштування комунікаційних систем, наприклад, довідкової лінії або сторінок інтрамережі.
— Звернення до наступного кольору.
— організація транспортної допомоги

Командна зустріч

Щоб заощадити час і уникнути плутанини під час інциденту, кожна команда повинна заздалегідь знати деталі наявних місць зустрічі (також відомі як командний центр). Слід також розуміти, які члени команди можуть прийняти рішення щодо найбільш підходящого місця зустрічі на основі наявної інформації про інцидент.

Залежно від типу інциденту, команда може працювати разом в одному місці або періодично зустрічатися протягом дня.

Стратегічні плани

План стратегічного рівня або план для кризових ситуацій - це план високого рівня, який визначає, наскільки стратегічні питання, що виникають внаслідок кризи або інциденту, повинні бути вирішені та керувати топ-менеджментом. Він має особливі характеристики, які диференціюють документ з тактичних та операційних планів.

Деякі кризи або інциденти не включають фізичні порушення організації та не можуть вимагати виклику плану безперервності бізнесу, однак, вони все ще потребують відповідності стратегічного рівня, наприклад, експонування шахрайства чи негативного інформації зі ЗМі, яка загрожує репутації організації.

Цей тип інциденту може призвести до мобілізації команд з відповідальністю за управління сферою постраждалих від бізнесу та потенційним заподіянням репутації. У цих ситуаціях майже завжди необхідно залучити команду стратегічного рівня, якщо тільки щоб їх усвідомлювати ситуації у випадку, якщо він посипає.

Загальні принципи

План стратегічного рівня повинен забезпечити високорівневу інформацію та керівні принципи підтримувати топ-менеджменту, або команду з управління кризою. Він повинен вирішувати стратегічні питання, що впливають на основні цілі організації та її пріоритетні продукти та послуги.

План стратегічного рівня повинен також вирішувати необхідність спілкування з та контрольною діяльністю між усіма зацікавленими особами, або вплинути на зацікавлених сторін. Зміст плану стратегічного рівня повинен мати відношення до розміру, складності та типу організації.

Він повинен містити резюме інформацію про різні частини організації та загальноосвітньої організації.

Концепції та припущення

Під час кризи або інциденту команда стратегічного рівня підтримують стабільність, безперервність та репутацію організації. Вони несуть відповідальність за реалізацію та адаптації реагування на досягнення найкращого результату для організації.

Реагування з комунікацій під час кризи чи інциденту зазвичай керує вище керівництво, яке працює зі спеціалістами з комунікаційних груп в організації.

Залежно від структури реагування організації може існувати окремий план комунікації або він може бути включений як частина стратегічного плану.

План комунікації повинен:

— Вирішувати, як слід керувати комунікацією з внутрішніми та зовнішніми зацікавленими сторонами.

— Визначати внутрішні та зовнішні зацікавлені сторони, та мати в собі контактні дані та, якщо це можливо,

— Визначати доступні методи та канали спілкування з кожною зацікавленою стороною, наприклад, соціальні мережі, електронна пошта, радіо та газети.

Тактичні плани

Плани тактичного рівня зосереджені на координації реагування на інцидент та сприянні безперервності пріоритетних заходів. Тактичні плани повинні містити вказівки, які допоможуть тактичній групі проаналізувати вплив інциденту, застосувати відповідні рішення з тих, які є в планах, забезпечити безперервність пріоритетних заходів та надати стратегічній команді оновлення прогресу.

Тактичні плани повинні ґрунтуватися на узгоджених рішеннях щодо

забезпечення безперервності бізнесу та розглядати реакцію на інцидент від початкового попередження до точки, коли порушена діяльність відновлюється. Тактичний план повинен бути зосереджений на координації діяльності залучених груп реагування для забезпечення їх ефективної спільної роботи. Якщо ресурси обмежені, тактичний план повинен надавати інформацію, яка допоможе тактичній групі розподілити доступні ресурси для пріоритетних заходів, визначених на етапі аналізу.

Ці плани повинні містити припущення щодо масштабів інциденту з точки зору масштабу, тривалості та оперативного або персоналу впливу. Якщо масштаб інциденту перевищує припущення, це слід передати команді стратегічного рівня та розглянути реакцію на кризове управління.

Конкретні обов'язки груп реагування, які будуть включені в тактичні плани, включають:

— координація та моніторинг реагування оперативних груп, залучених до інциденту.

— моніторинг послуг підтримки, що надаються оперативним групам, таких як ІКТ, людські ресурси, засоби та фінанси.

— розподіл доступних ресурсів на основі кількостей та часових рамок, узгоджених на етапі аналізу.

Оперативні плани

Плани оперативного рівня створюють окремі відділи або підрозділи, які беруть участь у реагуванні на інцидент. Плани нижчого рівня можуть ускладнитися, якщо всі процедури безперервності для організації будуть включені в один документ. У цьому випадку процедури реагування кожної бізнес-одиниці можуть бути розділені на один або кілька планів, які переходять у відповідальність відповідного бізнес-одиниці.

Плани оперативного рівня повинні підтримувати безперервність пріоритетної діяльності організації від початку інциденту до відновлення узгодженого рівня обслуговування та повернення до звичайного режиму. Вони повинні ґрунтуватися на узгоджених рішеннях щодо безперервності та визначених потребах у ресурсах, визначених на етапі аналізу життєвого циклу.

Плани оперативного рівня повинні включати відділи, які керують інфраструктурою організації, наприклад, служби ІКТ та інші спеціалізовані служби підтримки, які підтримують організацію під час інциденту. Ці плани оперативного рівня забезпечують структуру для відновлення ключових служб підтримки або надання альтернативних засобів, які підтримують безперервність інших відділів.

Складність і пріоритетність продуктів, послуг і процесів організації повинні визначати, чи може один план відділу охоплювати кілька видів діяльності, чи потрібен оперативний план для детального охоплення однієї діяльності. Якщо потрібно, ці більш детальні плани можуть містити інформацію та процедури реагування для конкретних місць, систем або обладнання.

1.2.6 Практика перевірки ВС (англ. Validation, PP6)

Практика перевірки(Validation) – це професійна практика в рамках життєвого циклу управління безперервністю бізнесу, яка підтверджує, що програма забезпечення безперервності бізнесу відповідає цілям, встановленим у політиці, і що наявні плани та процедури є ефективними.

Мета практики полягає в тому, щоб переконатися, що рішення щодо безперервності бізнесу та структура реагування відображають розмір, складність і тип організації, а також те, що плани є актуальними, точними, ефективними та повними. Повинен існувати процес постійного підвищення загального рівня організаційної стійкості.

Перевірка досягається за допомогою комбінації наступних трьох заходів:

— ***Активності по тестуванню***: процес навчання, тестування, оцінки, практики та покращення безперервності бізнесу організації.

— ***Технічне обслуговування:*** процес, який гарантує, що домовленості та плани організації щодо безперервності бізнесу залишаються актуальними, актуальними та оперативно готовими до реагування.

— ***Перегляд:*** процес оцінки придатності, адекватності та ефективності програми безперервності бізнесу та визначення можливостей для покращення.

Розробка програми заходів

Можливість організації бути стійкою до загроз не може вважатися надійною чи ефективною, доки вона не буде протестована. Незалежно від того, наскільки добре розроблене рішення для безперервності бізнесу або план безперервності бізнесу, слід використовувати реалістичні заходіви, щоб допомогти визначити проблеми та підтвердити припущення, які можуть вимагати уваги. Метою заходів є постійне вдосконалення можливостей управління безперервністю бізнесу та готовності шляхом забезпечення того, щоб отримані уроки були інтегровані в заходи попередження, пом’якшення, планування, навчання та майбутні тренування.

Активності по тестуванню спрямовані на досягнення різних результатів, зокрема:

— Оцінка спроможності організації здійснювати безперервну діяльність і досягати очікуваних МРН.

— Перевірка рішень щодо безперервності бізнесу та припущень, на яких вони засновані.

— Перевірка того, що задокументовані процедури в плані безперервності бізнесу є відповідними, повними та актуальними.

— Перевірка адекватності та практичності ресурсів, які підтримують рішення безперервності.

— Визначення областей для покращення або відсутньої інформації.

— Підтвердження компетентності та формування довіри до персоналу з відповідними ролями та обов'язками.

— Розвиток командної роботи.

— Підвищення обізнаності щодо безперервності бізнесу в усій організації, як описано в PP2.

Активності по тестуванню не є одноразовими. Їх слід запланувати та запрограмувати на серію подій та заходів, які дозволять організації поступово покращувати можливості з часом. Програма заходів має забезпечувати бажаний рівень здібностей шляхом:

- Репетиція всіх планів.
- Перевірка всіх рішень безперервності бізнесу.
- Перевірка всієї інформації, що міститься в планах.
- Тренування всього відповідного персоналу (включаючи заступників).

Програма заходів має починатися з простих заходів, щоб підвищити загальний рівень обізнаності та розуміння, і поступово наростати в плані складності та виклику. Програма заходів по тестуванню повинна використовувати комбінацію методів і прийомів заходів, щоб забезпечити досягнення запланованих результатів у всій організації протягом тривалості програми.

Політика та програма організації безперервності бізнесу визначає, як планувати і керувати програмою навчань, а також будь-яке навчання, яке має бути проведено, і необхідні ресурси, які необхідно визначити.

Програма заходів визначається як «процес підготовки, оцінки, практики та підвищення ефективності в організації»[4].

Якщо доставка продукту чи послуги була передана на аутсорсинг, відповідальність за виконання заходів залишається за організацією, яка володіє продуктом чи послугою. Організація повинна переконатися, що аутсорсингова компанія може продовжувати виконувати свої зобов'язання в разі збою.

Можливо, буде доцільно розглянути домовленості про спільні навчання з аутсорсинговими постачальниками послуг та ключовими постачальниками. Крім того, якщо на етапі аналізу життєвого циклу управління безперервністю бізнесу були визначені інші постачальники пріоритетних продуктів і послуг, процесів і видів діяльності, їх слід попросити продемонструвати власні можливості безперервності бізнесу за допомогою власних заходів.

Види заходів

Існує багато назв різних видів заходів, але в принципі вони поділяються на наступні п'ять категорій. Ці типи заходів мають спільні риси, і організації можуть вважати за доцільне комбінувати елементи з різних категорій заходів для досягнення своїх цілей заходів.

Заходи на основі обговорення - ці заходи найпростіші для організації та полегшення, а також найменші витрати часу на типи заходів. Це структуровані заходи, на яких учасники можуть досліджувати відповідні проблеми та ознайомитися з планами в умовах низького тиску. Цей тип заходів може зосередитися на певній області для покращення, яка була визначена з метою знайти бажане рішення.

Сценарні заходи – це часто використовувана діяльність, заснована на обговоренні, з використанням відповідного сценарію з часовими рамками. Заходи можуть виконуватися в режимі реального часу або включати стрибки в часі, щоб дозволити виконувати різні фази сценарію. Сценарні заходи зазвичай проводяться на столі. Очікується, що учасники будуть знайомі з планами, що виконуються, і

повинні продемонструвати своє розуміння того, як плани працюють, коли розгортається сценарій. Вони можуть включати деякі практичні репетиції відповідних заходів реагування, наприклад, заповнення контрольних списків оцінки або використання журналів.

Сценарні заходів можуть бути реалістичним, економічно ефективним методом.. Під час навчання групи реагування можуть виробляти практичні результати, такі як повідомлення для ЗМІ або комунікації співробітників.

Імітаційні заходи є більш складними і можуть залучати команди на стратегічному, тактичному або оперативному рівні. Учасники можуть бути розташовані по всій організації, усі працюють зі своїх звичайних місць.

Під час імітаційних заходів учасникам надається інформація таким чином, що імітує реальний інцидент. Деталі сценарію та запитання зацікавлених сторін, таких як персонал, клієнти та засоби масової інформації, можна вводити у заходіву за допомогою різних платформ, наприклад, телефонних дзвінків, електронної пошти, соціальних мереж та телевізійних новин.

Учасників заходів просять розглядати оновлення або запити на інформацію, як ніби це був реальний інцидент, і розробити та впровадити відповідну відповідь на сценарій, що розгортається. Імітаційні заходіви також дозволяють учасникам детально відпрацювати відповідні процедури, наприклад, сповіщення та ескалацію, прийняття рішень, комунікацію, реакцію ЗМІ та координацію команди, на додаток до тестування обладнання командного центру та інших ресурсів, необхідних для підтримки команди.

Живі заходи можуть варіюватися від невеликої репетиції однієї частини реагування, наприклад, евакуації, до повномасштабної репетиції всієї організації з потенційним залученням зацікавлених сторін у реальному часі. Живі заходіви розроблені таким чином, щоб залучити всіх, хто, ймовірно, буде залучений до цієї частини відповіді.

Навчання в прямому ефірі особливо корисні, коли існують законодавчі або нормативні вимоги або коли було виявлено високий ризик для організації, і плани реагування повинні бути повністю оцінені.

Вони є найбільш реалістичним способом навчання індивідів і виконання планів. Однак існує кілька проблем, які можуть означати, що заходіви в прямому ефірі не є найбільш підходящим форматом заходів. Наприклад, необхідні ресурси можуть бути значними і можуть мати фінансові наслідки. Слід подбати про те, щоб не порушити звичайні завдання організації, і слід враховувати будь-який вплив на репутацію.

Тест - визначається як «унікальний тип заходів, який включає очікування успішного або неефективного елемента в рамках мети або завдань заходіви, що планується». Зазвичай він застосовується до обладнання, процедур відновлення або технологій, а не до команд чи окремих осіб. Наприклад, перебудова сервера з резервних стрічок протягом заздалегідь визначеного періоду часу.

1.3 IS/IT Risk Assessment

Оцінка ризику виконується для вирішення однієї визначеної проблеми, а після вирішення проблеми оцінка ризику або відкладається, або посилається як модель для іншої оцінки ризику. Коли оцінки ризиків розглядаються як інформаційні технології, вони мають набагато ширший потенціал використання у формі сховищ структурованої інформації, середовища для комунікації, дозволяють асинхронну комунікацію та мають здатність вирішувати невизначене майбутнє. Забезпечуючи рекомендації з управління ризиками, кожна організація може переглянути компоненти ризиків своєї системи управління, які відповідають цілям плану управління ризиками.

Інструкції з управління ризиками призначені для забезпечення добровільного підходу до управління ризиками і не призначені як інструмент дотримання вимог або сертифікації. Принципи та рекомендації щодо управління ризиками можуть застосовуватися до будь-якої організації (державної або приватної), зацікавлені сторони, зацікавлені в процесі управління ризиками, можуть використовувати ці рекомендації як глобальний довідник, обсяг управління ризиками може бути передано в організаційному контексті та сприяти навчальним і навчальним програмам з управління ризиками в організації.

Оцінка ризиків IS/IT

Процес управління IT-ризиками - постійне виявлення, оцінка та зниження ризику, пов'язаного з IT, у межах допустимого рівня, встановленого виконавчим керівництвом підприємства. Метою цього процесу є інтеграція управління корпоративними ризиками, пов'язаними з IT, із загальною структурою ERM. Процес підтримує досягнення набору первинних IT-цілей, включених у структуру, пов'язану з відповідністю IT, відповідністю бізнесу зовнішнім законам та нормативним актам, управлінням бізнес-ризиками IT, прозорістю витрат на IT22, перевагами та ризиками, безпекою інформації, обробкою інфраструктура та додатки, надання програмних переваг (вчасно та за бюджетом), що відповідають вимогам та стандартам якості.[11]

IS та IT тісно вбудовані в архітектуру бізнес-підприємства як інструмент бізнес-процесу. Матеріалізація ризику IC/IT може спричинити згубні наслідки для бізнесу та призвести до кризи.

Ризики можуть включати збиток репутації, спричинений крадіжкою особистих даних, фінансові збитки від системних збоїв та нормативні штрафи через проблеми з невідповідністю Оскільки матеріалізація ризику IS/IT не відбувається окремо, важливо отримати вичерпне уявлення про взаємозв'язок між бізнес-процесами та ризиком IS/IT. Зокрема, в рамках управління ризиками стверджується, що «IT-ризик — це бізнес-ризик, пов'язаний із використанням, володінням, функціонуванням, залученням, впливом та впровадженням IT на підприємстві». Структура вказує, що ризик пов'язаний із подіями, пов'язаними з IT, які потенційно можуть вплинути на бізнес[12]. Бізнес-ризики представляють загрозу для здатності підприємства ефективно виконувати бізнес-процеси і створювати цінність для

клієнтів відповідно до стратегічних цілей. На більшості підприємств ІТ стали фундаментальною складовою бізнесу, і його функція має життєво важливе значення для зміцнення, підтримки та розвитку бізнесу. Це робить IS/IT критичним активом для підприємства, а його швидка еволюція певною мірою змінила спосіб розробки, підтримки та впровадження бізнес-процесів

Оцінка ризиків IS/IT в організації може виконуватися відділом внутрішнього аудиту як частина процесів RM або як окреме завдання. Часто внутрішній аудит проводить перевірку ризиків IS/IT у бізнес-процесах. Багато-дисциплінарний характер галузі робить для внутрішніх аудиторів більш складною задачу кількісної оцінки ризику. Керівникам бізнесу мають розвинути усвідомлення природи різних ІТ-ризиків для бізнесу, кількісно оцінити вплив на свій бізнес внаслідок втрати інформації або доступу до програм, зрозуміти діапазон інструментів, доступних для управління ІТ-ризиками. , узгодити вартість управління ІТ-ризиками з цінністю бізнесу та створити інституційну спроможність діяти та контролювати ІТ-ризики з таким же рівнем контролю, як якщо б це був фінансовий ризик.

Відмінність від стандартних рекомендацій з управління ризиками та оцінки ризиків IS/IT полягає в тому, що, перш за все, внутрішні аудитори повинні провести інвентаризацію ІТ-активів організації та визнати, які активи є критичними для ефективності бізнес-процесів. В результаті ризики, пов’язані з ІТ-процесами та діяльністю, керуються та оцінюються стосовно їхньої здатності впливати на досягнення бізнес-цілей [12].

Оцінка ІТ-ризиків та прийняття ІТ-рішень вимагають, щоб ІТ-ризики були окреслені чіткими діловими термінами. Для ефективного управління ризиками потрібен підхід для взаєморозуміння між ІТ та бізнесом щодо типів ризиків, які необхідно вирішувати, і надати обґрунтування, яким ризиком потрібно керувати і чому. Функція оцінки ризиків IS/IT залежатиме від стану зрілості, який існує на рівні підприємства в рамках процесів ERM, та рівня інтеграції між корпоративною стратегією управління ризиками та управлінням ризиками IS/IT.

Інформація створює цінність для бізнесу, тому необхідно захистити цей актив від запобігання матеріалізації ризиків. Вплив ризику IC/IT на бізнес полягає в наслідках, з якими стикається організація, коли інформаційні критерії не виконуються.

Бізнес-вимоги до інформації, які виражають умову, за якою інформація, яка надається через ІТ, повинна бути збережена, щоб бути корисною для підприємства.

Методи аналізу ризиків

Аналіз ризику включає аналіз ймовірності та останніх ідентифікованих небезпечних подій з урахуванням особливостей та ефективності застосовуваних способів управління. Дані про ймовірності подій та їх наслідки використовують для визначення рівня ризику.

Також аналіз ризику включає аналіз джерел небезпечних подій, їх позитивних та негативних останніх імовірностей появлення цих подій. При цьому повинні бути ідентифіковані фактори, впливаючи на ймовірність подій та його наслідки.. Також повинні бути включені результати застосування та ефективність існуючих методів

управління. Різні методи аналізу описані нижче. У складних ситуаціях може бути використано кілька методів.

Аналіз ризику зазвичай включає діапазон оцінки можливих останніх подій, ситуацій чи обставин та відповідних ймовірностей для визначення рівня ризику. Однак у деяких випадках, наприклад, коли наслідки незначущі чи ймовірні події надзвичайно низькі, для прийняття рішень може бути достатньо дослідження лише одного параметра. У деяких випадках останнє може бути результатом реалізації кількох подій або неідентифікованих подій. У цьому випадку оцінку ризику необхідно зосередитися на аналізі значимості та вразливості компонентів досліджуваної системи. При цьому слід визначити методи обробки ризику, відповідність рівня захисту та стратегії відновлення.

Методи, використовувані при аналізі ризику, можуть бути якісними, кількісними або змішаними. Ступінь глибини та деталізації аналізу залежить від конкретної ситуації, доступності достовірних даних і потреб організацій, пов'язаних з прийняттям рішень. Деякі методи та ступінь деталізації аналізу можуть бути встановлені відповідно до правових та обов’язкових вимог.

При **якісній оцінці ризику** визначають наслідки, ймовірність і рівень ризику по шкалі «високий», «середній» і «низький»; оцінка останніх і ймовірності може бути об'єднана; порівняльну оцінку рівня ризику в цьому випадку проводять відповідно до якісних критеріїв.

У змішаних методах використовують шкалу оцінок останніх, ймовірностей та їх поєднання для визначення рівня ризику відповідно до відповідної формули. Шкали можуть бути лінійними, логарифмічними або можуть бути побудовані за іншими принципами. Використані формули відповідно можуть бути різними.

При **кількісному аналізі** оцінюють практичну значимість і вартість останніх, їх ймовірність і отримують значення рівня ризику в певних одиницях, встановлених при розробці області застосування менеджменту ризику. Повний кількісний аналіз не завжди може бути можливим або бажаним із-за недостатньої інформації про аналізованій системі, видах діяльності організацій, недостатності даних, впливу на людський фактор тощо. п. або тому, що такий аналіз не потрібен, або трудозатрати на якісний аналіз занадто великих. У такому випадку ранжування ризиків висококваліфікованими спеціалістами може бути більш ефективно.

