ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»
Бізнес Школа КРОК

ПИЖОВ ОЛЕКСАНДР СЕРГІЙОВИЧ

Кваліфікаційна робота

«Оптимізація роботи відділу інформаційних технологій під час воєнних дій в умовах обмеження ресурсів»

073 МЕНЕДЖМЕНТ

«Бізнес адміністрування»

Подається на здобуття освітнього ступеня магістр

Кваліфікаційна робота містить результати власних доробок. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

О.С. ПИЖОВ

Науковий керівник: Кравченко Т.І., к.е.н.

Консультант: Корейба А.З., аспірант Університету КРОК

Київ - 2023

ЗМІСТ

РЕЗЮМЕ

24 February 2022. Ukraine. russia's full-scale invasion of Ukraine has begun. This is a new page in history that will be written in global history. But this is not only a war between two states, it is also a war for the health of the country. It is a war for resources that are constantly in short supply, a war for markets, a war to survive.

The work presented here is a real-life case study. The decisions in this case were made instantly, sometimes on a subconscious basis and most often on the knowledge gained during business school. Two technical support lines were able not only to support the existing business processes, but also to change the vector of work, to bring new methods of interaction between departments not only within the unit, but also between departments (matrix system).

During the war, it is very important to preserve jobs, salaries, and employees' belief that management does not only give instructions, but can also teach and enthuse. This paper shows that by introducing process standardisation and automation, it was possible to save the jobs of the second line of technical support and reduce the number of employees of the first line of technical support without reducing the SLA level. The new work standards have provided an unexpected economic effect when opening new departments and optimising the work of existing ones. Increased fault tolerance, implemented monitoring systems and a Help Desk. The process of transition to a service model of interaction has begun. Warehouses began to be stratified by their areas (hot, warm, cold, dead warehouses). During the optimisation process, new forms of attitude to the price of data and UpTime of services emerged. This led to the creation of backup sites to build a fault-tolerant model.

At the same time, the development of risk maps was able to provide more predictable results, which were used to implement new stages of development.

Holding strategic sessions allowed us to more clearly predict the next steps in the development of the IT department and to check the path we are on.

ВСТУП

Актуальність теми дослідження.

Економіка Україні сьогодні зіткнулась з новим викликом: після всемірної пандемії Covid-19 почалось повномасштабне вторгнення росії в Україну. Ці нові надскладні умови сильно відобразились чинять вплив на функціонування економіки, адже бізнеси функціонують і в умовах військової агресії, а українці щодня шукають і винаходять нові оптимальні способи менеджменту, маркетингу, інформаційних технологій тощо.

Технології стали звичними супутниками життя. Якщо під час першої та другої світових війн містян сповіщали через міську систему гучномовців, то зараз про небезпеку нас сповіщають гаджети. Гаджети нам вказують, де знаходиться найближче укриття, ведуть по дорогам та вказують найкоротший маршрут. Гаджети фільмують історію нашого життя. Гаджети замінюють нам співрозмовника, коли нам необхідно щось обговорити чи порадитись. Гаджети та мобільні застосунки й рішення допомагають управляти економічною ефективністю підприємств.

Як показав час, то ті хто зміг під налаштуватися працювати видалено, та перевести свій бізнес на on-line, мали можливість не тільки утриматись на ринку, а також провести збільшення своїх активів за рахунок поглинання збиткових компаній. Для того, щоб це все працювало якісно, потрібні сучасні інноваційні цифрові технології. Це все можливе, коли грамотно побудована мережева та серверна інфраструктура, наприклад, на підприємстві сфери медичного бізнесу.

Специфіка медичних закладів полягає в затребуваності медичних послуг в найскладніші часи: 24/7 під час пандемії, воєнного часу, при будь яких обставинах. В сучасних медичних закладах використовуються високонадійна комп’ютерна техніка. Але ці комп’ютери повинні обробляти інформацію з баз даних, які розташовані на спеціалізованих майданчиках (Дата Центрах). У разі відсутності плану відмовостійкості доступу до Дата Центрів, резервних майданчиків, віддаленої роботи, медичні заклади

можуть обмежено працювати на паперових носіях. Але більшість медичного обладнання потребує наявності комп'ютерного обладнання. Тому від якості побудованої мережі, швидкості серверів, локальної мережі, зовнішніх каналів зв'язку залежить точність та швидкість діагнозів, а це впливає на одужання пацієнтів. Отже, дане наукове дослідження присвячена пошуку шляхів ефективного управління підприємством на основі організації Дата Центру під час воєнних дій в умовах обмеження ресурсів.

Метою кваліфікаційної роботи є аналіз, впровадження нових стандартів та інновацій в інфраструктурному підрозділу відділу інформаційних технологій підприємства, а також створення відмовостійкої IT інфраструктури в Дата Центрах та підрозділах.

Відповідно до поставленої мети були сформовані такі **завдання дослідження**:

1. Проаналізувати існуючі бізнес-процеси на предмет використання в підрозділі.
2. Проаналізувати виконання стандарту по архітектури побудови серверних, комутаційних кімнат, розміщення мережевого та серверного обладнання. В разі відсутності стандартів – розробити та впровадити нові.
3. Створити резервні майданчики для побудови відмовостійкої архітектури роботи підприємства.
4. Розробити опис етапів та процесів зі скорочення серверної та мережевої техніки.
5. Розробити та підготувати до впровадження матричну модель взаємодії між першою та другою лініями технічної підтримки відділу інформаційних технологій.

Об'єкт дослідження – бізнес-процеси інфраструктурного IT підрозділу підприємства (медичного закладу).

Предмет дослідження - архітектура побудови серверного та мережевого обладнання, підготовчий процес переходу до сервісної моделі, введення системи моніторингу.

Методи дослідження. Під час роботи над проектом були застосовані теоретичні методи дослідження (аналіз першоджерел, порівняльний аналіз, гіпотези та наукове моделювання – побудова теоретичних карт), а також емпіричні методи дослідження (експеримент, спостереження, вимірювання).

Наукова новизна одержаних результатів:

1. Вперше для мережевого медичного бізнесу були розроблені стандарти з розміщення обладнання.
2. Проаналізовані бізнес-процеси взаємодії інфраструктурного підрозділу з іншими підрозділам мережі клінік та першою лінією технічної підтримки.
3. Розроблені стандарти побудови серверних, комутаційних кімнат, розташування мережевого та серверного обладнань.
4. Проведено аналіз та імплементація нового підходу в HR-стратегії роботи з персоналом IT-відділу в умовах воєнного часу.

Практичне значення одержаних результатів. Практичне значення полягає у тому, досліджені та впроваджені комплексні міри з забезпечення відмовостійкості IT інфраструктури на підприємстві надали можливість в умовах воєнного часу та обмеження по електропостачанню, каналів зв’язку, досягти стабільності в роботі підрозділів, що позитивно відбилось на економічних результатах функціонування мережі медичних закладів. Усі теоретичні матеріали, висновки та моделі були сформовані на основі реальних кейсів, пройшли випробування в реальних умовах воєнного часу і довели свою доцільність та ефективність. Методики, наведені в даній роботі, можуть бути застосовані не тільки для підприємств медичної галузі, але і для інших підприємств різних сфер економіки, форми власності та розмірів. Стандарти та інновації, які досліджуються в даному науковому

досліджені, можуть бути трансформовані в окремий напрямок бізнесу по забезпеченню відмовостійкості IT інфраструктур.

Робота складається зі вступу, трьох розділів та десяти підрозділів, висновку й списку використаної літератури.

РОЗДІЛ 1.
ТЕОРЕТИКО-ЕКОНОМІЧНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ РОБОТИ МЕДИЧНИХ ЗАКЛАДІВ З ІТ СЕРВІСАМИ.

1.1. Дата Центр як ІТ-сервіс, спрямований на оптимізацію процесів підприємств.

З кожним днем сучасний бізнес стає все більше залежним від інформаційних технологій. Цифрові рішення проникають в усі сфери господарської діяльності, створюючи необхідність у високоефективному інфраструктурному забезпеченні. Однією з ключових складових цього забезпечення є Дата Центр, по суті це сервіс, спрямований на оптимізацію процесів підприємств.

Дата Центр є потужним ІТ-сервісом, який має значний потенціал для оптимізації процесів підприємств. Він допомагає забезпечити ефективне використання ресурсів, зберігання та обробку даних, а також забезпечує високу доступність та безпеку інфраструктури.

Дата Центр – це комбінований комплекс обладнання, програмного забезпечення, мереж та процедур, призначений для зберігання, обробки та передачі даних. Він функціонує як централізована інфраструктура для обробки і управління інформаційними потоками, додатково забезпечуючи високу доступність, надійність та безпеку.

Основними превагами є:

- Скасування локальних розміщених серверних кімнат: Дата Центр дозволяє підприємствам уникнути обмежень, пов'язаних з розміщенням обладнання та даних на місцях. Це сприяє гнучкості та забезпечує можливість масштабування без значних інвестицій у фізичне обладнання.
- Ефективність ресурсів: Дата Центр дозволяє оптимізувати використання обчислювальних ресурсів, забезпечуючи їхню більш ефективну роботу та уникнення перевантажень.

- Висока доступність та надійність: Завдяки резервним системам живлення, охолодження та мережам, Дата Центр гарантує високу доступність та надійність обслуговування. Це дозволяє уникнути перебоїв у роботі підприємства.
- Забезпечення безпеки: Дата Центр використовує сучасні методи захисту даних, криптографію та контроль доступу, що робить його надійним місцем для зберігання конфіденційної інформації.
- Швидкість та продуктивність: Завдяки використанню передових технологій та обладнання, Дата Центр може забезпечити високу швидкість обробки даних та виконання обчислювальних завдань.

Основні напрями використання Дата Центрів:

- Обробка, аналіз даних: Дата Центр допомагає оптимізувати процеси обробки даних, забезпечуючи швидкий доступ та аналіз інформації.
- Хмарні рішення: Використання хмарних сервісів на базі Дата Центру дозволяє підприємствам ефективно використовувати обчислювальні ресурси та забезпечує гнучкість у використанні послуг.
- Резервне копіювання та відновлення: Дата Центр забезпечує можливість зберігання резервних копій даних та їхнє відновлення в разі випадкового видалення або втрати.
- Віртуалізація: З використанням віртуалізації Дата Центр може оптимізувати використання обладнання, забезпечуючи ефективне розподілення ресурсів
-
-

1.2. Концептуальні засади з організації роботи відокремлених підрозділів, зокрема Дата Центру.

