МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МЕТОДИЧНІ ВКАЗІВКИ
до практичних занять з дисципліни
«УПРАВЛІННЯ ІТ-ІНФРАСТРУКТУРОЮ ПІДПРИЄМСТВА»

Частина 2

Електронне видання

Харків 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МЕТОДИЧНІ ВКАЗІВКИ
до практичних занять з дисципліни
«УПРАВЛІННЯ ІТ-ІНФРАСТРУКТУРОЮ ПІДПРИЄМСТВА»
(частина 2)
для студентів усіх форм навчання
спеціальності 122 – Комп’ютерні науки

Електронне видання

ЗАТВЕРДЖЕНО
кафедрою ІУС.
Протокол № 19 від 04.05.2018.

Харків 2019

Методичні вказівки до практичних занять з дисципліни «Управління ІТ-інфраструктурою підприємства» для студентів усіх форм навчання спеціальності 122 – «Комп’ютерні науки» (частина 2) / [Електронний ресурс] Упоряд.: В.І. Шеховцова., І.А. Малькова – Електронне видання. – Харків: ХНУРЕ, 2019. – 53 с. – pdf 2,0 Mb.

Упорядники: В.І. Шеховцова,
І.А. Малькова

Рецензент О.В. Золотухін, канд. техн. наук, доцент каф. ШІ.

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Практичні роботи з дисципліни «Управління ІТ-інфраструктурою підприємства» розраховані на шість 4-годинних занять та охоплюють усі основні теми курсу. Дані методичні вказівки є другою частиною загального курсу та призначені для організації і проведення практичних занять у другому семестрі вивчення дисципліни. Вони є логічним продовженням виконання завдань, що були завершені в попередньому семестрі.

Протягом усіх робіт студенти мають розглядати одне підприємство за обраним варіантом, поступово виконуючи завдання з методичних вказівок.

На першому кроці студенти мають ознайомитися з принципом функціонування служби технічної підтримки ІТ на підприємстві ServiceDesk, зробити порівняльний аналіз існуючої пропозиції на ринку програмних продуктів, а також розробити власний варіант сервісної служби для ІТ-інфраструктури підприємства.

Друга робота присвячена ознайомленню з системою сертифікації стандарту ISO/IES 20000; студенти мають навчитись складати Угоду про рівень послуг (SLA) відповідно до проекту ІТ-інфраструктури підприємства.

У третій роботі обґрунтовується правомірність розробленої організації управління ІТ-інфраструктурою на підприємстві. Особлива увага приділяється методології CobiT, яка дозволяє проводити власний аудит якості моделі управління ІТ-інфраструктури підприємства.

Методичні вказівки мають перелік посилань на літературні та електронні джерела, де студенти зможуть знайти додаткову та розширену інформацію за всіма темами дисципліни.

1 ФУНЦІЯ SERVICEDESK – ТЕХНІЧНА ПІДТРИМКА IT-ІНФРАСТРУКТУРИ

1.1 Мета заняття

Ознайомитись з принципом функціонування служби технічної підтримки IT на підприємстві ServiceDesk, зробити порівняльний аналіз існуючої пропозиції на ринку програмних продуктів, а також розробити власний варіант сервісної служби для IT-інфраструктури підприємства.

1.2 Методичні вказівки з організації самостійної роботи студентів

1.2.1 Мета і принцип роботи служби ServiceDesk

Головне призначення Incidentmanagement – максимально швидка ліквідація проблем в IT-інфраструктурі: аварій, проблем з обладнанням тощо. Для цього утворюється спеціальна служба ServiceDesk у вигляді центру обслуговування користувачів, або HelpDesk – центру підтримки користувачів (рис. 1.1).

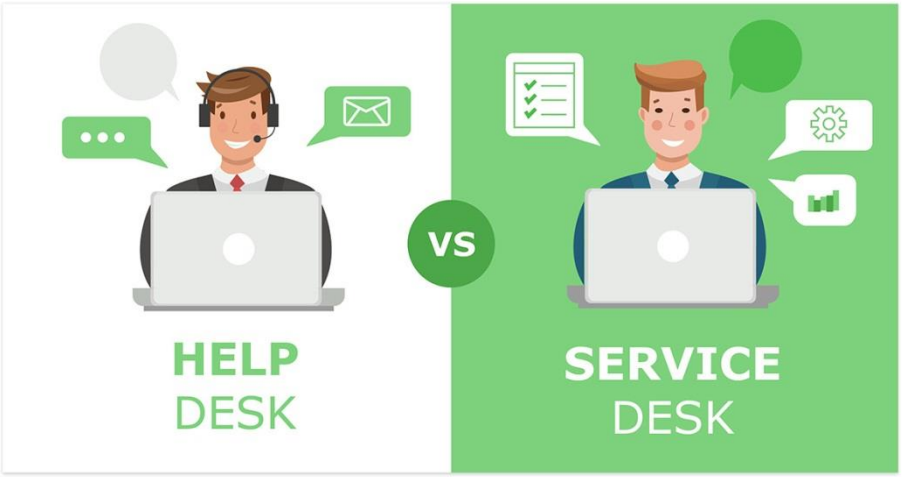

Рисунок 1.1 – Принцип організації служби ServiceDesk

Бібліотеки ITIL розглядають IT-підрозділ як постачальника визначеного списку послуг, що спрямовані на підтримку бізнес-процесів. Відповідно, рівень якості обслуговування закріплюється між виробником послуг служб ServiceDesk та їх споживачем через документ SLA (ServiceLevelAgreement). Наприклад, у ньому визначається допустимий максимальний період бездіяльності під час аварій.

Задачею ServiceDesk є реєстрація замовлень користувачів, надання їм потрібної допомоги та залучення співробітників IT-підрозділу для найшвидшого усунення проблем. Додатково така служба аналізує статистику інцидентів, спосіб та час їх усунення. Це необхідно для підвищення якості надання IT-послуг.

HelpDesk – вужче поняття, це інструмент технічної підтримки користувачів.

Процеси ServiceDesk регламентують усі ускладнення, що виникають в роботі IT-підрозділу:

Incident Management – процес, що відповідає за швидке розв'язання інцидентів – неполадок, пошкоджень, критичних помилок, що потребують відповідних дій. ServiceDesk реєструє статистику інцидентів і час їх ліквідації.

Problem Management – мета цього процесу полягає у зменшенні кількості інцидентів, що надходять у ServiceDesk. Для цього виявляються та усуваються їх причини.

Change Management – процес, що регламентує тільки осмислені зміни і узгодження їх реалізації серед усіх користувачів бізнес-сервісів.

Release Management – процес, що ставить умову не порушувати роботу компанії під час виконання будь-яких змін. Процес управління релізами виконує нагляд і встановлення оновлених версій програм та апаратних засобів через службу ServiceDesk.

ServiceLevel Management – процес, що визначає кількість і склад задіяних співробітників, а також якість послуг у службі ServiceDesk. За його допомогою йде моніторинг рівня якості та проводяться операції для зниження ймовірності того, що може бути наданий недоброякісний сервіс.

Financial Management – процес, який описує розпорядження фінансами для забезпечення діяльності інших процесів.

Availability Management – задачі, що належать до доступності послуг IT-підрозділу; виділяються ізольовані процеси, для того щоб їх можна було відслідковувати та робити висновки. Рівень доступності визначається стабільністю, ремонтоспроможністю та надійністю.

Capacity Management – задача, що відповідає за управління IT-активами.

Continuity Management – контроль безперервності IT-сервісів. Головні напрямки задачі – розробка, супровід, реалізація та перевірка дій із забезпечення безперервності діяльності бізнес-сервісів.

InformationSecurity Management – гарантія безперервної безпеки сервісу та інформаційна надійність.

Впровадження ServiceDeskiHelpDesk вигідно для власників бізнесу, менеджерів компанії, IT-підрозділу та кінцевих користувачів, оскільки усувають сповільнену реакцію IT-служби на запити. Особливо помітно це для організацій з територіально розкинутими офісами. Як наслідок – покращення безпеки IT-інфраструктури підприємства, зменшення витрат і можливість їх прогнозування.

Для користувачів впровадження ServiceDesk та HelpDesk характеризується зростанням рівня сервісу, що надається, та зменшенням періодів зупинки через проблеми в IT-інфраструктурі.

Для самих IT-служб це дає можливість обґрунтувати потреби на витрати, пов’язані з розвитком, покращенням та ремонтом IT-інфраструктури, планувати бюджет і роботи, формувати актуальні й достовірні звіти, розширяти доступність своїх послуг для користувачів.

Окрім того, впровадження ServiceDesk та HelpDesk дозволяє формувати певні вимоги до співробітників IT-підрозділів та розвивати у них необхідні навички. Нижче в таблиці наводиться статистика асоціації HDI за результатами звіту «2015 SupportCenterPractices&SalaryReport» (рис. 1.2).

	ПОДДЕРЖКА УРОВНЯ 1	ПОДДЕРЖКА УРОВНЯ 2	РУКОВОДИТЕЛЬ КОМАНДЫ ПОДДЕРЖКИ	МЕНЕДЖЕР СЕРВИС-ЦЕНТРА
Навыки обслуживания клиентов	72%	53%	42%	33%
Лидерские навыки	11%	21%	58%	63%
Управление персоналом (наставничество, управление продуктивностью и т. д.)	12%	15%	49%	61%
Управление проектами	8%	20%	30%	44%
Личный менеджмент (управление стрессом, временем и т. д.)	40%	39%	41%	42%
Навыки оказания услуг	28%	28%	36%	39%
Работа в команде	49%	45%	44%	41%
Знание технологий, используемых заказчиком	59%	59%	45%	36%
Знание технологий для оказания услуг	64%	61%	48%	38%
Разрешение проблем	58%	51%	40%	28%
Другие	8%	8%	9%	11%
Нет формальных тренингов	13%	14%	17%	13%

Рисунок 1.2 – Статистика асоціації HDI
(джерело: https://freshservice.com/it-trends/service-desk-skills-2017-blog/)

Вони ж запропонували 10 найважливіших навичок для співробітників ServiceDesk, які необхідно враховувати під час прийняття на роботу:

- вміння ставити питання;
- комунікабельність;
- спроможність швидко навчатися;
- навички діагностики та вирішення проблем;

- спроможність працювати у стресових умовах;
- адаптивність;
- навички роботи в команді;
- навички міжособистісного спілкування;
- досвід роботи у підтримці користувачів;
- чесність.

Таким чином, використання ServiceDesk дозволяє провести атестацію якості усього IT-департаменту.

Застосування ServiceDesk дозволяє зрозуміти, скільки звернень надходить до служби підтримки, як часто виходить з ладу техніка чи «завісає» програмне забезпечення, наскільки якісно надаються IT-послуги. Відповідно, заявки користувачів швидко надходять в обробку, керівництво має змогу контролювати роботу менеджерів, якість їх обслуговування та ефективність роботи IT-відділу. На основі цієї інформації можна робити висновки щодо слабких місць компанії, планувати розвиток IT-інфраструктури та навчати фахівців.

1.1.2 Розробка служби ServiceDesk для підприємства

ServiceDesk – спеціалізована функціональна одиниця, орієнтована на обробку специфічних сервісних подій, що надходять у формі звернень користувачів або повідомлень систем моніторингу.

Завдання ServiceDesk:

- Забезпечити єдину точку контакту між постачальником і замовником (SPOC – SinglePointOfContact).
- Підвищити доступність послуг і самої точки контакту для кінцевих користувачів.
- Підвищити якість і кількість вирішуваних запитів.
- Підвищити задоволеність і поліпшити сприйняття користувачів.
- Поліпшити комунікації та взаємодії.
- Надавати первинну інформацію про потреби бізнесу.
- Сприяти процесам управління IT-інфраструктурою.

Головне завдання (PrimaryAim) ServiceDesk: якнайшвидше відновлення нормального рівня сервісу, якщо він порушений.

Основні процедури ServiceDesk:

- Ідентифікація звернень – з чітким дотриманням робочих інструкцій!

- Обов’язкова реєстрація усіх запитів та інцидентів, включаючи короткі консультації і помилкові дзвінки.
- Принцип: спочатку реєструємо – потім вирішуємо !
- Класифікація звернення – пошук вирішення для якнайшвидшого відновлення нормальної роботи сервісів.
- Надання початкової підтримки.
- Розв’язання інцидентів.
- Моніторинг та ескалації.
- Забезпечення поінформованості користувачів – повідомлення користувачів, включаючи маркетингові акції.
- Закриття інцидентів (після підтвердження замовника!).

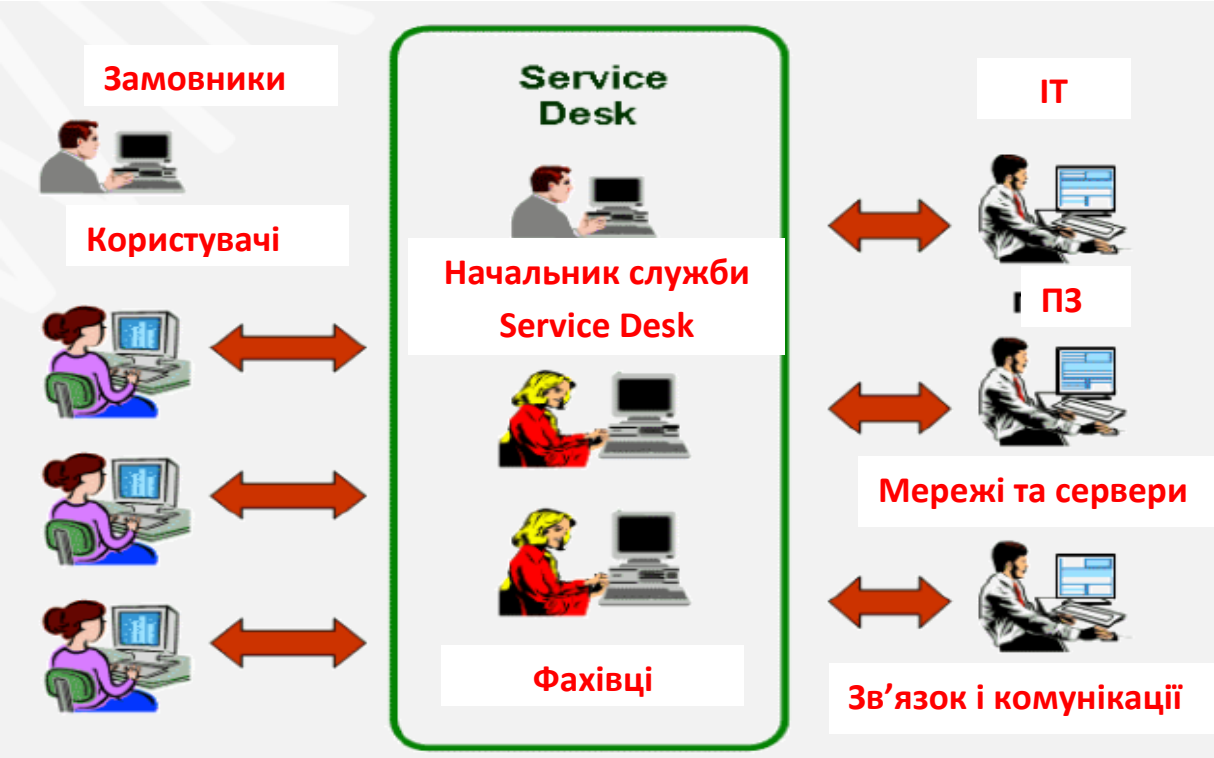

Рисунок 1.3 – Організація роботи служби ServiceDesk

Особливості побудови (впровадження) ServiceDesk:

- Необхідність підтримки керівництва.
- Необхідність чіткого фіксування бюджету.
- Організація робочого місця:
  - Достатня кількість природного освітлення і достатній обсяг внутрішнього простору.
  - Адекватний контроль рівня шуму.
  - Приємна робоча обстановка.