Якщо применений якісний аналіз ризику, чіткі пояснення всіх використовуваних термінів і принципів, що відповідають основі критеріїв, повинні бути зареєстровані у вигляді записів.

У разі застосування кількісного аналізу необхідно пам’ятати, що рівень ризику є лише оцінкою. Необхідно забезпечити узгодженість невизначеностей отриманих оцінок з рівнем точностіпрецизійності використовуваних методів і даних.

Рівні ризику повинні бути виражені у відповідних термінах для конкретного виду ризику в найбільш зручній формі. У деяких випадках значення ризику може бути виражено у вигляді розподілу ймовірності діапазону останнього[15]

1.4 Опис функції ITSCM

Важливе місце займає функція управління безперервністю IT-сервісів,(англ. IT Service Continuity Management ,ITSCM).

ITSCM відповідає життєвому циклу безперервності бізнесу та допомагає підготуватися до найгіршого сценарію. ITSCM не тільки те, як відновити бізнес після катастрофи, але й зупинити катастрофу, якщо це взагалі можливо. ITSCM досліджує, розробляє та реалізує варіанти відновлення, коли перерва в обслуговуванні досягає попередньо визначеної точки. Він має бути частиною загального плану забезпечення безперервності бізнесу і не розглядатися окремо.

ITSCM розглядає ризики, які можуть спричинити раптовий і серйозний вплив, елементи, які можуть негайно загрожувати безперервності бізнесу. Зазвичай вони включають такі речі, як:

— втрата, пошкодження або відмова у доступі до ключової інфраструктури;

— збої служб прикладних програм;

— непрацездатність (включаючи ймовірність того, що ваш постачальник зазнає катастрофи) критичних постачальників, дистриб'юторів або інші треті сторони;

— пошкодження ключової інформації;

— саботаж, вимагання або комерційне шпигунство;

— навмисна інфільтрація;

— атаки на критично важливі інформаційні системи[13].

На дуже високому рівні ITSCM включає в себе такі підпроцеси:

— ***Ініціація*** – на етапі ініціації політики, які визначають наміри та цілі керівництва, повинні бути задокументовані та донесені до всієї організації.

— ***Вимоги та стратегії*** – важливо визначити та задокументувати бізнес-вимоги щодо безперервності IT-послуг, щоб гарантувати, що бізнес зможе пережити катастрофу. Аналіз впливу на бізнес (BIA) та оцінка ризиків проводяться для розробки стратегії безперервності IT-послуг.

— ***Впровадження*** – планування впровадження визначає та координує різні бізнес- та технічні плани та результати в єдиний генеральний план BCM.

— ***Поточна експлуатація*** – Поточна експлуатація складається з заходів, пов’язаних із підтримкою, тестуванням та зміною планів безперервності, щоб гарантувати, що вони придатні для цілі з часом.

— ***Виклик.*** Керівництво та критерії для прийняття рішення використовувати Плани безперервності бізнесу та IT повинні бути ретельно задокументовані заздалегідь[14].

Incident Management (Управління інцидентами)

Управління інцидентами процес, що відповідає за управління життєвим циклом усіх інцидентів. Управління інцидентами забезпечує мінімізацію впливу

на бізнес і відновлення нормального функціонування послуг найшвидшим способом:

— Вхід до ITSCM

— Управління інцидентами покладається на персонал служби підтримки та можливості прийняття рішень/класифікації, визначені Управлінням інцидентами.

— Менеджер з інцидентів повинен вирішити, чи слід використовувати непередбачені обставини/здатності ITSCM і коли слід спрацювати (на основі рішень вищого керівництва)

— ITSCM відповідає за те, щоб усі знання, інформація та документація були доступні менеджеру з питань інцидентів для прийняття обґрунтованих рішень щодо виклику відновлення.

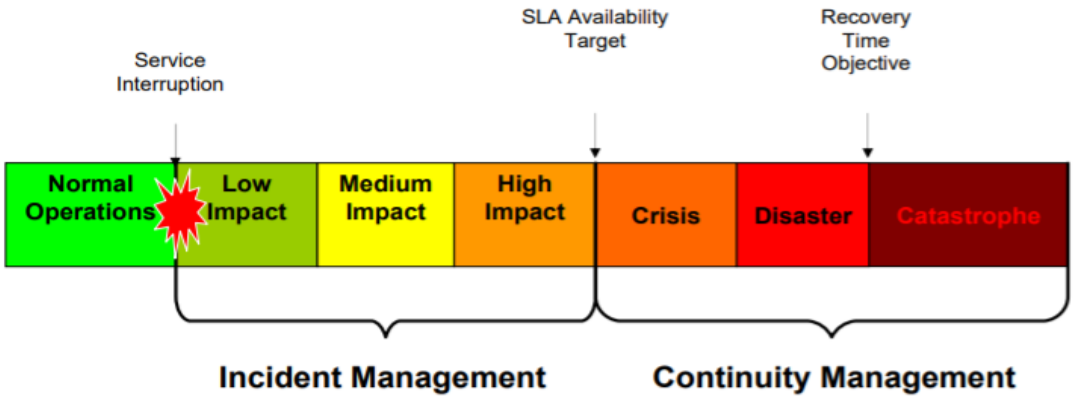


Рисунок 1.17 – Взаємозв’язок Incident Management BCM

Change management (управління змінами)

Всі ми так чи інакше маємо справу зі змінами того чи іншого роду, і ми маємо свої власні уявлення про управління ними. І тут важливо, щоб усі однаково уявляли контекст ситуації. Є спільні дії (збір запитів, оцінка їх впливу, пріоритизація, позиціонування), що входять у процес управління змінами, поведінкою, бізнес-процесами та IT-системами. Хоча багато речей будуть схожі, для повноти розуміння контексту необхідно розуміти ключові відмітні ознаки.

1. ITSCM включає в себе багато технічних компонентів, ймовірно, в різних місцях, які необхідно синхронізувати.
2. Якщо компанія покладається на віддалений центр обробки даних для забезпечення високої або постійної доступності додатків, обидва центри повинні підтримувати однакові рівні коду та типи інфраструктури.
3. Процес керування змінами, який не надає сповіщення про те, що невідкладна зміна впливає на компоненти «відновлення» або «відмови», означитиме збій для ITSCM.

Поліпшення управління ризиком

Будь-яка зміна створює ризик руйнування чогось в оточенні. Управління змінами дозволяє зрозуміти ці ризики та прийняти поінформоване рішення про необхідні зміни.

Включення координації та відстеження змін

ІТ-оточення бувають складними, з великою кількістю змін. Управління змінами допомагає координувати окремі зміни, щоб уникнути конфліктів та мінімізації збоїв.

Комунікація між технічними відділами та користувачами

Деякі зміни не торкаються функцій для користувачів, але таких меншість. Управління змінами гарантує, що користувачі в курсі змін та здатні отримати з них користь.

.

2 ІНФОРМАЦІЙНА ПЛАТФОРМА OMNITRACKER ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРВНОСТІ БІЗНЕС ТА ІТ – ПРОЦЕСІВ

З розвитком ІТ сфери з кожним роком Українські компанії ростуть у ІТ-напрямі і з цим стрімким рухом грані між поняття бізнес- процес та ІТ процес майже стерлися, адже в багатьох компаніях для побудови чіткої структури використовують чітку архітектуру та ереархію, забезпечену великою кількістю ІТ-процесів.

Отже, почну розділ с понять «бізнес-процес» та «ІТ – процес», для чіткого розуміння як вони пов’язані з інформаційною платформою OMNITRACKER .

1. Бізнес-процес — це діяльність або набір заходів, які можуть досягти певної організаційної мети. Бізнес-процеси повинні мати цілеспрямовані цілі, бути максимально конкретними та мати послідовні результати.

Категорії бізнес-процесів

Залежно від організації, галузі та характеру роботи бізнес-процеси часто поділяють на різні категорії. Ці категорії включають:

— Операційні процеси - або первинні процеси. Вони мають справу з основним бізнесом і ланцюгом створення вартості. Ці процеси приносять цінність клієнту, допомагаючи виробляти продукт або послугу. Операційні процеси являють собою важливу бізнес-діяльність, яка досягає бізнес-цілей, наприклад, отримання доходу. Деякі приклади цього включають прийом замовлень клієнтів та управління банківськими рахунками.

— Допоміжні процеси -- або вторинні процеси: допоміжні процеси підтримують основні процеси та функції в організації. Приклади процесів підтримки або управління включають бухгалтерський облік, управління персоналом та безпеку на робочому місці. Однією з ключових відмінностей між операційними та допоміжними процесами є те, що процеси підтримки не надають цінності клієнтам безпосередньо.

— Процеси управління: процеси управління вимірюють, контролюють і контролюють діяльність, пов'язану з бізнес-процедурами та системами. Приклади процесів управління включають внутрішні комунікації, управління, стратегічне планування, бюджетування та управління інфраструктурою або потенціалом. Як і допоміжні процеси, процеси управління не надають цінності безпосередньо клієнтам

Управління бізнес-процесами

Управління бізнес-процесами — це стратегія, яку організації використовують для нагляду за своїми бізнес-процесами, щоб забезпечити їх безперервну роботу. Вона може допомогти покращити процеси, допомагаючи огляду керівництва, а також може контролювати організаційні процеси, щоб гарантувати, що вони ефективні та результативні. Організації використовують програмне забезпечення BPM для моніторингу та контролю автоматизованих і неавтоматизованих бізнес-процесів, а також для покращення процесів управління.

Діяльність з управління бізнес-процесами включає такі етапи, як моделювання бізнес-процесів, виконання, моніторинг та оптимізація.

Моніторинг бізнес-процесів

Моніторинг бізнес-процесів – це метод використання аналітики для моніторингу ефективності процесу. Моніторинг процесу використовується для виявлення таких елементів, як час технологічного циклу, помилки та вартість.

Організації використовують функціональний моніторинг для оцінки функціональної ефективності процесу. Технічний моніторинг допомагає вимірювати технічну ефективність програми шляхом нагляду та реєстрації таких аспектів, як час відповіді та простої.

2. IT процес

IT-процеси – це не що інше, як цінний інструмент, сукупність знань і досвіду, накопиченого протягом багатьох років різними компаніями та спеціалістами. Вони усвідомили правильні та неправильні повсякденні дії та вирішили систематизувати передовий досвід, щоб динамічно протистояти типовим ризикам роботи, мінімізуючи шанси на помилки під час виконання найрізноманітніших робіт.

IT-процеси стандартизують всю діяльність компанії, пов'язану з інформаційними технологіями, доводячи їх до високого рівня якості та досконалості. Завдяки бізнес-процесам IT послуги можуть забезпечити доставку, незалежно від того, хто їх виконує.

Відсутність чітко визначених IT бізнес-процесів збільшує шанси на помилки в процесах компанії. В результаті при майбутній заміні співробітників вся структура буде скомпрометована. Навпаки, наявність IT-управління з добре змодельованими процесами дозволяє будь-якому працівнику району задовільно займатися проектами, навіть у критичних та надзвичайних ситуаціях. Це працює як план безперервності бізнесу.

IT-процеси є джерелом проблем номер один — більше, ніж технології. IT-процеси мають найбільший вплив на здатність IT робити внесок у бізнес. Щоб керувати ефективною IT-організацією, потрібно серйозно подумати про свої IT-процеси та спосіб управління новими вимогами, змінами, продуктивністю, потужністю, проблемами, конфігураціями, активами, версіями програмного забезпечення, катастрофами та безпекою. Завдяки чітко визначеним процесам ви можете вирішити багато пріоритетних ініціатив з управління IT. Наприклад, можна запровадити ефективні засоби контролю, переконатися, що IT тісно співпрацює з бізнес-підрозділами для визначення вимог до проекту, узгодити життєвий цикл розвитку системи та інфраструктури та формалізувати систему для постійного вдосконалення IT-послуг.

2.1 Інформаційна платформа Omnitracker

Omnitraker – программне забезпечення, що було створено німецькою компанією Omninet. Його було розроблено як платфоому для бізнес-процесів.

Це модульне ПЗ, що використовується по всьому світу найбільшими комапніями та підприємствами для управління безперервністю, менеджменту самих процесів та та їх оцінки.

Основна область застосування програми - управління безперервністю процесів,, підтримка процесів, відповідних рекомендацій ITIL, а також управління проектами, вимогами, помилками, клієнтськими запитами, починаючи з першого завдання та до їх виконання. Omnitraker сертифікований Німецькою федеральною асоціацією IT-підприємств, а також має сертифікат PinkVerify.

Відпочатку Omnitraker розроблявся для оптимізації процесів менеджменту якістю та розробки ПО , пізніше його доробили і наразі він використовується як одна з критичних систем у сервісних та технічних процесах.

Інформаційна платформа Omnitraker має готові стандартні рішення «з коробки» та має функію, що відповідає за доробку платформи «під клієнта» за потрібними клієнту рішеннями.

Багатокористувальна платформа складається з базової системи, модульних базових компонентів і клієнтів. Необмежені розширення можуть налаштовуватися під копистуівача та бути керовані через відкриті інтерфейси. Платформа має вбудований графічний редактор потоків робіт, гнучку систему інформування та ескалацій, базу знать, базу активів чи інше, що буде потрібно контретному користувачу. Модель даних, а також концепція розмежування прав і ролей вільно конфігуруються.

Омнітрекер має понад 12 стандартних додатків «із коробки», які базуються на платформі бізнес-процесів (ядре програми). Найбільш поширеними з них є: IT Service Management Center V3 (ITSM) – управління ITSM-процесами згідно з рекомендаціями ITIL, Project Management Center – планування та управління проектами, Stock & Order Management – підтримка процесів замовлень і доставки, Contract Management Center – управління договорами, а також Центр системної інженерії – управління процесом розробки ПО.

Модуль IT Service Management Center -– ефективне, масштабне та високовиробниче рішення для управління IT-процесами (ITSM). Додаток відповідає актуальним найкращим практикам ITIL і інтегрується з іншими допоміжними процесами. Це дозволяє вам управляти складними IT-середовищами від А до Я. За допомогою IT Service Management Center можливо систематичатизувати по категоріям вхідні звернення(запити на обслуговування, інцидетни), автоматично позначати їх відповідальним співробітникам, налаштовувати базу систем/сервісів та звязки міжними, управляти Change management процеів. IT Service Management Center допоможе знизити негативний вплив інцидентів на IT-послуги, а також стандартизує систему запитів на обслуговування всієї організації.

GRC Center - Governance, Risk and Compliance Center підтримує вас у кожному управлінському рішенні та допомагає вам вести бізнес прибутково та відповідно до закону. Модуль GRC Center забезпечує наступне:

— Система управління: В області управління ви визначаєте якісні та кількісні цілі, формуєте відносини із зацікавленими сторонами та керуєте

найважливішими контрактами. У більш широкому сенсі йдеться про юридично регульовану відповідальність організації та взяті нею на себе зобов'язання. Дві інші області, управління ризиками та дотримання вимог, допомагають вам досягти поставлених цілей та дотриматися всіх (правових) норм.

— Управління ризиками: Управління ризиками з використанням програмного забезпечення включає раннє виявлення, систематичний збір, аналіз та оцінку ризиків. З іншого боку, забезпечується управління стратегіями ризику (уникнення, зменшення, передача, прийняття), і навіть ітераційна обробка ризиків. Тут необхідно враховувати всі види бізнес-ризиків, наприклад, стратегічні ризики, ринкові ризики, ризики дефолту, ризики невідповідності законодавству та операційні ризики. У цьому контексті ризики визначаються як події, що впливають на досягнення цілей компанії. При аналізі ризику важливими є такі параметри, як причина ризику, вплив (розмір шкоди) та ймовірність. Основна мета управління ризиками полягає в мінімізації суми та серйозності всіх потенційних ризиків, щоб досягати бізнес-цілей у більш передбачуваному режимі.

— Дотримання вимог (комплаєнс): Комплаєнс означає дотримання внутрішніх та зовнішніх вимог. Цими вимогами можуть бути (міжнародні) закони, правила та стандарти або внутрішні норми поведінки у компанії. Це свідомо контрольоване дотримання правил спрямоване на уникнення юридичних санкцій або шкоди іміджу компанії, а також підвищення якості та передбачуваності ділової активності. Наприклад, контрольні переліки, системи управління та галузеві стандарти, а також загальнозастосовні правові вимоги є елементами контролю. Додаток GRC Center допомагає безперешкодно виконувати та документувати виконання всіх нормативних вимог, оскільки тисячі індивідуальних вимог можуть бути дотримані паралельно.

2.2 Архітектура Omnitracker

Центральна частина системи, Omnitracker Enterprise Server, є виключно потужним і гнучкий механізм створення та управління інформаційними об'єктами.

1. Інформаційний об'єкт — будь-яка сутність, визначена у системі. Наприклад, заявка, інцидент, проблема, послуга, вбрання на роботу, співробітник, договір, проект та ін.Omnitracker дозволяє створювати будь-яку кількість інформаційних об'єктів.
2. Атрибут – властивість інформаційного об'єкта. Наприклад, атрибутами інциденту є номер, статус, час виникнення, для співробітника – прізвище, ім'я, адреса електронної пошти, табельний номер та ін. Omnitracker дозволяє для будь-якого інформаційного об'єкта створювати будь-яку кількість атрибутів будь-якого типу (числових, текстових, посилальних та ін.).
3. Платформа дозволяє визначати різні зв'язки між інформаційними об'єктами (всіх типів - 1:1, 1:N, N:M) та забезпечує автоматичний контроль цілісності посилання. Наприклад, із наряду на роботу зробити посилання на

послугу, з батьківського інциденту зробити посилання на дочірні інциденти та ін.

4. Логіка або правила виконання того чи іншого процесу (поведінка інформаційних об'єктів) може бути реалізована двома способами:

— візуальні засоби конфігурування;
— програмування.

Завдяки гнучкості візуальних засобів конфігурування більшість функцій може бути реалізована без програмування, що значно скорочує терміни впровадження та складність підтримки та розвитку.

На базі сервера Omnitracker можуть бути реалізовані інші бізнес-процеси, якщо з будь-яких причин вони не можуть бути реалізовані в інших системах (висока вартість, недостатня функціональність або відсутність такої).

Omnitracker має наступні варіанти роботи з будь-якими прикладними пакетами:

— windows-клієнт;
— веб-клієнт (Internet Explorer, Mozilla Firefox);
— Мобільний клієнт (PDA, смартфони, Mobile Tablet-PC).
— Підтримується авторизація через MS Active Directory та LDAP.

Omnitracker має виключно гнучкі можливості обробки вхідної та вихідної електронної пошти. Обробляються всі можливі формати електронних листів:

— Plain text;
— HTML;
— RTF;
— із вкладеннями;
— із впровадженими об'єктами (Embedded Objects);
— будь-яку кількість вхідних та вихідних облікових записів;
— будь-яку кількість правил обробки вхідних та вихідних листів, у тому числі з використанням скриптів;
— створення виходячи з вхідних листів будь-яких інформаційних об'єктів.

Windows-клієнт інтегрований із телефонними станціями, що підтримують протокол TAPI 2.0. Телефонні станції, що не підтримують протокол TAPI 2.0, можуть бути інтегровані за допомогою спеціалізованого інтерфейсу Omnitracker (COM-based Telephony Integration Interface).

Інтеграція Omnitracker з телефонною станцією дозволить автоматизувати реєстрацію та аналіз вхідних дзвінків, наприклад, автоматичне отримання контактних даних по телефону, список відкритих звернень, запис розмов, вихідний дзвінок та ін.

Omnitracker має вбудовані механізми інтеграції даних та подій, наприклад інтеграція з кадровими та фінансовими системами, системами інвентаризації та моніторингу тощо.

2.2.1 Проектування процесів (Workflow)

Omnitracker має потужний механізм проектування процесів (Workflow):

— визначаються кроки процесу з правами видимості для користувачів на кожному кроці;

— визначаються правила переходу - з перевірками та умовами;

— визначаються автоматичні дії для різних умов – зміна статусу, часові обмеження, зміна атрибутів.

— Для кожного інформаційного об'єкта може бути визначено необмежену кількість процесів та кроків у кожному процесі.

2.2.2 Створення моделі даних (об’єкти, атрибути, зв’язки)

Поряд у проектуванням процесів Omnitracker має потужні механізми створення моделі даних (інформаційних об'єктів та зв'язків між ними):

— підтримуються всі існуючі елементарні типи даних (числові, текстові, довідкові та ін.);

— можна створити будь-яку кількість атрибутів будь-яких типів з будь-якими посиланнями (наприклад, створювати ієрархію інцидентів або створювати посилання на послугу з наряду на роботу);

— підтримуються комплексні типи даних:

— Attachments, Вкладення — поле, в якому зберігаються файли або посилання на файли, можна створювати будь-яку кількість атрибутів-вкладень, налаштовуючи правила зберігання та типи вкладень, що зберігаються;

— Auto Number, Автонумератор - з можливістю вказівки префіксів та суфіксів;

— Memo - Time Stamped, Коментарі з тимчасовою міткою - при додаванні інформації автоматично встановлюється її автор і час додавання з можливістю редагування;

— Reference to object – посилання на БУДЬ-ЯКИЙ об'єкт (зв'язок 1:1);

— Reference to list of objects — посилання на список будь-яких об’єктів об'єктів (зв'язок (1:N);

— Schedule, Графік – завдання графіка виконання завдань – ідеальний засіб для формування графіків планових/регламентних робіт та ін.;

— Workflow, Послідовність дій - дозволяє у графічному вигляді створювати бізнес-процес;

— графічний зручний механізм створення зв'язків усіх типів:

— 1:1 (один до одного);

— 1:N (один до багатьох);

— N:M (багато хто до багатьох);

— забезпечується автоматичний контроль цілісності посилань;

— налаштовуються правила спільного доступу до інформаційних об'єктів та атрибутів (заборона, лише читання, попередження тощо.