Підрозділи можуть мати такі статуси:

- Не автономний. Підрозділ вважається не автономним, коли всі IT сервіси надаються видалено. В разі втрачання каналу зв'язку з Дата Центром, повністю зупиняються всі IT сервіси, підрозділ може обмежено функціонувати в паперовому(ручному) режимі.
- Частково автономний. Підрозділ вважається частково автономним, коли більшість IT сервісів надається видалено. В разі втрачання каналу зв’язку з дата центром може частково надавати послуги та тимчасово зберегти (наприклад, знімки комп’ютерної томографія, рентген, тошо) дані.
- Повністю автономний. Підрозділ вважається повністю автономний коли всі IT сервіси надаються безпосередньо в відділені, та не залежать від стану каналу зв’язку з Дата Центром.

Для виконання бізнесових задач кожний підрозділ повинен бути оснащений наступною технікою:

- Робоча станція, для виконання робочих завдань, заповнення карт пацієнтів, проведення конференцій, навчання, то шо.
- IP Телефон, для внутрішньої комунікації між колегами, зв’язком зі страховими компаніями.
- Принтер або багатофункціональний печатний пристрій, для друку медичних заключень, згод, та інших медичних паперових документів.
- Спеціалізований принтер друку штрих кодів, для друку етикеток зі штрих-кодами для нанесення на медичні ємності для збору аналізів.
- Медичне обладнання, яке може передавати результати дослідження в МІС
- Система відеоспостереження, для фіксації перебування пацієнтів на території підрозділу.

- Бездротовим доступом WiFi для пацієнтів клініки та осіб що супроводжують пацієнтів.
- Фіскальні принтери, які друкують чеки при розрахунках з клієнтами.
- Банківські термінали для оплати банківськими картками.

В підрозділи має бути облаштована зона комутації мережевого та серверного обладнання. Обладнання може знаходиться:

- В окремій кімнаті. Окреме приміщення , в якому розташовані все комутаційне та серверне обладнання. Для таких приміщень є стандарти побудови, в яких зазначені температурні режими, пожежна безпека та системи керування доступом. Частіше за все в таких кімнатах встановлюється мережеве та серверне обладнання яке дуже чутливе до кліматичних вимог.
- Окремі закриті комутаційні шафи. Шафи висотою до 42 юніти, яки можуть знаходитись в будь-якому місці приміщення підрозділу.

Все обладнання котре потребує доступу до ІТ сервісів має бути підключено до мережевого обладнання. Підключення відбуватися:

- Від головного мережевого обладнання до розеток (портів) пачт-панелі за допомогу патч-кордів.
- Від розеток(портів) патч-панелі до розеток в кабінетах, за допомогою спеціалізованого кабелю відповідної категорії з дотриманням певних умов прокладання
- Від розетки в кабінеті до кінцевого обладнання, за допомогою патч-корду.

На підрозділах повинні працювати такі сервіси:

- Медична інформаційна система в якій ведеться повний облік введення пацієнтів
- 1С для взаєморозрахунків з клієнтами
- Стаціонарна телефонія
- Спеціалізовані медичні системи для забезпечення роботи медичного обладнання.

- Доступ в Інтернет.
- Система відеоспостереження

Дата Центром може виступати будь яка технічна площадка яка буде відповідати технічним вимогам по забезпеченню відмово стійкості. Дата центри можуть бути:

- Само побудовані. Це відокремлені приміщення (серверні кімнати) в яких встановлені відкриті серверні стійки, або перфоровані серверні шафи. Зазвичай, мають один електричний ввід, до двох каналів зв'язку Інтернет. Мають один або два побутових кондиціонера для підтримки температурного балансу. Без цілодобового нагляду з боку моніторингу, та систем безпеки.
- Повноцінні, на самообслуговуванні. Відокремлені приміщення (серверні кімнати), в яких встановлені відкриті серверні стійки на яких розміщуються серверне обладнання. Мають 2 відокремлених електричних ввода, зовнішня резервування (генератор). Побудовану систему кондиціювання по системі «гарячих» та «холодних» коридорів. Систему пожежогасіння, з відповідним сертифікатом.
- Орендовані в дата центрах. Це оренда окремих юнітів, або шаф в професійно побудованих Дата Центрах, які мають відповідні сертифікати.

Для забезпечення доступу до Інтернету використовуються канали зв'язку яку надають провайдери. За ознакою провайдери поділяються на

- Дротові
- Бездротові.

До дротових провайдерів відносять тих провайдерів які надають доступ до інтернету за допомогою дротів. Це можуть бути:

- Мідні дроти, де середовищем для передачі сигналу виступає дріт (в більшості випадків мідний). В залежності від необхідних швидкостей підбирається кабель.

- Оптоволоконні дроти, де середовищем для передачі є скло. Використовується в тих випадках коли потрібно передати інформацію на далекі відстані та на великій швидкості.

До бездротових провайдерів відносять провайдерів які надають доступ до послуг Інтернету по повітрю. Це можуть бути:

- WiFi, використовується в публічних місцях, або як радіо міст в тих випадках коли неможливо провести дроти.
- Стільниковий (мобільний зв'язок), використовується в тих місцях де неможливо прокласти дроти
- Супутниковій, використовується в тих місцях де неможливо прокласти дроти, немає інших засобів зв’язку

Кожен із типів каналів зв'язку має свої критерії надійності. Наприклад, канал зв’язку по оптоволоконну буде один із самих надійних та дешевих в обслуговуванні, але може бути пошкоджений під час ремонтних робіт, або не обережного користування (людський фактор) . Стільниковий зв'язок буде одним з нестабільних, але його доступність в межах великих міст дає можливість використовувати його як тимчасово резервний канал зв’язку.

Для того щоб об’єднати всі підрозділи , які територіально розгалужені, в єдину логічну мережу використовують технологію VPN (virtual private network) побудовану на базі протоколу IPSEC. Це дозволяє захищати комерційні дані, від спроби компрометування. Також за цією технологією є можливість надати доступ користувачам які працюють видалено, за межами офісу. Якщо є можливість, то офіси можливо об’єднати за допомогою «точка-точка». Це коли провайдери або самостійно (за наявності технічної можливості) будуються прямий канал зв’язку між офісами.

Всі канали зв’язку характеризуються переліком технічних критеріїв які впливають на його якість. Одним з ключових критеріїв це синхронність. Топ то якість каналу зв’язку на змінення його пропускної швидкості за проміжок часу. Цей критерій впливає на якість чутливого трафіку, такий як телефонія, відео контент, відео конференції. Для потреб домашнього Інтернету, або

видавленого підключення до робочого місця, достатньо не гарантованих каналів зв’язку (вони дешеві, але не надійні).

Для побудови відмово стійкості постійного доступу до Інтернет використовують комбінацію з двох різних провайдерів, та різної середи передачі даних. Наприклад: у Дата Центрі агрегують два або більше провайдерів по оптоволоконній технології, так як в Дата Центрі більш чутливі дані, які потребують більш високої якості каналів зв’язку. Для видаленого офісу з не критичними (за часом) даними, може використовуватися система «активного-пасивного» режиму роботи, коли основній провайдер буде подаватися по оптоволоконної технології, а резервний по стільниковій(мобільної) 4G технології. У такому випадку, основній канал буде в стані «актів» через нього буде проходити весь трафік. Стільниковий зв'язок буде використовуватися в режимі «пасів». В разі відсутності зв’язку через основний канал, весь трафік піде через резервний стільниковий(мобільний)4G. Після відновлення основного каналу, трафік повернеться у звичний режим роботи. Така схема більш оправдана з економічної точки зору, так як затрати на стільниковий(мобільний) 4G канал значно дешевші ніж оплата оптичного синхронного каналу зв’язку.

Кожен з підрозділів має сервіс друку якій складається:

- Пристрої для друку на папері. Використовується для печаті будь якої інформації яка потрібна у виробничих цілях. Розподіл техніки відбувається таким чином:
    - В кабінетах встановлені принтери для друку результатів досліджень, висновків, то шо.
    - На рецепції встановлений багатофункціональний пристрій якій має функцію сканування, копіювання. В разі виробничої можливе встановлення багатофункціонального пристрою в кабінеті лікаря.

- Пристрої для друку штрих кодів. Встановлюються в кабінетах за виробничої потреби. В багатьох випадках, використовуються для штрих кодування аналізів.
- Пристрої друку паперових чеків по взаєморозрахункам с клієнтами. Встановлюється на касових місцях, обов'язково повинні бути під'єднані до мережі Інтернет для передачі даних до державних служб.
- Пристрої друку результатів досліджень на плівках. Використовуються тільки разом з медичним обладнанням.

В центральному офісі, центру обслуговування клієнтів, друк проводиться:

- Пристрій друку на папері, для друку службової інформації
- Багатофункціональний пристрій, для друку, скануванні, копіюванні службової інформації.

Кожен кабінет оснащений стаціонарним телефонним зв'язком. Він необхідний для зв'язку з іншими кабінетами та страховими компаніями. Для достовірності інформації яка була розкрита, всі розмови записуються, а потім аналізуються.

Зв'язок може забезпечуватися:

- Власною апаратною автоматичною телефонною станцією. Застарілий спосіб, але виправдовує себе коли є невелика кількість користувачів. Дешевий в обслуговуванні.
- Міською автоматичною телефонною станцією. Використовується, коли є мала кількість користувачів які не потребують внутрішніх комунікацій за допомогою телефона.
- Власною програмно-апаратною автоматичною станцією на базі сервера з операційною системою.
- Орендованої у оператора зв'язку програмно-апаратною автоматичною стацією на базі віртуальних серверів.

Для потреб контакт центру налаштовується власний програмно апаратний комплекс який складається:

- Програмного апаратна автоматична телефонна станція
- Модуль Робоче місце оператора контакт центру
- База знань
- Система запису та зберігання телефонних розмов.
- Інтеграція з іншими медичними системами.