    - Окреме місце відпочинку.
    - Окреме від IT-служб иприміщення.
- Персонал:
    - Підготовка персоналу.
    - Забезпечення обладнанням та засобами комунікацій (добрий комп'ютер, телефон з гарнітурою, виділений інтернет тощо).
    - Автоматизація: запис розмов, запис викликів, розпізнавання номера тощо.
    - Призначення керівника СД або ролі.
    - Забезпечення дублювання операторів.
    - Навчання і тренінги співробітників (тренінги регулярно повторювати).
    - Розробка програми підготовки нових співробітників.
    - Розробка робочих інструкцій
    - Мотивація і управління «плинністю».

Очікувані труднощі за недостатньої підготовки до впровадження:

- Протидія користувачів.
- Спроби обходу процедур, прихований або явний саботаж.
- Протидія співробітників.
- Протидія керівництва.
- Відсутність підтримки і ресурсів.

Рекомендовані Метрики ServiceDesk (KPI):

- Ключовий показник – рівень задоволеності користувачів !!!
- Доступність у черзі (швидкість реакції).
- Кількість інцидентів на 1 співробітника СД .
- Кількість інцидентів, вирішених на 1 лінії.
- Середня тривалість вирішення (за приорітетами).
- Середній час ескалації інциденту.
- Середній час закриття вирішеного інциденту.
- Загальна кількість дзвінків (за часом доби і днями тижня).
- Відсоток звернень, вирішених у рамках (за рамками) SLA.
- Кількість нових сервісів та інтерфейсів – реклама, має використовуватися регулярно і показово!!! Девіз SD: новий сервіс – щотижня!!!
- Опитування споживачів на предмет їх задоволеності (Customer Satisfaction Survey). Опитування як різновид реклами. Дуже ефективні веб-інтерфейси, книги скарг тощо. Парадоксально, але скарги можуть

підвищувати задоволеність!!! При правильній роботі з ними і грамотному наданні результатів замовнику!

Вибір структури служби ServiceDesk здійснюється за результатами атестації співробітників (рис. 1.4).

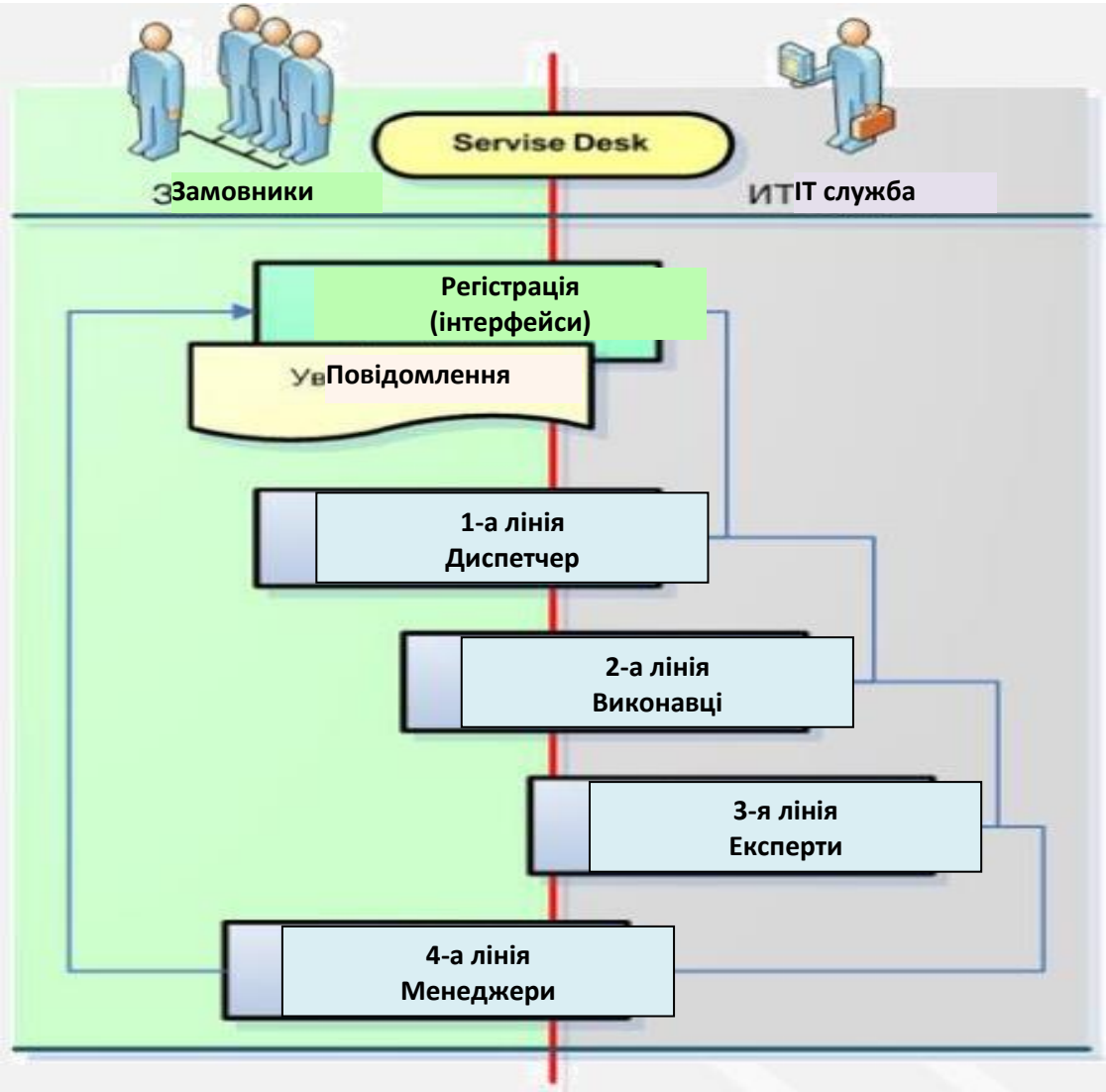

Рисунок 1.4 – Структура служби ServiceDesk за рівнем експертизи

Відповідно за рівнем експертизи виділяють 4 лінії кваліфікації фахівців:

- Загальної кваліфікації (1 лінія).
- Частково кваліфікований (2 лінія).
- Кваліфікований (3 лінія).
- Експерт (4 лінія).

1.2.3 Класифікація служби ServiceDesk за структурою

1. Локальний ServiceDesk: розміщується на одному об’єкті, разом з користувачами (рис. 1.5).

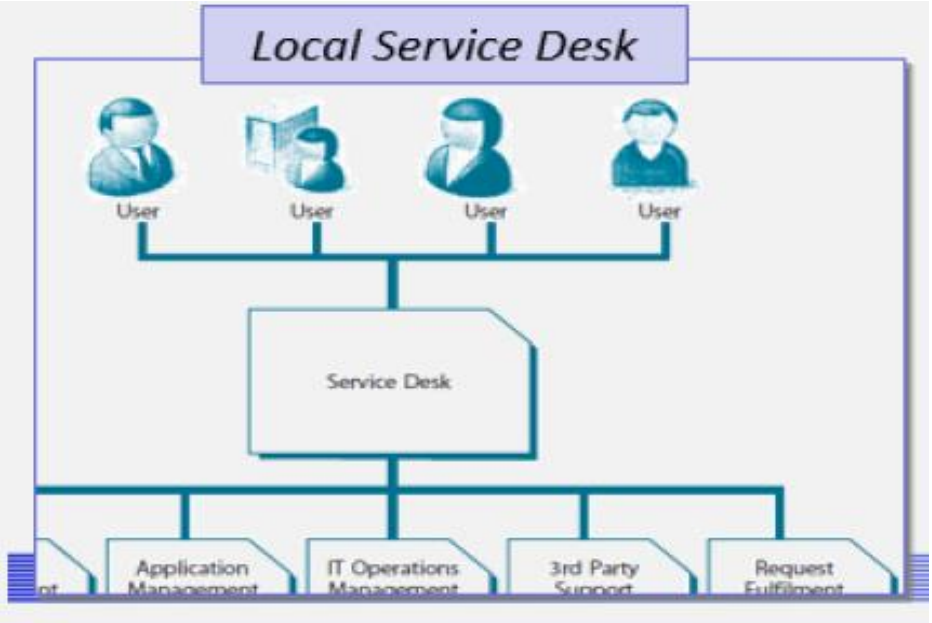

Рисунок 1.5 – Локальний ServiceDesk

Централізований ServiceDesk: єдина точка контакту для декількох, розподілених майданчиків з розділеними функціями за напрямками і нерідко – суміщений з першими лініями підтримки (рис. 1.6).

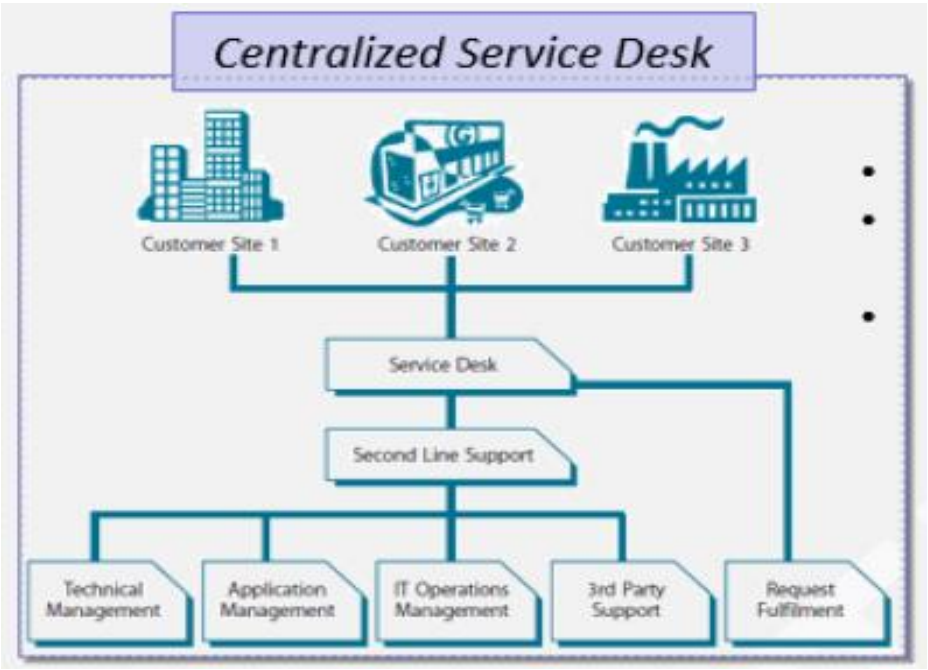

Рисунок 1.6 – Централізований ServiceDesk

2. Віртуальний ServiceDesk: кілька локальних служб, що об’єднані єдиною віртуальною системою (рис. 1.7).

Запис про інцидент має включати (ідентифікація):

- Унікальний ідентифікатор інциденту.

- Категорію інциденту.
- Терміновість інциденту. Терміновість (urgency) – міра того, наскільки швидко з моменту своєї появи інцидент, проблема або зміна набуде істотного впливу на бізнес.

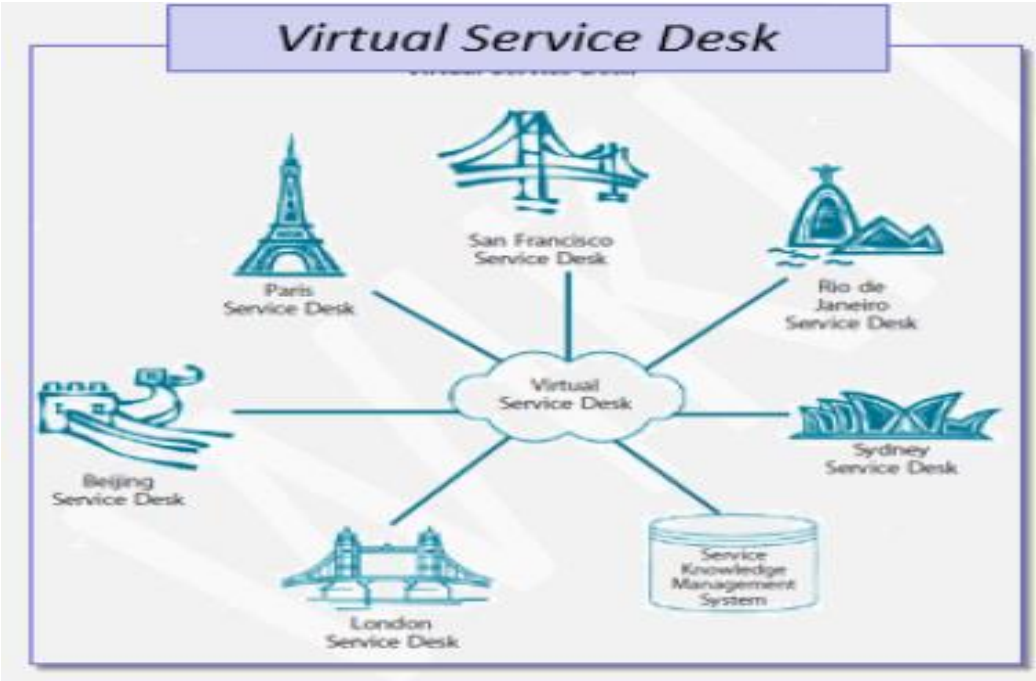

Рисунок 1.7 – Віртуальний ServiceDesk

Наприклад, інцидент з високим рівнем впливу може мати низьку терміновість до тих пір, поки цей вплив не зачіпає бізнес у період закриття фінансового року.

Вплив і терміновість використовуються для призначення пріоритету:

- Вплив інциденту.
- Пріоритет інциденту.
- Дата і час запису.
- Ім’я / id людини або групи, яка зробила запис про інцидент.
- Метод повідомлення.
- Ім’я / відділ / номер / розташування користувача.
- Метод зворотного зв’язку.
- Опис симптомів.
- Статус інциденту.
- Пов’язані конфігураційні одиниці.
- Група підтримки / співробітник, до кого переадресовано інцидент.
- Пов’язана з інцидентом проблема / відома помилка.
- Діяльності, здійснені для вирішення інциденту.

- Час і дата дозволу інциденту.
- Категорія закриття.
- Час і дата закриття.

Приклад матриць для визначення пріоритету інциденту і часу, протягом якого його необхідно розв’язати, наведено на рисунку 1.8.

Код приоритета определяют влияние и срочность	Влияние		
	Высокое	Среднее	Низкое
Высокая	1	2	3
Средняя	2	3	4
Низкая	3	4	5

Код приоритета	Описание	Крайний срок исполнения
1	Критический	1 час
2	Высокий	8 часов
3	Средний	24 часа
4	Низкий	48 часов
5	Планируемый	В соответствии с планом

Рисунок 1.8 – Матриці для визначення пріоритету інциденту і часу (Скріншот роботи програми)

Етап початкової діагностики в ServiceDesk:

- Якщо ServiceDesk не може розв’язати інцидент або терміни першого ступеня розв’язання інцидентів закінчився, інцидент має бути негайно переданий далі.
- Ескалація (Escalation) – діяльність, спрямована на отримання додаткових ресурсів, коли це необхідно для досягнення цільових показників рівня послуги або очікувань замовників:
- Функціональна ескалація – передбачає передачу інциденту в групу підтримки з більш високою кваліфікацією і компетенцією. Відповідальність за повідомлення користувача про хід вирішення інциденту залишається на ServiceDesk, незалежно від того, де інцидент розглядається на даний момент.
- Ієрархічна ескалація – передбачає залучення або просто інформування керівників вищого рівня про виникнення інциденту. Вона сприяє своєчасному прийняттю рішень щодо виділення додаткових ресурсів і залучення зовнішніх організацій у процес розв’язання інциденту.