2.2.3 Формування логіки

Візуальні засоби конфігурування логіки системи мають виключно гнучкі можливості, що дозволяє обійтися без програмування:

— скорочують час внесення змін та подальшого тестування;

— скорочують кількість помилок;

— зменшують складність підтримки.

Для будь-якого інформаційного об'єкта можна визначити будь-яку кількість правил та умов:

— при визначенні умов можливі:

— вибір будь-якого поля, включаючи будь-яке поле пов'язаного об'єкта;

— порівняння з будь-яким полем, включаючи будь-яке поле пов'язаного об'єкта;

— при модифікації поля - використання як нового, так і СТАРОГО значення поля;

— будь-яке поєднання умов І/АБО/НЕ;

— при визначенні правил можливі:

— визначення різних видів дій:

— зміни атрибутів;

— надсилання електронних листів;

— виклик зовнішніх програм;

— взаємодія із мобільними клієнтами;

— виконання скриптів;

— оповіщення користувачів за допомогою механізмів самої системи;

— зміна значення будь-якого поля, зокрема будь-якого поля пов'язаного об'єкта, з використанням значень інших полів, зокрема полів пов'язаних об'єктів;

— будь-яке поєднання умов І/АБО/НІ.

Крім того, Omnitracker має практично необмежені можливості розширення функціональності за рахунок можливості написання серверних та клієнтських скриптів на VBScript або COM-компонент.

2.2.4 Правила відповіді

Omnitracker дозволяє гнучко визначати різні правила оповіщення груп користувачів або окремих користувачів про настання тих чи інших подій (створення заявок, призначення роботи, зміна даних тощо):

— оповіщення можуть надсилатися електронною поштою;

— використовуючи додаткові компоненти можна формувати оповіщення іншими каналами, наприклад, факс, SMS;

— Omnitracker має вбудовану email-подібну систему оповіщень.

— Усі оповіщення настроюються у візуальному редакторі.

2.2.5 Правила ескалації

Omnitracker дозволяє гнучко налаштовувати дії, що автоматично виконуються, залежать від часу (наприклад, підвищення пріоритету інциденту, не усуненого в строк):

— зміна атрибутів об'єкта;
— оповіщення (електронною поштою та ін.);
— виклик зовнішньої програми;
— виконання VB-скрипту.

Права доступу

Omnitracker дозволяє гнучко налаштовувати права та привілеї користувачів системи:

— права можуть лунати лише на рівні кожного конкретного атрибута;
— та кожної операції (перегляд, зміна, видалення);
— на групи чи конкретних користувачів;
— з урахуванням контексту (наприклад, право на зміну, якщо поточний користувач є відповідальним за виконання цієї заявки);
— для спеціальних типів полів вбудовані механізми розмежування прав на виконання специфічних операцій (наприклад, як на малюнку, для поля "Коментарі" визначено спеціальні дії: додати коментар, видалити чужий коментар, змінити свій останній коментар тощо);
— редактор правил дозволяє задати будь-яке поєднання умов І/АБО з будь-яким атрибутом поточного об'єкта або пов'язаних з ним об'єктів;
— у системі вбудований механізм "заступників" - права можуть задаватися на користувача та/або його заступників (proxy) у тому числі відповідно до потрібного календаря;
— якщо інформаційні об'єкти мають ієрархічні залежності, права успадковуються.

Крім того, платформа забезпечує підвищену безпеку при обміні файлами-вкладеннями: доступ до сховища вкладень має тільки сервер ОТ програм (клієнти - не мають). Надається можливість зберігати як вкладення як самі файли, а й посилання ними.

2.2.6 *Дизайнер екранних форм*

Інтегрований у системі візуальний дизайнер дозволяє створювати екранні форми інформаційних об'єктів без жодних обмежень:

— будь-які шрифти, кольори, розміри та розташування;

— будь-які типи інтерфейсних об'єктів, пов'язаних та незв'язаних з атрибутами;

— будь-яку кількість екранних форм кожного об'єкта;

— динамічний вибір екранної форми, що настроюється;

— права доступу, що динамічно настроюються.

Функціональність екранних форм (за потреби) може бути значно розширена клієнтськими скриптами (OnOpen, OnChange, OnClick та ін.)

2.2.7 Дизайнер уявлень

Подання (view) визначає зовнішній вигляд (колір, розмір та тип шрифту), набір атрибутів, їх порядок, сортування та фільтрацію інформації:

— шрифти, кольори та розміри, що настроюються - по контексту з використанням будь-яких атрибутів поточного об'єкта і з ним пов'язаних, а також із застосуванням логічних операцій І/АБО/НІ;

— будь-яку кількість екранних форм кожного об'єкта;

— права доступу, що настроюються: створення, зміни, використання;

— визначення власне зовнішнього вигляду та правил фільтрації задаються окремо, що значно скорочує можливу кількість уявлень, і, отже, час їх створення і підтримку;

— подання може інтерактивно "запитувати" користувача значення параметрів фільтрації.

Доступний лише адміністратору системи механізм базових фільтрів (Base Filter) дозволяє не просто фільтрувати дані, а й робити їх повністю ізольованими для різних користувачів. Так, наприклад, може бути організована діяльність різних груп/підрозділів/організацій, що працюють в одній системі, але повністю ізольовані одна від одної.

Omnitracker , крім стандартних видів, має додаткові види уявлень, що значно підвищують зручність та ефективність користування системою.

Уявлення типу TreeView показує в собі об'єкти, пов'язані з поточним. Наприклад, малюнку - по інциденту показується ініціатор інциденту пов'язані з нею конфігураційні елементи.

Подання типу TimeLine дозволяє на часовій шкалі відображати положення інформаційних об'єктів у часі (наприклад, нарядів на роботу, інцидентів, змін та ін. – у прив'язці до виконавців та робочих груп). Відсоток виконання можна візуалізувати.

Повнотекстовий пошук інформації

Omnitracker має налаштований механізм індексації та подальшого пошуку інформації в будь-яких об'єктах системи - за аналогією з відомими пошуковими Інтернет-системами:

— індексуватися можуть усі або вибрані атрибути інформаційних об'єктів;

— індексуватися може вміст вкладень (Word, Excel, PDF-файли та ін.);
— пошуковий механізм підтримує логічні операції І/АБО/НЕ;
— пошуковий механізм підтримує нечіткий (fuzzy) пошук, що дозволяє шукати слова із синтаксичними помилками;
до індексування можна включити записи з історії змін.

2.2.8 Мультисистемний ландшафт

Платформа підтримує трисистемний ландшафт:
— система розробки;
— тестова система;
— продуктивна система.

Платформа має вбудований механізм перенесення бізнес-логіки (правил, скриптів, прав доступу та ін.) між різними системами. При цьому даний механізм може бути використаний не тільки для перенесення змін "розробкою", "тестом" та "продуктивом", але також може використовуватися при тиражуванні налаштувань між різними продуктивними системами територіально-розподіленої децентралізованої моделі.

Цей механізм дозволяє:
— скоротити кількість помилок під час впровадження змін;
— підвищує якість тестування;
— прискорює та спрощує процедури тиражування зміни;
— скорочує кількість адміністраторів системи, що особливо важливо у великих територіально-розподілених організаціях;
— підвищує рівень контролю за змінами та ін.

2.2.9 Імпорт та експорт данних

Платформа надає широкі можливості для імпорту та експорту будь-якого об'єкта (підрозділи, співробітники, інциденти, послуги та ін.):

1. у базовому варіанті пропонується робота з такими джерелами даних:
— ODBC;
— LDAP;
— XML;
— MS Excel;
— Outlook;
— MDB;
— Inventory scanner - завантаження даних із систем інвентаризації;
— Omnitracker Folder - завантаження даних з інших систем та папок

Omnitracker (дана можливість дозволяє синхронізувати дані у територіально-розподіленій системі, побудованій у федеративній моделі);

2. передбачені автоматичні процедури нормалізації даних, що настроюються;
3. передбачені різні режими, що настроюються:

— лише додавання даних;
— додавання та зміна даних;
— додавання, зміна та видалення даних;
— додавання лише нових даних;
— зміна лише існуючих даних;
— лише оновлення зв'язків;

4. права доступу на імпорт та експорт даних налаштовуються (із застосуванням умов І/АБО/НЕ);
5. налаштування імпорту та експорту можуть іменуватися, зберігатися, а також самі по собі імпортуватися та експортуватися між системами;
6. імпорт і експорт можна запускати в автоматичному режимі, що періодично повторюється.

2.2.10 Програмний інтерфейс (OLE Automation Interface)

Програмний інтерфейс Omnitracker надає на основі технології ActiveX доступ до всіх інформаційних об'єктів системи:

— будь-які дії, які виконуються користувачем вручну, можуть бути автоматизовані;

— програмний інтерфейс складається з набору динамічних бібліотек DLL, які можуть бути використані через мережу і можуть розташовуватися і викликатися окремо від сервера Omnitracker;

— програмний інтерфейс повністю описаний та забезпечений прикладами використання.

2.2.11 WEB-сервіси

На додаток до програмного інтерфейсу Omnitracker забезпечений механізмом web-сервісів, що дозволяє інтегрувати його не тільки з windows-додатками, але й додатками, побудованими на інших платформах:

— з використанням web-сервісів можна створювати, змінювати та видаляти інформаційні об'єкти Omnitracker, отримувати про них інформацію та викликати системні скрипти;

— web-сервіси повністю документовані та забезпечені прикладами використання.

2.2.12 Інтеграція з телефонними станціями

Omnitracker дозволяє інтегруватися з телефонними станціями:

— windows-клієнт інтегрований з телефонними станціями, що підтримують протокол TAPI 2.0;

— телефонні станції, що не підтримують протокол TAPI 2.0, можуть бути інтегровані за допомогою спеціалізованого інтерфейсу OMNITRACKER(COM-based Telephony Integration Interface);

— підтримується інтеграція вхідних та вихідних викликів;

— дана можливість дозволяє прискорити та спростити реєстрацію та аналіз вхідних дзвінків, наприклад, автоматичне отримання контактних даних по телефону, список відкритих звернень;

— організація вихідного обдзвону та ін.

Omnitracker підтримує інтеграцію з Контактними Центрами, побудованими на базі Genesys, що дозволяє отримати такі глобальні переваги:

— повністю абстрагуватися від особливостей конкретної телефонної станції; Genesys має інтерфейси практично до всіх існуючих станцій;

— логіка диспетчеризації дзвінків, контролю доступності операторів, автоматичні голосові оповіщення та ін. – все це залишається у зоні відповідальності Genesys;

— запис розмов та їх зберігання у відповідних об'єктах (заявках, інцидентах та ін.)

2.2.13 Обробка електронної пошти

Omnitraker має виключно гнучкі можливості обробки вхідної та вихідної електронної пошти:

1. протоколи, що підтримуються:
— POP3;
— IMAP4;
— MAPI;
— SMTP;
2. обробляються всі можливі формати електронних листів:
— Plain text;
— HTML;
— RTF;
— із вкладеннями;
— із впровадженими об'єктами (Embedded Objects);
3. електронні листи у своєму оригінальному форматі зберігаються у системі;

4. на підставі вхідних листів можна створювати будь-які інформаційні об'єкти (інциденти, запити на зміни тощо);
5. зв'язок між листом та об'єктом встановлюється автоматично;
6. налаштовуються посилання на інші об'єкти, наприклад, за адресою електронної пошти встановлюється зв'язок між інцидентом та працівником-заявником;
7. вкладення автоматично прикладаються до об'єкта Omnitraker;
8. повідомлення про доставку можуть оброблятись окремо та зв'язуватися з вихідними повідомленнями, наприклад, користувач може інформуватися про те, що в заданий час не надійшло повідомлення про доставку;
9. користувачі можуть інформуватися про те, що повідомлення не було доставлено;
10. можна працювати з будь-якою кількістю вхідних та вихідних облікових записів;
11. можна визначати будь-яку кількість правил обробки вхідних та вихідних листів, у тому числі з використанням скриптів;
12. налаштовуються правила автоматичного аналізу форматованих листів (з використанням службових символів та слів);
13. на поштові повідомлення поширюється дія індексування та повнотекстового пошуку;
14. автоматично створювані електронні листи можуть бути попередньо спрямовані на погодження потрібному співробітнику або співробітникам (повідомлення, спрямоване на погодження, може бути змінено, надіслано або скасовано на вимогу відповідного узгоджуючого);
15. email-шлюз системи дозволяє обробляти SNMP-traps.

2.2.14 Підтримка WEB-клієнтів

Доступ web-клієнтів до системи забезпечується через спеціальний шлюз - Web Gateway:

— забезпечує доступ до системи через стандартні провідники (Internet Explorer, Mozilla Firefox);

— стильове оформлення web-сторінок може бути змінено під корпоративні стандарти замовника, використовуючи CSS (Cascading Style Sheets);

— доступний механізм повнотекстового пошуку;

— завантаження та вивантаження даних та вкладень;

— можна створювати будь-яку кількість web-форм для кожного інформаційного об'єкта (наприклад, окремо для виконавців, окремо для замовників, окремо для зовнішніх контрагентів);

— права доступу можуть бути гнучко налаштовані для різних груп та окремих користувачів - наприклад, можливість подання заявки до Служби підтримки через web та перегляд тільки своїх заявок, або участь у процедурах

узгодження певних змін, або перегляд потрібного розділу бази знань);

— забезпечується інтеграція із MS Active Directory.

2.2.15 Система звітності

Вбудований генератор звітності забезпечує формування кількох видів звітів:

— друковані форми (наприклад, завдання на роботу, замовлення наряд тощо) - може бути згенеровано у вигляді форматованого word-документа або звіту Crystal Report;

— статистичні звіти - табличний чи графічний вигляд різних аналітичних параметрів;

— панель приладів (Dash Board) - семафори, що періодично оновлюються, та ін.

— Генератор звітів дозволяє зберігати дані у форматі звітів Crystal Reports, MS Word, MS Excel xml, вивантажувати до зовнішніх баз даних[16].

3. ДОСЛІЖДЕННЯ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ ПЛАТФОРМИ OMNITRACKER В КОМПАНІЇ «ПРОЦЕСІНГ»

В цьому розділі буде досліджено інформаційну платформу, що функціонує в компанії «Процесінг».

3.1 Опис серверної частини

На момент проведення дослідження, в серверній кімнаті компанії «Процесінг» інформаційна платформа Omnitraker функціонувала на сервері HP Proliant DL 360e G8.

Сервер HP Proliant DL 360e G8

Сервер HP ProLiant DL360e Gen8 забезпечує достатню потужність та об'єм пам'яті у форм-факторі 1U для традиційних серій 100 та 300. Сервер HP ProLiant DL360e Gen8 оснащений 2 процесорами Intel Xeon E5-2400 і підтримує до 12 модулів пам'яті DDR3 DIMM. Він також містить останні інновації в управлінні iLO та новітнє обладнання HP, зокрема HP Smart Storage, HP SmartMemory та HP Smart Socket Guide. Сервер HP ProLiant DL360e Gen8 підтримує механізм керування HP iLO, набір вбудованих функцій керування, що підтримують весь життєвий цикл сервера: від початкового розгортання та регулярного керування до сповіщень про необхідність обслуговування та віддаленої підтримки. Механізм управління HP iLO входить до стандартної комплектації всіх серверів HP ProLiant Gen8 і включає: HP iLO, технологію HP Intelligent Provisioning (раніше відому як SmartStart), HP Agentless Management, систему HP Active Health та HP Embedded Remote Support.

Риснуок 3.1 –зображення серверу HP Proliant DL 360e G8

Складові серверу приведені нижче в Таблиці 3.1

Таблиця 3.1 - Складові серверу HP Proliant DL 360e G8

Категорія	Сервер HP DL Proliant Gen8
Габарити (Ш (с ушами) х Г (с блоком живлення) х В), мм	436 (483) x 734 (768) x 44
Форм-фактор дисків	2.5" (SFF)
Кількість слотів під HDD/ SSD	8x 2.5"
Тип оперативної пам'яті	DDR3
Процесор	2 x Intel XEON Six Core E5-2420 1.90 GHz/15M (SR0LN) 95 W
Форм-фактор корпусу	1U Rackmount
Кількість сокетів під процесори	2
Кількість ядер ядерної системи	6
Дисковий контролер	RAID-Контролер P420 + Cache FBWC 1GB + Capacitor
Об'єм оперативної пам'яті	24GB (6x4GB) DDR3 ECC Registered
Кількість встановлених HDD/ SSD	2
Інтерфейс HDD/ SSD	SATA, SAS
Об'єм HDD/ SSD	SSD SATA 50 GB DELL 3Gb/s 50G5MPQ-0VAD3 DP/n (0G914J)
Кількість LAN (RJ-45)	4x порта 1Gb Ethernet
Кількість встановлених БЖ	2 шт. Блок живлення HP G8(750W)
Зовнішній стрічковий накопичувач	HP 1U USB Rack-Mount Kit, A8007B
Куллери	HP DL360e Gen8 Redundant Fan Kit, 2 шт,661530-B21

Продуктивність

Цей сервер на базі чіпсету Intel C600 підтримує до двох процесорів Xeon E5-2400 або E5-2400 v2. Intel представила новий виробничий процес зі своїми процесорами v2, щоб створити потужніший процесор.

Оперативна пам'ять

Кожен процесор у цій платформі із двома сокетами містить три канали пам'яті, які підтримують до двох слотів DIMM пам'яті DDR3. Конфігурації з одним процесором можуть підтримувати до шести модулів DIMM, щоб забезпечити до 16 ГБ пам'яті, тоді як конфігурації з двома процесорами підтримуватимуть удвічі більше слотів DIMM, щоб забезпечити максимальний об'єм пам'яті 32 ГБ. Цей

сервер підтримує модулі пам'яті без буферизації (UDIMM), зареєстровані (RDIMM) та зі зменшеним навантаженням (LRDIMM), але змішування різних типів пам'яті не підтримується. HPE SmartMemory спеціально розроблений для підвищення продуктивності серверів ProLiant Gen8 та розблокує деякі розширені функції для зниження енергоспоживання.

Зберігання даних

Ця система підтримує конфігурації приводу малого форм-фактора (SFF). Конфігурації SFF підтримують до восьми дисків, забезпечуючи до 9,6 ТБ пам'яті при використанні дисків SAS ємністю 1,2 ТБ. Обидві конфігурації залишають місце для установки оптичного приводу, якщо це необхідно. Адміністратори можуть легко визначити стан жорсткого диска за допомогою розширеної діагностики HPE SmartDrive.

Можливості розширення

Сервер HPE DL360e Gen8 підтримує один низькопрофільний слот PCIe 2.0 та один повнорозмірний/повнорозмірний слот PCIe 3.0 для додаткових комунікацій та зберігання. На сервері можна знайти до семи USB-портів: два розташовані на передній панелі корпусу, чотири на задній панелі та один внутрішній порт[17].

Операційна система з якою працює сервер - Windows Server 2012 R2

Оновлена версія Windows Server 2012 R2, випущена 18 жовтня 2013 року, заснована на Windows 8.1 та отримала різні покращення, включаючи віртуальні машини на базі UEFI, багаторівневі дискові простори, дедуплікацію VHD та інші покращення.

Операційна система Windows Server 2012/2012 R2 поставляється в чотирьох редакціях, основна відмінність яких у підтримуваній кількості процесорів та користувачів, а також можливостях використання віртуалізації[18].

3.2 Опис функціонування інформаційної платформи Omnitracker в компанії «Процесінг»

Бізнес компанія «Процесінг» налаштований для надання послуг і сервісів зарубіжним та Українським банкам. Оскільки сфера надання сервсів – це сфера IT, відповідно більшість бізнес процесів проходять як IT процесии. Тому компанія використовує інформаційну платформу Omnitraker у якості ITSCM та BCM та Change Management, Incident management функцій, що були надані за допомогою окремого модуля для цих них вендором OmniWay. Наразі підтримка платформи відбувається у компаніїї своїми силами, за забезпечення оптимізації, адміністрування, розробки та супроводження оновлень чи нових функцій лежить на співробітниках компанії «Процесінг»

Функції ITSCM та BCM та Change Management, Incident management мають на увазі під собою:

— аварійне відновлення після інцидентів;

— повідомлення про інцидент чи аварію що могла статися з ПО, сервером, системою і тд.;

— прискіпливе та уважне документування систем та сервісів, що забезпечують роботу компанії;

— створення заявок на обслуговування (починаючи від налаштування принтеру до видання ноутбуку);

— Change Management - забезпечує процес контролю внесення змін у IT-архітектуру компанії (сервери, системи, конфігурація сервісів та ПО);

— перелік активів компанії, що використовуються (від робочої станції, принтеру и тд. до переліку серверів та комплектуючих);

— Incident management – напевно одна з головних функцій, що відображає перелік інцидентів, що виникли в компанії та підтримується персоналом Servicedesk.

Також Omnitraker використовується господарчим, HR та бізнес відділами. Всі ці функції можна побачити на наступному Рисунку 3.2 та 3.3. На цих рисунках зображений доступ до платформи з windows-клієнт. Всі користувачі ідентифікуються у Active Directory та заходять до платформи під своїм логіном та паролем.