Сервери на підрозділах розподіляються за наступними напрямками:

- Які потребують постійної кліматичної сцени. Вони розміщуються в окремих кімнатах або залах, де підтримується певна температура.
- Які не потребують постійної кліматичної температури. Частіше за все це сервери до спеціалізованого медичного обладнання, яке розташоване в окремих приміщеннях безпосередньо біля обладнання та кваліфікованого персоналу.

До кожного сервера обов’язково встановлено джерело безперебійного живлення, яке захищає його від перепаду напруги, а в разі відсутності напруги – завершує його роботу, в автоматичному режимі, без втрат даних.

Для резервування критичних даних, на підрозділах можуть встановлювати дискові полки великої ємності. Такі пристрої можуть бути:

- Стаціонарними, які мають розміщуватись в серверних приміщеннях з постійною кліматичною сценою. Забезпечені безперебійним живленням, та розміщуватися в шафах або на стійках.
- Переносними. Можуть розміщуватись в будь яких комутаційних шафах, не потребують температурних умов.

В кожному кабінеті, за функціональної потреби, встановлюється комп’ютер. Комп’ютер може бути:

- Стаціонарним, коли кабінет загального користування без прив'язки до конкретного співробітника.
- Мобільним(ноутбук), коли для виконання, потрібно переміщати комп’ютер, наприклад для зняття діагностичних даних.
- Мобільним в составі медичного обладнання. Цей спеціалізований комп’ютер слугує тільки для проведення дослідження та його збереження.

В більшості випадків до кожного комп’ютера, крім мобільних, приєднані джерела безперебійного живлення, які забезпечують захист від перенапруги та дозволяють завершити роботу комп’ютера без втрати даних, при раптовій відсутності напруги.

Для забезпечення безпеки та нагляданням за переміщенням пацієнтів на підрозділі, застосовується загальна система відеоспостереження. Система розміщується в серверній кімнаті, на окремому обладнані (сервери зберігання відеоінформації та мережеві комутатори) керується виключно видалено. Для оперативного контролю за ситуацією на підрозділі та попереднього запобігання нештатним ситуаціям, на робоче місце служби безпеки виводиться зображення з цих камер. Для керівництва і уповноважених осіб є можливість переглядати архів видалено.

Для контролю доступу в приміщенні, використовуються системи контролю доступу, які розташовані по всьому підрозділу, але головний вузол керування знаходиться в серверній кімнаті або комутаційної шафі. Система відео нагляду та контролю доступу підключається до джерел безперебійного живлення збільшеної ємності задля того щоб забезпечити процес керування доступом та відео наглядом, під час відсутності електроенергії.

1.3. Загальні відомості по організації мережевого забезпечення в підрозділах

Мережеве обладнання для підрозділів формується на базі виробничих потреб та навантаження. В розрахунок обов'язково враховується необхідність резервування, та безперебійність процесу надання сервісів. Для відокремлених підрозділів характерна така побудова:

- За ознаками сервісу. Це коли мережеве обладнання поділяється за ознаками сервісу яке працює на підрозділі. Наприклад: сервіс друку, сервіс телефонії, сервіс комп'ютерів
- Без розділення на сервіси:
  - Порт-Порт. Це коли всі розетки шо є на підрозділи підключені до портів мережевого обладнання, в незалежності використовуються вони, чи ні.
  - Порт-Обладнання, Це коли до мережевого обладнання під'єднано обладнання яке використовується та працює.

Мережеве обладнання на підрозділах має такі функційні обов'язки:

- Пограничні, це так обладнання яке знаходиться на границі між зовнішнім канал утворюючим обладнанням, наприклад обладнання провайдерів Інтернет, та внутрішнім обладнанням яке встановлено на підрозділі. До такого типу обладнання відносять роутери, комутатори, спеціалізоване мережеве обладнання яке аналізує або захищає мережу.
- Внутрішнє, це те обладнання яке знаходиться у внутрішньому периметрі підрозділа та служить для обслуговування внутрішніх потреб підрозділа.

РОЗДІЛ 2.
АНАЛІЗ ПОБУДОВИ ВЗАЄМОДІЇ ІТ СЕРВІСІВ НА ПІДПРИЄМСТВІ

2.1. Архітектура ІТ-інфраструктури для забезпечення оптимального функціонування підприємства.

Для забезпечення бізнесових потреб в компанії була побудована наступна система з основними центрами концентрації інформаційних сервісів:

- Підрозділи (клініки)
- Контакт центр
- Центральний офіс
- Хмарний дата центр
- Дата центр (орендовані шафі)

Система базувалась на тому, шо в кожному з підрозділів була частина сервісів які надавалися для всієї мережі.

Наприклад, в головному офісі знаходилися два основних підрозділи, це головний офіс та контакт центр. В серверній кімнаті знаходяться всі сервери які відповідають за роботу контакт центру, та головного офісу (в основному це файлові шари). Таке розміщення спровокувало неможливість надання сервісу для контакт центру, коли було виявлено задимлення приміщення внаслідок загоряння електричного кабелю. Де який час Добробут не міг обробляти телефонні дзвінки у тому числі Швидкої допомоги. Другий приклад, центральний сервер аутентифікації знаходиться на одному з підрозділів. Під час відсутності електроенергії або каналів зв’язку на цьому підрозділі, все підприємство не мало змогу працювати. Частіше за все лікарі які були закріплені за іншим підрозділом, не могли працювати на іншому, в зв’язку з тим шо маршрутизація між підрозділами не працювала, або підрозділ зовсім не працював.

Всі підрозділи мають канали зв’язку від місцевих провайдерів з пропускною швидкістю від 100 до 1000 mbit/. Зазвичай це 2 провайдери з не

гарантованою швидкістю. Поверх цих каналів були побудовані VPN тунелі до кожного підрозділу. Канали VPN будувалися за технологію «Mesh» -це коли кожен підрозділ мав мінімум один тунель VPN до кожного підрозділу. В зв'язку з нестабільною маршрутизацію між підрозділами по каналам VPN, почалося впровадження об'єднання всіх підрозділів та дата центру технологією L2. Пропускна здатність каналів L2 від 100 до 1000 mbit/s. Побудовані вони, за принципом «зірка» центр зірки знаходиться у провайдера. Топ то, увесь внутрішній трафік, без захисту, проходить через мережу провайдера. В процесі побудови, було прийнято рішення робити канал L2 через двох провайдерів, так як один провайдер не зміг фізично покрити всі підрозділи.

Після низки подій, було прийнято рішення про агрегацію критичних серверів на більш захищених майданчиках. Для цього були орендовані:

- Дві серверні шафи у вітчизняного провайдера по розміщенню серверів в Дата Центрі.
- Виділені сервери у хмарного провайдера за межами території України.

Попередньо, була узгоджена схема побудови як розподілена зірка, з можливістю повної автономії підрозділів.

На кожному підрозділі була розведена локальна мережа, та побудована серверна кімната. Якщо приміщення були взяті в оренду, без можливості проведення ремонту, вся локальна мережа термінувалася в комутаційні шафи. При первинному ремонті або модернізації приміщень не було стандартів та вимог на прокладання кабелів локальної мережі і побудов серверних кімнат.

Кожен підрядник виконував ці роботи на свій розсуд. Якщо купували приміщення з прокладеною мережею то взагалі не проводилося її тестування на пропускну здатність. Також після ремонтів не проводилися роботи з атестації і перевірки на пропускну здатність

локальних мереж. Це призвело до того шо в підрозділах може бути швидкість від 10 Mbit/s хоча при цьому потрібно 1Gbit/s.

На робочих місцях в типових кабінетах необхідно мінімум 3 розетки для підключення до мережі:

- Стаціонарний комп’ютер або ноутбук
- Стаціонарний принтер або багатофункціональний пристрій
- Стаціонарний телефон

В деяких кабінетах потрібні були додаткові розетки для підключення медичного обладнання, наприклад апарати УЗД. (в більшості випадків, бізнес не знав де буде встановлено медичне обладнання, тому 4-ту розетку не проклали)

Підключення провайдерів здійснювалось за допомогою оптоволоконної технології. Якщо підрозділ базувався в жилому будинку, були випадки коли під’єднання «останньої милі» відбувалося звичайним кабелем 5е категорії. В кожен підрозділ заходить мінімум 2 провайдери інтернет і один провайдер L2. Договорів по SLA немає. Швидкість каналів зв'язку до 1 Gbit/s. На критичних підрозділах, швидкість каналу зв’язку була гарантована. На не критичних – плаваюча, так як основний зв'язок був через канали L2. Навантаження розподіляється наступним чином:

- Весь службовий трафік йде через канал L2 до дата центрів і інших підрозділів
- Доступ до Інтернету з робочих місць персоналу підрозділу та телефонія, через основного провайдера Інтернет.
- Доступ пацієнтів, гостей, особистих мобільних пристроїв співробітників підрозділу, через другого провайдера Інтернет.

В разі якщо не доступний канал зв’язку L2, то автоматично весь трафік йде через канал VPN, який побудовано через першого провайдера. При цьому трафік який йде до Дата Центру надається пріоритет перед трафіком який йде до Інтернету.

Якщо перший провайдер не може надати доступу в Інтернет для побудови каналу зв'язку через VPN, тоді канал зв’язку будується через другого провайдера. При цьому доступ до Інтернету надається самий найнижчий пріоритет.

В автоматичному режимі це не працювало, бо було не налаштовано. Локальна мережа будувалась за наступним принципом:

- Головний мережевий пристрій, якій виконує роль пограничного пристрою (термінує VPN підключення, надає та контролює доступ в Інтернет) та центрального маршрутизатора на підрозділі.
- Головний комутатор, рівня дистрибуції (так звані root), які комутують всі комутатори підрозділу, організовують відмово стійкість, маршрутизацію, безпеку. (В більшості випадків відсутні, а якщо присутні то не налаштовані)
- Комутатори рівня доступу. Виступають кінцевими точками котрі під’єднані до кінцевого обладнання. Поділяються за ознаками сервісу для яких були призначені. Наприклад, комутатори для сервісу печаті, комутатори для сервісу телефонніі, комутатори для точок доступу Wi-Fi.
- Бездротовий доступ, на базі технології WiFi. Точки доступу розташовані хаотичним образом, за принципом куди можливо дотягнутися дротом з серверної кімнати. Планування, радіорозвідка не проводилася взагалі. На кожному підрозділу був свій віртуальний контролер який повинен керувати точками доступу.
- Комутатори рівня доступу застосовувались для різних ролей, починаючі з збільшення кількості портів в кабінетах до передачі живлення для обладнання.