Етап розв’язання інцидентів – дослідження і діагностика:

- Встановлення того, що саме не працює або що саме шукає користувач;
- Визначення хронології подій;
- Оцінка впливу інциденту, в тому числі кількості користувачів, яких він торкнувся;
- Пошук у базі знань аналогічних випадків в минулому.

Закриття інциденту:

- Закриття категорування – проводиться перевірка коректності спочатку встановленої категорії інциденту. Якщо вона виявилася неправильною, її виправлення та занесення змін до запису про інцидент;
- Опитування задоволеності користувачів – здійснюється за дзвінком або електронною поштою для статистики і відображення ефективності роботи ServiceDesk;
- Перевірка повноти запису про інцидент;
- Визначення того, яка проблема викликала інцидент, є вона постійною або періодично повторюється. Сюди належить також визначення проактивних дій щодо запобігання інцидентів цього типу в подальшому і формування запису про проблему, якщо вона нова;
- Формальне закриття інциденту – формальне закриття запису про інцидент.

Метрики ефективності процесу Управління інцидентами:

- Загальна кількість жертв інцидентів;
- Кількість інцидентів, які перебувають на різних стадіях – закритий, у роботі, переданий тощо.
- Розмір поточного логу про інциденти;
- Кількість значних інцидентів;
- Середній час вирішення інцидентів;
- Відсоток інцидентів, розв’язаних в узгоджений час вирішення інцидентів;
- Середні витрати на інцидент;
- Кількість повторно відкритих інцидентів та їх процентне співвідношення до загальної кількості інцидентів;
- Кількість інцидентів, неправильно призначених у команди підтримки;
- Кількість інцидентів, для яких були неправильно визначені категорії;
- Кількість віддалено розв’язаних інцидентів (без персональної присутності);
- Кількість інцидентів, розв’язаних з використанням кожної моделі інцидентів;
- Кількість інцидентів у розрізі певних періодів дня.

Для ефективного управління інцидентами необхідно забезпечити:

• Спроможність виявляти інциденти якомога раніше. Це включає в себе навчання користувачів невідкладно повідомляти про інциденти та конфігурування інструментів управління подіями;

• Переконати персонал у тому, що всі інциденти мають бути занесені у журнал;

• Доступність інформації про відомі проблеми і помилки. Це дозволить персоналу застосовувати досвід попередніх інцидентів;

• Взаємодія з CMS для визначення взаємозв'язків конфігураційних одиниць та звернення до їх історії для підтримки першого рівня;

• Взаємодія з SLM для коректної оцінки інцидентів, визначення приорітетів та виконання процедур ескалації. SLM може використовувати інформацію про управління інцидентами для визначення того, що цільові рівні продуктивності реалістичні та можуть бути досягнуті.

Основні ризики для процесу Управління інцидентами:

• Велика кількість інцидентів, які не можуть бути розв'язані у встановлені терміни в зв'язку з браком ресурсів або їх недостатньою підготовкою;

• Призупинення розв'язання інцидентів через некоректну роботу підтримуючих інструментів;

• Недостатність або несвоєчасність інформації через некоректну роботу підтримуючих інструментів або поганий взаємозв'язок з іншими процесами;

• Невідповідності з основними контрактами та угодами, які виникають внаслідок їх поганого опрацювання і не-реалістичності узгоджених цільових показників.

1.3 Зміст звіту

Звіт має містити:

1. Титульний аркуш із зазначенням теми роботи.
2. Мету і завдання на виконання з прив'язкою до варіанта IT-інфраструктури конкретного підприємства за власним варіантом.
3. Алгоритм реалізації функції ServiceDesk.
4. Схема бази даних замовлень та їх вирішення службою ServiceDesk.
5. Журнал обліку замовлень та їх вирішення службою ServiceDesk.
6. Висновки про виконану роботу.

1.4 Контрольні запитання і завдання

1.4.1 Контрольні запитання

1. Який принцип роботи служби ServiceDesk?
2. Наведіть основні процедури ServiceDesk
3. Яка класифікація структур служби ServiceDesk?
4. Які Ви знаєте етапи обробки замовлень службою ServiceDesk?
5. Які обов’язкові елементи запису журналу обліку ServiceDesk?

1.4.2 Контрольні завдання

До розробленої на попередніх (Частина 1, № 1–3) практичних роботах IT-інфраструктури підприємства створити власний варіант служби ServiceDesk.

ServiceDesk має містити журнал обліку замовлень з послідовністю проходу всіх етапів їх обробки. Для наочності технології обробки заявок розробити алгоритм реалізації функції ServiceDesk.

Перевірити дієздатність розробленого продукту на декількох прикладах замовлень.

2 СТРУКТУРА, ПРАКТИЧНЕ ЗАСТОСУВАННЯ Й СИСТЕМА СЕРТИФІКАЦІЇ (СТАНДАРТ ISO/IES 20000). РОЗРОБКА SLA

2.1 Мета заняття

Ознайомитись із системою сертифікації стандарту ISO/IES 20000; навчитись складати Угоду про рівень послуг (SLA) відповідно до проекту IT-інфраструктури підприємства.

2.2 Методичні вказівки з організації самостійної роботи студентів

2.2.1 Система сертифікації згідно зі стандартом ISO/IES 20000. Інформація про ключові компанії

EXIN – Examination Institute for Information Science, це незалежна некомерційна організація, яка розробляє та ухвалює сертифікаційні іспити у сфері інформаційних технологій. Незалежна перевірка та сертифікація сприяють підвищенню якості підготовки менеджерів, фахівців і користувачів, що працюють із IT.

Іспити EXIN щодня ухвалюються в більш ніж 125 країнах світу на 15 мовах. З початку 1990-х EXIN сертифікував понад 1 мільйон людей.

Керування IT-послугами займає особливе місце в портфелі сертифікації, пропонованому EXIN. EXIN – найбільший провайдер сертифікації ITIL у світі. Крім сертифікації фахівців, EXIN також акредитує навчальні центри, що працюють в області керування IT, і курси, які готують фахівців до сертифікації.

Додаткова інформація – **www.exin-exams.com**

Компанія **Cleverics** спеціалізується на наданні консультаційних послуг і проведенні курсів і тренінгів у сфері керування IT, насамперед – на основі підходу ITSM.

Статуси **Accredited Training Provider** і **Accredited Courseware Provider** дають компанії право проводити курси, спрямовані на підготовку слухачів до відповідних іспитів, а також надавати розроблені курси для використання іншими навчальними центрами.

Статус **Accredited Examination Center** дозволяє ухвалювати будь-які іспити EXIN.

З проходженням пробного іспиту на отримання сертифіката в галузі управління IT-послугами за стандартом ISO 20000 (за інформацією, що

стосується іспиту звертатися до викладача) необхідно відповісти на запитання, та самостійно оцінити рівень реальних вимог для отримання сертифікації Foundation і свою готовність до здачі відповідного іспиту.

2.2.2 Структура і зміст Угоди про рівень послуг (SLA – Service Level Agreement)

Угода про рівень обслуговування (англ. Service Level Agreement **SLA**) – термін методології ITIL, що означає формальний договір між замовником послуги та її постачальником, та містить опис послуги, права й обов'язки сторін щодо узгодженого рівня якості надання даної послуги. Процес SLA описаний у книзі «ITIL – Проектування послуг (ServiceDesign)».

SLA – це міні-договір, який встановлює параметри якості надаваних бізнесу IT-послуг.

У SLA описуються умови надання послуг (сервісів), встановлюється перелік таких послуг, а також правила, за якими замовник користуватиметься цими сервісами. Водночас SLA – один з основних механізмів, що дозволяє керувати якістю IT-послуг і управляти очікуваннями користувачів.

Складові SLA:

1. Опис сервісів або послуг, що надаються згідно з даною SLA (певна частина каталогу сервісів, що надаються IT-службою).

2. Опис умов надання послуг, зокрема і порядок роботи з замовленням щодо надання конкретних сервісів.

3. Параметри якості послуг, які можна вимірювати. Вони мають співвідноситися з бізнес-цілями організації та бути відображенням потреб бізнес-користувачів, у тому числі в способах надання їм IT-послуг. Такими параметрами якості можуть бути час усунення інцидентів, час, протягом якого сервіс має бути відновленим, тощо. Так, наприклад, створення e-mail для нового співробітника має займати у IT-служби не більше 4 годин.

Отже, для IT-підрозділу SLA – це набір параметрів ключових IT-процесів, а дотримання SLA – основний показник ефективності (KPI) IT-відділу.

Метою будь-якої SLA є закріплення правил гри з визначеною категорією бізнес-користувачів, за якими IT-служба з ними співпрацюватиме. При цьому важливо розуміти, що SLA – це не внутрішній документ IT, а договір, який складається спільно з представниками бізнесу, та про який проінформовано всіх користувачів.

Типова угода про рівень послуг (SLA) має містити такі розділи:

- Контактні дані сторін, що залучені до угоди та термін її дії;
- Опис послуги;
- Технічну інформацію про послугу;
- Абонентське обладнання, що підтримує оператор;
- Рівень і якість обслуговування;
- Засоби моніторингу та звіти SLA;
- Центр технічної підтримки;
- Механізм резервування та відновлення послуги;
- Порушення обслуговування і компенсації;
- Тарифи та виставлення рахунків;
- Процес поліпшення SLA;
- Порядок припинення надання послуг.

Під час розробки угоди про рівень послуг необхідно визначити:

- Перелік ключових показників: типова SLA має містити технологічні (KPI) та організаційні (KQI) показники послуги. Кожен показник повинен однозначно трактуватися і мати узгоджену формулу для його розрахунку.
- Цільові значення показників: для кожного показника має бути визначено цільове значення, виходячи з потреб бізнесу, надання інформаційних і телекомунікаційних послуг. Наприклад, цільові значення послуги VPN визначаються, виходячи з вимог верхніх сервісів. Під час використання додаткових засобів шифрування каналів дана задача стає не тривіальною й потребує лабораторних досліджень з застосуванням спеціалізованих засобів або визначення даних показників емпіричним шляхом (методом «тику»).
- Засоби контролю та звітності: для кожного показника має бути визначена методика вимірювання та засоби контролю його значень. Узгодження інструменту моніторингу показників якості є важливим моментом у ході підготовки угоди про рівень надаваних послуг. Звіти SLA мають формуватися в автоматичному режимі сертифікованими засобами.
- Компенсації та знижки: компенсація за неналежне виконання SLA є не самоціллю для клієнта. Даний момент стає засобом управління взаємовідносинами з постачальником. Клієнт має бути впевненим, що оператор зробить усе можливе для досягнення цільових значень показників якості надаваних послуг. При цьому клієнт має бути готовим заплатити за «страховку», щоб з настанням «страхового випадку» отримати компенсацію.

Насправді, SLA – це предмет перемовин. Тут багато параметрів, які можна змінювати. А ціна конкретної угоди може значно відрізнятися залежно від взятих забов'язань постачальника. Тому залучення експертів галузі та кваліфікованих юристів для складання SLA дозволить компанії уникнути помилок та бути впевненою у вірності прийняття рішення під час вибору постачальника послуг.

2.2.3 Типові помилки під час складання SLA

а) Нечітко визначена зона відповідальності.

В угодах постачальники нерідко намагаються перекласти ризики взаємодії зі своїми партнерами на клієнтів чи розпливчасто визначають зону своєї відповідальності. Необхідно чітко визначати точку демаркації і способи контролю показників у цій точці.

Приклад з угоди:

Значення параметрів якості (процент втрачених пакетів, середня мережна затримка) приведені тільки для IP-пакетів, що передаються між магістральними маршрутизаторами власної мережі Оператора (без урахування міжнародних вузлів доступу).

Правильний варіант:

Значення параметрів якості (процент втрачених пакетів, середня мережна затримка) приведені тільки для IP-пакетів, що передаються між вимірювальними зондами (посилання на сторінку з зондами), які підключені до маршрутизаторів Клієнта, не залежно від маршруту проходження трафіка, застосованої технології передачі та мережі третіх сторін.

б) Доступність або готовність.

З питання Availability і Accessibility написано багато. В будь-якому варіанті в угоді необхідно вказувати час, протягом якого послуга не придатна до використання або може бути використана з обмеженнями. При цьому необхідно явно вказувати критерії неготовності послуги.

Приклад із угоди:

Готовність послуги за місяць 99.7%.

Правильний варіант:

Готовність послуги 99.7%. Сумарний час відмови послуги не перевищує 129 хвилин на місяць (26 годин 15 хвилин в рік).

в) Не вказується період усереднення параметрів.

Середні значення показників якості послуги є розрахункові величини. Якщо в SLA не прописаний інтервал усереднення, то за замовчуванням постачальник послуги говорить про середнє значення за звітний період. Замовник очікує, що дані середні значення будуть дотримані за будь-який період вимірювань.

Приклад із угоди наведено в табл. 2.1.

Таблиця 2.1 – Приклад із угоди

Доступність мережі за місяць	Процент втрачених пакетів за місяць	Середня мережна затримка на наземних каналах за місяць
Не менше 99,7%	Не більше 1%	Не більше 200 мсек

Правильний варіант:

Середня мережна затримка пакетів на інтервалі 5 хвилин.

г) Використання усереднених значень метрик.

Насправді середні значення метрик не такі важливі. Найбільший інтерес викликає процент часу, протягом якого значення показників не перевищує заданих порогових значень.

Інтервал часу, за який значення показників не відповідали нормі, називається деградацією якості. Як правило, деградація якості враховується в сумарному часі неготовності послуги з коефіцієнтом 0.5 (Degradation Factor).

д) Розмите визначення готовності послуги.

Готовність (Availability) – це ключовий показник якості послуги, на основі якого визначається розмір штрафних санкцій за неналежне надання послуг. Чим чіткіше буде прописано у SLA визначення Готовності послуги, тим вище шанси на отримання знижки у випадку проблем з боку оператора.

Приклад з угоди:

Доступність мережі – відношення часу знаходження компонентів Магістральної мережі Оператора в робочому стані до загальної тривалості інтервалу нагляду (доступність за добу, тиждень, місяць).

Послуга вважається недоступною, якщо вона вийшла з ладу у зв’язку з несправністю. Під несправністю розуміється стан Послуги, коли вона не готова до експлуатації.

Правильний варіант:

Готовність послуги обраховується за формулою:

Готовність послуги %= 100% – Неготовність послуги%.

Неготовність послуги розраховується за формулою:

Неготовність послуги %= Сума інтервалів неготовності / Тривалість звітного періоду * 100%.

Послуга вважається неготовою, якщо коефіцієнт втрати пакетів більше 10% на інтервалі 15 або більше хвилин. Періоди неготовності менше 15 хвилин не враховуються.

е) Методи контролю показників.

В угоді не прописуються методи контролю вказаних показників якості. Для більшості показників якості мають бути передбачені методи неперервного контролю показників з можливістю перегляду.

Окрім зазначення в угоді показників якості та методики їх розрахунку, необхідно вказувати засоби для здійснення.

ж) Розмір знижки за порушення SLA.

Типова угода SLA провідних гравців послуг VPN пропонує оператору за кожну годину простою компенсацію 1/720 від вартості послуги (в середньому в місяці 720 годин).

Це означає, що якщо послуга була недоступна 10 з 30 днів, то клієнт має сплатити 2/3 від вартості послуги.