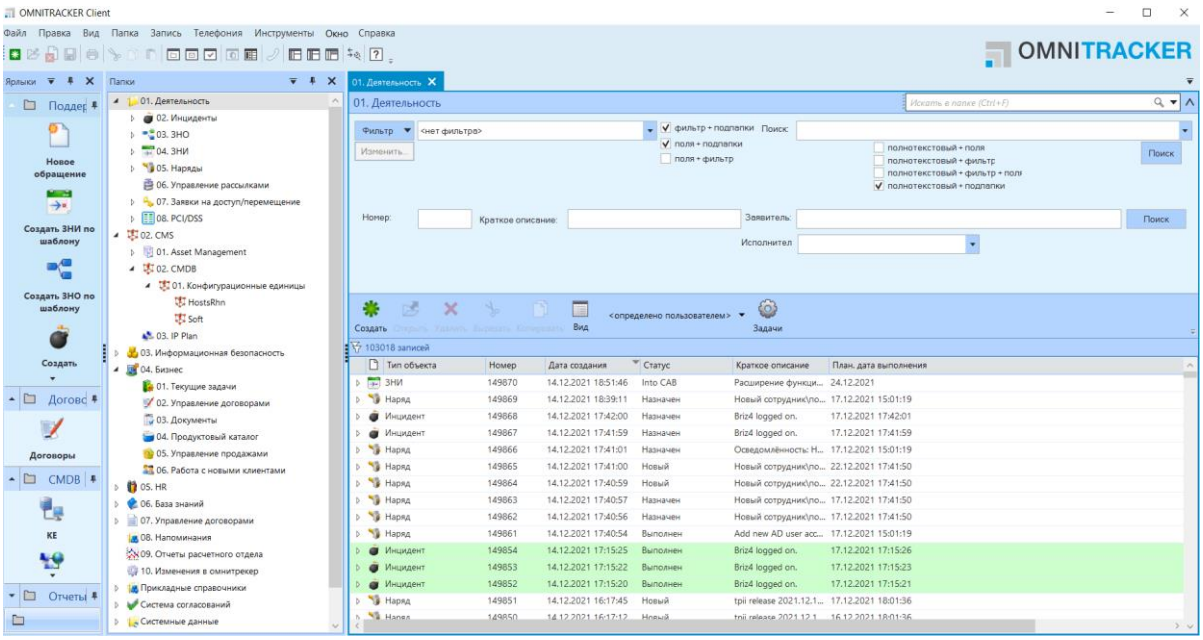


Рисунок 3.2 - Функції Omnitraker, що використовуються компанією “Процесінг” windows-клієнта

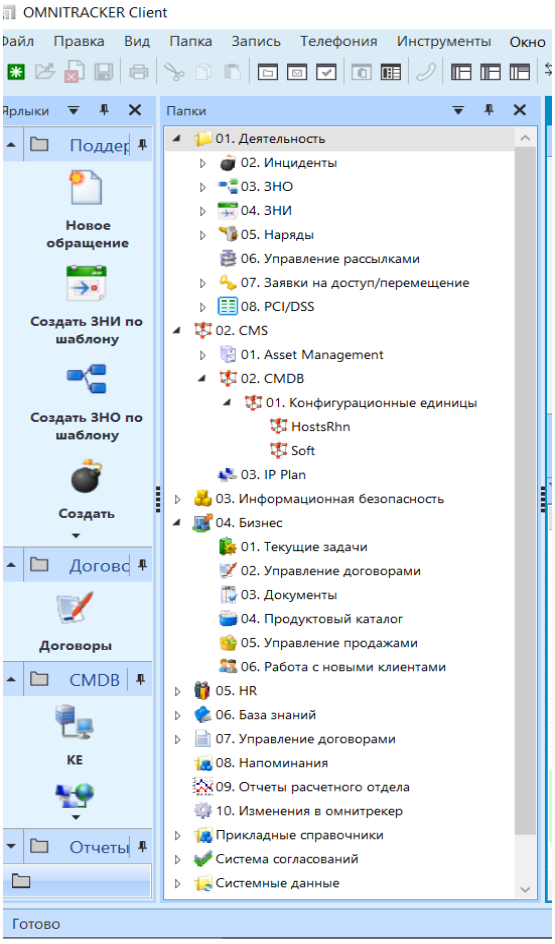


Рисунок 3.3 - Функції Omnitraker, що використовуються компанією “Процесінг”

Підтримка web-клієнта

Також, для всіх користувачів доступна web-версія, це зображено на рисунках 3.4 та 3.5

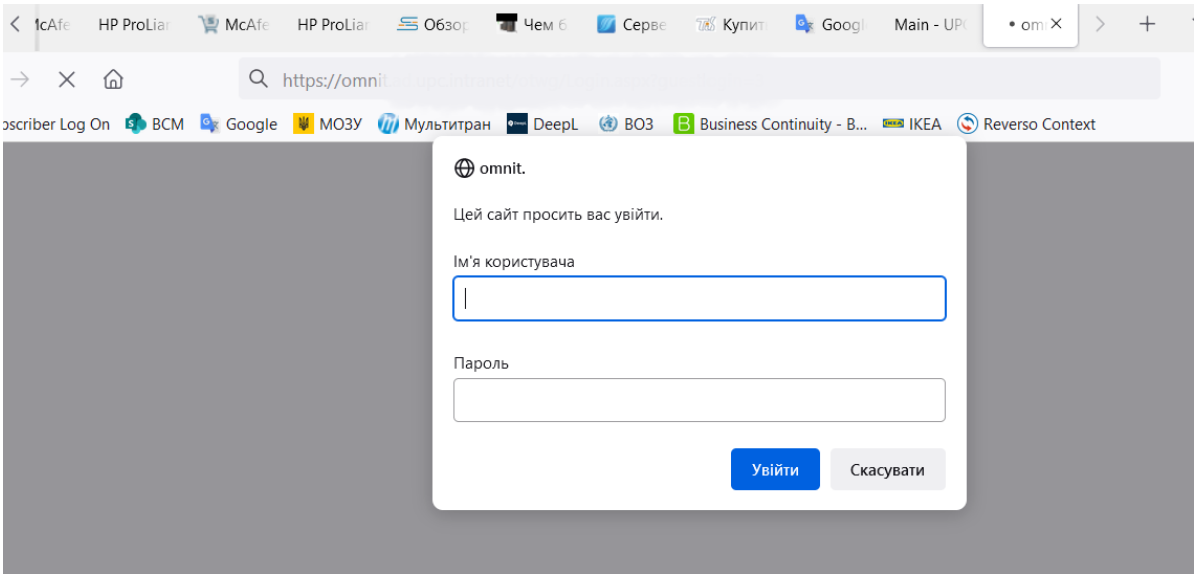


Рисунок 3.4 - Підтримка веб-версії платформи

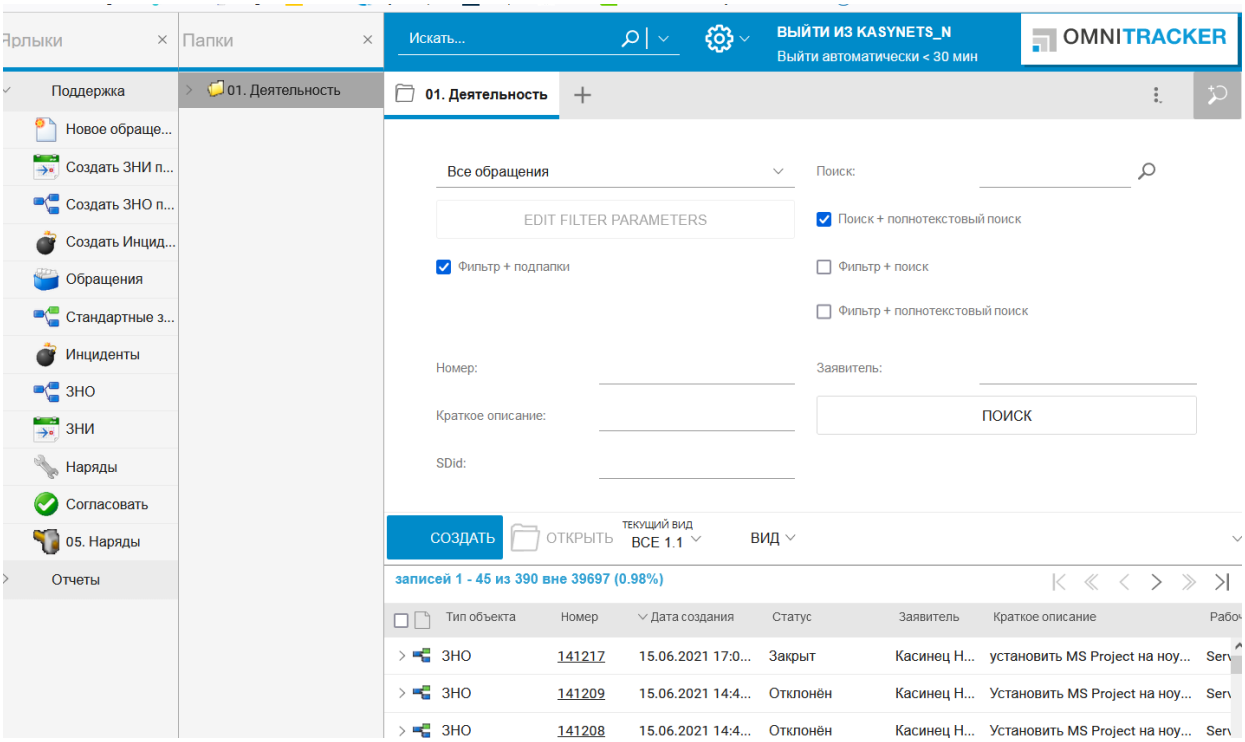


Рисунок 3.5 – Огляд платформи з веб-версії

Концепція розмежування прав і ролей

За розмежування прав відповідає адміністратор платформи, що в свою чергу має права на редагування, видалення і розробку об’єктів, скриптів і т.д.

Адміністратори сервісів та систем – це користувачі платформи, що мають права на перегляд об’єктів, реєстрацію нових конфігураційних одиниць та їх зміну, створення заявки на доступ та інше, що пов’язане з його посадовою інструкцією.

Простий користувач, що не є співробітником відділів пов’язаних з IT має доступ на створення звернень(які потім можуть стати заявками на доступ, заявками на обслуговування, заявками на зміну, інцидентом).

Користувачі групи ServiceDesk - володіють знаннями щодо класифікації звернень простих користувачів і мають права створення не тільки звернень, а і інцидентів , заявок на доступ, заявок на обслуговування(ЗНО), заявок на зміну(ЗНИ).

Користувачі групи інцидент менеджменту відповідають за визначення статусів інцидентів та приймають рішення щодо їх закриття.

Користувачі групи Change Management – мають право на визначення статусів ЗНИ та продовження життя циклю ЗНИ до статусу «закритий». Також без погодження користувачів цієї групи на етапі «Погодження» адміністратори систем та сервісів не мають право вносити зміни до IT-інфраструктури чи архітектури компанії «Процесінг».

Обробка електронної пошти

Компанією «Процесієнг» використовуються майже всі достумні функції платформи, в тому числі і обробка електронної пошти. Обробляються всі можливі формати електронних листів:

- Plain text;
- HTML;
- RTF;
- із вкладеннями;
- із впровадженими об'єктами (Embedded Objects);

Ці листи можуть бути як вкладення до будь-яких із функцій та обєктів ITSCM та BCM та Change Management, Incident management, HR, Bussines, Asset management, facility management.

3.3 Функції Omnitracker в компанії «Процесінг», що є найбільш важливими

Оскільки галузь безперервності бізнесу насамперед пов’язана з ITSCM (Change Management, Incident management), то ці функції найбільше використовуються користувачами платформи.

До функцій ITSCM належать функції керуваннння IT частиною компанії, в Omnitracker глобальна за це відповідають такі об’єкти як заявки на обслуговування, рестарція активів, стаорення конфігураційних одиниць, що є складовими сервісів і тд.

Запити на обслуговування(ЗНО)

До ЗНО відносяться звернення щодо обслуговування клієнтської частини (налаштування доступів, паролів, зміни складу робочих груп, ролей тощо). У цьому випадку таке звернення фіксується диспетчером Сервіс Деска та/або черговим інженером.

Призначення виконання ЗНО проводиться д користувачем групи ServiceDesk у стандартному режимі шляхом заповнення форми створення Нового ЗНО це показано на Рисунку 3.6

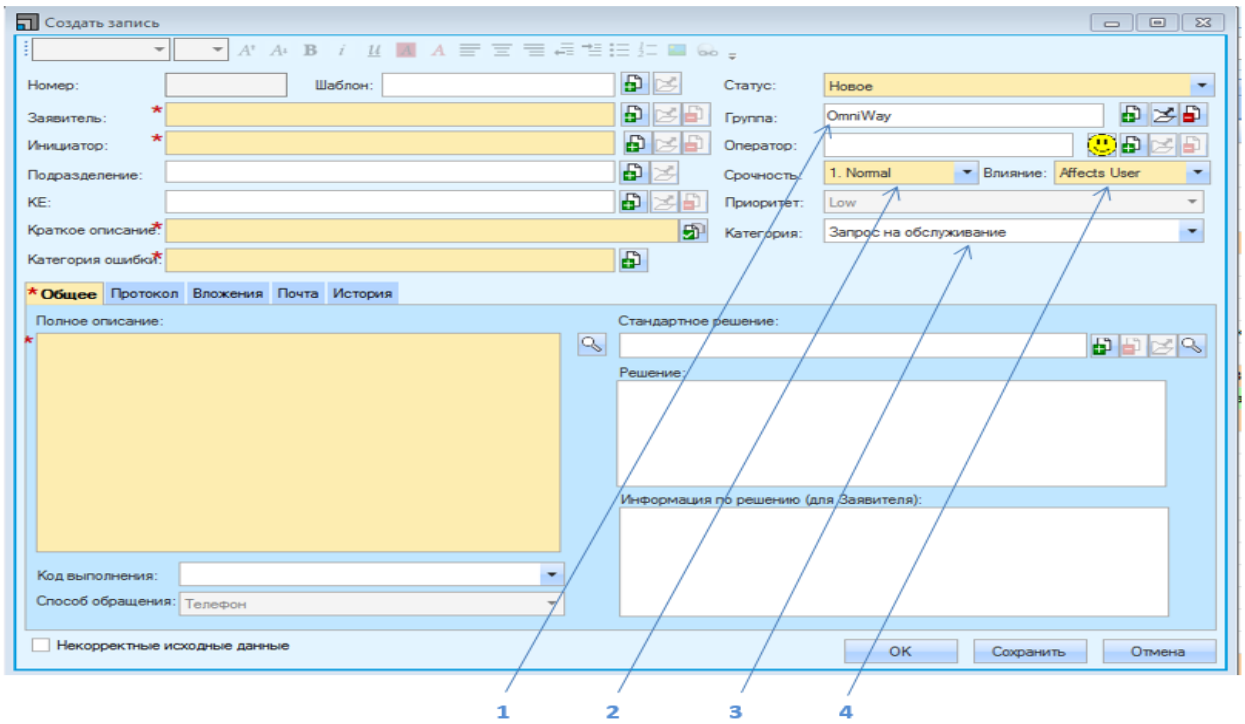


Рисунок 3.6 – Оформлення ЗНО в Omnitraker

1- призначення відбувається на групу «OmniWay»/ «ServiceDesk» (1);
2- статус терміновості – «Normal» (2);
3- Категорія - "Запит на обслуговування";
4- Статус впливу - "Affects User".

Нижче на Рисунку 3.7 відображений інструмент Workflow, що налаштовується адміністартором Omnitraker у відповідності до життєвго циклу ЗНО.

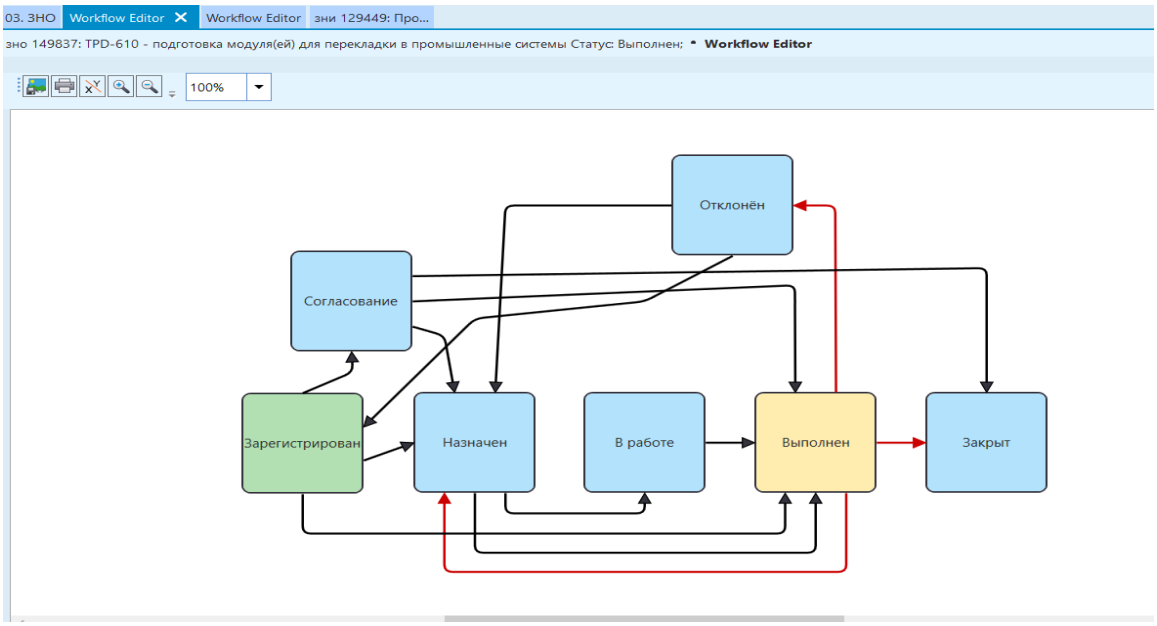


Рисунок 3.7 – Життєвий цикл ЗНО

Функція Change Management

Якщо говорити, про функцію Change Management, то головними об’єктами в Omnitraker є заявка на зміни(ЗНИ) та керування ниими.

До **ЗНИ** відносяться звернення щодо змін настроювальних параметрів системи (зміна інтерейсу користувача та адміністратора, додавання/зміна/видалення полів, шаблонів, груп погодження, нових розділів, заклади та супроводу бізнес-процесів). У цьому випадку таке звернення фіксується користувачем групи ServiceDesk.

Роботи в Omnitracker, що проводяться відповідно до запитів співробітників, поділяються на запити на обслуговування (ЗНО) та запити на зміни (ЗНИ).

Призначення виконання ЗНИ проводиться користувачем групи ServiceDesk у стандартному режимі шляхом заповнення форми створення Нової ЗНИ.

Призначення нарядів та погоджень відбувається за певною схемою відповідно до настройок, встановлених у Шаблоні «Зміни в налаштуваннях».