З метою підвищення відмовостійкості на кожному підрозділи, в серверних кімнатах були встановлені сервері в різних варіантах виконання. Де була можливість – в серверних шафах, де не було можливості – на полу. Більша частина серверів мала по два блока живлення, для підвищення

відмовостійкості. На сервері була встановлена система віртуалізації яка централізовано керувалась з центрального Дата Центру. Кожен вузол виртуалізації мав наступні віртуальні сервери:

- Локальный домен контроллер, для забезпечення авторизації та додаткових сервісів
- Локальный сервер файловий, для зберігання профілів користувачів та інших папок загального доступу та обміну (в тому числі аналізів)
- Локальний сервер телефонії, для забезпечення підрозділу стаціонарною телефонію.
- Локальний сервер контролер точок доступу Wi-Fi
- Локальний сервер системи контролю допуску
- Локальний сервер системи резервного копіювання
- Локальний сервер медичного призначення для зберігання та обробки знімків (КТ, МРТ)

Для зберігання резервних копій, а також для розширення дискового простору сервера, на підрозділах встановлювали дискові сховища збільшеного розміру. Основний функціонал – зберігання резервних копій локальної системи віртуалізації.

Системи відео нагляду знаходилися в окремій підсистемі та ІТ відділом не обслуговувалась.

В кожній стійкі знаходилось мінімум 2 джерела безперебійного живлення для забезпечення двох незалежних канали електроживлення для обладнання (Наприклад, в серверах, дискових сховищах будо встановлено по 2 блоки живлення, для підвищення автономності в разі виникнення аварійної ситуації). Сумарно було не менше 4-х джерел безперебійного живлення:

- 2 джерела на сервер та дискове сховище
- 2 джерела на мережеве обладнання та систему відеонагляду.

В зв’язку з тим шо кожне обладнання що встановлено в серверній кімнаті виділяє теплову енергію, були встановлені 2 кондиціонери, які працювали

цілодобово. Для систему допуску були передбачені системи контролю, але вони не застосовувалися.

Аналіз роботи підрозділу виявив наступні глобальні проблеми.

Автономність при відсутності доступу в Дата Центр:

- В разі не доступності медичної програми, підрозділ не може працювати з пацієнтами (не можуть переглянути історію, аналізи, заповнити результати візиту, то що)
- Не можуть авторизуватися користувачі, так як не були зроблені налаштування
- Користувачі які були закріплені за даним підрозділом, не можуть отримати доступ до своїх робочих даних (профілі користувачів)
- Не працює принтери на підрозділі.
- Доступ до резервних копій серверів і файлів користувачів, які зберігалися локально.

На кожному підрозділі є

- інформація яка дублюється, топ то на всіх підрозділах є інформація яка повинна бути в одному екземплярі.
- сервери які не використовуються за призначенням, або їх використання недоцільне.
- Налаштування не стандартизовані, як і конфігурації серверів
- Немає стандартизації по локальній мережі
- Немає стандартів по резервному копіюванню даних, немає карти створення резервних копій.

Приклад 1. На кожному підрозділу є загальна папка в який копіювалися результати аналізів. Папка займала простір порядку 12 ГБ на кожному с серверів. Користувачі періодично заходили на цю папку і переглядали результати. Ця схема працювала за історичним принципом. Була побудована коли канали Інтернет були не надійні. Моніторинг доступу

показав наступні результати, в середньому 1 користувач заходив до 5 разів за чергування. Максимальна кількість користувачів до 3-х (основна кількість користувачів, це працівники маніпуляційних кабінетів). Середня кількість заявок про непрацюючий сервіс – 2 протягом 3 днів. В залежності від зайнятості адміністраторів, час вирішення заявки через систему Help Desk до 1 години.

Приклад 2. В зв'язку з тим що все мережеве обладнання підключається за принципом надання сервісів, більшість мережевого обладнання було не до навантажено. Мінімальна кількість портів для мережевого обладнання 24. Для підключення точок доступу Wi Fi, використовується 6. Утилізація портів вираховується: 1 порт для під'єднання к комутатору рівня дистрибуції + кількість портів які використовується. Чім більше включено портів в роботу, тім дешевше буде ціна порта в комутаторі. Ціна порта коммутатора вираховується:

Вартість обладнання / кількість портів які задіяні = ціна порта

Якщо в нас 24 портовий коммутатор, який коштує 260 000 у.грн. то при повному заповнені вартість порта буде складати 10 840 у.е При заповнені у 7 портів – 37 160 у.грн.

Маємо дуже високу ціну за надання сервісу і низку використання обладнання. Це призводить до збільшення кількості обладнання та збільшення вартості сервісів

Приклад 3. Кількість віртуальних серверів при первинному аналізі склала більше ніж 320 одиниць. Робочий тиждень має 40 годинний ліміт робочого часу. Середній час котрий має витрати системний адміністратор для того щоб перевірити працездатність та проаналізувати роботу буде:

(40 годин * 60 мінут)/320 серверів = 7,5 хвилин. Це при тому шо системний адміністратор більш не чім займатися не буде.

Приклад 4. На кожному підрозділі встановлений сервер телефонії. На кожен сервер заведено мінімум 4 номерних телефонних лінії + 2-3 без номерних телефонних лінії. На пряму, в підрозділ можуть дзвонити тільки

персонал підприємства якій знає міські номера. Напряму з контакт центру або з другого підрозділу подзвонити – немає технічної можливості. Лікарі дзвонять тільки страховим компаніям. Моніторинг показав пік одночасних дзвінків – 4. Кількість піків – 2 за місяць.

Таблиця 1. SWOT аналізи за напрямками на 24.02.2022 (Взагалі по інфраструктурі)

Нове обладнання Резервне обладнання	Відсутність стандартів Відсутність спеціалістів Застаріло обладнання Неліцензійне програмне забезпечення
Готовність бізнесу к новим стандартам роботи Впровадження Service Desk (роботи по заявкам).	Зупинка роботи бізнесу - Кібер загроза - Відмова заліза - Ліцензійні проблеми

Таблиця 2. SWOT аналізи за напрямками на 24.02.2022 (По серверній архітектурі)

Велика кількість серверів (железа)	Відсутність спеціалістів Велика кількість обслуговування Наявність ліцензій Застаріле програмне забезпечення Безпека Відсутність документації
Економія Оновлення програмного забезпечення за рахунок існуючого серверного парку.	Простої бізнесу при відмові серверної частини (железо, софт) Часткове або повне відновлення працездатності на власному серверному парку.

Таблиця 3. SWOT аналізи за напрямками на 24.02.2022 (По мережевому обладнанню)

Сучасне обладнання Наявність резерву Мониторинг	Відсутність спеціалістів Застаріле обладнання Відсутність знань за напрямками Відсутність мережевої безпеки Відсутність інформаційної безпеки Відсутність стандартів та описів «Мертвий склад»
Стандартизація	Простої бізнесу при відмові мережевого обладнання

2.2. Роль ІТ-відділу в управлінні медичним закладом з оглядом на виклики, спричинені військовою агресією російської федерації.

Ключові показники котрі були поставлені перед групою

Якщо підрозділ працює:

- 100% доступність основних сервісів для забезпечення підрозділу (SLA не меньше 90%)

Якщо підрозділ не працює:

- Доступність до даних (ресурси загального користування, профілі користувачів які зберігалися локально на підрозділах)

Для досягнення таких показників було переведений попередній аналіз роботи підрозділів. В результаті цього аналізу було виявлено групи підрозділів:

- Які працюють цілодобово (24/7/365)
- Які працюють тільки в години прийому, але не працюють під час повітряних тривог
- Які не працюють, але мають електроживлення, канали зв’язку.
- Які не працюють, не мають електроживлення.

За результатами аналізу були визначені підрозділи які в першу чергу потребують переміщення даних. Був повторний проведений аналіз з яких причин підрозділи не працюють. Основна причина: Немає достатньої кількості персоналу або економічно не вигідно (немає достатньої кількості пацієнтів).

В зв’язку з цим був розроблений план дій який включав в себе наступні дії:

1. Вирішення де буде знаходиться основний центр обробки інформації, резервний центр обробки інформації, третій (свідок) центр обробки інформації.
2. Вирішення куди буде копіюватися інформація з підрозділів які тимчасово не працюють але є електроживлення та канали зв'язку

3. Вирішення куди буде переміщуватися техніка з підрозділів на яких відсутнє електроживлення або канали зв’язку.
4. Зменшення кількості серверів та об’єму даних.
5. Розробка нової схеми резервних копій:

- Критичних даних
- Користувацьких даних

6. Розробка розташування резервних копій:

- Гарячих даних, які мають актуальність не більш ніж 24 години, та можуть використовуватись у негайному відновлені працездатності.
- Теплі дані, які мають актуальність не менше одного тижня та можуть використовуватися у повному або частковому відновленні.
- Холодні дані, які мають актуальність під час всього періоду зберігання, яке регламентується внутрішнім наказом або законодавством.

Були поставлені наступні критерії працездатності ІТ сервісів для підрозділу (за період – місяць):

- Якщо працює підрозділ, на якому є електроживлення та канали зв’язку – 90%
- Якщо працює підрозділ, на якому є електроживлення але не має каналів зв’язку або обмежене – 60% (згідно переліку сервісів)
- Якщо на підрозділі відсутні електроживлення та зв'язок -10 % (забезпечення внесення даних з паперових носіїв, та синхронізація фіскальних принтерів з державною службою)
- Якщо підрозділ знаходиться на консервації – не застосовується але на вимогу можуть бути надані.

Обчислення простою за вини відсутності ІТ сервісів обчислювалось за таким принципом:

1. Лікарі. Розрахунковий час прийому лікаря 30 х.в. на один візит. Умовна ціна одного візиту становить 1 300 у.грн. (умовних одиниць). Кожен лікар повинен вести всі дані в Медичну Інформаційну Систему

(МІС). На це уходить приблизно 1/3 його робочого часу (прийом пацієнта).