Але хто компенсує клієнту репутаційні ризики, що пов’язані з неможливістю надання послуги своїм клієнтам або великій роздрібній мережі за недоступність проведення операцій з оплати товарів?

Типова угода зарубіжних операторів зв’язку за замовчуванням включає прогресивну знижку за порушення SLA. Наприклад, AT&T пропонує своїм клієнтам знижку 100% за 16 годин простою.

Приклад із угоди наведено в табл. 2.2.

Для отримання перерахунку вартості за недотримання рівня гарантованих параметрів якості Послуги Оператор має відправити Акт звірки технічних перерв з наданням Послуг, який підтверджує факт перерви.

Правильний варіант подано на рисунку 2.1.

За порушення SLA клієнту надається знижка згідно з таблицею вище на основі звіту щодо якості послуги у вигляді перерахунку вартості послуги за наступний місяць.

Таблиця 2.2 – Приклад із угоди

Загальна перерва в роботі менше або дорівнює 720*(1-SA/100) години	Відшкодування не надаються	
	Схема тарифікації на основі фіксованих щомісячних платежів (п. 5.1. Додатка 1) та за максимальним завантаженням порта (п. 5.3. Додатка 1)	Розмір відшкодування розраховується пропорційно кількості хвилин перерви в роботі. Формула розрахунку розміру відшкодування: CompenSA=(MRS/Qmonth)*Tcompen/24, де MRS (MonthlyReccuringCharges) – сума фіксованих/обов'язкових щомісячних платежів за Послугу в даній точці; Qmonth – загальна кількість днів у місяці; Tcompen – загальна тривалість несправностей (у годинах), що перевищує 720*(1-SA/100); CompenSA – сума відшкодування

Время восстановления		Группа стран					
Равно или больше чем:	Меньше чем:	Группа 1 (%)	Группа 2 (%)	Группа 3 (%)	Группа 4 (%)	Группа 5 (%)	DSL (%)
1 мин	1 ч	3,30	3,30	3,30	3,30	3,30	0
1 ч	2 ч	3,30	3,30	3,30	3,30	3,30	0
2 ч	3 ч	10,0	3,30	3,30	3,30	3,30	3,30
3 ч	4 ч	10,0	10,0	3,30	3,30	3,30	3,30
4 ч	5 ч	25,0	10,0	10,0	10,0	3,30	10,0
5 ч	6 ч	25,0	10,0	10,0	10,0	3,30	10,0
6 ч	7 ч	25,0	25,0	10,0	10,0	3,30	10,0
7 ч	8 ч	25,0	25,0	10,0	10,0	3,30	10,0
8 ч	9 ч	50,0	25,0	25,0	10,0	10,0	10,0
9 ч	10 ч	50,0	25,0	25,0	10,0	10,0	10,0
10 ч	11 ч	50,0	50,0	25,0	10,0	10,0	10,0
11 ч	12 ч	50,0	50,0	25,0	25,0	10,0	10,0
12 ч	13 ч	50,0	50,0	50,0	25,0	10,0	10,0
13 ч	14 ч	50,0	50,0	50,0	25,0	10,0	10,0
14 ч	15 ч	50,0	50,0	50,0	50,0	10,0	10,0
15 ч	16 ч	50,0	50,0	50,0	50,0	10,0	10,0
16 ч	17 ч	100,0	50,0	50,0	50,0	10,0	25,0
17 ч	18 ч	100,0	50,0	50,0	50,0	10,0	25,0
18 ч	19 ч	100,0	100,0	50,0	50,0	10,0	25,0
19 ч	20 ч	100,0	100,0	50,0	50,0	10,0	25,0
20 ч	21 ч	100,0	100,0	100,0	50,0	10,0	25,0
21 ч	22 ч	100,0	100,0	100,0	50,0	10,0	25,0
22 ч	23 ч	100,0	100,0	100,0	50,0	10,0	25,0
23 ч	24 ч	100,0	100,0	100,0	100,0	10,0	25,0
24 ч	36 ч	100,0	100,0	100,0	100,0	10,0	25,0
36 ч	48 ч	100,0	100,0	100,0	100,0	10,0	50,0

Рисунок 2.1 – Правильний варіант нарахування розміру знижки за порушення SLA (Скріншот роботи програми)

з) Відсутня форма звіту.

В угоді має бути прописана форма звіту, яку оператор надає за кожен звітний період. На основі даного звіту здійснюється розрахунок знижки за порушення SLA. Якщо у вимогах до послуги прописані значення показників якості за 15 хвилин, то мають бути надані всі п'ятнадцятихвилинні періоди, коли було порушене SLA.

Підсумок.

Щоб SLA для підприємства мало значення і досягало своїх цілей, надана послуга має бути:

- Досяжною. Вимоги та дизайн мають бути зрозумілими та оформленими відповідно, щоб гарантувати досягнення цих вимог в обслуговуванні.
- Визначеною. SLA має бути визначеною в термінах, що відповідають клієнту й постачальнику.
- Інструментально підтвердженою. У системи має бути спроможність самоконтролю, щоб гарантувати відповідність, попередження та запобігання невідповідностей вимірювання.
- Здійснимою. Штрафи за невідповідність та винагороди за високу ефективність мають бути чітко визначені, щоб діяти як стимул.

2.2.4 Практичні рекомендації щодо складання SLA

1. Предмет угоди

ООО «Зелені тапки», надалі «Замовник», в особі генерального директора Козюпи В.А., який діє на підставі Уставу, з одного боку, і ООО «Рога і копита», надалі «Виконавець», в особі генерального директора Пупкіна А.С., який діє згідно з Уставом, з іншого боку, уклали Угоду про рівень надаваного сервісу в межах діючого Договору IT-аутсорсингу.

Цей документ визначає критерії оцінки якості послуг та їх вартості, що надаються у відповідності з Договором, та є невід'ємною частиною Договору. Дана Угода відміняє укладені раніше угоди про рівень надаваного сервісу і вартості робіт, якщо такі мали місце.

2. Робочий час

Сторони домовились про те, що робочим часом є проміжок з 9:00 до 18:00 в усі дні, крім суботи, неділі та загальнодержавних святкових днів.

3. Метрики сервісу

Сторони домовились про використання таких метрик рівня сервісу.

1) Час реакції на звернення користувача – час, що пройшов з моменту надходження і реєстрації запиту на обслуговування (повідомлення користувача про проблему) до моменту фактичного початку робіт за фактом звернення.

Часом надходження звернення вважається момент надходження електронного листа на адресу support@pupkinservice.ua, реєстрації повідомлення через онлайн-службу реєстрації інцидентів, що надана Виконавцем, або телефонного дзвінка до служби технічної підтримки з повідомленням про проблему.

2) Час розв'язання проблеми – час, що пройшов з моменту фактичного початку робіт над проблемою до закриття замовлення.

Часом початку роботи над проблемою вважається момент відправки Замовнику повідомлення про початок робіт.

Часом розв'язання проблеми вважається момент відправки Замовником повідомлення, що підтверджує закриття замовлення.

Підтвердження чи спростування виконання робіт має бути відправлено Замовником протягом 1 години з моменту надходження від Виконавця повідомлення про виконання замовлення на обслуговування.

У протилежному випадку замовлення вважається закритим автоматично, а часом закриття замовлення стає момент відправки повідомлення про завершення робіт. Повідомлення про початкові завершення робіт направляються Виконавцем представнику Замовника, від імені якого надійшло замовлення на обслуговування, електронною поштою, телефоном або через Службу Онлайн-Замовлень.

З) Час життя інциденту – сумарний час, що пройшов з моменту надходження і реєстрації звернення, до моменту закриття замовлення на обслуговування.

4. Рівні сервісу

Сервіс, що надає Виконавець, поділяється на рівні відповідно зі встановленими значеннями метрик у табл. 2.3.

Таблиця 2.3 – Рівні сервісу

Рівень критичності	**Опис інциденту**
Аварійний	• Повна відмова інформаційної системи внаслідок технічної чи експлуатаційної аварії; • Відмова критичних сервісів за неможливості віддаленого розв’язання проблеми; • Часткова чи повна відмова мережі, внаслідок якої виведені з ладу понад 25 % робочих станцій; • Повна відмова системи електропостачання чи акумуляторного живлення; • Неможливість завантаження серверів і сервісів внаслідок перезавантаження чи апаратного збою.
Середній	• Вихід із ладу одного з резервованих чи дублюючих елементів або одного з декількох елементів однакової функціональності; • Часткова відсутність вхідного й вихідного зв’язку; • Відсутність зв’язку чи каналу інтернет з причини несплати за рахунками; • Відмова критичних сервісів і служб за можливості віддаленого розв’язання проблеми.
Низький	• Недієздатність окремих ПК і сервісів; • Програмні й апаратні несправності, що не впливають на роботу Інформаційної системи в цілому; • Запити на встановлення/вилучення ПЗ, модифікацію апаратного забезпечення. • Інші дрібні та незначні операції.

У відповідності з класифікацією, кожному виду інцидентів призначається час реакції і час усунення в робочих годинах. Відповідальність Виконавця, визначена в гривнях, за кожний факт недотримання нормативів метрик наведено в табл. 2.4.

Таблиця 2.4 – Призначення часу реакції і часу усунення вудповідно з класифікацією сервісу

Назва рівня сервісу	**Наявність віддаленого доступу**		**Відсутність віддаленого доступу**		**Неустойка за невиконання нормативів (грн/час)**
	Час реакції	**Час усунення**	**Час реакції**	**Час усунення**	
Аварійний	20 хвилин	1 – 3 години	30 хвилин	1,5 – 5 години	300
Середній	30 хвилин	2 – 4 години	40 хвилин	3,5 – 5 години	200
Низький	1 година	За узгодженням	1 години	За узгодженням	150

5. Перелік заходів з технічної підтримки IT-інфраструктури Замовника

Виконавець виконує за дорученням Замовника такі заходи, що пов’язані з обслуговуванням і підтримкою діючої IT-інфраструктури:

• надання консультацій користувачам ІС Замовника, розв’язання проблем користувачів, які пов’язані з функціонуванням ІС Замовника та її складових частин;

• підтримка дієздатності та доступності основних мережних служб замовника на рівні, що вказаний у даній угоді;

• проведення моніторингу елементів та підсистем ІС замовника, а також профілактичних робіт, що спрямовані на підтримку дієздатності ІС замовника в цілому;

• здійснення резервного копіювання (у випадку надання Замовником відповідних програмних і апаратних засобів у розпорядження Виконавця);

• інформування Замовника про необхідність модернізації ІС та її елементів, а також заміни елементів, що вийшли з ладу;

• консультації щодо придбання комп’ютерної, копіювальної та іншої оргтехніки для нужд Замовника;

• поставка комп’ютерної, копіювально-розмножувальної та офісної техніки за цінами Виконавця відповідно до вимог Замовника;

• установка оновленої системи «1С Предприятие» версії _____ (у випадку надання Замовником ліцензійних ідентифікаторів доступу до серверів оновлення щодо вказаних Програмних продуктів);

• супроводження продуктів 1С на рівні адміністрування ресурсів системи та Бази даних;

• установка оновлень інформаційно-правової системи _____ (у випадку надання Замовником ліцензійних ідентифікаторів доступу до серверів оновлення вказаних Програмних продуктів).

До робіт щодо здійснення технічної підтримки не належать роботи, що пов'язані з частковим або повним виконанням посадових обов'язків співробітників Замовника. Зокрема, співробітникам Виконавця заборонено виконувати за дорученням співробітників Замовника такі роботи, як:

• Створення, редагування, форматування та інша робота з документами з використанням офісних додатків типу MS Word, MS Excel, MS PowerPoint та подібних їм;

• Створення і редагування графічних, аудіо- та відеофайлів, флеш-презентацій та інших медіафайлів;

• Редагування, наповнення та верстка web-сайтів, у тому числі з застосуванням CMS;

• Написання і відправлення повідомлень електронною поштою, ведення листування від імені співробітників Замовника;

• Пошук інформації в мережі Інтернет;

• Розміщення файлів на FTP-серверах та скачування файлів;

• Відправлення факсів;

• Друк і сканування документів, виготовлення ксерокопій документів;

• Ремонт обладнання, що не належать до ІС Замовника;

• Виконання вантажно-розвантажувальних робіт;

• Виконання кур'єрських доручень, окрім передачі Виконавцю документів, що пов'язані з виконанням цього договору.

Останній пункт – з цінами, але тут вже відносно ситуації на момент часу.

Дана угода – це абстрактний набір послуг метрик та не є вичерпним і зразковим, він просто відображує напрямок розвитку SLA в невеликих аутсорсингових компаніях. Але подібної угоди буває достатньо для убезпечення себе (постачальника) від непорозуміння з боку замовника та його співробітників.

2.3 Зміст звіту

Зиіст має містити:

1. Титульний аркуш із вказівкою теми роботи.

2. Мету і завдання на виконання із прив’язкою до варіанта розглянутої ІТ-інфраструктури конкретного підприємства.

3. Розроблену Угоду про рівень послуг SLA відповідно до розробленої ІТ-інфраструктури підприємства за варіантом.

4. Висновки щодо виконаної роботи.

2.4 Контрольні запитання і завдання

2.4.1 Контрольні запитання

1. Яка основна мета розробки і підписання Угоди про рівень послуг SLA?

2. Які складові елементи Угоди SLA?

3. Хто розробляє та узгоджує положення документу?

4. Хто підписує і несе відповідальність за дотримання положень SLA?

5. Які додаткові документи, нормативи чи стандарти можуть бути використані в ході складання SLA?

2.4.2 Контрольні завдання

Розробити Угоду про рівень послуг для власного продукту, що був створений на попередніх практичних роботах.

Готова Угода може бути основою для підписання акту впровадження розробленої системи ІТ-інфраструктури на підприємстві. Тому обов’язковим є перелік усіх складових елементів з реальними показниками функціоналу та його дієздатності.

3 ОЦІНКА ЯКОСТІ МОДЕЛІ УПРАВЛІННЯ ІТ-ІНФРАСТРУКТУРОЮ ПІДПРИЄМСТВА

3.1 Мета заняття

Ознайомитись з методологією CobiT та на її основі навчитися проводити власний аудит якості моделі управління ІТ-інфраструктурою підприємства.

3.2 Методичні вказівки з організації самостійної роботи студентів

3.2.1 Принципи та підходи методології CobiT

Для того, щоб забезпечити організацію управління ІТ-інфраструктурою на підприємстві, потрібно управляти ресурсами ІТ за допомогою сукупності процесів, що об'єднані у логічні групи.

Але як організація може контролювати ІТ в такий спосіб, щоб отримувати інформацію, необхідну для досягнення своїх корпоративних цілей? Як управляти ризиками та забезпечувати безпеку тих ІТ-ресурсів, від яких ця організація настільки залежить? Як організація може бути певна в тому, що ІТ реалізує поставлені цілі та підтримує розвиток бізнесу?

Насамперед, керівництво має визначити цілі контролю, які, в свою чергу, визначають кінцеву мету впровадження політик, планів і процедур, а також організаційних структур, необхідних для забезпечення прийнятного рівня впевненості, що:

- бізнес-цілі будуть досягнуті;
- небажані події буде попереджено або виявлено, а їх наслідки ліквідовано.

По-друге, у складних сучасних умовах керівництво постійно знаходиться в пошуку інформації для швидкого та успішного прийняття рішень стосовно цінності активів, ризиків і контролів.

Що потрібно вимірювати та яким чином?

Організації мають потребу в об'єктивних критеріях оцінки свого поточного стану та тих вдосконалень, яких вони потребують, а також в інструменті, за допомогою якого керівництво могло б оцінити ці вдосконалення.

Відповіддю на ці вимоги щодо визначення та моніторингу рівня контрольованості та ефективності у сфері ІТ є подані нижче визначення, які дає CobiT®.