Наряд- є об’єктом Omnitraker, у якому фіксуються усі дії, що будуть виконуватися користувачем інших груп крім ServiceDesk при роботі з ЗНИ, ЗНО, на яких безпосередньо і буде назначатися ЗНО чи ЗНИ

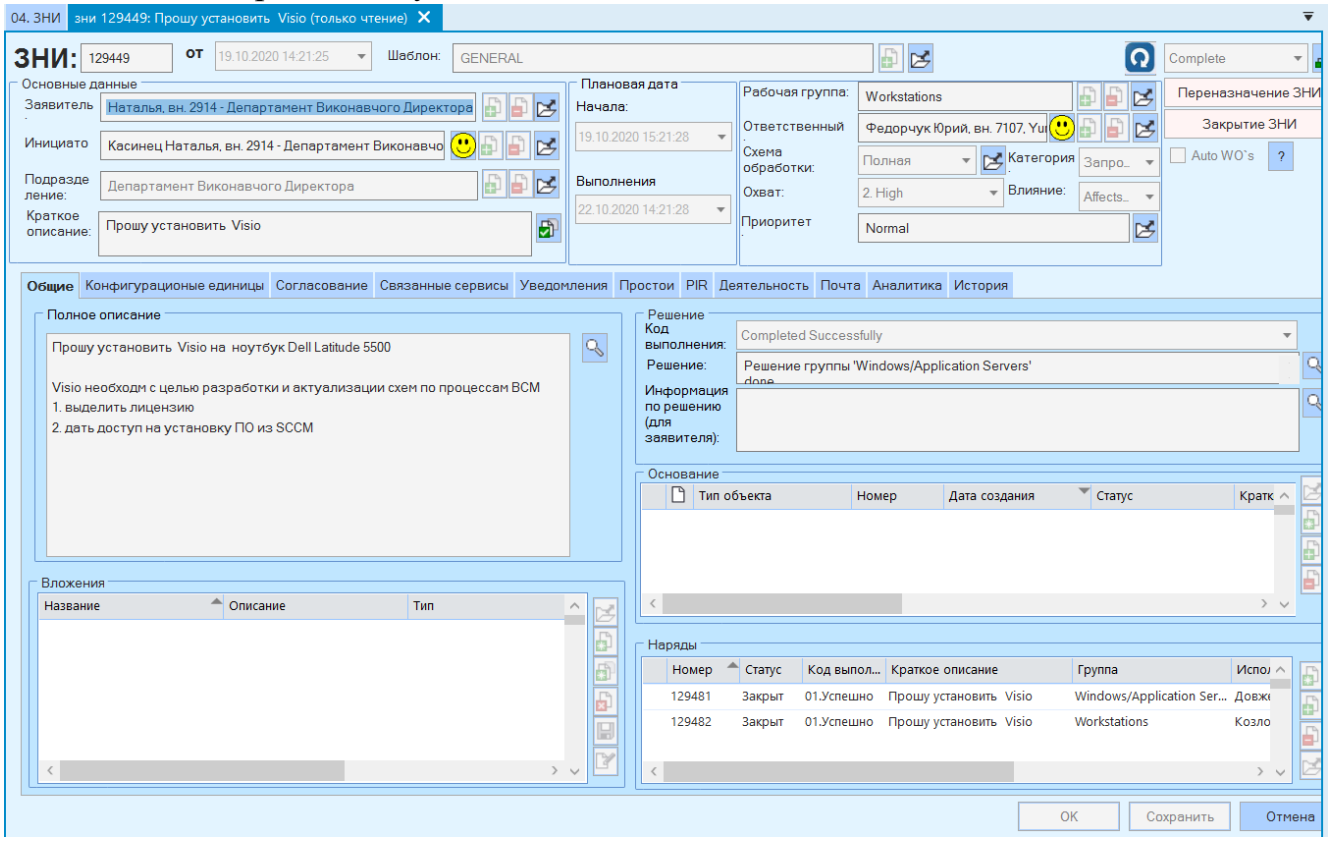


Рисунок 3.8 – Оформлення ЗНИ в Omnitraker

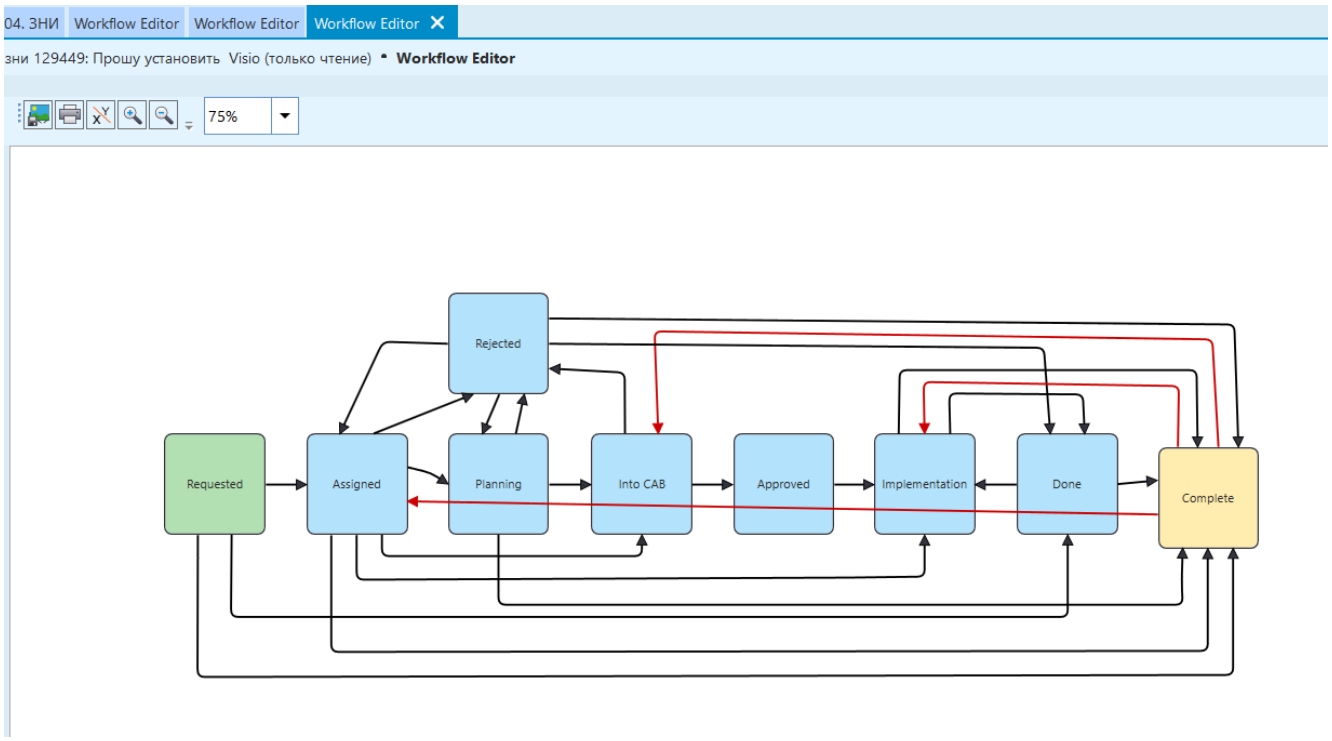


Рисунок 3.9 –Workflow ЗНИ в Omnitraker

На Рисунку 3.9 відображений інструмент Workflow, що налаштовується адміністартором Omnitraker у відповідності до життєвго циклу ЗНО.

Конфігураційні одиниці, як частина ITSCM

Компанія «Процесінг» в Omnitraker заводить всі конфігураційні одиниці сервісів\систем, що можуть якимось чином змінюватися для оптимізації або в інших цілях. Ця складова використовується і у Change Management під час змін. На Рисунку 3.10 відображені всі Конфігураційні одиниці(КЕ) компанії

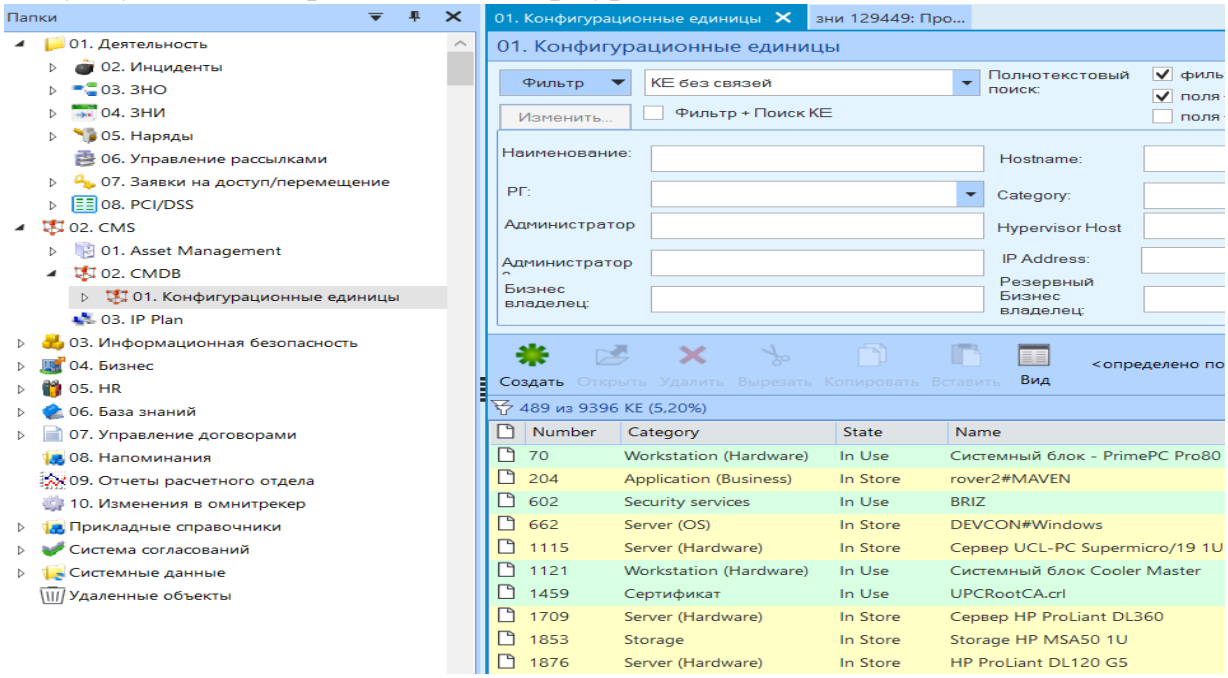


Рисунок 3.10 – КЕ в Omnitraker

Реєстрація активів

Реєстрація активів потрібна для переліку всіх пристроїв, які у використанні у користувачів чи відділів. Нижче на Рисунку 3.11 представлено всі активи компанії.

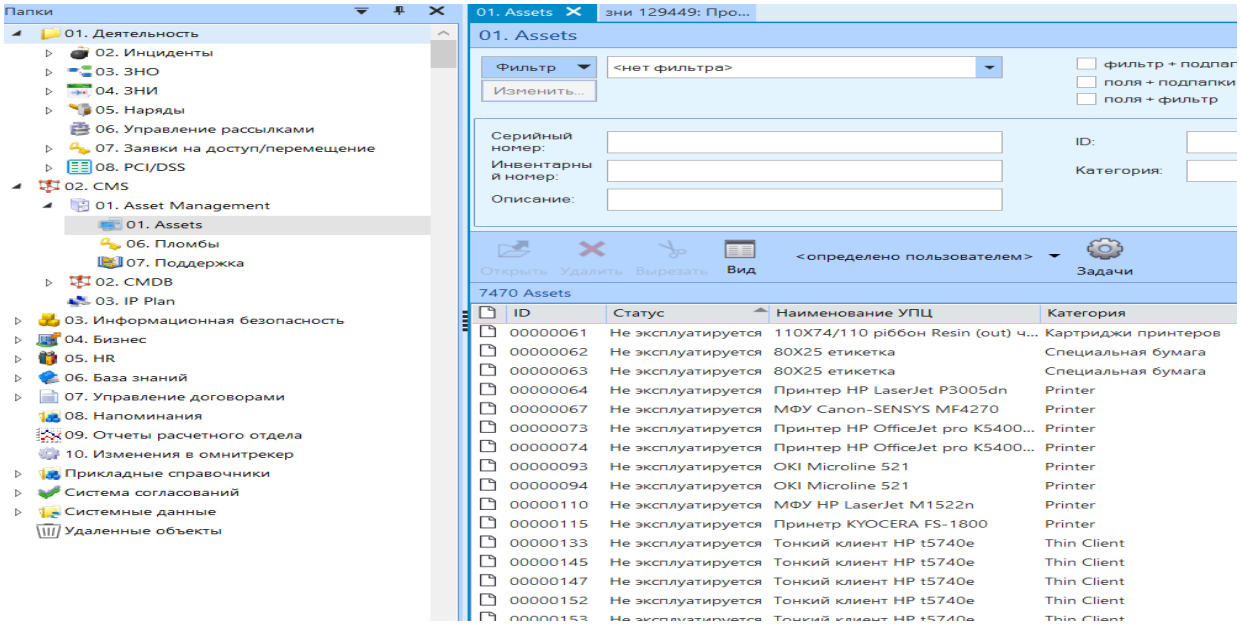


Рисунок 3.11 –Активи в Omnitraker

Функція Incident management

За термінологією ITIL, інцидент – це подія, яка ставить під загрозу виконання бізнес-процесів та може знизити рівень надання послуг. Немає доступу до сервера, не працює телефонія, нестійкий сигнал Wi-Fi – кожна з цих проблем потребує негайного вирішення. На допомогу приходить керування інцидентами. Його основне завдання – якнайшвидше відновити послугу, мінімізувати вплив збою на користувача та компанію, а також запобігти фінансовим втратам.

В Omnitraker компанією «Процесінг» ведеться весь процес керування інцидентами за ITIL. Цей процес зображений на рисунку 3.12

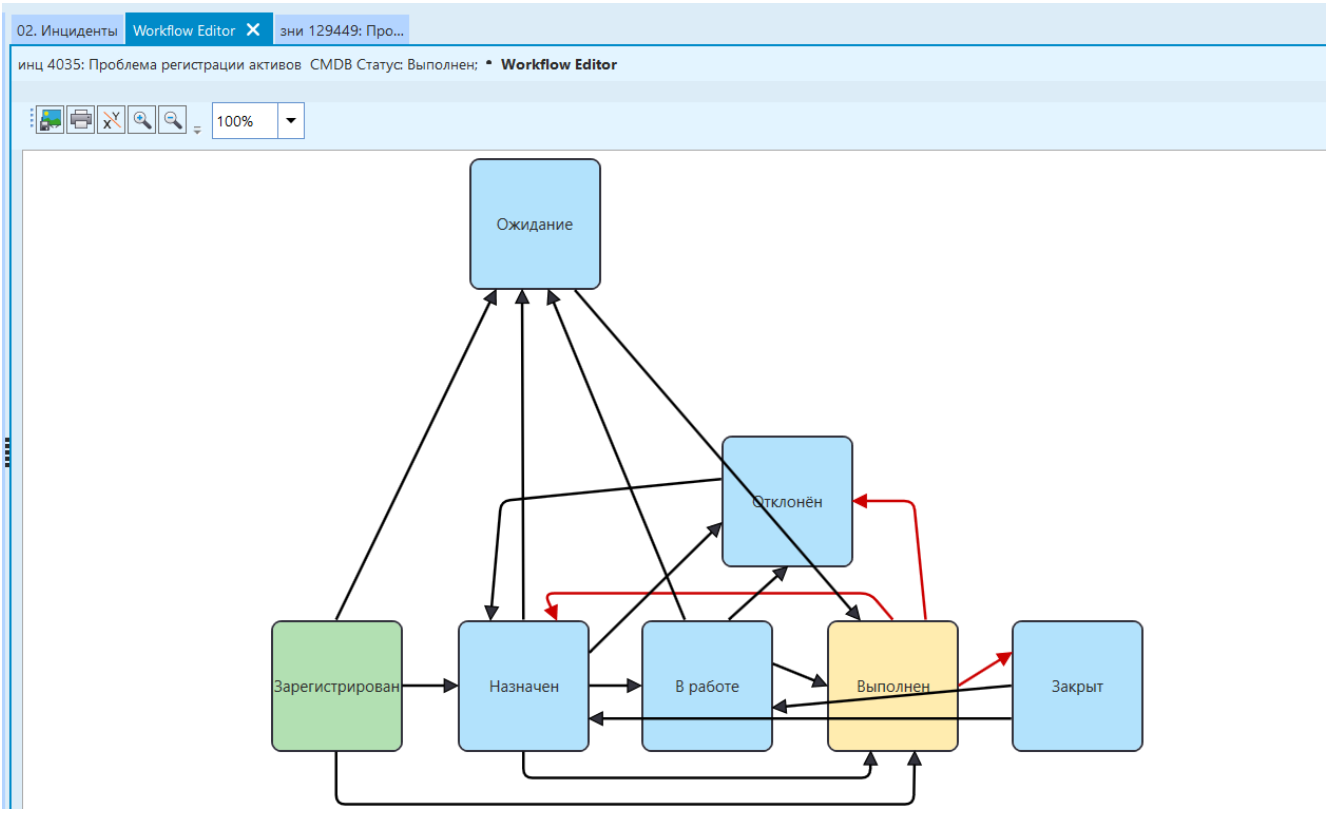


Рисунок 3.12 - Процес керування інцидентами

Сам інцидент в компанії «Процесінг» може фіксуватися системами через E-mail, або ж безпосередньо працівником компанії, якщо цей інцидент пов'язаний з будь-якою системою чи сервісом, які не можуть відправляти повідомлення.

На Рисунках 3.13 та 3.14 відображено створення інциденту в Omnitraker. Автоматично системою надається унікальний «Номер» звернення, який згодом і присвоюється створеному Інциденту.

Кожному виконавцю , який згідно з бізнес-процесом передбачено взяти в ньому участь на тому чи іншому етапі за допомогою електронної пошти надходить повідомлення про те, що необхідно зареєструватися в Omnitracker і зареєструвати виконання певних дій.

Так як інцидент призначається на робочу групу, яка може складатися з кількох виконавців, то в полі «Виконавець» співробітник, який приймає на себе виконання наряду, вибирає зі списку себе, змінює статус наряду з «Призначений» на «У роботі» і задіявши * зберігає зміни.

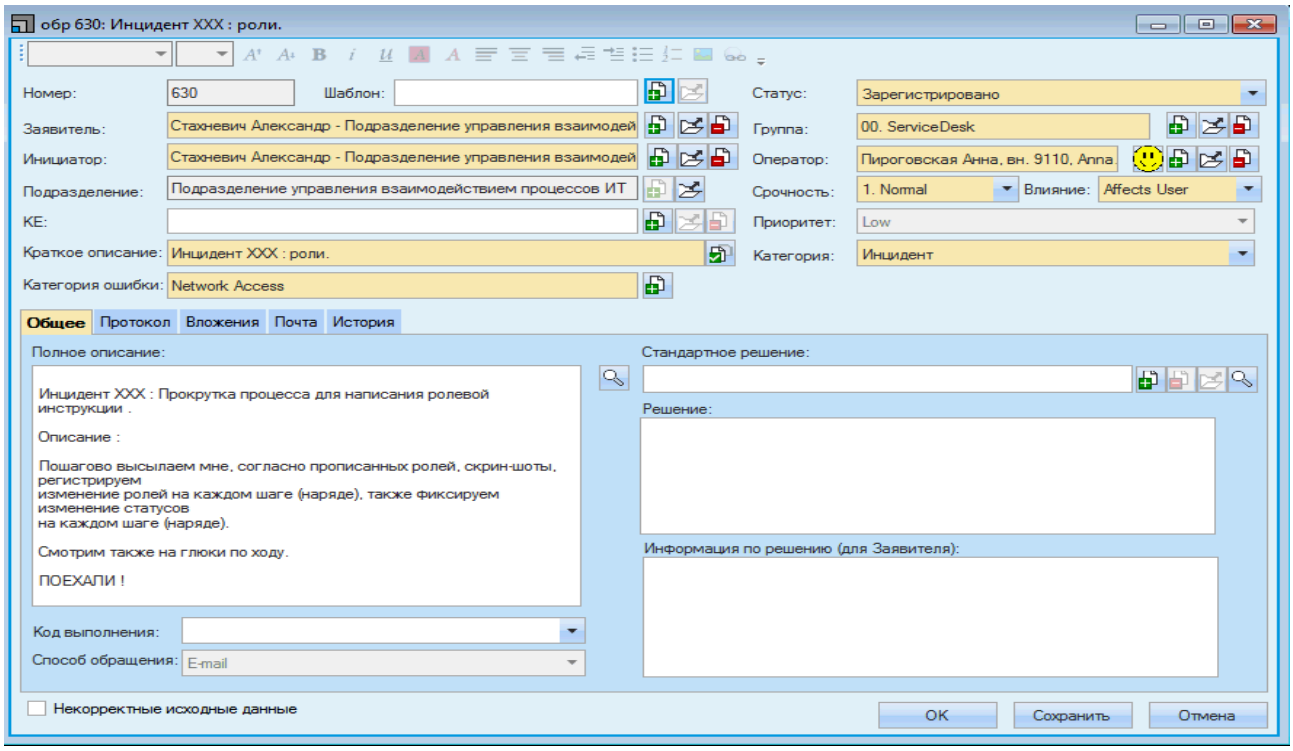


Рисунок 3.13 – Створення інциденту

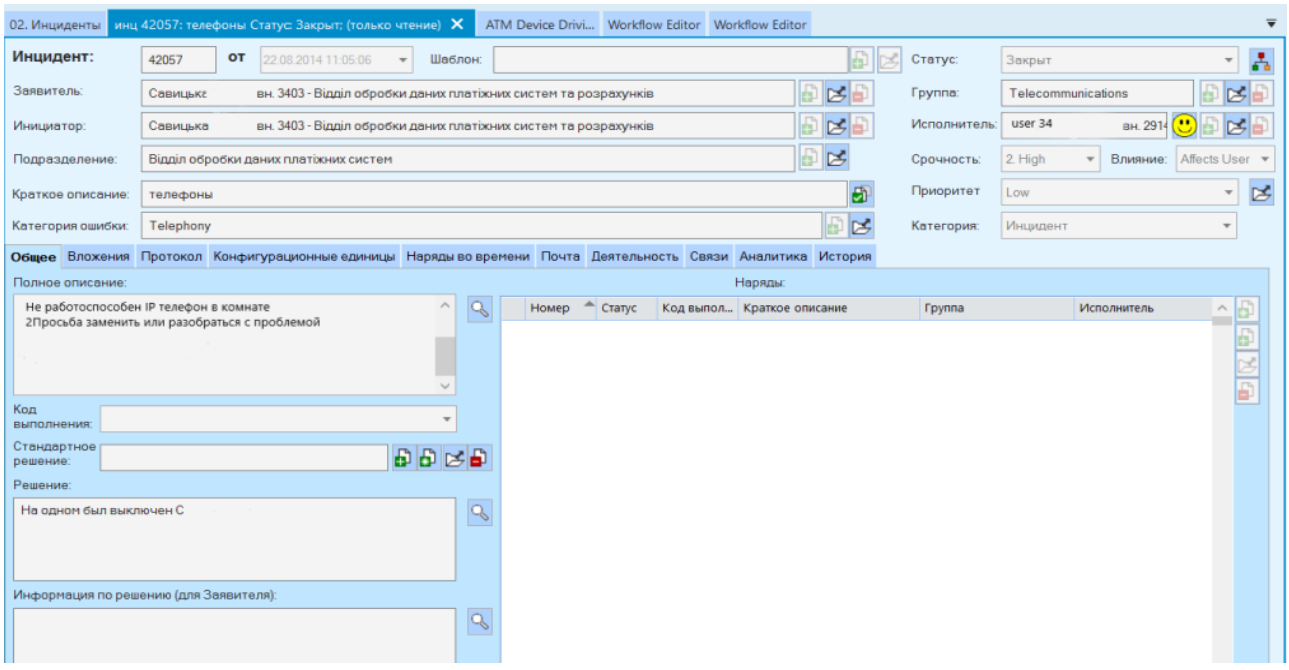


Рисунок 3.14 – Стан закритого інциденту

Одним із головних вкладок з роботою інциденту є вкладення «Конфігураційні одиниці» та «Аналітика». В цих вкладках обов'язково необхідно вказувати задіяні системи вибрані із конфігураційних одиниць, та у вкладці «Аналітика» - заповнювати поля з датою та часом. На рисунку 3.15 відображені вкладки з якими необхідно працювати, більш детально відоборжена вкладка «аналітика»