- Якщо не працює робоче, це приблизно до 1 години на заміну кабінету. Топ то вартість простою буде 2600 у.грн. (Якщо є така можливість). В разі якщо такої можливості немає, лікар працює з паперовими носіями.
- Як шо у лікаря не працює система МІС, то лікар тимчасово переходить до паперових носіїв. Після основних часів прийому, він переносить дані до системи МІС, розрахунок приблизно до 10 хвилин. Топ то час на перенесення складає 433,33 у.грн. за один візит.
- Якщо у лікаря не працює принтер, то час простою розраховується як 5хв, які потребується доктору для того шоб забрати роздруковані паперові документи з рецепції. Топ то час простою 216,6 у.грн.

2. Рецепція. Не береться до уваги якщо є вихід одного з двох робочих місць.
3. Рецепція-Касове місце. Не береться до уваги, так як важлива синхронізація фіскального принтера (72 години) з державними службами
4. Маніпуляційний кабінет. В зв'язку з тим що не можливо визначити чіткій потік пацієнтів, в розрахунок беремо 1 300 у.грн. за годину.

Приклад 1. У лікаря не працює МІС на протязі 3 годин. Розрахунок буде виглядати таким чином: кількість візитів помножена на ціну візита та додаткові роботи по перенесенню даних з паперових носіїв

Простій=(кількість візитів * 1 300) + (кількість візитів * 433,33) = 10 399,98 у.грн.

В цьому випадку слід більш ретельно перевіряти за яких умов не працював МІС (фізичних, програмних, організаційних).

Приклад 2. В Підрозділі не працювали мережеве обладнання внаслідок виходу з ладу систем безперебійного живлення. Тоді для обчислення приймались витрати 50 000 грн в годину простою клініки.

Приклад 3. Ірпінь. Підрозділ працював за таким розкладом:

- Без світла. На паперових носіях, після закінчення робочого дня переносили данні в МІС в м. Києві.
- На генераторі, без каналів зв’язку .Працювали на паперових носіях, ввечері привозили до Києва паперові носії та фіскальний принтер для передачі даних до державних органів.
- На генераторі, канал зв’язку через мобільного оператора. Працювали видалено, тільки лікарі які потребували занесення даних до МІС та рецепція. Частково працювала аптека.

При такому розкладу, реакція на проблему збільшувалась до 6 годин.

2.3. Оптимізація роботи медичного закладу в умовах, пов’язаних з обмеженням ресурсів (електромереж, каналів комунікації).

В зв’язку з погіршенням ситуації навколо відмово стійкості, було проведений аналіз доступності даних та їх збереження.

Потенційні види загрози:

- Кібератака, втручання третіх осіб в роботу системи, які призводять до повної або часткової зупинки роботи.
- Катастрофічні, фізичні руйнування інфраструктурних пристроїв, які призводять до повної або часткової зупинки роботи.

Розподіл по загрозам. Кібератака 35% Катастрофічні 65%. Такий розподіл обумовлено ракетними загрозами при котрих є загроза втрачання резервних копій, які розміщені на магнітних дисках. Задачі від бізнесу– збереження даних та можливість відновлення, на будь яких потужностях.

Для зменшення впливу фізичного втрати інфраструктури та даних, була прийнята стратегія створення другої та третьої (свідок) майданчиків.

Перший майданчик – Дата Центр у котрому розташовані 90% даних. В даному Дата Центрі є всі необхідні умови, та додатково резервна серверна шафа.

Другий майданчик – корпус С на Севастопольської площі. На цьому майданчику сконцентровані 3 корпусу. Даний майданчик, генерує приблизно 50% всього доходу компанії. В разі недоступності всіх підрозділів цей майданчик обраний як опорне місце збору. Серверна кімната розташована у підвальному приміщенні, має два кондиціонери, резервування по живленню від генератора, джерела безперебійного живлення.

Третій майданчик (на момент обговорення ще проект) – підрозділ на пр. Бажана. Був обраний як резервний (свідок) на якому повинні зберегтися холодні дані, та повні резервні копії (дені, тижневі, місячні) Це обумовлено розташуванням серверного приміщення. Воно розташоване на останньому

поверсі, шо підвищує ризики втрачання серверної кімнати та повного руйнування обладнання без можливості відновлення.

Доповнення: До початку повномасштабного вторгнення розглядалися варіанти розміщення повного архіву даних за межами міста. Розглядалися два майданчика на базі підрозділів. Але під час перших днів воєнних дій , доступ до цих майданчиків був втрачений. Інформація яка була розташована на серверах - під загрозою потрапляння третім особам.

У разі критичного руйнування інфраструктури, 2 або більше майданчиків, розглядається варіант розгортання всіх сервісів в хмарному Дата Центрі.

Схема розташування сервісів: всі сервіси розташовані в Дата Центрі. Кожної ночі з Дата Центру робиться дві копії даних. Одна копія зберігається на дисковому просторі на другого майданчику, а ще одна на одному з підрозділів (третій майданчик ще не був введений в експлуатацію).

На всіх підрозділах були введені правила по резервному копіюванню даних, та архівацій. Одна копія даних повинна зберігатися локально, на підрозділі, а друга копія на другому майданчику.

В разі настання критичної ситуації, коли потрібно евакуювати техніку, то була обрана схема:

- Як шо серверне обладнання має критичне значення, то воно переміщується на перший майданчик – Дата Центр.
- Якщо серверне обладнання застаріле, може потребувати негайного технічного обслуговування, переміщуємо на другий майданчик. (Доступ до серверного обладнання в Дата Центрі здійснюється за попередньої домовленості, розташованій в другому кінці міста, що суттєво затрудняє оперативне обслуговування. Так як застаріле обладнання має високий ризик виходу з ладу та в умовах обмеження по персоналу, раціональне розташовувати обладнання як можна ближче до центру компетенції з обслуговування)

Канали зв’язку використовуємо існуючи:

- Канал L2 як основний, між підрозділами для критичної інформації та резервних копій.
- Перший провайдер, для виходу в Інтернет для медичних працівників за службовими обов’язками. В разі відсутності L2, виступає основним для критичної інформації.
- Другий провайдер, для виходу в Інтернет пацієнтів та супроводжуючих. В разі відсутності L2 і Першого провайдера , виступає основним для критичної інформації.
- В разі відсутності першого і другого провайдера, Інтернет трафік буде ходити через L2 з наименьшим приоритетом.
- Супутникові канали зв'язку не розглядаються у зв'язку з з великою вартістю та низькою швидкістю (це стосуються сервісів телефонії та відеоконференцій).
- Віддалений доступ надаємо в існуючих рамках, навантаження балансуємо на декількох адрес підключення. Це пов'язане в першу чергу з доступністю сервісу поза межами України. По друге, це давало змогу більш рівномірно навантажити обладнання і канали зв’язку.

KPI: SLA на перший і другий майданчики не менше 90% за умов якщо є електроживлення та канали зв’язку.

Проведений аналіз показав, шо роботи по переналаштуванню можемо виконати самостійно в робочий час.

Обмеження 1. Переміщення по місту під час активних воєнних дій обмежене. Доступ до приміщення Дата Центру, також обмежене. Топ то потрапити до серверів в Дата Центр дуже важко з логістичних питань. Тому було прийнято рішення про тимчасове переміщення техніки з підрозділів на яких немає електроживлення на другий майданчик.

Обмеження 2. Персонал який має обслуговувати техніку та робити пере налаштування роботи сервісів, знаходився на значній відстані від міста,

без постійного доступу до Інтернету. Це ускладнювало роботу діючих підрозділів. Тому було прийнято рішення, про групування переліку робіт під які знаходили спеціалістів.

Наприклад: під час воєнного часу, на другому майданчику були реорганізовані дві серверні кімнати. Ці роботи проводились у вихідні дні. Для цього було залучено 2 спеціаліста другої лінії технічної підтримки, які відповідали за налаштування мережевих приладів, виявляли збої в роботі і 3 спеціалісти першої лінії підтримки, які займалися комутацією та перевіркою працездатності кінцевого обладнання. Попередньо, цей самий проект оцінили не доцільним в зв'язку з великим обсягом робіт і неможливістю укластися в технологічні вікна так як працює швидка допомога та реанімаційна.

При проведенні аналізу було виявлені великі обсяги інформації котру необхідно тримати на серверах, які розміщуються на серверах. Внаслідок цього, резервні копії займають багато місця, що погано позначається на швидкості копіювання інформації на перший майданчик.

Великі за розміром об'єми даних були виявлені:

- Профілі користувачів. В цих профілях зберігалась інформація, яка стосувалась роботи користувача в папках “Робочій стіл”, “Мої документи”, електронна пошта, тимчасові папки для різноманітних програм. Наприклад месенджери, веб переглядачі.
- Папки загального користування. В цих папках знаходяться файли загального користування, від скановані копії документів. По факту виявити власників цих документів не було можливості. Чим довше працює підрозділ - тим більше невідомої інформації.
- Папки з результатами аналізів. В Цих папках зберігалась інформація про результати аналізів які приходили на загальну електронну пошту від лабораторій. На кожному підрозділі повна копія всіх результатів

аналізів. При цьому всі аналізи автоматично потрапляють до системи МІС.

Оптимізація: скорочення розмірів об’єму папок.

Очікуваний ефект який потрібно досягти:

- Зменшення часу загрузки профілів користувачів.
- Збільшення вільного простору на дисках, шо призведе до збільшення використання дискового простору без збільшення та оновлення серверів.

Економічний ефект який потрібно досягти:

- Завдяки зменшенню часу на обслуговано об’єму інформації, вивільняється час системних адміністраторів.
- Зменшується кількість заявок про недоступність сервісу
- Економія на закупках дискового простору, оновленню серверного парку, дискових полиць.