Порівняльний аналіз (Benchmarking) – систематизований підхід до порівняння результатів діяльності організації з результатами діяльності схожих

організацій та конкурентів, з метою вдосконалення діяльності організації (наприклад, порівняльний аналіз зрілості процесів розробки програмного забезпечення, відповідно моделі зрілості процесів, що створена Інститутом програмної інженерії (Software Engineering Institute (SEI)).

Цілі та метрики ІТ-процесів необхідні для визначення та оцінки їх результатів та ефективності, що ґрунтуються на принципах системи збалансованих бізнес-показників, що запропонована Робертом Капланом та Девідом Нортоном.

Дії – спрямовані на безпосереднє управління ІТ-процесами, що ґрунтуються на цілях контролю CobiT®.

Оцінка потужності процесу на основі моделей зрілості CobiT® є ключовою складовою впровадження ІТ-управління.

Після ідентифікації критичних ІТ-процесів і контролів, моделювання зрілості дозволяє ідентифікувати та подати керівництву організації виявлені розбіжності.

Області уваги ІТ-управління:

• Узгодженість зі стратегією робить акцент на зв'язку між вимогами бізнесу та планами ІТ, оцінюванні корисності ІТ, а також на встановленні відповідності між діяльністю ІТ та бізнесу.

• Забезпечення цінності являє собою реалізацію плану розвитку ІТ в такий спосіб, який гарантує те, що ІТ забезпечують обіцяні вигоди відповідно до бізнес-стратегії, при цьому акцент робиться на оптимізації витрат та доведенні внутрішньої цінності ІТ.

• Управління ресурсами присвячене питанням, пов'язаним з управлінням критичними ІТ-ресурсами, а саме: оптимізації інвестицій та належному управлінню прикладними системами, інформацією, інфраструктурою та персоналом. Ключові питання стосуються оптимізації знань та інфраструктури.

• Управління ризиками потребує обізнаності вищого керівництва в області ризиків, чіткого розуміння схильності організації до ризиків, розуміння необхідності дотримання існуючих вимог, прозорості відносно суттєвих ризиків, до яких схильна організація, та впровадження системи управління ризиками.

• Оцінка ефективності являє собою контроль реалізації стратегії, виконання проектів, використання ресурсів, ефективності процесів та надання послуг.

Для цього застосовуються, зокрема, системи збалансованих показників, які перетворюють стратегію у послідовність дій, результати яких вимірюються методами, відмінними від традиційних методів бухгалтерського обліку.

Методологія CobiT®: дослідження, розробка та пропаганда сучасної, прийнятної в міжнародному масштабі методології управління ІТ з метою її

впровадження організаціями та повсякденного використання керівниками організацій, спеціалістами з IT та аудиторами.

В основі методології CobiT® лежить принцип: забезпечити інформацію, якої потребує організація для досягнення своїх цілей, у яку організація має робити інвестиції та надати можливість управління та контролю IT-ресурсів з використанням структурованої сукупності процесів, що забезпечують необхідну організації інформацію.

Управління та контроль інформації є основою методології CobiT® та спрямовані на забезпечення відповідності вимогам бізнесу (рис. 3.1).

Рисунок 3.1 – Основні принципи CobiT®

3.2.2 Інформаційні критерії стандарту Cobit®

Ефективність означає відповідність та релевантність інформації бізнес-процесам, а також її своєчасне надання у коректній, послідовній та придатній для використання формі.

Продуктивність означає надання інформації з використанням ресурсів в оптимальний (максимально продуктивний та економічно вигідний) спосіб.

Конфіденційність стосується забезпечення захисту секретної інформації від несанкціонованого розголошення.

Цілісність стосується достовірності та повноти інформації, а також її корисності з точки зору цінності та очікувань бізнесу.

Доступність передбачає наявність інформації у той момент, коли цього потребує бізнес-процес у поточний момент часу та в майбутньому. Це також передбачає захист необхідних ресурсів і пов’язаних з ними можливостей.

Відповідність означає дотримання діючого законодавства, нормативно-правових актів та зобов'язань за контрактами, які мають стосунок до даного бізнес-процесу, тобто дотримання зовнішніх бізнес-критеріїв та внутрішніх політик.

Надійність означає надання керівництву належної інформації, необхідної для керування організацією та виконання ним зобов'язань як довірених осіб та управлінців.

Визначення IT-цілей та архітектури IT в організації подано на рисунку 3.2.

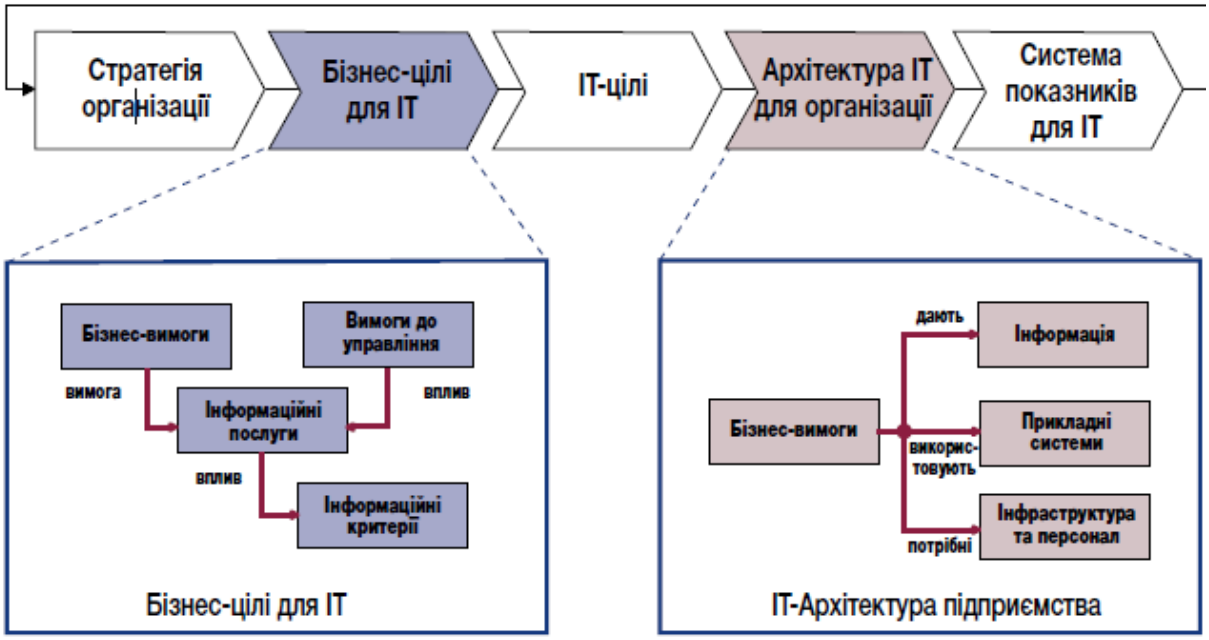

Рисунок 3.2 – Визначення IT-цілей та архітектури IT в організації

3.2.3 IT-ресурси, що визначені в CobiT®

IT-ресурси, що визначені в CobiT®, можна визначити так.

Прикладні системи – автоматизовані системи для користувачів та ручні процедури для обробки інформації.

Інформація – це дані у всіх можливих видах, які надходять, обробляються та виходять з будь-яких інформаційних систем, що використовуються організацією.

Інфраструктура – це технологія та засоби (тобто, апаратне забезпечення, операційні системи, системи управління базами даних, комп'ютерні мережі, мультимедійні засоби та середовище, в якому вони розміщуються та функціонують), які створюють умови для роботи прикладних програм.

Персонал – це персонал, необхідний для планування, придбання, впровадження, постачання, обслуговування, керування та оцінювання результатів роботи інформаційних систем і послуг. Персонал може бути власним, стороннім або таким, що працює за контрактом.

На рисунку 3.3. відображено вплив бізнес-цілей для ІТ на спосіб управління ресурсами ІТ, яке здійснюється ІТ-процесами з метою досягнення ІТ-цілей.

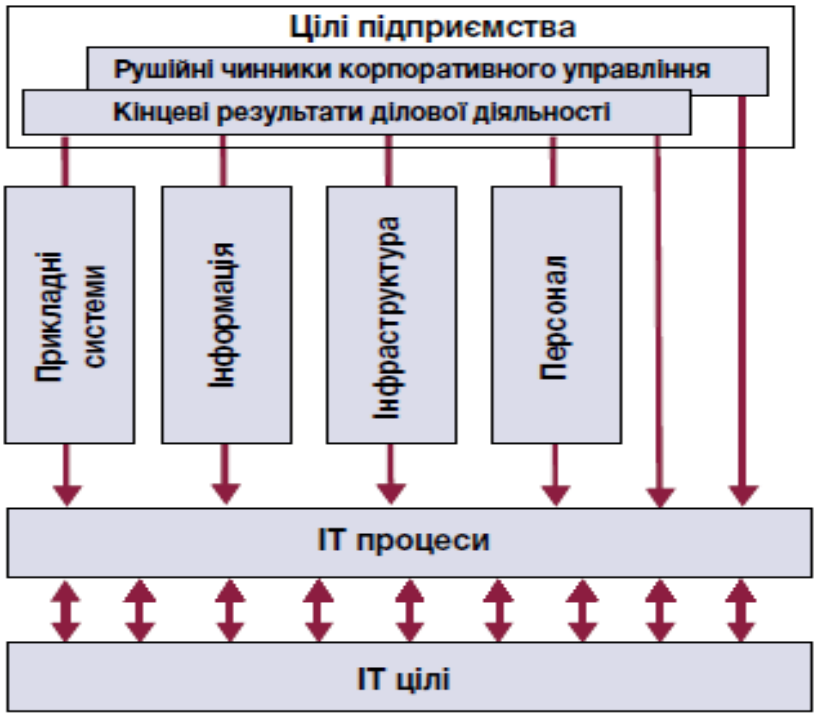

Рисунок 3.3 – Вплив бізнес-цілей на ІТ-цілі

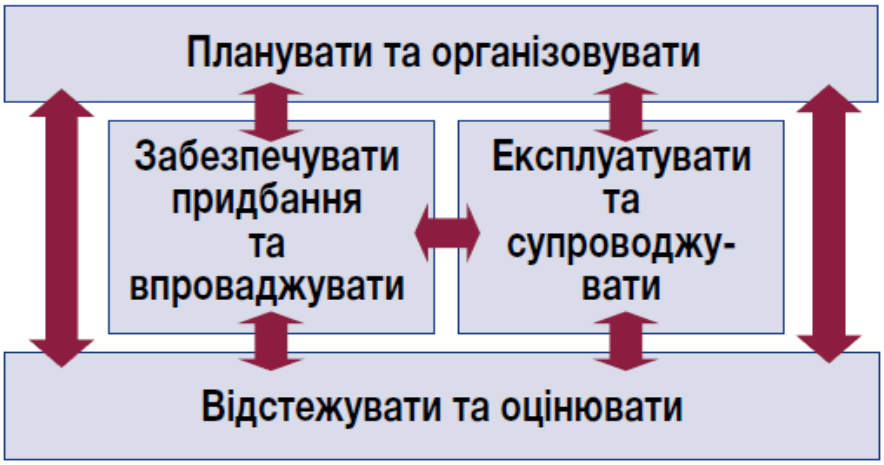

Рисунок 3.4 – Управління ресурсами ІТ

Контроль – це система політик, процедур, практик та організаційних структур, передбачених для забезпечення розумних гарантій того, що бізнес-цілі будуть реалізовані, а небажані події буде попереджено, або виявлено та вжито коригувальних заходів щодо їх наслідків.

Цілі контролю у сфері ІТ являють собою завершену сукупність вимог високого рівня, які має взяти до уваги керівництво, щоб забезпечити ефективний контроль кожного ІТ-процесу.

Вони:

− є підтвердженням дій керівництва, спрямованих на підвищення бажаних результатів або зниження ризиків;

− складаються з політик, процедур, практик та організаційних структур;

− розроблені з метою забезпечення розумних гарантій того, що бізнес-цілі буде реалізовано, а небажані події буде попереджено або виявлено та вжито коригувальних заходів щодо їх наслідків.

Керівництво організації має зробити вибір стосовно цілей контролю шляхом:

− вибору тих, які є прийнятними;

− прийняття рішення щодо того, які з них буде запроваджено;

− вибору способу їх втілення (частота, період, автоматизація тощо);

− прийняття на себе ризику, обумовленого не впровадженням тих, які можуть виявитись необхідними.

Модель контролю подана на рисунку 3.5.

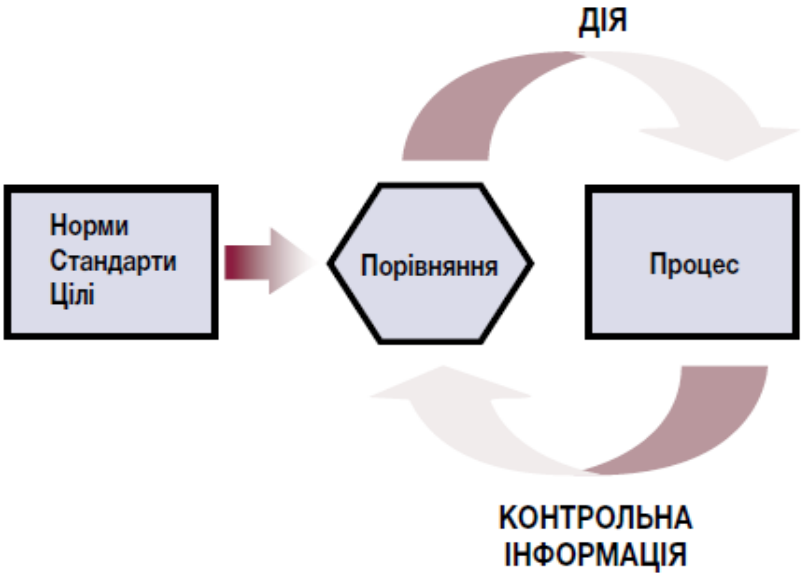

Рисунок 3.5 – Модель контролю

Цілі контролю позначаються посиланням на відповідний домен, що складається з двох символів (PO, AI, DS та ME) та номером процесу і номером цілі контролю.

3.2.4 Загальні вимоги контролю

На додаток до цілей контролю для кожного процесу у стандарті CobiT® є загальні вимоги контролю, які позначено як PC (номер контролю процесу). Їх слід розглядати у сукупності з цілями контролю процесу, щоб мати повне уявлення про вимоги контролю.

PC1 Цілі та завдання процесу

Визначити та повідомити конкретні, такі, що можуть бути виміряні, такі, що дають підстави для дій, реалістичні, орієнтовані на отримання результатів та своєчасні (SMART) цілі та завдання процесу з метою ефективного виконання кожного IT-процесу. Переконатися, що вони пов'язані з бізнес-цілями та супроводжуються системою відповідних показників.

PC2 Призначення власників процесів

Призначити власника кожного IT-процесу та чітко визначити ролі та обов'язки власника процесу. Включити, наприклад, відповідальність за розробку процесу, взаємодію з іншими процесами, облік та звітність щодо кінцевих результатів, кількісне оцінювання результатів процесу та виявлення можливостей для вдосконалення.

PC3 Відтворюваність процесу

Розробити та впровадити кожен ключовий IT-процес як такий, що може бути відтвореним та постійно давати очікувані результати. Створити логічну але гнучку та змінювану послідовність дій, виконання яких призведе до бажаних результатів, та достатньо мобільною, щоб реагувати на нестандартні та надзвичайні ситуації. Там, де це можливо, використовувати уніфіковані процеси і адаптувати їх тільки у випадку неможливості.