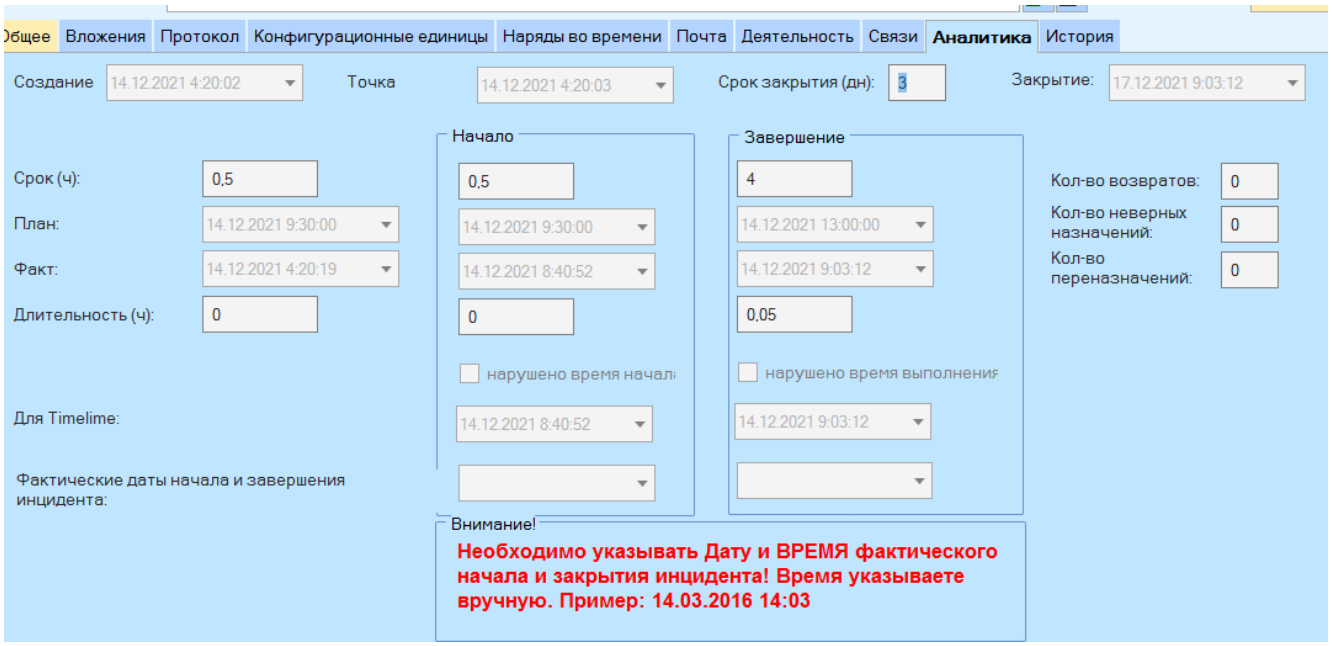


Рисунок 3.15 – Стан закритого інциденту

Система моніторингу та контролю

Системою передбачено ведення моніторингу відповідності часу виконання нарядів встановленим метрикам. Контроль виконання метрик здійснюється автоматично на основі обліку зміни статусів виконання нарядів. У системі реалізована можливість розсилки відповідальним виконавцям і керівництву поштових повідомлень про проходження процесів.

Система таких повідомлень постійно модернізується та розширюється. Рисунок 3.16 відображає одне з повідомлень системи моніторингу через e-mail.

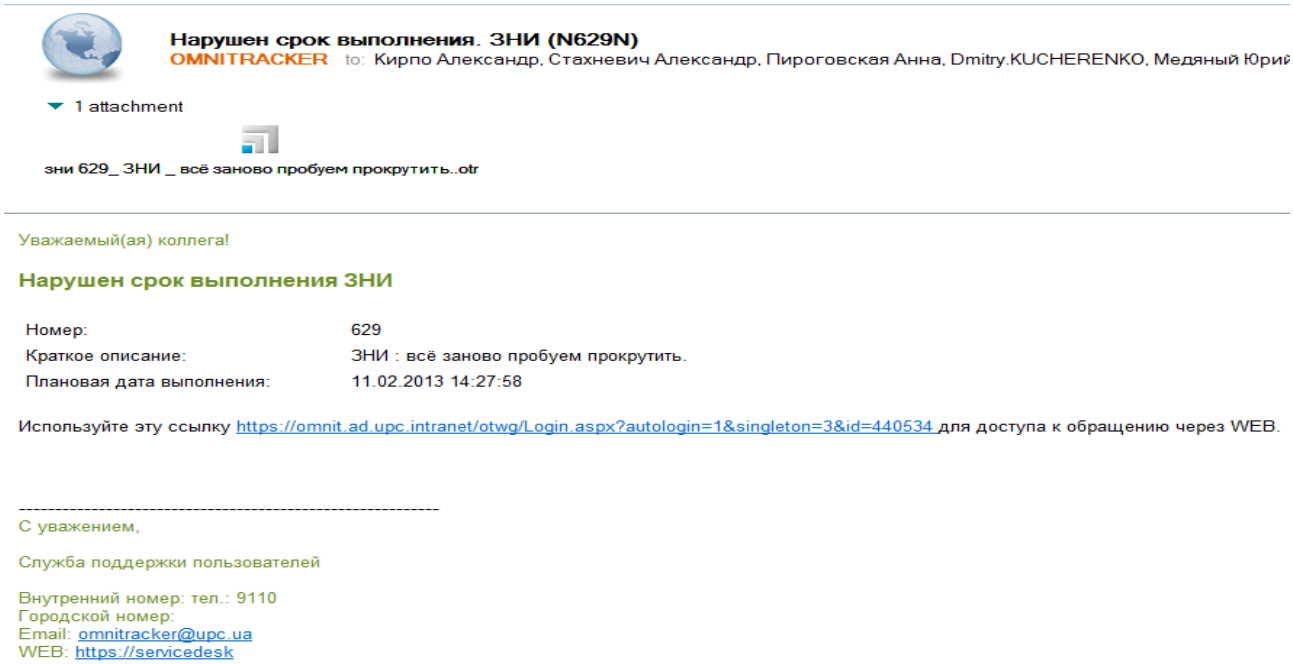


Рисунок 3.16 - Система моніторингу Omnitraker через e-mail

Адміністрування платформи Omnitraker

Функції Адміністрування належать лише адміністратору платформи.звісно адміністратор має повні права для доступу до всіх функцій, як це вже було зазначено вище. З адміністраторськими правами також доступне тестове середовище розробки, в якому відповідно проводять тестування всіх скриптів чи змін перед виконанням у виконавчому середовищі.

З адміністраторськими правами можливо виконувати різні завдання та функції, що відображені на наступному Рисунку 3.17 та знаходяться за шляхом «Файл» - «Адміністрування».

На Рисунках 3.19-3.21 зображені скрипти, що розробляються адміністраторами для оптимізації Платформи в плані реагування, швидкості закриття інцидентів, автоматизації всіх процесів, що можуть виконуватися у платформі користувачами(від автоматичного назначення інциденту на групу ServiceDesk до більш-складних завдань як – створення ЗНИ по шаблону і тд.)

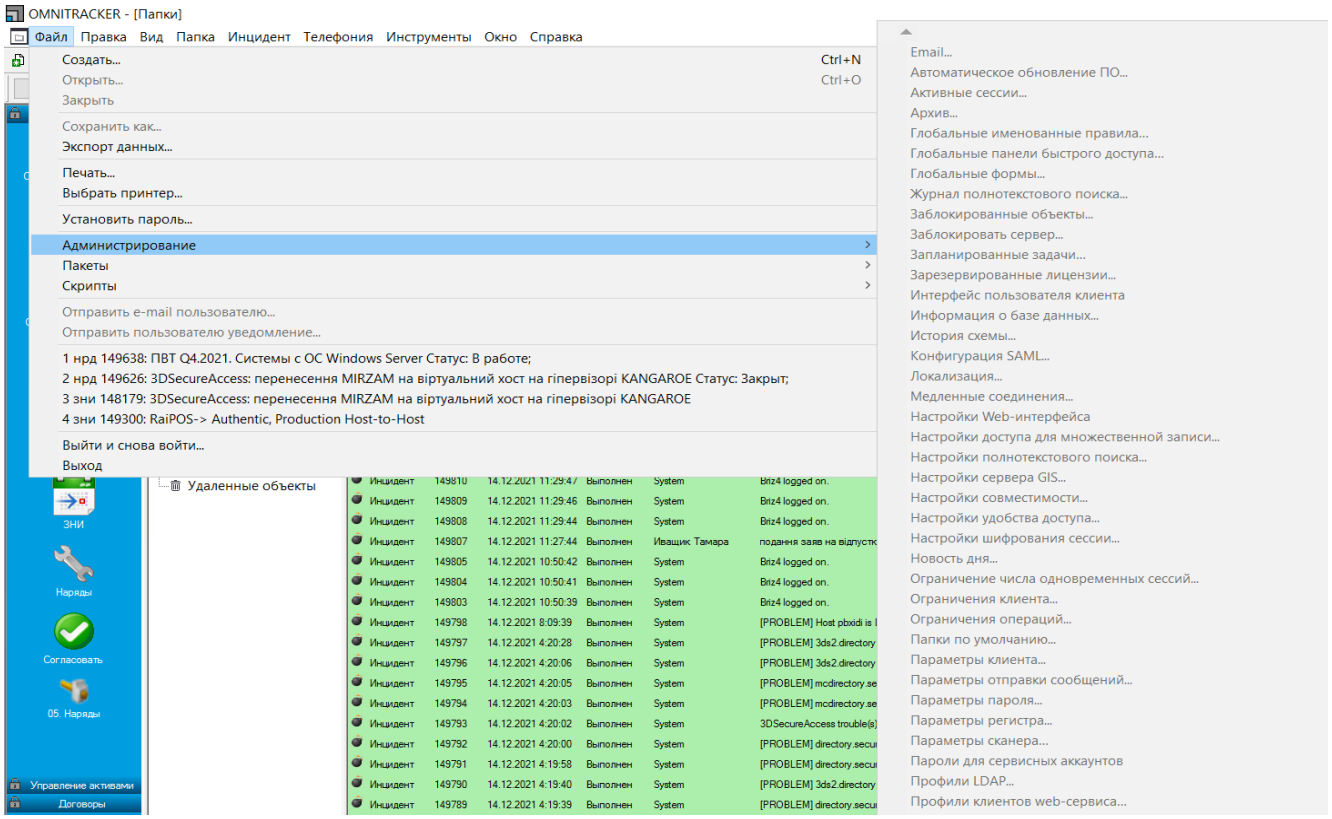


Рисунок 3.17- Вкладка Адміністрування, що доступна для адміністраторів

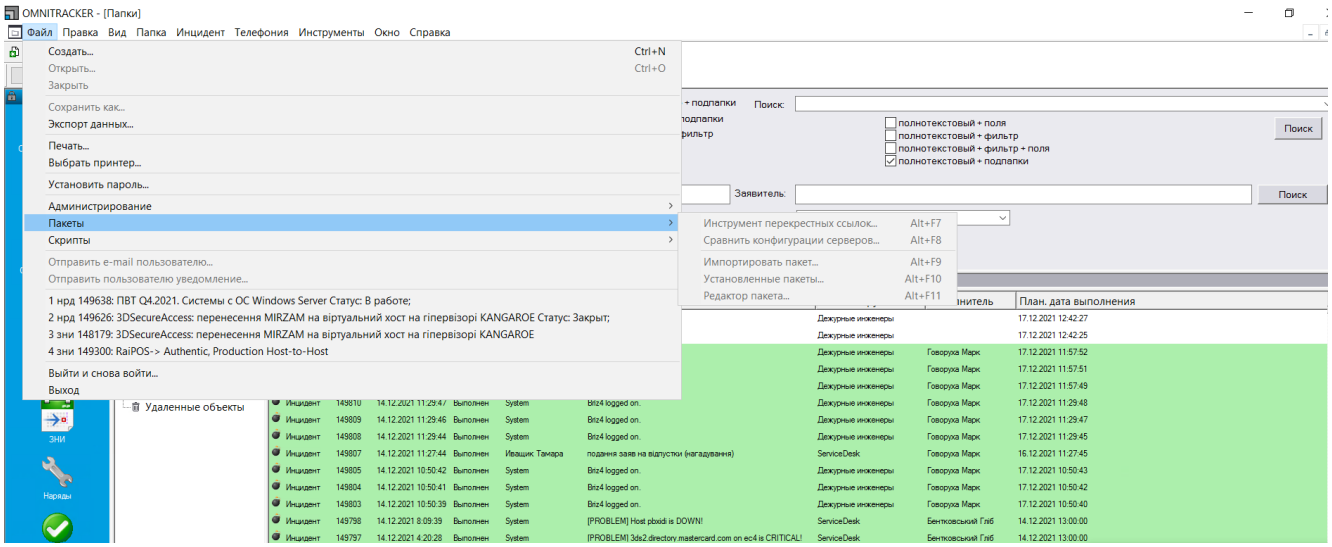


Рисунок 3.18 – Вкладка пакети, що доступна для адміністраторів

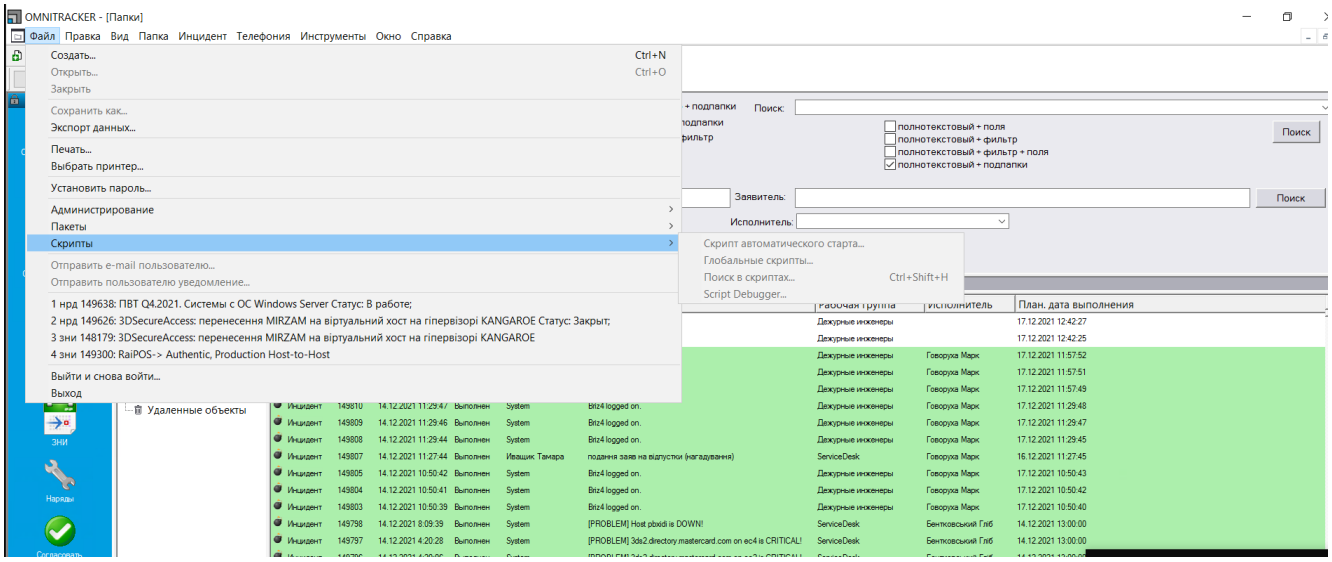


Рисунок 3.19 – Вкладка скрипти, що доступна для адміністраторів

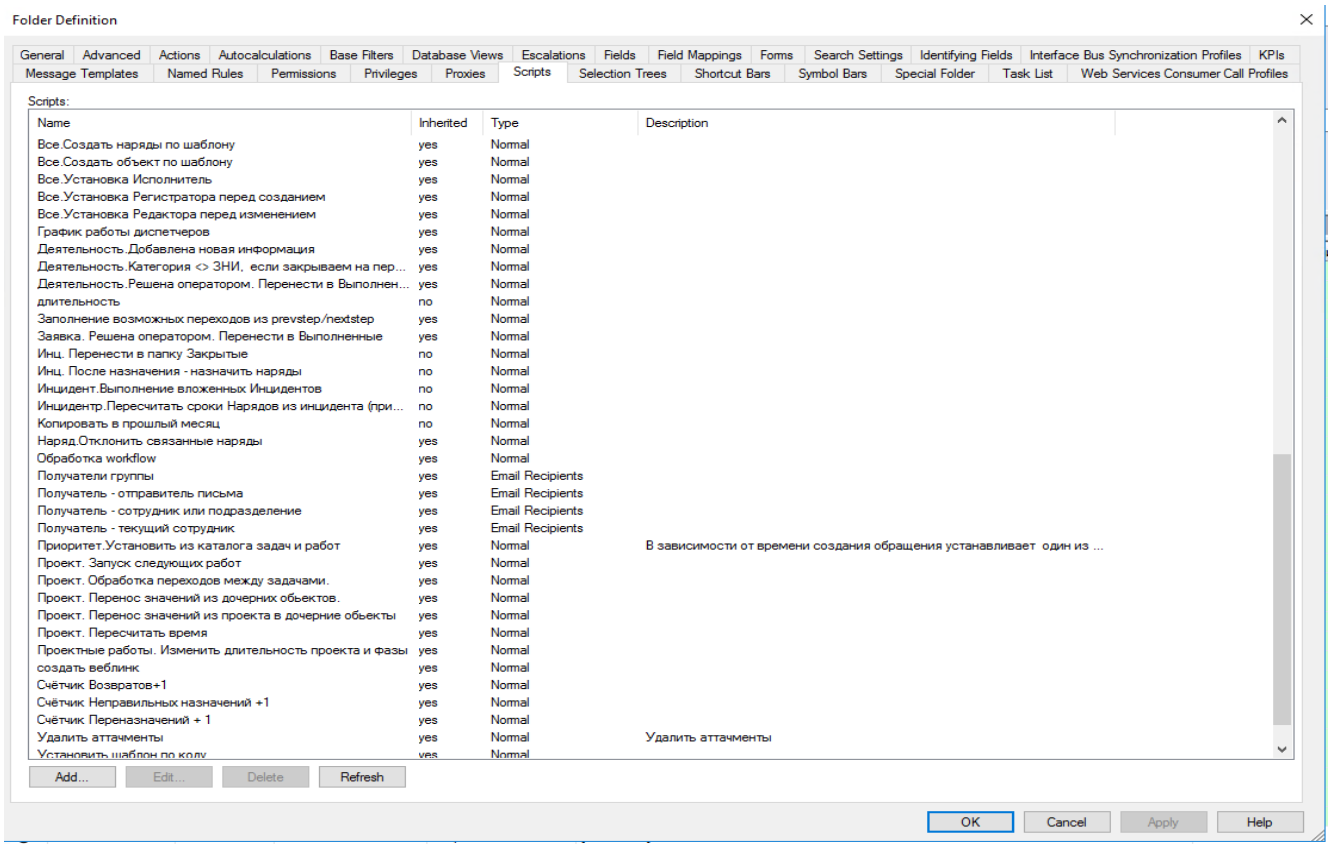


Рисунок 3.20 – Скрипти, що вже є в Omnitraker

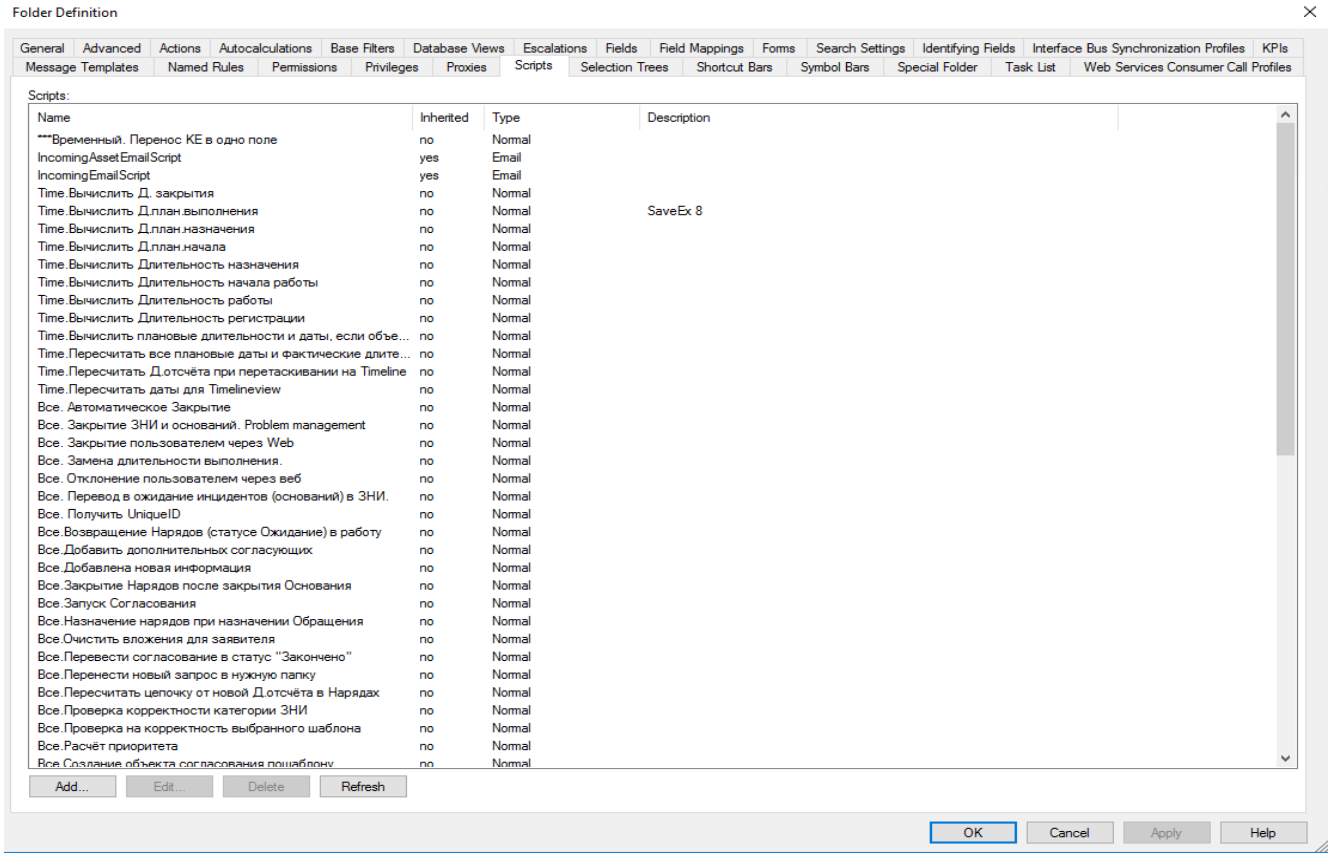


Рисунок 3.21- Скрипти, що вже є в Omnitraker

4. ОПТИМІЗАЦІЯ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ ПЛАТФОРМИ З БЕЗПЕРЕРВНОСТІ БІЗНЕС ПРОЦЕСІВ

Оскільки безперервність бізнесу (BCM), як було описано розділі 1 забезпечується не лише способом покращення IT-інфраструктури, а й покращенням архітекрури і функцій сервісу чи програмного забезпечення.