Кінцева розробка плану:

- Порівняння існуючих користувачів з неіснуючими (звільненими). Ефект – до 15% загального вільного простору відносно всього занятого.
- Стандартизація профілів користувачів. Був створений перелік месенджерів якими повинні користуватися лікарі та медичний персонал на робочих місцях. Вся інформація яка стосується пацієнтів і передається засобами месенджерів, павина бути занесена в МІС. Затверджений перелік веб переглядачів якими мають користуватися лікарі та медичний персонал. Тимчасові папки цих програм не мають інформаційної можливості, не приймають участь у резервному копіюванні, та можуть бути видалені без узгодженням с користувачем. Папки «Мої документи», «Робочій стіл», зберігаються окремо, маю дискову квоту згідно посадових обов’язків лікаря або медичного персоналу. Ці папки приймають участь у резервному копіюванні, можуть бути відновлені з архіву (глибина архіву не

менше 10 діб). Доступ до електронної пошти відбувається засобами веб переглядачами в режимі On-Line. Ефект – до 20% загального вільного простору відносно всього занятого.

- Стандартизація папок для сканування. Була розроблена концепція сканування, за якої кожен підрозділ сканує в свою папку. Через певний час, ця папка автоматично видаляється. З бізнесом погоджена така схема роботи. Ця папка не бере участь у резервному копіюванні. Ефект – до 3% загального вільного простору відносно всього занятого.
- Скорочення папок з результатами аналізів. Замість того щоб тримати на кожному підрозділі повну копію з результатами аналізів, було прийнято рішення про інсталяцію одного сервера, на якому буде повний перелік всіх аналізів. Так як між підрозділами є повний зв'язок по локальній мережі це дає змогу всім користувачам, яким потрібен доступ, заходити на цю папку. Це прозоро для користувачів, так як переключення проводилось поступово. Ефект – 30% загального вільного простору відносно всього занятого.

Крім вивільнення вільного простору необхідне було проаналізувати кількість серверів для можливості оптимізації.

Аналіз проводився в декількох напрямках:

- Кількість серверів ті їх ролі в інфраструктури компанії
- Час початку і кінця резервного копіювання

Аналіз кількості установок серверів та їх ролі в інфраструктури компаній виявив основні напрямки, які потребували подальшого аналізу. Аналіз повинен містить в собі, повну інформацію о доцільності інсталяції і кількість інсталяцій. Показники які показували успішність аналізу:

- Зменшення кількості серверів на 20-30%,
- Вивільняти вільного часу для адміністраторів
- Зменшення часу на обслуговування
- Зменшення звернень користувачів на відсутність сервісу
- Збільшення вільного простору

- Зменшення розмірів резервних копій

Сервери були згруповані у наступні групи:

- Домен контроллер. Ці сервера повинні були виконувати роль автономних центрів авторизації користувачів та сервісів. Між усіма контролерами повинна проходити повна синхронізація.
- Файлові сервери. Ці сервера мають папки загального користування в котрих розташовані папки загального користування та профілі користувачів. Повинні були забезпечити доступ до інформації при автономності роботи підрозділу.
- Сервери телефонії. Ці сервери забезпечували стаціонарний телефонний зв'язок.
- Сервер резервного копіювання. Ці сервери забезпечували резервне копіювання серверів які розташовувалися локально, на локальну дискову полицю і на віддалений репозиторій.
- Віртуальні контролери бездротових мереж (WiFi) Ці контролери відповідають за налаштування точок доступу WiFi на підрозділах.
- Сервери медичного призначення. Ці сервери займаються зберіганням медичної інформації або приймають участь в обслуговуванні медичного обладнання, яке встановлено в підрозділі.
- Сервери контролю доступу. Ці сервери контролюють рівні доступу до службових приміщень.
- Інші сервери. Ці сервери знаходяться на підрозділах для допоміжних цілей

План по оптимізації

- Домен контроллер. Повний аналіз показав, шо сервери налаштовані не вірно. Не виконують свої прямі ролі. Синхронізація між серверами може відбуватися до 3х діб. Топ то, якщо користувачу потрібно було надати нових прав в домені або змінити пароль, то це відбувалось в ручному режимі, тривало до 1 години. Встановлення оновлень на сервери тривало 1 тиждень у нічні часи. Для виправлення даної ситуації було прийнято

рішення про скорочення с 22 серверів до 4х, без втрати у продуктивності. Час на встановлення оновлень 2 години. Час відновлення з резервної копії до 3х годин всіх контролерів. Зменшення кількості ліцензій, якими потрібно покрити ці сервери. (Наприклад, ліцензія на Windows 2019 коштує приблизно 50 000 у.грн. При економії 18 ліцензій це приблизно 900 000 у.грн.. Це без врахування ліцензій на доп. Програмне забезпечення, наприклад антивірус)

- Файлові сервери, Повний аналіз показав шо кількість серверів може бути скорочена з 22 до 2х. Необхідно оптимізувати розташування інформації. Це дасть можливість встановлювати оновлення за 2 годинне технологічне вікно, а у разі якщо сервери будуть працювати в режимі кластеру, то встановлення оновлень буде прозоро для користувачів. (Наприклад, ліцензія на Windows 2019 коштує приблизно 50 000 у.грн. При економії 20 ліцензій це приблизно 1000000 у.грн.. Це без врахувань ліцензій на доп. Програмне забезпечення, наприклад антивірус).
- Сервери телефонії. Повний аналіз показав, шо за рахунок скорочення кількості серверів з 22 до 2х, можливо запровадити єдину наскрізну телефонну нумерацію, що підвішує комунікацію та знижує собівартість дзвінку між підрозділами. Як шо інтегрувати систему телефонії в систему контакт центру, це ще більше повисить гнучкість системи, зменшить ціну дзвінка між підрозділами. За рахунок зменшення кількості серверів можливо відмовитись від більшості міських телефонних номерів, шо призведе до економії до 70% без втрат продуктивності. Також це призведе до зменшення потенційних точок відмови, зменшення кількості часу на обслуговування та встановлення оновлень.
- Сервери резервного копіювання. Повний аналіз показав, шо треба пере побудувати схему керування процесом резервного керуванням. Кількість серверів не зміниться але економія бюджету порядку 22 ліцензій на Windows Server 2019 (1 100 000 у.грн.), можлива за рахунок переходу на

іншу операційну систему, та переміщення цих серверів більш захищений мережевий сегмент.

- Сервери медичного призначення. Цей сегмент серверів не розглядається, в зв’язку з тим шо він потребує більш глибокого аналізу із залученням медичних інженерів та інженерів постачальників медичного обладнання.
- Віртуальні контролери бездротового доступу WiFi. Повний аналіз показав, шо можливо скорочення з 22 контролерів до 1 го. За рахунок того шо, точки доступу можуть працювати де який час автономна, без контролеру, це дає можливість економити на кількості контролерів, та знизити кількість резервних копій. Економічний ефект досягається за рахунок зменшення кількості часу на регулярне обслуговування з боку системних адміністраторів.
- Сервери контролю доступу. Цей сегмент серверів не відноситься до зони відповідальності ІТ відділу. Потенційно можливо скорочення більш ніж на 50%, але потребує залучення спеціалістів компаній які монтували системи доступу. В зв’язку з тим шо цих компаній які монтували обладнань багато, працівники які монтували, не документували налаштування та розміщення обладнання, питання оптимізації не доцільно на даному етапі.
- Інші сервери. Аналіз не проводився так як не виявлені або неможливо отримати інформацію про власника сервісу який працює на даному сервері. В більшості випадків це сервери з компаній які були поглинуті, сервери знаходяться в режимі «Холодні дані», для того щоб можливо було отримати інформацію за минулий час.

Таким чином бізнес поставив задачі по зниженню витрат на обслуговування на 30%, без змін в обслуговуванні. Керівництво ИТ відділом очікувало зменшення витрат за рахунок перерозподілу технічних ресурсів ті вивільнення робочого часу системних адміністраторів. Це було необхідно враховуючи гібридний графік роботи адміністраторів. Гібридність полягала в тому, щоб рівномірно загрузити адміністраторів тою

роботою, яку вони можуть виконувати в обмежених воєнними діями ситуаціях. Наприклад: адміністратори які були в Києві займались фізичним обслуговуванням техніки. Адміністратори які знаходились видалено, займались оптимізацією та налаштуванням обладнання. Також, в нових умовах було зрозуміло шо закупку нового обладнання не будуть проводити в зв'язку з нестабільністю цін, поганою логістикою. Тому було треба формувати свій запас обладнання в декількох локаціях.

Після перших ударів по критичної інфраструктурі стало зрозуміло шо попередній аналіз про оптимізацію інфраструктури був вірним напрямом, але між аналізом, планом впровадження, імплементацією потрібно зменшувати проміжки часу. Це можливо зробити у разі якщо всі перетворення можуть бути зроблені власними силами і на власному обладнані.

Перши відключення електроживлення виявили наступні проблеми:

- Джерела безперебійного живлення в серверних кімнатах не були підключені по схемі відмово стійкості. Обладнання що мало було підключено не було збалансовано по джерелам безперебійного живлення. У деяких джерел безперебійного живлення, обладнання було підключено до розеток на були включені лише фільтри по електроживленню, без резервування.
- У більшості джерел безперебійного живлення застарілі акумуляторні батареї, автономність яких до 10 хвилин (цього часу було достатньо для проведення місцевих переключень).
- Регламентних робіт про тривалість роботи джерел безперебійного живлення не проводили, тому часу автономії розрахувати було неможливо.
- В більшості джерел безперебійного живлення відсутній моніторинг, що призводило до того шо, сервери були не вірно вимкнені. (якщо

сервери були раптово вимкнені, це може призвести до втрачання інформації. До цього дуже чутливі сервери баз даних).

Так як підрозділи були підключені по електроживленню як звичайні підприємства, а не медичні заклади, це призвело до раптового зникнення електроживлення. На декількох майданчиках сталась ситуація коли робочі комп'ютери продовжували працювати від локально встановлених джерел безперебійного живлення, а доступу до сервісів не було (джерела безперебійного живлення в серверних кімнатах вимикались в зв'язку з старими акумуляторними батареями).