PC4 Ролі та обов'язки

Визначити ключові операції та кінцеві результати процесу. Чітко розподілити й повідомити ролі та обов'язки з метою ефективного і продуктивного виконання ключових операцій та їх документального оформлення, а також обліку і звітності стосовно процесу та його кінцевих результатів.

PC5 Політики, плани та процедури

Визначити та повідомити, в який спосіб всі політики, плани та процедури, які керують IT-процесом, слід документувати, редагувати, підтримувати, затверджувати, зберігати, доводити до відома та використовувати для навчання. Здійснити розподіл обов'язків та відповідальності за виконання кожного зі вказаних видів діяльності та в належний час перевіряти, чи правильно вини виконуються. Вжити необхідних заходів щодо того, аби ці політики, плани та процедури були доступними, правильними, зрозумілими та актуальними.

РС6 Покращення показників процесу

Запровадити систему показників, яка дає уявлення про результати та показники процесу.

Встановити планові показники, які відображають цілі процесу та визначити показники результативності, які сприяють досягненню цілей процесу.

Визначити спосіб, у який слід отримувати дані.

Порівняти фактичні результати з плановими та вжити заходів у випадку виникнення відхилень у разі необхідності.

Узгодити ці показники, планові показники та методи із концепцією моніторингу загальних показників ІТ.

Система внутрішнього контролю організації впливає на ІТ на трьох рівнях:

• На рівні вищого керівництва, на якому визначаються бізнес-цілі, впроваджуються політики та приймаються рішення щодо того, як розподіляти та управляти ресурсами організації з метою реалізації її стратегії.

• На рівні бізнес-процесу, де контролі використовуються в межах конкретних бізнес-операцій.

Більшість бізнес-процесів автоматизовано та інтегровано у прикладні ІТ-системи, внаслідок чого більшість контролів на цьому рівні також здійснюється автоматично. Подібні контролі мають назву автоматизованих контролів на рівні прикладних систем.

Проте, контроль деяких бізнес-процесів реалізується з використанням процедур, що здійснюються вручну, наприклад, санкціонування операцій, розділення обов’язків та звіряння.

Тому контролі на рівні бізнес-процесів є комбінацією ручних контролів, застосування яких продиктоване вимогами бізнесу, та автоматизованих контролів бізнес-процесів на рівні прикладних систем.

• ІТ сприяють здійсненню бізнес-процесів, надаючи ІТ-послуги, як правило, це послуги, що спільно використовуються багатьма бізнес-процесами, оскільки ціла низка ІТ-процесів з розробки та експлуатації виконуються в межах організації в цілому, а більша частина інфраструктури ІТ надається для загального користування (наприклад, мережі, бази даних, операційні системи та засоби збереження інформації).

Контролі, що застосовуються для всіх ІТ-послуг, що надаються, називаються загальними ІТ-контролями.

На рисунку 3.6 подано межі відповідальності бізнесу, загальні контролі та контролі рівня прикладних систем.

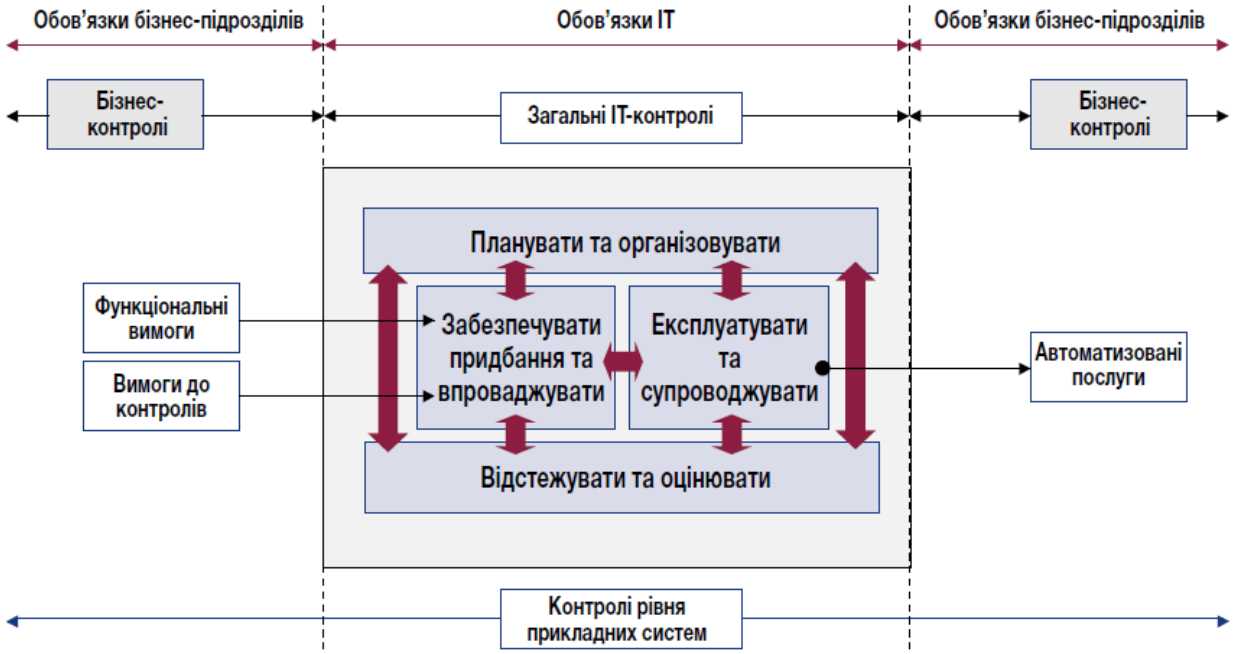

Рисунок 3.6 – Межі відповідальності бізнесу,
загальні контролі та контролі рівня прикладних систем

3.2.5 Рекомендований перелік цілей контролю рівня прикладних систем

Цілі контролю позначають сполученням АС з номером контролю рівня прикладних програм.

АС1 Підготовка та дозвіл на використання вихідних даних

Впевнитись, що вихідні документи підготовлені уповноваженим та кваліфікованим персоналом згідно зі встановленими процедурами з урахуванням розділення/виділення обов'язків у частині створення та ухвалення подібних документів.

Кількість помилок і пропусків можна звести до мінімуму, якщо подати вхідні дані у належній формі. Виявити помилки та невідповідності, щоб їх можна було внести до звіту та виправити.

АС2 Накопичення та введення вхідних даних

Встановити порядок, згідно з яким введення даних здійснюється своєчасно уповноваженими та кваліфікованим персоналом.

Коригування та повторне введення даних, які було введено з помилками, слід здійснювати у спосіб, який не поставить під загрозу початкові рівні авторизації операцій.

Якщо це доцільно для відновлення, зберігати оригінальні вихідні документи протягом належного проміжку часу.

АС3 Перевірки точності, повноти та автентичності даних

Переконатися, що операції є точними, повними та дійсними. Оцінити дані, які було введено, та відредагувати їх або відправити назад для коригування якомога ближче до місця їх походження (джерела).

АС4 Цілісність та достовірність даних під час обробки

Зберігати цілісність і достовірність даних протягом усього циклу їх обробки. Виявлення помилкових операцій не порушує процесу виконання дійсних операцій.

АС5 Аналіз вихідних результатів, звіряння та обробка помилок

Визначити процедури та пов'язані з ними обов'язки, що гарантують належну обробку вихідних результатів, доставку їх належному адресату та захист протягом процесу передачі; забезпечують виконання перевірки, виявлення та коригування точності вихідних результатів і гарантують використання інформації, що міститься у вихідних результатах.

АС6 Аутентифікація операції та цілісність даних

Перш ніж здійснити передачу даних ланцюжком внутрішніх операцій та бізнес/операційних функцій (у межах або за межами підприємства), перевірити відповідність адресата, автентичність походження та цілісність змісту. Підтримувати автентичність та цілісність даних протягом процесу передачі або перенесення даних.

У стандарті CobiT подано модель зрілості для аналізу системи внутрішнього контролю, яка ілюструє рівень зрілості організації у сфері впровадження та функціонування системи внутрішнього контролю.

Часто виконання подібного аналізу є відповіддю на зовнішні стимули, але в ідеалі його потрібно запровадити як документовані процеси стандарту CobiT®.

РО6 *«Поінформованість щодо цілей керівництва та вказівок»* (Communicate management aimsand directions) та ME2 *«Діяльність з моніторингу системи внутрішнього контролю та оцінки результатів»* (Monitoran devaluatein ternalcontrol).

Можливість, охоплення та контроль є трьома вимірами зрілості процесу, як показано на рис. 3.7.

Модель зрілості дозволяє здійснити оцінку рівня розвитку процесів управління, тобто, наскільки вони насправді є дієздатними.

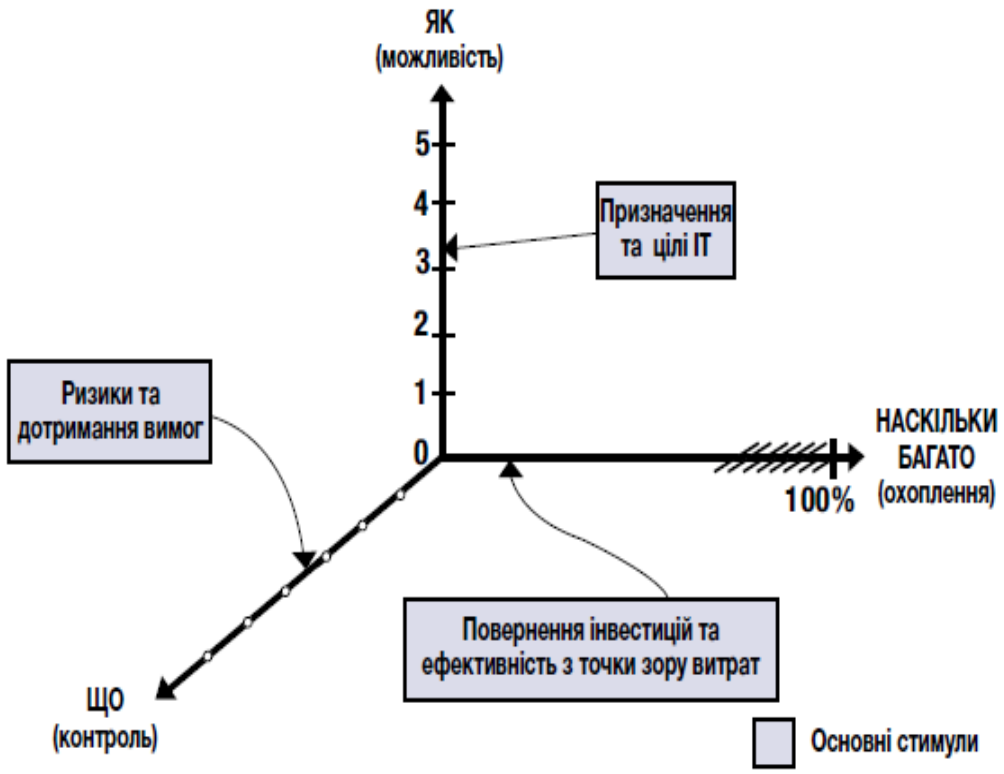

Рисунок 3.7 – Три виміри зрілості

Високий рівень розвиненості або дієздатності процесу насамперед визначається цілями IT та потребами бізнесу, підтримку яких забезпечують інформаційні технології.

Ступінь фактичної зрілості процесу переважно визначається тим обсягом повернення інвестицій, які організація хоче отримати.

Наприклад, можуть існувати критичні процеси та системи, які потребують більш ретельного управління безпекою, ніж інші, які мають менш критичний характер.

З іншого боку, ступінь і складність контролю, що має бути вжитий до процесу, більшою мірою визначається схильністю організації до ризиків та застосовними вимогами, яких потрібно дотримуватися.

Модель зрілості допоможе спеціалістам пояснити керівництву організації, де саме в управлінні IT-процесами існують недоліки, та визначити відповідні завдання, які потрібно виконати.

Щоб правильно визначити рівень зрілості, потрібно врахувати бізнес-цілі організації, операційне середовище та найкращі практики, що існують в даній галузі.

Зокрема, рівень зрілості управління визначатиметься залежністю організації від IT, складністю технологій та, що найбільш важливо, цінністю її інформації. Ознаки зрілості управління наведені у табл. 3.1.

Таблиця 3.1 – Ознаки зрілості управління

Усвідомлення проблем та комунікації	**Рівень політик, планів та процедур**	**Застосування інструментів та автоматизація процесів**	**Професійні знання та досвід**	**Відповідальність та підзвітність**	**Визначення цілей та «вимірювання результатів»**
1	**2**	**3**	**4**	**5**	**6**
Зароджується визнання необхідності управлінням процесами Комунікації стосовно проблем, що існують, мають епізодичний характер	Мають місце спеціалізовані процеси та Практики. Процеси та політики не визначені.	Можуть застосовуватись деякі інструменти, а саме стандартизовані інструменти для настільних ПК. Не існує планування у підході до використання стандартизованих інструментів.	Не визначено рівень професійного досвіду, необхідний для виконання процесів. Не існує плану навчання, формальне навчання не проводиться.	Не існує визначення відповідальності та підзвітності. Люди приймають на себе відповідальність за проблеми, реагуючи на них та виходячи зі своєї власної ініціативи.	Цілі не є чітко визначеними, вимірювання результатів не виконується.
Існує чітке усвідомлення необхідності діяти. У сфері комунікацій управління є більш формалізованим та структурованим.	Прояви використання «найкращих практик». Процеси, політики та процедури стандартизовані та документовані для всіх ключових дій.	Складено план використання та стандартизації інструментів управління та автоматизації процесу управління. Інструменти управління використовуються за їх основним призначенням, але не у всьому можуть відповідати узгодженому плану та можуть не бути інтегровані один з одним.	У всіх сферах визначено та документовано вимоги до кваліфікації персоналу. Розроблено план формалізованого навчання, але формалізоване навчання все ще проводиться, виходячи з індивідуальних потреб.	Відповідальність та підзвітність за управління процесом визначено, встановлено власників процесів. Імовірно, власник процесу не має повного права на виконання цих обов’язків.	Визначено деякі цілі та метрики ефективності, але немає належної комунікації, існує чіткий зв’язок з бізнес-цілями. Мають місце процеси вимірювання, але вони не застосовуються послідовно. В організації прийнято ідею збалансованих карт оцінки бізнесу, аналіз першопричин застосовується час від часу.

Продовження табл. 3.1

1	2	3	4	5	6
Існує повне розуміння проблем управління. Застосовуються ретельно обдумані методики комунікацій та стандартні інструменти комунікацій.	Процес є чітко визначеним та довершеним; застосовуються внутрішні найкращі практики Всі аспекти процесу документовані та можуть бути відтворені. Політики затверджені та підписані керівництвом. Стандарти розробки та здійснення процесів і процедур прийняті та дотримуються.	Інструменти управління впроваджено згідно із стандартизованим планом, деякі з них інтегровані з іншими пов'язаними інструментами управління. У більшості сфер використовуються іструменти, призначені для автоматизації управління процесом та моніторингу найважливіших дій та заходів контролю.	Вимоги до кваліфікації персоналу постійно оновлюються у всіх сферах, професійність працівників, що працюють у всіх найважливіших сферах, гарантовано, наявність сертифікату (диплому) заохочується. Застосовуються ретельно розроблені методики навчання згідно з планом навчання, заохочується обмін знаннями. Всі внутрішні спеціалісти в предметних областях залучені до бізнес-процесів, здійснюється оцінка ефективності навчального плану.	Відповідальність та підзвітність за виконання процесу розподілені та встановлені в такий спосіб, що власник процесу може виконувати свої обов'язки в повному обсязі і несе за них відповідальність. Існує система преміювання працівників, яка стимулює до здійснення дій з позитивним результатом.	Здійснюється вимірювання показників ефективності та продуктивності, встановлено їх взаємозв'язок з бізнес-цілями та стратегічним планом в сфері IT. В деяких сферах запроваджено карти збалансованих показників, за виключеннями, відомими керівництву, порядок аналізу першопричин формалізовано. Має місце постійне вдосконалення процесів.