Якщо говорити про оптимізацію самої платформи, як ПЗ, то існує ще два недоліки які були знайдені під час дослідження платформи:

1. Автоматично не створюються інциденти переважно від Телекомунікаційного сервісу компанії «Процесінг», що забезпечує оновлення критичної телеком. системи;
2. Автоматично не закриваються вже вже виконані інциденти, що мають статус «виконано».

Про оптимізацію самої платформи буде у підрозділі 4.1.

З точки зору BCM та аналізу ризиків, методом мозкового штурму та обговорень, було знайдено *один недолік*, який може повипливати на репутацію компанії «Процесінг» та збільшити такі параметри як MBCO, RTO RPO, а це не припустимо – це факт того, що інформаційна платформа з забезпечення безперервності бізнесу процесів Omnitraker розміщується на не за дубльованому сервері. Цей недолік можливо усунути за допомогою кластеризації серверу на якому знаходиться платформа. Про це піде мова у підрозділі 4.2.

4.1 Оптимізація автоматичного створення та закриття інциденту інформаційної платформи з безперервності бізнес-процесів Omnitraker

Оптимізація полягає в мінімізації часу виконання інцидентів відповідальної людини, що займається закриттям інциденту, оскільки чим більше кнопок потрібно натиснути виконавцю – це буде впливати на час простою , і це в свою чергу буде мати вплив на компанію. Тобто основною метою оптимізації є – автоматизація процесів, що виконує виконавець у Omnitraker.

Отже як було визначено раніше, існує щонайменше два недоліки, пов’язані з мінімізацією часу для роботи з інтерфейсом платформи.

Недолік 1: Автоматично не створюються інциденти переважно від Телекомунікаційного сервісу компанії «Процесінг», що забезпечує оновлення критичної телеком. системи.

Недолік 2: Автоматично не закриваються вже виконані інциденти, що мають статус «виконано»

Для забезпечення необхідно створити скрипти, що будуть щоразу виконувати певні дії, що автоматизують процеси по створенню та закриттю інцидентів, цим

самим зменшить час роботи користувача у системі, а значить користувач зможе більше часу приділити на вирішення інциденту.

Використовувані мови програмування для автоматизації процесу створення та закриття інцидентів:

— для першого недоліку буде використовуватися мова програмування - Visual Basic;

— для другого недоліку буде використовуватися мова програмування - python.

Програмне забезпечення для використання мов Visual Basic та python:

— Notepad++ для Visual Basic;

— Visual Studio Code для python.

Оскільки у компанії використовують як українську мову, так і російську, в деяких рядках коду можуть зустрічатися обидві мови.

Сам код цих скриптів буде наведений у «Додатку А» та «Додатку Б».

На рисунках 4.1 та 4.2 зображено відображення скриптів для оптимізації недоліків у Notepad++ для Visual Basic та Visual Studio Code для python відповідно.

change.log | создания инцидента на стороне омнитрекер.vbs

```
Option Explicit

'обявлення зміних
Dim strEmailSubject, strRefAssetNumber, strEmailText, strEmailTo, strRefAssetNumber
Dim objIncomingMsg, objRefRequest, objFolder, objFilter, objRequests, objRequest, IsIncident, item, usermail, objRefRequest1
Dim objFld ' As OtRequestFolder
Dim currentdatetime, objList, objCounter, Count, mcafee, TemplInTo, Waf
Dim blnAgree

Log("" & vbCrLf & "начало скрипта")
strEmailSubject = ""
strEmailSubject = EmailSubject
strEmailText = EmailText


LogMessage "incommingemailscr"
Set objIncomingMsg = ActiveSession.GetRequestByUniqueId(LoggedEmail.UniqueId) ' вхд лист як OtRequest
Log("000001")

If Left(strEmailSubject, 7) = "*Critical*" Then ' перевірка сабжекта листа на існування значення по якому триггериться створення інциденту
    Call CreateIncident
    CreateNewRequest = False
End If

Sub CreateIncident
    LogP("-------Старт-------")
    Dim FullText, OldV, OldVStart, NewV, NewVStart, Obj, OldVNumb, NumbOld, NumbNew, NewVNumb
    FullText = objIncomingMsg.UserFields("Body Plain Text").TValue
    'шукаємо старую и нову версію з тела листа
    NumbOld = 13
    OldV = InStrRev(FullText, "pre_version")
    OldVStart = OldV + NumbOld
    OldVNumb = Mid(FullText, OldVStart, 11) 'Стара версія

    NumbNew = 13
    NewV = InStrRev(FullText, "new_version")
    NewVStart = NewV + NumbNew
    NewVNumb = Mid(FullText, NewVStart, 11) 'Нова версія

    LogP("Шукаємо робочу групу")
    Dim objFolderWG, objFilterWG, ObjWG, wg
    Set objFolderWG = ActiveSession.RequestFolders("Workgroups")
    Set objFilterWG = objFolderWG.MakeFilter
    objFilterWG.UserField("Name") = "Дежурные инженеры"
    Set ObjWG = objFolderWG.Search(objFilterWG, True)
    If ObjWG.Count = 1 Then
    LogP("Рабочая группа найдена")
    Set wg = ObjWG.item(0)
    Else
```

Рисунок 4.1 - зображено відображення скриптів для оптимізації недоліків у Notepad++

```python
import win32com.client #библиотека для работы с COM
import pythoncom #библиотека для работы с COM

IncNumber = argv #Передача номера инцидента системой в виде аргумента.
#Номер инцидента система получила из письма при его создании. См. "пример создания", строка 122
OtHost = "localhost"
OtPort = "555"
OtLogin = "login"
OtPassword = "password"
OtLang = "ua"
pythoncom.CoInitialize()
application = win32com.client.Dispatch("OtAut.OtApplication")
session = application.MakeSessionEx(OtHost, OtPort, OtLogin, OtPassword, OtLang) #создание сессии для конекта к омнитрекеру

pythoncom.CoInitialize()
folder = session.RequestFolders("Incidents")
objfilter = folder.MakeFilter()
objfilter.SetSpecialField("Number", IncNumber) # поиск инцидента
obj = folder.Search(objfilter, False)
if obj.count != 0: # если инцидент найден, тогда закрываем его
    objIncident = obj.Item(0)
    objIncident.UserFields("Status").TValue = "Closed"
    objIncident.Save() # сохраняем изменения
```

Рисунок 4.2 - зображено відображення скриптів для оптимізації недоліків у Visual Studio Code ++

4.2 Оптимізація серверної частини інформаційної платформи з безперервності бізнес-процесів Omnitraker

Для будь-якого підприємства та його функціонування на бізнес ринку надважливим є безперервність надання послуг та відмовостійка IT-інфраструктура. Це стосується кожної організації адже під час аварії чи при виході з ладу обладнання ціле підприємство може залишитися без критичних пристроїв, ПЗ, світла, води і т.д., а це в свою чергу буде мати фінансовий і репутаційний вплив на компанію.

Для забезпечення стабільної роботи програмного забезпечення серверне обладнання має відповідати високим вимогам щодо надійності. Одним з основних методів підвищення надійності сервера є резервування його підсистем шляхом дублювання компонентів: процесора, оперативної пам'яті, мережевих підключень, дискових та твердотільних накопичувачів, пристроїв охолодження, блоків живлення. Відмова дубльованого компонента не призводить до відмови сервера в цілому, але може зменшити його продуктивність. Усунення несправності зазвичай виконується без зупинки роботи сервера шляхом "гарячої" заміни компонента, що відмовив. Проте повне резервування у межах традиційної серверної архітектури неможливе. Такі компоненти сервера як системна плата та контролер дисків зазвичай не дублюються. Тому їх вихід з ладу означатиме відмова сервера в цілому і, як наслідок, аварійну зупинку всіх програм.

З цього випливає, що потрібно звертати увагу на функціонування компанії в цілому і приділяти велике значення IT-інфраструктурі.

Як і було зазначено на початку розділу 4, після проведення SPOF meeting (Single point of Failure), Аналізу ризиків (BIA) та дослідження інфраструктури було визначено ризик втрати інформаційної платформи Omnitraker у разі відмови серверу, на якому вона знаходиться.

Втім, при втраті одного з компонентів сервера його потрібно буде замінювати і налаштовувати все наново, на це буде витрачено якнайменше 24 годи (доставка сервера від вендора послуг та налаштування).

Для ***оптимізації серверної частини інформаційної*** платформи з безперервності бізнес-процесів було запропоновано засовувати всесвітньовідому практику дублювання або кластеризацію серверів.

На момент проведення дослідження сервер був одноюнітовий, що ніяк не був зарезервований. Було прийнято рішення на заміну обладнання, для створення кластеру, що дозволить зменшити до 0 параметр RPO (Recovery Point Objective, RPO), оскільки відновлення данній ПЗ омнітрекер буде відбуватися з зезервної копії ПЗ, наветь при втраті однієї ноди з кластеру високої готовності.

Кластер високої готовності (далі - кластер) - це різновид кластерної системи, призначений для забезпечення безперервної роботи критично важливих додатків або служб. Застосування кластера високої готовності дозволяє запобігти як неплановим простоям, що викликаються відмови апаратури та програмного забезпечення, так і плановим простоям, необхідним для оновлення програмного забезпечення або профілактичного ремонту обладнання.

Кластеризація дозволяє реплікувати дані між системами/серверами, що дозволяє вам отримувати ці дані з основного джерела в разі локальної катастрофи.

Якщо додаток виходить із ладу на робочому сервері, копія на вторинному сервері зберігається і додаток залишається в робочому стані

Усі підсистеми кластера мають резервування, тому при відмові будь-якого елемента кластер в цілому залишиться у працездатному стані. Більше того, заміна елемента, що відмовив, можлива без зупинки кластера.

Кластер буде забезпечувати безперервність роботи серверу, навіть коли він буде потребувати заміни деяких компонентів.

Оптимізація серверної частини з заміною обладнання на HPE ProLiant BL460c Gen9

Для того, щоб впровадити цю зміну необхідно вирішити чи потрібне оновлення обладнання на більш нове та продуктивне.

CIO компанії «Процесінг» вирішив придбати новый сервер HPE ProLiant BL460c Gen8 у кількості 2шт, для розширення можливостей компанії та створення кластеру, для віртуалізації, що забезпечить безпервність систем, що будуть його використовувати.

Оскільки обраний сервер – це блейд-сервер, а значить він буде ефективний, коли буде працювати в кластері(мінімум два сервери). Для цього потрібно створити блейд ссистему.

Конструкція blade server цікава, хоч і проста. Складові реалізуються зазвичай

таким чином:

— Загальний корпус (кошик) , куди згодом вставляються сервери-леза. По суті, корпус є шасі, в який можна помістити модулі з можливістю гарячої заміни.
— Самі модулі. Вони, по суті, є звичайними серверами, але спеціальний корпус та оптимізовані деталі допомагають значно скоротити розміри модуля.
— Додаткові модулі. Це можуть бути блоки живлення, внутрішні з'єднання та інші речі.

На Рисунку 4.3 выдображено один з варыантыв використвння блейд-шасі.

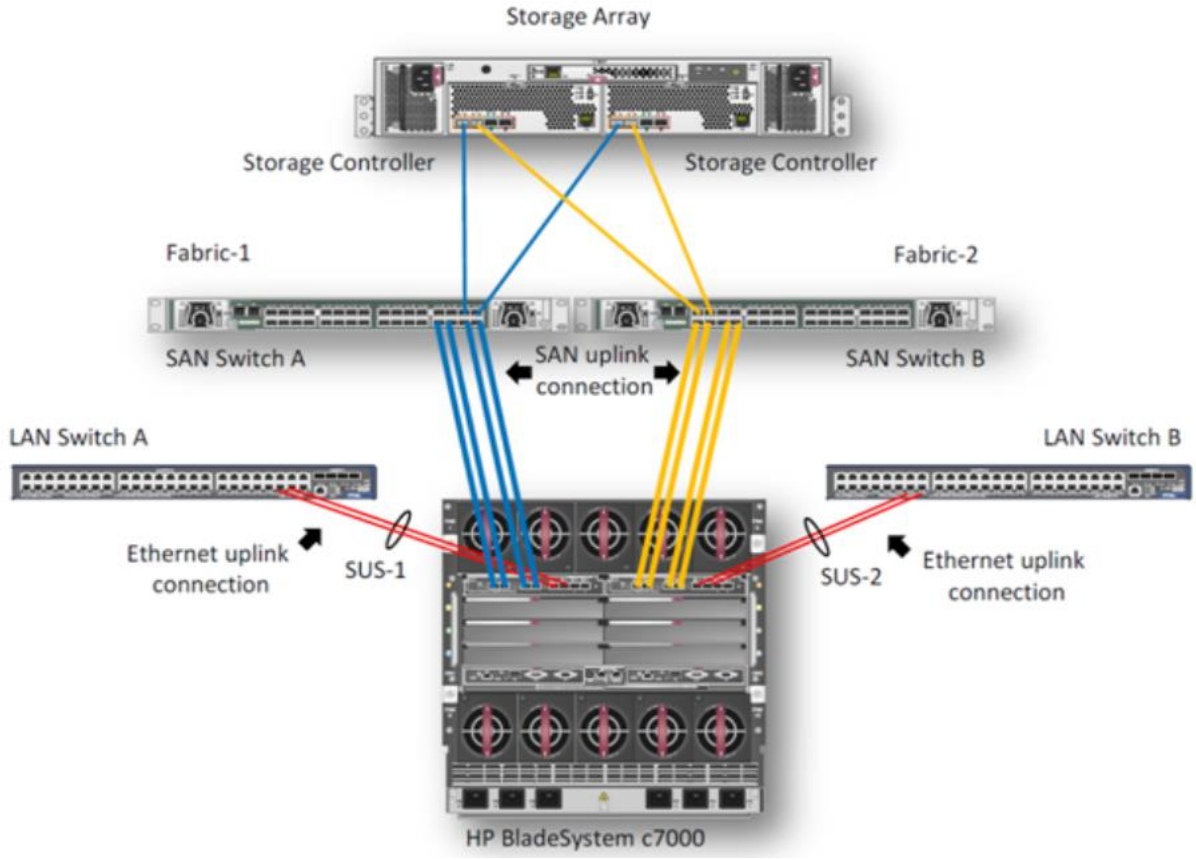


Рисунок 4.3 -Використання блейд шасі

Для цього потрібно придбати блейд-шасси HP BladeSystem c7000 Enclosure та заповнити відповідно до таблиці 4.1. Blade-шасі c7000 було вибрано через зміну стратегічних задач, оскільки планується додавання ще як мінімум 4 блейд-серверів.

Таблиця 4.1 - складові блейд системи на основі блейд-шассі HP BL c7000 Chassis

Блейд-шассі HP BL c7000 Chassis	1шт
Блейд-Сервер HP BL460c Proliant Gen8	— Процессоры: 2 x Xeon E5-2660v2 10-core (2.2 GHz, Ivy Bridge-EP, 25 Mb, 95W) — RAM: HPE 32Gb (4x8Gb) DDR3-12800 — Raid контролер: HP Smart Array P220i/512MB — Сетевой адаптер FLB: HP FLEX-10 10GB 2-PORT 530FLB — SSD – HP 300GB SAS 15k
Система зберігання HP P8100 EVA	Блок живлення 2шт.,HP24500 Жорсткий диск4 * SSD HP AG691B Вентилятор: 2шт,HP single Active Cool Fan Option Kit (499243-B21) Контроллер HDD : HP Smart Array P220i/512MB
Блок живлення cold High efficiency Redundant Hot-Plug PWS(499243-B21)	6шт
Вентилятори HP single Active Cool Fan Option Kit (499243-B21)	10шт

Корпус HP BladeSystem c7000 забезпечує ресурси живлення, охолодження та введення-виведення, необхідні для підтримки модульних серверних компонентів, перемикання та зберігання даних з поточними та майбутніми потребами. Корпус має висоту 10U і вміщує до 16 блейд-модулів для сервера та/або модулів зберігання даних, а також додаткових модулів для підключення систем зберігання даних до мережі. HP BladeSystem c7000 Enclosure також включає звичайну високошвидкісну з'єднувальну панель з продуктивністю NonStop 5 Тбіт/с з технологією одиничного підключення блейд-серверів до мережі та спільного сховища. Живлення здійснюється по одному контуру з комбінованим підключенням, а гнучка потужність блоків живлення дозволяє використовувати однофазний або трифазний змінний струм і постійний струм -48 В. При поєднанні нового модуля з HP Single Phase AC Intelligent Power Module з розподільними платами функція Intelligent Power Discovery HP Intelligent і HP Platinum автоматично розподіляє сервери для джерела живлення, перевіряє наявність резервного джерела живлення.Розрахунок

відмовостійкості при використанні кластеру

Як вже зазначалося раніше у розділі 1.1 про коефіцієнт готовності за формулою 1.1 можливо прорахувати готовність сервера. Тоді був наведений приклад розрахунку коефіцієнту готовності сервера при кластерній роботі.

Прорахуємо цей коефіцієнт для одного блейд-серверу і для кластеру, щоб було наочно зрозуміло, чому використання кластеру це більшбезпрограшний варіант.

$$К_г = \frac{t_p}{t_p + t_b} = \frac{\mathbf{MTBF}}{\mathbf{MTBF+MTTR}} \quad (1.1)$$

З формули:

MTBF (Mean Time Between Failure) – середній час напрацювання на відмову, надійність на вдмову.

MTTR (Mean Time To Repair) – середній час відновлення працездатності.

Зазвичай виробники компонентів серверів визначають MTBF шляхом тестування якоїсь кількості компонентів певний час. Тому цей параметр можна занйти в документації виробників.

Методика розрахунку MTBF передбачає, що кількість відмов у одиницю часу завжди протягом усього терміну експлуатації. Але на це впливає факт того, що відмови можуть бути різними і за графіком інтенсивності відмов[20].

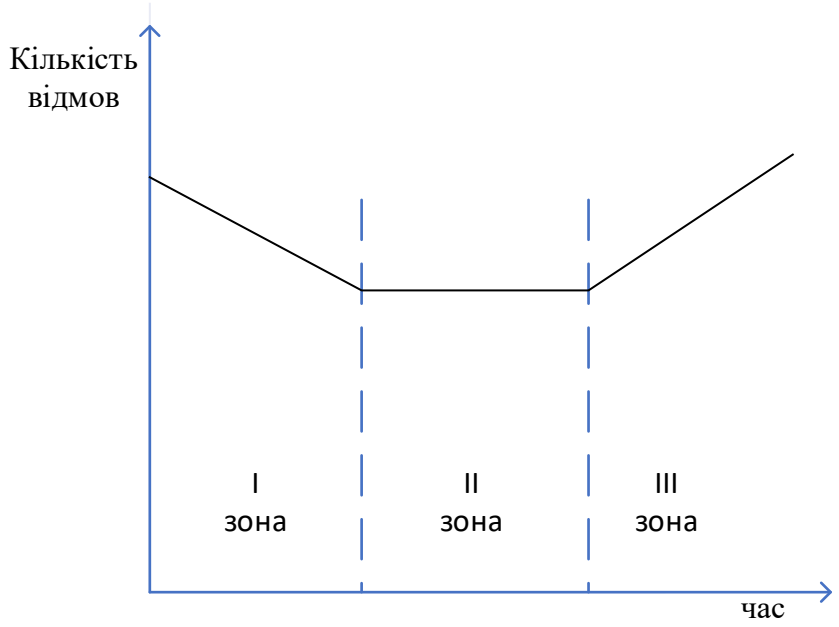


Рисунок 4.4.-графік інтенсивності відмов

I - період підробітку та відмов неякісних виробів;
II - період нормальної експлуатації, інтенсивність відмов приблизно постійна;
III - період старіння (відмови викликані зносом деталей та/або старінням матеріалів).