Після другої хвилі атак на енергогенеруючі підприємства виявили наступні проблеми:

- Після перших атак пройшло досить мало часу для того щоб змогли повністю зарядитися акумуляторні батареї. Як виявилося, до повного заряду потрібно до 2х діб. Топ то, після другої хвилі відключень, автономність серверних кімнат скоротилась на 70%. В тих шо тримали до 10 хвилин -практично до 3х хв.
- Після подачі електроживлення спостерігаються великі перевантаження на електричну мережу, шо призводить до переходу джерел безперебійного живлення в режим аварійності.
- Відключення електроживлення відбувається не одночасно по всьому місті. Це призводить до того, шо частково не доступні сервіси.
- Більшість інтернет провайдерів мають проміжні точки підключення, в яких також пропадає живлення. Частіше за все, «остання миля» йде з одного технічного приміщення. Якщо в цьому приміщенні пропадає електроживлення, то у обох провайдерів шо були заведені в підрозділ, як незалежні – продає зв'язок.
- При віялових відключеннях не доступні профілі користувачів які працюють на інших підрозділах.
- Після раптових відключень світла, де які сервери частково виходили з ладу.

- В результаті помилки в архітектурі розміщення серверів, стався випадок, коли раптове зникнення електроживлення призвело до відключення центрального домен контроллера, якій відповідає за аутентифікацію користувачів в домене. Це призвело до неможливості авторизуватися новим користувачам, заходити через віддалений доступ іншим користувачам.

Згодом виявились шо більшість провайдерів інтернет не має на опорних точках резервування по електроживленню (електрогенератори), ті шо були - не працювали. Не вистачало кваліфікованих спеціалістів для робіт по відновленню мережі. Тому в перші дні склалась катастрофічна ситуація коли на підрозділі могло бути відсутнє електропостачання та канали зв'язку або було електропостачання але не було каналів зв'язку. Це призвело до того шо всі контакт центри не змогли приймати дзвінки. В тому числі швидка допомога.

Після наради з представниками від бізнесу були визначенні наступні напрямки та пріоритети:

- Швидка допомога
- Стаціонар
- Контакт центр
- Підрозділи
- Центральний офіс

Після проведення додаткових нарад по оптимізації розміщення користувачів, було прийнято рішення про об'єднання деяких напрямків на одній локації які були запечене електроживленням:

- Швидка допомога (контакт центр по прийому дзвінків) зі стаціонаром на Севастопольській площі, на опорній базі Швидкої допомоги.
- Контакт Центр по різним локаціям де була можливість. Наприклад, частково розміщення працівників в адміністративному поверху на Севастопольської площі. Частина розміщувалась в приміщенні актової зали в підрозділі на Оболоні.

- Працівники які працювали в Центральному Офісі могли працювати видалено або на будь якому підрозділі який був забезпечений електроживленням. (під час вимушеного перебування на підрозділі, працівнику офісу не гарантувалось виділене робоче місце на час роботи)

Попередні вимоги показників від бізнесу для стаціонарів з цілодобовим графіком роботи стали (з умов постійного руйнування енергетичної системи, каналів зв'язку):

- Локально розміщені сервери: не менше -90% (SLA-2,5 години на добу)
- Локально розміщене мережеве обладнання - 90% (SLA-2,5 години на добу)
- Для сервісів які надаються локально – 90% (SLA-2,5 години на добу)
- Для сервісів які надаються по каналам зав’язків які не належать та не обслуговуються підприємством – 70% (SLA -7 годин на добу)

Попередні вимоги показників від бізнесу для підрозділів за графіком роботи стали (з умов постійного руйнування енергетичної системи, каналів зв'язку):

- Локально розміщені сервери: не менше -90% (SLA-2,5 години на добу)
- Локально розміщене мережеве обладнання - 90% (SLA-2,5 години на добу)
- Для сервісів які надаються локально – 90% (SLA-2,5 години на добу)
- Для сервісів які надаються по каналам зав’язків які не належать та не обслуговуються підприємством – 60% (SLA -9,5 годин на добу)

По суті було припущення що підрозділи можуть не працювати, так як може бути відсутнє електроживлення і канали зв’язку.

Попередні вимоги показників від бізнесу для Центрального Офісу стали (з умов постійного руйнування енергетичної системи, каналів зв'язку):

- Локально розміщені сервери: не менше -90% (SLA-2,5 години на добу)
- Локально розміщене мережеве обладнання - 90% (SLA-2,5 години на добу)
- Для сервісів які надаються локально – 90% (SLA-2,5 години на добу)
- Для сервісів які надаються по каналам зав’язків які не належать та не обслуговуються підприємством – 60% (SLA -9,5 годин на добу)

Для працівників центрального офісу було запропоновано працювати віддалено, за наявністю електроживлення ті каналів зв’язку.

Перше чергові заклади стосувалися підвищення автономності серверних кімнат. Для цього був проведений збір інформації про автономність роботи серверних кімнат. Це були усні скарги користувачів і дані моніторингу з серверів. Були сформовані три групи:

- Перша. Джерела безперебійного живлення які не тримають автономність, або автономність менше 10 хв. Інформація про заміну акумуляторних батареї відсутня, або взагалі не проводилися заміна.
- Друга. Джерела безперебійного живлення, автономність яких сягає до 20 хв. Інформація про заміну акумуляторної батареї або проведення технічного огляду / тестування має дворічну давнину
- Третя. Нові джерела безперебійного живлення, які введені в експлуатацію менше року.

Перша група потребувала негайної заміни. Для цього були проведені пошукові роботи з залученням оптимізації.

Приклад: Підрозділ в місті Ірпінь був повністю знеструмлено тривалий час під час окупації та відновлення. На час коли були відсутні електроживлення та канали зв’язку, сервер та дискова полиця були переміщені до м. Київ. Після відновлення електроживлення та каналу зв’язку, обладнання було повернуто до серверної кімнати. Під час віялових відключень, було прийнято рішення про переміщення усього серверного обладнання до Дата Центру (у другу резервну шафу).

Мережеве серверне обладнання перемістити на склад (холодний резерв). Джерела безперебійного живлення (2шт), перемістити на склад для подальшого розподілення на підрозділ якій потребує заміни. Ті, шо залишилися повинні були забезпечувати електроживлення для мережевого обладнання, системи контролю допуску, системи відеонагляду. Таким чином було досягнуто ряд переваг:

- Автономність підрозділу підвищується приблизно на 40% за рахунок того що всі основні тяжкі споживачі були переміщені до Дата Центру (Пояснення: найпотужнішими споживачами електроенергії є електродвигуни. В серверах це вентилятори системи охолодження на материнської платі, блоках живлення, жорстких дисках. Чим тепліше або гарячиш становиться в серверній кімнаті, тім швидкість обертання вентиляторів зростає. Це обумовлено тим що серверне обладнання виділяє багато теплоти, а повинно працювати за певних теплових умов. При відключені електроенергії, в серверній кімнаті відключається кондиціювання. Так роблять в 99% при проектуванні серверних кімнат. Тому маємо споживання, яке зростає на протязі того як росте температура в середні серверної кімнати. Мережеве обладнання має теж вентилятори охолодження, але вони менш потужні. Мережеве обладнання більш стійке к високим температурам. Таким чином автономність праці мережевого обладнання порівняно з серверним, значно довша)
- Доступність профілів користувачів, які базувались локально на підрозділі, підвищилась до 99%

Задля досягнення енергетичного балансу між мережевим обладнанням та системою відеонагляду, було прийнято рішення про підключення їх на різні джерела безперебійного живлення. Це дало змогу продовжити роботу мережевого обладнання ще на 10%. (Пояснення: Система відео нагляду складається з серверу в якому є жорсткі диски,

вентилятори та активного мережевого обладнання, які живлять камери. Ці пристрої споживають багато електроенергії)

Таким чином на підрозділі залишилось два джерела безперебійного живлення, які забезпечують автономність підрозділу. Якщо на підрозділі буде відсутнє електроживлення або канали зв'язку, це не як не позначиться на роботі інших підрозділів якщо там будуть працювати лікарі з непрацюючого підрозділу. Інші два джерела безперебійного живлення будуть використані на іншому підрозділу. Ремонт, діагностика, заміна акумуляторних батарей буде проводитись коли на це буде змога та наявність батарей на складі у постачальника.

Друга група потребувала заміни також як і перша. Виняток був тільки в тому випадку, якщо друга група знаходилась на підрозділі в якому встановлений генератор. Час автономності не повинен перевищувати 15 хв. 5 хв, це резерв який відведено на те шо перші спроби запустити в роботу генератор були невдалими.

Третя група розглядались як донори, які після оптимізації змогли стати гарячим резервом.

Під час проведення аналізу стало зрозуміло шо прогнозувати відключення електроживлення неможливо, так як відключення ставалися раптово (без попереднього попередження), генератори були не на всіх підрозділах.

Після спілкування з представниками бізнесу було прийнято рішення, шо підрозділи переходять на паперовий режим роботи підприємства у світлу пору доби, якщо раптово зникає світло. Контакт центр направляє пацієнтів тільки в ті підрозділи в яких є світло. Там де є можливість забезпечити мед обладнання джерелами безперебійного живлення з резерву відділу інформаційних технологій – пропонуємо.

На базі групи системних адміністраторів другої лінії був сформований загін швидкого реагування. Основна задача якого буда демонтувати всю серверну техніку з підрозділів в яких вимкнуто електроживлення. Потім

перемістити цю техніку до Дата Центру або на резервну площадку (корпус С на Севастопольській площі). Дозволений час – після заходу сонця, так як тоді припиняв роботу підрозділ, як шо в нього не було світла. Складність поставленої задачі полягає в тому що більшість підрозділів знаходиться на значній відстані від кінцевих пунктів, в серверних кімнатах немає світла, після того як техніку демонтують немає можливості протестувати працездатність підрозділу. Попередньо були проведені розробки плану дій, так як треба було демонтувати техніку, відвести її в Дата Центр, встановити, ввімкнути, скомутувати, перевірить шо вона працює, потом повернуться до дому. Це все до початку комендантської години. Були приговорені маршрути поїздок.

Попередньо, домовилися з операційними директорами підрозділів про візити до них, під час відключення електрики. Домовились зі службою охорони про те шо співробітники відділу інформаційних технологій мають право забирати техніку з підрозділів без дозвільних документів або підтверджень.