Продовження табл. 3.1

1	2	3	4	5	6
Має місце поглиблене розуміння управління, проблем та рішень ІТ, а також перспектив. Здійснюється проактивне узгоджене управління проблемами на основі аналізу тенденцій, застосовуються ретельно продумані методики комунікацій, використовуються інтегровані інструменти комунікацій.	Застосовуються найкращі практики інших організацій та зовнішні стандарти. Документування процесів забезпечує автоматизацію бізнес-процесів. Процеси, політики та процедури стандартизовані та інтегровані, що дає змогу підвищувати якість управління та ефективність роботи організації, а також здійснювати постійне вдосконалення.	У масштабах всієї організації застосовуються стандартизовані пакети інструментів. Інструменти повністю інтегровані з іншими пов'язаними інструментами, що забезпечує комплексну підтримку процесів. Інструменти використовуються з метою вдосконалення процесів та забезпечують автоматизоване виявлення нестандартних ситуацій в системі контролю.	Організація офіційно заохочує прагнення до постійного підвищення кваліфікації, виходячи з чітко визначених особистих цілей та цілей організації. Навчання спрямоване на використання найкращих практик інших організацій та передових підходів і методик. Обмін знаннями є частиною культури організації, розгортаються системи, засновані на використанні знань. Керівну участь беруть сторонні спеціалісти та організації, що займають провідне місце в галузі.	Власники процесів мають право приймати рішення та вживати заходів. Прийняття відповідальності на себе послідовно розповсюджене зверху донизу в масштабах усієї організації.	Існує інтегрована система вимірювання показників ефективності, яка пов'язує результати у сфері ІТ з бізнес-цілями через збалансовані карти показників ІТ. Нестандартні ситуації цілком та повністю відомі керівництву, першопричини всіх проблем та відхилень ретельно аналізуються. Постійне вдосконалення процесів – це спосіб життя організації.

3.2.6 Цілі та метрики

Цілі та метрики (показники) визначено в CobiT® згідно з трьома рівнями.

Цілі ІТ та показники, які дозволяють визначити, чого саме бізнес-підрозділи очікують від ІТ та як вимірювати ці результати.

Цілі процесу та відповідні показники, які дозволяють визначити, що саме ІТ процес має забезпечити на підтримку ІТ-цілей та як вимірювати відповідні результати.

Цілі діяльності та відповідні показники, які встановлюють, що має статися у межах процесу, щоб були досягнуті заплановані результати, та як їх вимірювати.

На рис. 3.8 зображено взаємозв'язок цілей трьох рівнів.

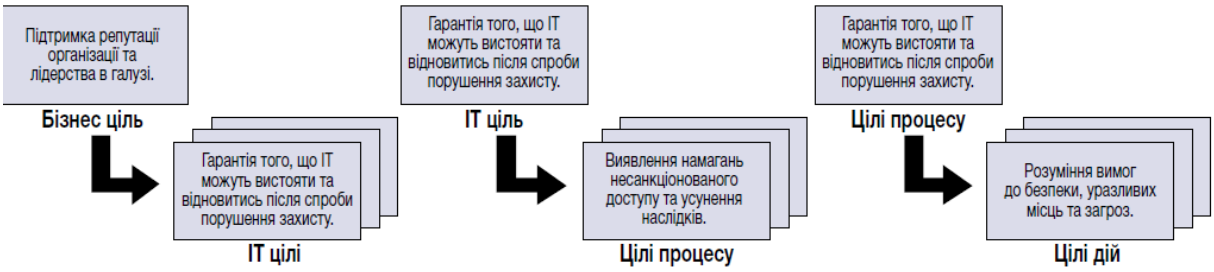

Рисунок 3.8 – Приклад взаємозв'язку цілей

Цілі визначено зверху донизу так, що бізнес-ціль визначає сукупність цілей ІТ, які її підтримують. Ціль ІТ реалізується одним процесом або внаслідок взаємодії сукупності процесів. Тому цілі ІТ визначають різні цілі процесів. У свою чергу кожна ціль процесу потребує здійснення сукупності дій, таким чином визначаючи цілі дій.

Терміни «Ключовий індикатор досягнення цілі» (KGI) та «Ключовий індикатор ефективності» (KPI), використані в попередніх версіях стандарту CobiT®, було замінено двома видами метрик:

• Показники кінцевих результатів (Outcomemeasures), раніше – ключові індикатори досягнення цілі (KGI), показують, чи були досягнуті цілі.

Їх можна виміряти тільки після фактичного настання події, тому їх називають «показниками відставання» («lag indicators»).

• Показники ефективності (Performance indicators), раніше – ключові індикатори ефективності (KPI), показують, чи можуть бути досягнуті цілі.

Їх можна виміряти ще до того, як будуть зрозумілі кінцеві результати, тому їх називають «показниками випередження» («lead indicators»).

Показники кінцевих результатів нижчого рівня набувають значення показників результативності вищого рівня.

У прикладі з рис. 3.8 показник кінцевих результатів, який підтверджує, що здійснюється виявлення спроб несанкціонованого доступу та реагування на них, водночас показує, що, імовірніше за все, IT-послуги можуть встояти проти подібних атак та мають здатність до відновлення.

Тобто, показник кінцевих результатів став показником результативності високорівневої цілі.

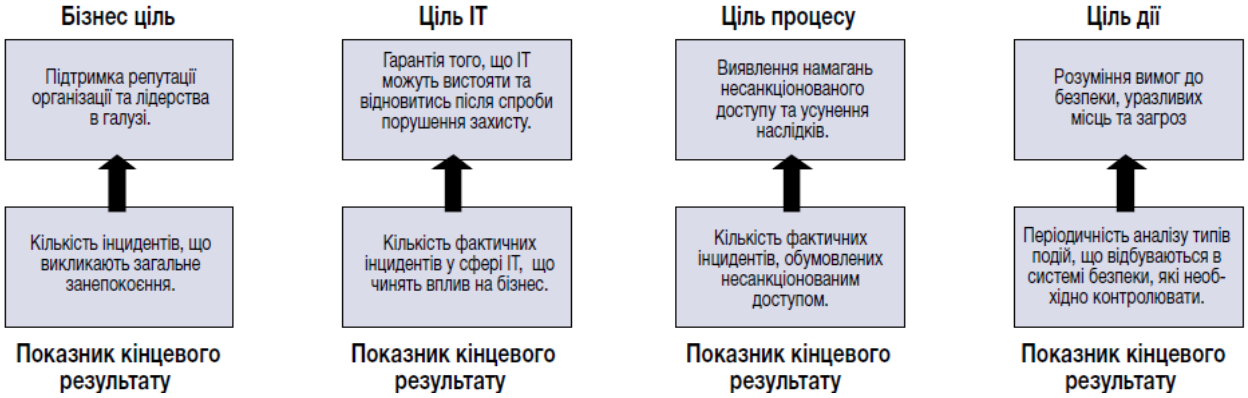

Рисунок 3.9 – Можливі показники кінцевих результатів для прикладу з рис. 3.8.

На рис. 3.10 показано, як показники кінцевих результатів з даного прикладу перетворюються на метрики ефективності (performance metrics).

Показники кінцевих результатів визначають метрики, на підставі яких керівництво може зрозуміти – чи досягли функція IT, процес або дія своїх цілей.

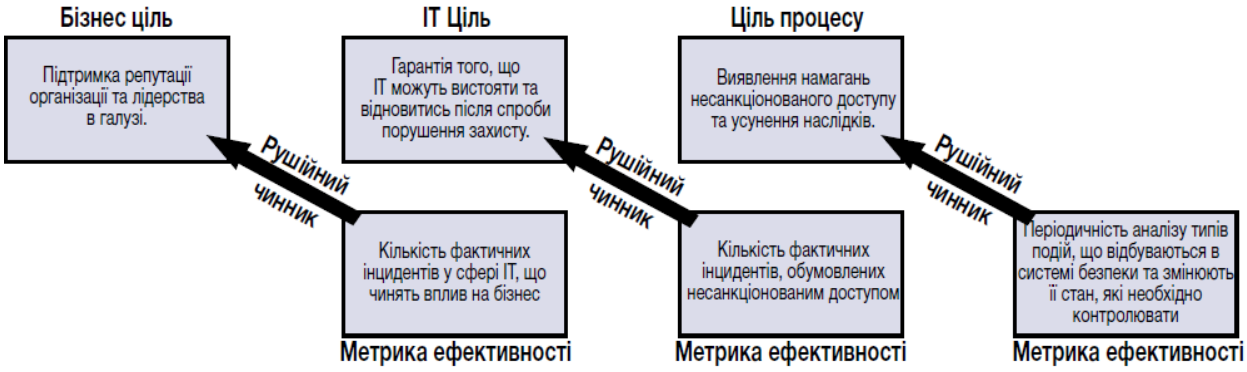

Рисунок 3.10 – Можливі рушійні чинники прикладу з рис. 3.8

Показники кінцевих результатів IT часто виражають через інформаційні критерії (вимоги до інформації):

– доступність інформації, необхідної для підтримки потреб бізнесу;

– відсутність ризиків, пов’язаних з порушенням цілісності та конфіденційності інформації;

– рентабельність процесів та операцій;
– підтвердження надійності, ефективності та узгодженості інформації.

На рис. 3.11 показано взаємозв’язок між бізнес-цілями, цілями IT, цілями процесу та різноманітними метриками.

Зверху зліва направо наведено послідовність цілей. Під ціллю подано показник кінцевого результату для цієї цілі.

Маленька стрілка вказує, що одна й та сама метрика є показником результативності для високорівневої цілі.

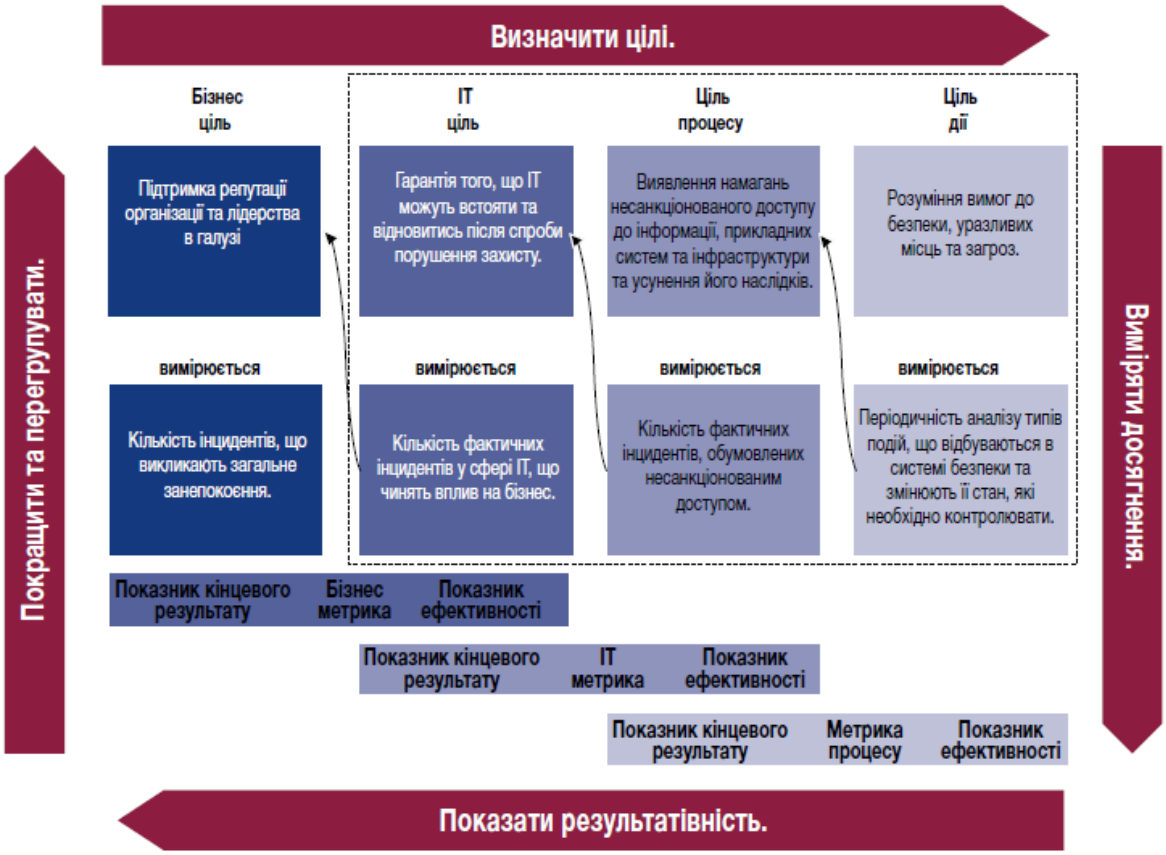

Рисунок 3.11 – Взаємозв’язок між процесами, цілями та метриками (DS5)

Стандарт CobiT® орієнтований на цілі та обсяг IT-управління, при цьому забезпечувана ним структура системи контролює універсальну, узгоджену з принципами корпоративного управління організацію, і тому він є прийнятним для рад директорів, виконавчого керівництва, аудиторів та працівників регулятивних органів.

На рис. 3.13 показано, як різні елементи структури стандарту CobiT® поставлено у відповідність до основних зон уваги корпоративного управління в сфері IT.

На рис. 3.14 подано приклад оцінки стану та розвитку IT-процесів на підприємстві.