У зоні I виявляються відмови виробів, які мають дефекти виготовлення. У III зоні починають позначатися втомні зміни. У зоні II відмови викликаються випадковими чинниками та його число постійно в одиницю часу. Виробники компонентів, що "поширюють" цю зону на весь термін експлуатації. Реальна статистика відмов протягом всього терміну експлуатації підтверджує, що ця теоретична модель цілком близька до дійсності[19].

Перейдемо до розрахунків, оскільки вірогідність (P) виходу з ладу одного з компонентів серверу дорівнює 1 протягом усього MTBF, то вірогідність виходу з ладу компонента протягом 1 року буде дорівнювати :

$$\mathbf{P} = \frac{\mathbf{1}}{\mathbf{MTBF}} \tag{4.1}$$

P- вірогідність виходу з ладу компонента протягом 1 року.

За цією формулою визначають вірогідність виходу з ладу компонентів недубльованих.

Відмова дубльованого компонента призведе до відмови сервера лише за умови, що компонент-дублер теж вийде з ладу протягом часу, необхідного для "гарячої" заміни компонента, який відмовив першим. Якщо гарантований час заміни компонента становить 24 години (1/365 року) (що відповідає практиці обслуговування серверного обладнання, що склалася), то ймовірність такої події протягом року:

$$\mathbf{P}_{\boldsymbol{d}} = \frac{\boldsymbol{P}*\boldsymbol{P}}{\mathbf{365}} * \mathbf{2} \tag{4.2}$$

Тоді вірогідність виходу з ладу цілого серверу($\mathbf{P}_{\boldsymbol{s}}$) буде вираховуватися за такою формулою:

$$\mathbf{P}_{\boldsymbol{s}} = \mathbf{1} - \prod(\mathbf{1} - \boldsymbol{P}) \tag{4.3}$$

Оскільки відмови сервера (відмови компонентів) розподілені в часі рівномірно, то, знаючи можливість відмови сервера протягом року, можна визначити час його напрацювання на відмову (час, через який сервер вийде з ладу з ймовірністю 100%):

$$\mathbf{MTBF} = \frac{\mathbf{1}}{\mathbf{P}_{\boldsymbol{s}}} \tag{4.4}$$

Відповідно формула 1.1 буде справедливою для усього серверу.

Отож , взявши MTBF з сайту [20] можна заповнити таблицю 4.1 та зробити розрахунки при використанні одного блейд серверу HP BL460c Proliant Gen8в корзині:

Таблиця 4.1 – розрахунок вірогідностей відмови компонентів блейд-серверу

Компоненти серверу Сервер HP Proliant BL460e G8	MTBF (годин) - заявлено	MTBF (лет)	P (в-ність відмови за рік)	К-сть ел-тів в сер.	Вірогідність відмови якщо є дублювання
Блок живлення	90 000	10,27	0,09733	6	0,000156
Системна плата	300 000	34,25	0,02920	1	0,029200
Процесор №1	1 000 000	114,16	0,00876	1	0,008760
Процесор №2	1 000 000	114,16	0,00876	1	0,008760
RAM, модуль №1	1 000 000	114,16	0,00876	1	0,008760
RAM, модуль №2	1 000 000	114,16	0,00876	1	0,008760
HDD	300 000	34,25	0,02920	2	0,000005
Вентилятор №1	100 000	11,42	0,08760	4	0,000084
Вентилятор №2	100 000	11,42	0,08760	2	0,000042
Контроллер HDD	300 000	34,25	0,02920	1	0,029200
Плата сопряжения	300 000	34,25	0,02920	1	0,029200
Смужковий накопичувач	300 000	34,25	0,02920	1	0,029200
					Ps
					0,152127

Звідси :

— Імовірність відмови сервера протягом року: 0,152127;

— MTBF сервера (років): 1/ 0,152127 = 6,5737 років;

— Середній час усунення несправності (годин): 24 год (стандарт для всіх серверів)

— Коефіцієнт готовності сервера (%): (8760- годин в році)

$$К_s = \frac{\text{MTBF}}{\text{MTBF+MTTR}} = \frac{6.573*8760}{6.573*8760 +24} = 99{,}9583;$$

— Середній час простою на рік (годин): 3,65;

—

Кластер складається з двох вузлів HP BL460c Proliant Gen8в корзині та зовнішнього дискового масиву HP P8100 EVA з 4 дисками. Порушення працездатності кластера відбудеться або у разі відмови дискового масиву або у разі одночасної відмови обох вузлів протягом часу, необхідного для відновлення вузла, що першим вийшов з ладу.

Таблиця 4.1 – розрахунок вірогідностей відмови компонентів дискового масиву

Компоненти дискового масиву	MTBF (годин) - заявлено	MTBF (лет)	P (в-ність відмови за рік)	К-сть ел-тів в сер.	Вірогідність відмови якщо є дублювання
Блок живлення	90 000	10,27	0,09733	2	0,00005191
Жорсткий диск	400 000	45,66	0,02190	4	0,00000263
Вентилятор	100 000	11,42	0,08760	2	0,00004205
Контроллер	300 000	34,25	0,02920	2	0,00000467
				Р(масиву)(Pm)	0,00010126

— Імовірність відмови масиву протягом року: Pm = 0,0001013

— Імовірність відмови вузла протягом року: Ps = 0,152127

— Імовірність одночасної відмови вузлів:

$$\mathbf{P2_s = \frac{P_s * P_s}{365} * 2 = \frac{0{,}152127 * 0{,}152127}{365} * 2 = 0{,}001667};$$

— Імовірність відмови кластера протягом року:

$$\boldsymbol{P_s = 1 - (1 - P_m) * (1 - P2_s) = 0.01768};$$

— Час напрацювання на відмову кластера (років): MTBFc = $\frac{\mathbf{1}}{\mathbf{P_s}}$= 56.561;

— Час відновлення після відмови (годин): MTTR = 24;

— Коефіцієнт готовності кластера (%):

$$\mathbf{K = \frac{MTBF}{MTBF + MTTR} = \frac{56{,}561 * 8760}{56{,}561 * 8760 + 24}} = 99{,}999952:$$

— Середній час простою протягом року (секунд): T = 20.

З цих обрахунків видно що коефіцієнт кластеру 99,99995%, а коефіцієнт готовності одного з серверів 99,9583%

Отже створювати безперебійну інфраструктуру набагато вигідніше.

ВИСНОВКИ

В рамках магістерської роботи було проведено дослідження галузі BCM та інформаційної платформи, що забезпечить налаштувати та запровадити весь життєвий цикл безперервності та аварійного відновлення на підприємствах та організаціях.

В рамках магістерської роботи було вперше досліджено та проаналізовано інформаційну платформу з безперервності бізнес процесів Omnitraker у компанії «Процесінг», що використовується у роботі компанії.

На основі проведених досліджень визначено ризики, що могли повипливати на саму інформаційну платформу платформу та життя компанії, та запропоновано методи їх вирішення.

Вперше було сформульовано задачу на оптимізацію платформи Omnitraker шляхом мінімізації часу виконання закриття таких об'єктів як «інциденти» та мінімізації часу користувача в роботи з цими об'єктами, також було створено скрипти, що виконують автоматичне закриття інцидентів, що вже мають статус «Виконано» та автоматично створюють створють інциденти від телекомунікаційного сервісу і обладнання компанії «Процесінг».

В ході написання магістерської роботи було досліджено математичним методом, що кластер серверів має більший коефіцієнт готовності, ніж один сервер.

Вдале використання автоматизації програмних застосунків шляхом мінімізації часу є запорукою успішності компанії. Отримані скрипти можна використовувати при роботі з інформаційною платформою Omnitraker.

Наукова новизна роботи полягає в тому, що раніше не було досліджено інформаційну платформу Omnitraker з безперервності бізнес-процесів та не було описано способи оптимізації об'єктів платформи можна виконувати через створення автоматизації за допомогою написання алгоритмів(скриптів) мовою Visual Basic та Phyton.

У процесі виконання магістерської роботи мета була досягнута, а поставлені завдання вирішені. У роботі було проаналізовано основні джерела по обраній темі.

Визначено, що BCM — важлива складова функціонування компаній і державних організацій в аварійних ситуаціях. Специфіка конкретного бізнесу визначає пріоритети відновлення: які з сервісів або компонентів потребують негайного відновлення, а які можуть бути відновленими вже після інциденту.. Елементами управління служать дислокація, персонал, обладнання, а також процедури відновлення даних.

Задача BCM — зменшити наслідки переривання ділової активності,

скоротити час заміни активів, налагодити цілісний підхід вибудовування процесу безперервності,а також забезпечити безпервність організації після руйнівного збою за конкретний час RTO. Необхідно забезпечувати безперервність операцій, і навіть захист співробітників, клієнтів, інвесторів. Захисту потребують засоби виробництва, інфраструктура, інформація, торгова марка. Якщо передусім підходи до забезпечення безперервності були специфічними кожної області діяльності, і найчастіше кожен підрозділ займався цією проблемою незалежно від інших, сьогодні необхідний єдиний підхід до проблеми збереження стійкості бізнесу організації у цілому.Для мінімізаціїї витрат необхідно своєчасно передбачати та попереджувати сбої, шляхом проведення аналізу ризиків та впровадженням програми BCM на підприємстві.

Забезпечення безперервності бізнесу перетворюється на забезпечення його стійкості, за якої гнучка IT-інфраструктура дозволяє організації відновити роботу після будь-яких збоїв у режимі реального часу. Така інфраструктура надасть усім співробітникам, партнерам та іншим зацікавленим сторонам доступ до будь-якої інформації, необхідної для виконання важливих бізнес-операцій. У разі надзвичайної ситуації віддалений доступ, гетерогенні комунікаційні середовища, бездротові технології негайно перетворяться із засобів підтримки штатної роботи на засоби, що підтримують функціональність організації в період аварії або збою. Подібна властивість є ключовою для забезпечення нульового часу простою, а ця вимога стає все більш поширеною в сьогоднішньому швидко мінливому високо конкурентному світі бізнесу.

Аварійне відновлення в свою чергу – це частина BCM, що має на меті – відновлювати дані у випадку аварії. Максимально допустимий обсяг данних, втрачених при руйнівному збої, визначається цільовим простоєм резервної копії (Recovery Point Objective, RPO).

Процес управління безперервністю діяльності є важливим елементом належного управління діяльністю організації, надання послуг та підприємницької розважливості.

Менеджери та власники несуть відповідальність за підтримку можливості організації до безперебійного функціонування. Усі організації мають моральні та соціальні зобов'язання, особливо якщо вони забезпечують допомогу у надзвичайних ситуаціях або займаються наданням громадських чи добровільних послуг

Діяльність всіх організацій схильна до загрози виникнення нештатних ситуацій, наприклад, у разі, терористичних актів, технологічної аварії, повені, відключення електроживлення та ін.

Тому одним з рішень є використанні платформ для забезпечення безпервності бізнес та IT процесів.

Нині управління безперервністю діяльності слід розглядати не як дорогий процес планування, бо як процес, який підвищує вартість організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. IBM, “Cloud Computing Reference Architecture v2.0” [Електронний ресурс]: [Інтернет-сайт].-Режим доступу: http://www.opengroup.org/cloudcomputing/ (дата звернення 11.10.2021). – Назва з екрана.
2. Проблема 2000 року [Електронний ресурс]: [Інтернет-сайт].-Режим доступу: https://uk.wikipedia.org/wiki/проблема 2000_року (дата звернення 11.10.2021). – Назва з екрана.
3. ISO 22301 [Електронний ресурс]: [Інтернет-сайт].-Режим доступу: (https://www.iso.org/) (дата звернення 11.10.2021). – Назва з екрана.
4. ISO 22301 [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso:22301 (дата звернення 11.10.2021). – Назва з екрана.
5. ISO 22316 [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://www.iso.org/obp/ui#iso:std:iso:22316 (дата звернення 20.10.2021). – Назва з екрана.
6. Momani, N.M. 2010. Business continuity planning: are we prepared for futuredisasters. American Journal of Economics and Business Administration, 2(3):272±279
7. Gallagher, M. 2005. The road to effective business continuity management. Accountancy Ireland, 37(2):66±68
8. ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения
9. BCI, Good Practice Guidelines 2018 -115c.
10. [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://www.iso.org/standard/77008.html (дата звернення 20.10.2021). – Назва з екрана.
11. Cornell, E. and Cox, L. (2014). Improving Risk Management: From Lame Excuses to Principled Practice. Risk Analysis, 34 (7), 1228-1238
12. O’Donnell, E. (2005). Enterprise risk management: A systems-thinking framework for theevent identification phase. International Journal of Accounting Information Systems, 6 (3), 177-180
13. ITSM [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу fhttps://itsm.ucsf.edu/it-service-continuity-management
14. Процес управління IT- процесами; [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://www.itexpert.ru/rus/ITEMS/proces/(дата звернення 20.10.2021). – Назва з екрана.
15. ДСТУ, керування ризиком, методи загального оцінювання ризику [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://khoda.gov.ua/image/catalog/files/dstu%2031010.pdf (дата звернення 23.10.2021). – Назва з екрана.
16. Архітектура OMNITRACKER [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: http://www.omniway.ua/products/Omnitracker /OMNITRACKER

_architecture (дата звернення 05.11.2021). – Назва з екрана.

17. HP сервери [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://server-shop.ua/server-hp-proliant-dl-360e-g8(дата звернення 05.11.2021). – Назва з екрана.

18. Windows Server [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://www.comss.ru/page.php?id=9612 (дата звернення 05.11.2021). – Назва з екрана.

19. Кластер надійності і звичайний сервер[Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://www.team.ru/server/stbl_compare.shtml (дата звернення 10.11.2021). – Назва з екрана.

20. Крива відмов [Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://ru.wikipedia.org/wiki/Интенсивность_отказов (дата звернення 10.11.2021). – Назва з екрана.

21. Архів MTBF[Електронний ресурс]: [Інтернет-сайт]. – Режим доступу: https://www.datasheetarchive.com/hp%20server%20mtbf-datasheet.html (дата звернення 10.11.2021). – Назва з екрана.

Додаток А

Скрипт написаний мовою Visual Basic для усунення першого недоліку (Автоматичного створення інцидентів переважно від Телекомунікаційного сервісу компанії «Процесінг») з коментарями українською:

```
Option Explicit

'обявлення зміних
Dim strEmailSubject, strRefAssetNumber, strEmailText, strEmailTo, strRefAssetNumber
Dim objIncomingMsg, objRefRequest, objFolder, objFilter, objRequests, objRequest, IsIncident, item, usermail, objRefRequest1
Dim objFld ' As OtRequestFolder
Dim currentdatetime, objList, objCounter, Count, mcafee, TemplInTo, Waf
Dim blnAgree

Log("" & vbCrLf & "начало скрипта")
strEmailSubject = ""
strEmailSubject = EmailSubject
strEmailText = EmailText

LogMessage "incommingemailscr"
Set objIncomingMsg = ActiveSession.GetRequestByUniqueId(LoggedEmail.UniqueId) ' вхд лист як OtRequest
Log("000001")

If Left(strEmailSubject, 7) = "*Critical*" Then ' перевірка сабжекта листа на існування значення по якому триггериться створення інциденту
   Call CreateIncident
   CreateNewRequest = False
End If

Sub CreateIncident
    LogP("-------Старт-------")
    Dim FullText, OldV, OldVStart, NewV, NewVStart, Obj, OldVNumb, NumbOld, NumbNew, NewVNumb
    FullText = objIncomingMsg.UserFields("Body Plain Text").TValue
    'шукаємо старую и нову версію з тела листа
    NumbOld = 13
    OldV = InStrRev(FullText, "pre_version")
```

```
OldVStart = OldV + NumbOld
OldVNumb = Mid(FullText, OldVStart, 11) 'Стара версія

NumbNew = 13
NewV = InStrRev(FullText, "new_version")
NewVStart = NewV + NumbNew
NewVNumb = Mid(FullText, NewVStart, 11) 'Нова версія

LogP("Шукаємо робочу групу")
Dim objFolderWG, objFilterWG, ObjWG, wg
Set objFolderWG = ActiveSession.RequestFolders("Workgroups")
Set objFilterWG = objFolderWG.MakeFilter
objFilterWG.UserField("Name") = "Дежурные инженеры"
Set ObjWG = objFolderWG.Search(objFilterWG, True)
If ObjWG.Count = 1 Then
LogP("Рабочая группа найдена")
Set wg = ObjWG.item(0)
Else
LogP("Рабочая группа не найдена")
End If

LogP("Ищем пользователя")
Dim objFolderUsr, objFilterUsr, ObjUsr, Usr
Set objFolderUsr = ActiveSession.RequestFolders("Contacts")
Set objFilterUsr = objFolderUsr.MakeFilter
objFilterUsr.UserField("Name") = "Resp. User"
Set ObjUsr = objFolderUsr.Search(objFilterUsr, True)
If ObjUsr.Count = 1 Then
LogP("Пользователь найден")
Set Usr = ObjUsr.item(0)
Else
LogP("Пользователь не найден")
End If

LogP("Ищем департамент")
Dim objFolderDep, objFilterDep, ObjDep, Dep
Set objFolderDep = ActiveSession.RequestFolders("OrgStructure")
Set objFilterDep = objFolderDep.MakeFilter
objFilterDep.UserField("Name") = "Відділ телекомунікацій"
Set ObjDep = objFolderDep.Search(objFilterDep, True)
If ObjDep.Count = 1 Then
```

```
LogP("Департамент найден")
Set Dep = ObjDep.item(0)
Else
LogP("Департамент не найден")
End If

Dim NetRecord, objRequests, objFolder, objFilter, keyIncs, templ, OpenCheck
LogP("Ищем темплейт инцидента")
Set objFolder = ActiveSession.RequestFolders("ServiceRequestTempl")
Set objFilter = objFolder.MakeFilter
objFilter.UserField("Number") = "444"
Set objRequests = objFolder.Search(objFilter, True)
If objRequests.Count = 1 Then
LogP("Темплейт найден")
Set templ = objRequests.item(0)

End If

Dim oFolder, oFilter, oRequest, errObj
LogP("Ищем категорию ошибки")
Set oFolder = ActiveSession.RequestFolders("ErrorCategory")
Set oFilter = oFolder.MakeFilter
oFilter.UserField("Name") = "05. Telecommunications"
Set oRequest = oFolder.Search(oFilter, True)
If oRequest.Count = 1 Then

Set errObj = oRequest.item(0)
LogP("Категория ошибки найдена")

End If

Dim objFolderINC, NewInc, Inc_Email
Set objFolderINC = ActiveSession.RequestFolders("ServiceRequest")
Set NewInc = objFolderINC.Requests.Add
LogP("Запускаю создание инцидента")
NewInc.UserFields("Template").TValue = templ
NewInc.UserFields("ErrorCategory").TValue = errObj
NewInc.UserFields("AssignmentGroup").TValue = wg
NewInc.UserFields("Initiator").TValue = Usr
NewInc.UserFields("ReportingPerson").TValue = Usr
```

```
        NewInc.UserFields("Summary").TValue = "Проверка выполнения обновлений. Старая Версия: " _
        & OldVNumb & vbCrLf & " Новая версия: " & NewVNumb
        NewInc.UserFields("Description").TValue = "Прошло обновление сигнатур. Необходимо проверить по инструкции." & vbCrLf & "Старая Версия: " _
        & OldVNumb & " Новая версия: " & NewVNumb & vbCrLf & "" & vbCrLf & FullText
        NewInc.UserFields("State").TValue = "Registered"
        NewInc.UserFields("InitiatorDepartment").TValue = Dep

        NewInc.SaveEx 256 ' otSaveDoNotCheckPrivileges
        Set Inc_Email = NewInc.GenerateEmail("incident_creation")
        Inc_Email.Send 'отправка письма сервису, создавшему инцидент, с информацией по инциденту
        LogP("Инцидент создан")
        LogP("-------Завершение-------")

    End Sub
```

Додаток Б

Скрипт написаний мовою Phyton для усунення другого недоліку (Автоматичного створення інцидентів переважно від Телекомунікаційного сервісу компанії «Процесінг») з коментарями українською:

```
import win32com.client #бібліотека для роботи с COM
import pythoncom #библиітека для роботи с COM

IncNumber = argv # Передача номера інциденту системою як аргумент. Номер інциденту система отримала з листа під час його створення.
OtHost = "localhost"
OtPort = "555"
OtLogin = "login"
OtPassword = "password"
OtLang = "ua"
pythoncom.CoInitialize()
application = win32com.client.Dispatch("OtAut.OtApplication")
session = application.MakeSessionEx(OtHost, OtPort, OtLogin, OtPassword, OtLang) # створення сесії для конекту до омнітрекера
pythoncom.CoInitialize()
folder = session.RequestFolders("Incidents")
objfilter = folder.MakeFilter()
objfilter.SetSpecialField("Number", IncNumber) # пошук інцидентів
obj = folder.Search(objfilter, False)
if obj.count != 0: # якщо інцидент знайдений, тоді закриваємо його
    objIncident = obj.Item(0)
    objIncident.UserFields("Status").TValue = "Closed"
    objIncident.Save() # зберігаємо зміни
```

Додаток В. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)