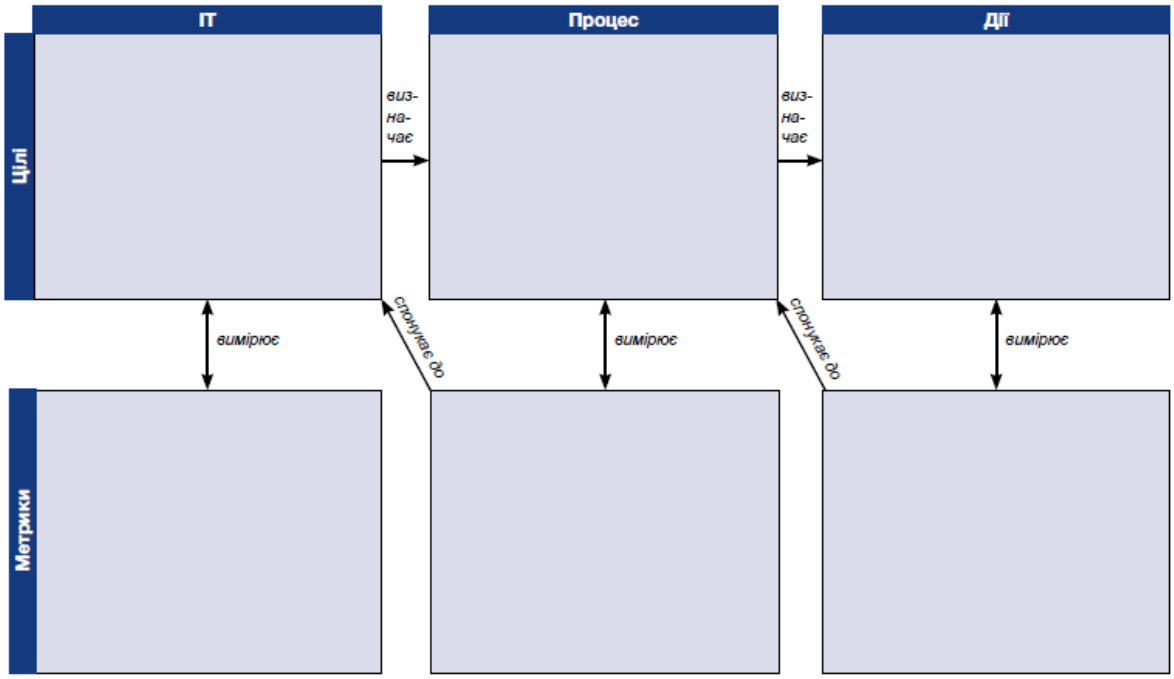

Рисунок 3.12 – Подання цілей та метрик

	Цілі	Метрики	Практики	Моделі зрілості
Узгодженість зі стратегією	P	P		
Забезпечення цінності		P	S	P
Управління ризиками		S	P	S
Управління ресурсами		S	P	P
Оцінка ефективності	P	P		S

P=основний інструмент реалізації S=другорядний інструмент реалізації

Рисунок 3.13 – Структура CobiT® та основні зони управління IT

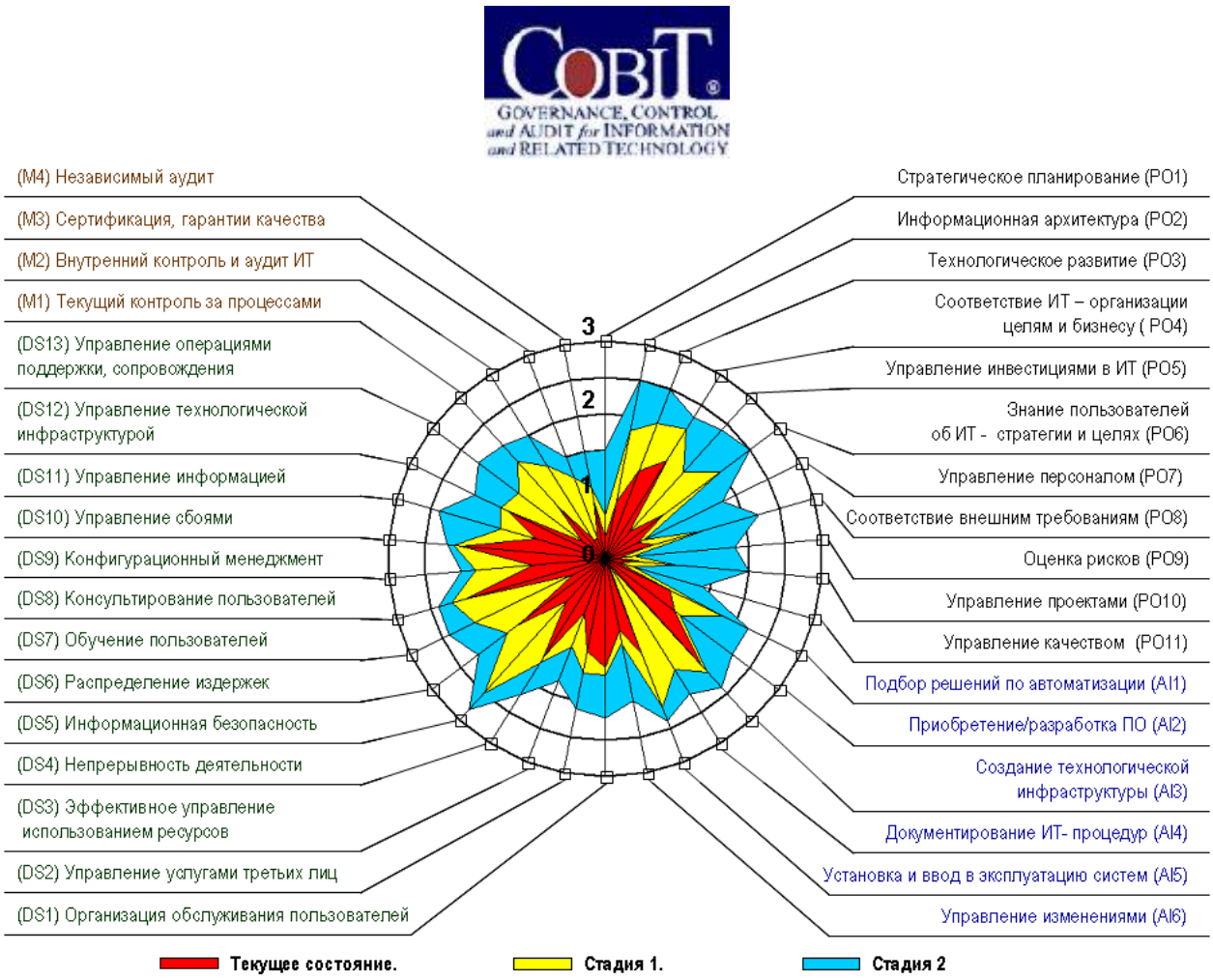

Рисунок 3.14 – Приклад оцінки стану та розвитку IT-процесів на підприємстві (Скріншот роботи програми)

3.3 Зміст звіту

Зміст має містити:

1. Титульний аркуш з темою роботи.
2. Мету та завдання на виконання з прив’язкою до варіанта IT-інфраструктури конкретного підприємства, що розглядається.
3. Результат виконання п. 3 попереднього розділу.
4. Висновки за результатами аналізу.

3.4 Контрольні запитання і завдання

3.4.1 Контрольні запитання

1. Для чого і ким використовується методологія CobiT?
2. Як пов’язані бізнес-цілі та IT-цілі на підприємстві?

3. Дайте стислий опис методики оцінювання якості моделі управління IT-інфраструктурою на підприємстві.

4. Які показники найбільше впливають на якість управління IT-інфраструктурою?

5. Хто несе персональну відповідальність за якість надання IT-послуг на підприємстві?

3.4.2 Контрольні завдання

1. Вивчити основні принципи й підходи методології CobiT щодо оцінки стану та розвитку IT-процесів на підприємстві (відповідно до варіанта, що розглядається на попередніх заняттях).

2. Визначити бізнес-цілі та відповідні ним IT-цілі згідно з методологією CobiT. Оформити у вигляді таблиці із зазначенням шифрів стандарту.

3. Користуючись шаблоном аналізу за кожним процесом, розробити 4 розділи:

3.1 Опис процесу у вигляді каскаду (рис. 3.15).

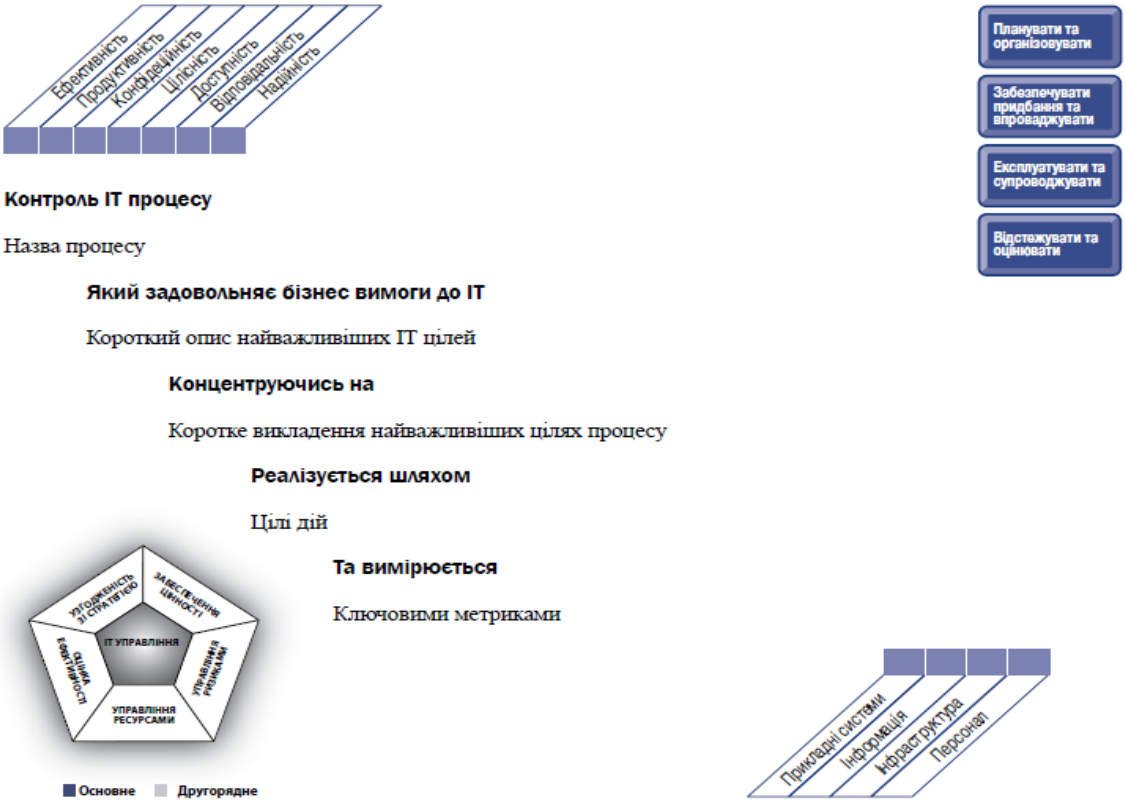

Рисунок 3.15 – Приклад опису процесу у вигляді каскаду

3.2 Цілі контролю цього процесу.

Вхідні ресурси процесу – це те, чого власник процесу вимагає від інших.

Цілі контролю в описі процесу відображають те, що власник процесу має зробити.

Результати процесу – це те, що власник процесу має подати.

Цілі та метрики показують, як слід вимірювати цей процес.

RACI-діаграма відображає, що і кому слід доручити.

Модель зрілості показує, що слід зробити для поліпшення ситуації.

3.3 Вхідні ресурси процесу та результати, діаграма RACI, цілі та метрики.

Ролі в RACI-діаграмі для всіх процесів такі:

- вища посадова особа в організації (CEO);
- фінансовий директор (CFO) ;
- керівники бізнес-підрозділів;
- директор з інформаційних технологій (CIO) ;
- власник бізнес-процесу;
- виконавчий директор (Head operations) ;
- головний архітектор (Chief architect) ;
- керівник підрозділу з розробки ПЗ (Head of development) ;
- керівники адміністративних функцій IT (для великих організацій керівники таких служб як відділ кадрів, служби фінансового планування та служби внутрішнього контролю) ;
- відповідальний за управління проектам (PMO) ;
- служби дотримання існуючих вимог, аудиту, управління ризиками та забезпечення безпеки (групи спеціалістів, наділені обов'язками в області контролю, а ніж IT-персонал, задіяний в операційних задачах).

3.4 Модель зрілості процесу.

4. Зробити висновки та оформити звіт.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Олейник А.И. Методологические основы управления ИТ-инфраструктурой предприятия. – М.: Изд-во «Открытые системы», 2009. – 422 с.
2. Ван Бон Ян. ИТ-сервис менеджмент. Введение. – М.: «Инфра-М», 2007. – 450 с.
3. Экономическая информатика: Введение в экономический анализ информационных систем: Учебник. – М.: «ИНФРА-М», 2005. – 958 с.
4. Ермошкин Н.Н., Тарасов А.А. Стратегия информационных технологий предприятия. – М.: Изд-во Моск. Гум. университета, 2003. – 315 с.
5. Bernard, Scott A. Introduction to Enterprise Architecture; Publisher: authorHOUSE™; 2005.
6. Долженко А.И. Управление информационными системами. – Ростов-на-Дону, 2007.
7. Олейник А.И., Сизов А.В. ИТ-инфраструктура. – Москва, 2009.
8. Потоцкий М.А. ITSM, как современный подход к ИТ-менеджменту // «Директор ИС», № 05, 2002.
9. Решения Microsoft для повышения эффективности ИТ-инфраструктуры / Microsoft. – М.: Русская редакция, 2005.
10. Google Lab: BigTable. – http://labs.google.com/papers/bigtable.html
11. Google Lab: MapReduce: упрощенная обработка данных на больших кластерах. – http://labs.google.com/papers/mapreduce.html
12. Google Lab: интерпретирование данных. Параллельный анализ с помощью Sawzall. – http://labs.google.com/papers/sawzall.html
13. Google Lab: Файловая система Google (GFS) – http://labs.google.com/papers/gfs.html
14. HP OV Service Desk / http://www.hp.ru/openview/products/servicedesk/
15. ITIL – библиотека передового опыта организации ИТ-служб / http://www.cio-world.ru/weekly/251017/page3.html
16. Management Software: HP OpenView / http://h20229.www2.hp.com/
17. META Group. Executive Insights. Enterprise Architecture Desk Reference, 2002.
18. Microsoft® Operations Framework 4.0. Published at 2008, April.
19. MSF for Agile Software Development Process Guidance. Published at 2006, November.
20. MSF for CMMI® Process Improvement. Published at 2006, November.

21. Rob England, Introduction to Real ITSM, ISBN 1438243065 9781438243061, год 2008

22. Информация о Data Protection Manager // http://www.microsoft.com/rus/systemcenter/dpm/evaluation/default.mspx

23. Как работает Google от David Carr в Baseline Magazine. – http://www.baselinemag.com/c/a/Infrastructure/How-Google-Works-1/

24. System Center Reporting Manager 2006 Overview // http://www.microsoft.com/systemcenter/scrm/evaluation/overview/default.mspx

25. Tivoli / http://www-128.ibm.com/developerworks/ru/tivoli/

26. White Paper, The HP IT Service Management Reference Model, http://www.hp.com/hps/hpc/itsm/briefs/wp_v2-1.pdf

27. Решение HP OpenView Network Node Manager (NNM) / http://www.hp.ru/openview/nnm/

28. Решения IBM Tivoli для растущих компаний / http://www-306.ibm.com/software/ru/tivoli/smb/products.html#express

29. Системы управления ИТ инфраструктурой на базе IBM Tivoli / http://www.r-style.com/rubrs.asp?rubr_id=214&art_id=954

30. Технологии IBM для управления информационными системами / http://www.tivoli.computel.ru/article?id=a0018

31. Федерация Flickr: Тур по архитектуре Flickr – http://www.bytebot.net/blog/archives/2007/04/25/federation-at-flickr-a-tour-of-the-flickr-architecture

32. Центр безопасности Microsoft / http://www.microsoft.com/rus/security/default.mspx

33. http://www.microsoft.com/rus/SystemCenter/overview/default.mspx

34. CobiT 4.1. Методологія. Цілі контролю. Поради з управління. Моделі зрілості процесів. http:// www.itgi.org.

Електронне навчальне видання

МЕТОДИЧНІ ВКАЗІВКИ
до практичних занять з дисципліни
«УПРАВЛІННЯ ІТ-ІНФРАСТРУКТУРОЮ ПІДПРИЄМСТВА»
(частина 2)
для студентів усіх форм навчання
спеціальності 122 – «Комп'ютерні науки»

Упорядники: ШЕХОВЦОВА Вікторія Іванівна
МАЛЬКОВА Ірина Анатоліївна

Відповідальний випусковий В.М. Левикін
Редактор О.Г. Троценко
Комп'ютерна верстка Л.Ю. Свєтайло

План 2019 (друге півріччя), поз. 37

Підп. до використання 08.07.2018 Формат pdf. Об'єм даних 2,0 Mb

ХНУРЕ. Україна. 61166, Харків, просп. Науки, 14, E-mail: info@nure.ua

Підготовлено в редакційно-видавничому відділі ХНУРЕ
Свідоцтво суб'єкта видавничої справи ДК №1409 від 26.06.2003