План дій був наступний:

- Група вирушала на підрозділ по дзвінку адміністратора підрозділу о том шо світло зникло.
- Після того як група провела демонтаж обладнання, вони повідомляли старшого адміністратора по мережі, для того щоб він починав пере комутацію маршрутизації.
- Після того як обладнання будо встановлено в серверну шафу та скомутоване в Дата Центрі, старший групи повідомляв старшого мережевого адміністратора про початок фізичного тестування наявності обладнання в мережі. Поки проводилось тестування, заповнювалися документи в Дата Центрі. Група не покидала приміщення Дата Центру поки старший мережевий адміністратор все не перевірить та не підтвердить працездатність.

- З моменту підтвердження працездатності встановленого обладнання, старший мережевий адміністратор проводить всі мережеві налаштування (в нічний неробочий час), для того щоб з самого ранку підрозділ міг працювати в повному обсягу.
- Під час нічного тестування працездатності мережевих підключень на підрозділі, була залучена нічна зміна технічної підтримки першої лінії.

Під час демонтування, також вивозилися джерела безперебійного живлення на другу резервну площадку (корпус С Севастопольська площа), в якості «гарячого резерву». Після того як на підрозділі були вивезені джерела безперебійного живлення та серверне обладнання почали звільнятися серверні стійки, серверні шафи шо призвело до збільшення вільної площі.

В даній ситуації дуже не хватало поінформованості про відсутність електроживлення, каналів зв’язку на підрозділах. В деяких джерелах безперебійного живлення, були відсутні плати моніторингу. В деяких вони не були налаштовані. В тих шо були встановлені, не давали повної інформації так як канали зв’язку, з вини провайдерів, були недоступні до того моменту як пропадає живлення. Також, ця ситуація дуже дратувало керівництво, так як вони рахували те шо немає каналів зв’язку це вина відділу інформаційних технологій. Для підвищення поінформованості керівництва, та підвищення оперативності в вирішенні питань передачі провайдерам інформації про відсутність каналів зв’язку, було прийнято рішення про застосування системи моніторингу підрозділів по інтернет провайдерам. В хмарному Дата Центрі було налаштовано сервер моніторингу, який відслідковував доступність провайдерів, а через них – наші підрозділи з інтернету. Налаштування серверу моніторингу каналів зв'язку, дало змогу зняти навантаження на адміністраторів відділу інформаційних технологій, тому шо заявки з недоступність каналів зв’язку приймаються до розгляду тільки тоді коли всі канали були

недоступні. Але потім це вже трансформувалось в те шо, у керівного складу компанії був постійно відкритий моніторинг каналів, якщо немає зв'язку, то цім питанням вже займається відділ інформаційних технологій. Ще одним з важливих моментів, який показав моніторинг каналів зв’язку, те шо стало зрозуміли критерії надійності провайдерів (розглядалися два критерія - час відсутності каналу зв'язку, технічна підтримка).

Після того як на з підрозділів була демонтована серверна техніка, постало питання про переведення роботи підрозділів на генератори. В зв’язку з тим шо була відсутня інформація по фактичному електричному навантаженню на підрозділах, були придбані слабкі однофазні побутові генератори. Перші пуски генераторів показали шо джерела безперебійного живлення в серверних кімнатах в процесі зарядки практично навантажують генератори на всі 100% , це без урахування роботи техніки на підрозділі. Встановлювати великі професійні не було можливості по ряду причин, починаючи з того шо нема місця на вулиці, закінчуючи тим що їх не було в наявності.

Для забезпечення роботи підрозділів треба було повністю переглядати навантаження на генератори, тим самим оставляти тільки те шо необхідно для роботи підрозділу під час відключення електроенергії.. Після наради з системними адміністраторами першої лінії технічної підтримки, медичними інженерами, аптекарями, операційними директорами були надані наступні групи, які повинні працювати від генераторів:

- Серверна або комутаційна кімната
- Кабінети лікарів (кількість регламентується по навантаженню на генератор і не повинна перевищувати кількість прийомів)
- Маніпуляційні (холодильне обладнання, де зберігаються ліки, вакцини котрі потребують певних температурних умов)
- Зона рецепції з касовим обладнанням.

- Світло в кабінетах та коридорі.

План дій наступний. Після вимкнення електроенергії кабінети продовжують працювати в звичайному режимі. На джерела безперебійного живлення підключені тільки комп'ютери, принтери на пряму в розетки (впровадження такої схеми дало змогу працювати автономна приблизно в середньому від 20 до 30 хв). Якщо лікарю потрібно було надрукувати заключення або інший документ, він печатав на рецепцію. (нажаль, не на всіх підрозділах були зроблені окремі групи споживачів електричної енергії. Була домовленість, шо розподілом електричної частини займається інший відділ) Також в кабінетах де були встановлено спеціалізоване медичне обладнання, були встановлені серверні джерела безперебійного живлення (за умов акустичного шуму). Це давало змогу закінчити обстеження і зберегти результати.

Також були приговорені сервіси які повинні бути доступні з підрозділів:

- Медична інформаційна система
- Інтернет (службовий та гостьовий)
- Телефонія (стаціонарна)
- Система друку
- Система відеоспостереження та контролю доступу.

Після проведення наради, треба було вміститися в ті потужності які може видати генератор. Для цього були проаналізовані споживачі які знаходяться в серверній або комутаційної кімнатах. Ці споживачі наступні:

- Сервери, споживають багато енергії та виділяють багато тепла, можуть працювати тільки в певних кліматичних умовах.
- Мережеве обладнання, споживає не багато електроенергії, виділяють помірну кількість тепла, можуть працювати при підвищених температурах.
- Джерела безперебійного живлення споживають багато електроенергії під час заряду, виділяють багато тепла під час автономної роботи.

- Кондиціонери, споживають помірну кількість електроенергії під час роботи, але бувають пікові сплески електроенергії під час включення компресору.

По факту, все серверне обладнання та два джерела безперебійного живлення були переміщені до Дата Центру або резервних точок. При такому розкладі, в серверних, комутаційних точках зникає необхідність в кліматичному забезпечені. Топ то, можемо вимкнути кондиціювання серверних приміщень. Це знижує споживання десь приблизно на 50%. Але ті джерела безперебійного живлення, що залишаються, дуже потужні для існуючих в наявності генераторів. Проаналізувавши споживачів виявили дві категорії:

- Мережеве обладнання і обладнання інтернет провайдерів.
- Системи відеоспостереження та контролю доступу.

Було прийнято рішення провести тестове переключення всього обладнання на одне джерело безперебійного живлення потужністю 3000 КВА (це приблизно 2 кВт). Після переключення, стало зрозуміло шо джерело безперебійного живлення потребує професійного генератора.

Було прийнято рішення використовувати менше потужні джерела безперебійного живлення, які використовують для комп'ютерів але сумарна споживана потужність мережевого обладнання перевищувала потужність джерела безперебійного живлення та не забезпечувала потрібного часу автономісті.

Після нарад с адміністраторами першої лінії технічної підтримки був проведена аналіз по оптимізації мережевого обладнання. Було прийнято рішення про пере комутацію мережевого обладнання.

Перша група, це ті комутатори які будуть підключені до генератора. В них входять:

- Комутатори та обладнання провайдерів
- Комутатори які надають доступ до локальної мережі та принтерів на рецепції

- Комутатори які надають доступ до телефонії та надають живлення до телефонних апаратів.
- Комутатори які надають доступ до інтернету через Wi Fi та надають живлення до точок WiFi. В разі можливості, треба об’єднувати точки доступу WiFi та стаціонарні телефони на одному комутаторі.

Друга група, це те обладнання яке приєднане до існуючих джерел безперебійного живлення, та не бере участь в роботі мережі під час роботи від генератора. Наприклад, це комутатори медичного обладнання, принтери. До цієї групи було віднесено відеоспостереження та систему контролю доступу .

Завдяки такій схеме розподілу навантаження вдалося вивільнити близько 30% зайвих комутаторів які були навантажені не більш як на 40-60%, шо дало до 20 хв автономності, поки запускають генератор.

Найголовніше, шо підрозділи почали використовувати, як центри незламності в яких є постійний доступ до інтернету через гостьову мережу Wi Fi (безкоштовно та без обмежень часу і швидкості)

Висновки. При реорганізації серверних кімнат, з'явились наступні позитивні моменти:

1. Зменшилось електричне навантаження та споживання електроенергії на 50%, за рахунок переміщення серверного обладнання до Дата Центру
2. З'явився склад резервних джерел безперебійного живлення.
3. З'явився моніторинг каналів зв'язку, та почало з'являтися розуміння технічних вимог до провайдерів інтернету.
4. Зменшилися заявки від користувачів на відсутність сервісу та документів з папок загального користування
5. Звільнилося обладнання яке можливе використовувати в інших локаціях під інші цілі.
6. Збільшилась лояльність до бренду завдяки тому шо були відкриті пункти незламності з постійним доступом до мережі інтернет.

РОЗДІЛ 3.
ПОБУДОВА ВІДМОВОСТІЙКОЇ ІНФРАСТРУКТУРИ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ РОЗРОБЛЕНИХ ІННОВАЦІЙ

3.1. Високотехнологічні рішення для забезпечення сталого функціонування підприємства.

Приклад необхідності розуміння різних видів резервного копіювання. В середині літа 2022 року компанія розробник медичної інформаційної програми повідомила про те що і її програмі є помилка яка може призвести до зупинки всієї програми. Був розроблений план по тестуванню цієї помилки на тестової базі, потім приймати рішення як її долати. Вся складність полягала в тому шо потрібно було зупиняти роботу медичної інформаційної системи. Розробка варіантів виправлення цієї помилки були закінчені на початку жовтня 2022 року. Почалося тестування по виправленню цієї помилки. Після початку відключення електроживлення, роботи зупинилися так як не було вільних людських ресурсів, постійні проблеми з каналами зв'язку, відсутність електропостачання на площадках розробників програмного забезпечення. Після того як з'явилась можливість повернутися до тестування виправлення помилки, ситуація почала бути критичної. Після розробки карти ризику та численних нарад, був обрано один варіант котрий потрібно було протестувати. До цього моменту розробники не мали уяви як себе поведе система, чи буде вона працездатна після виправлення помилки.

Під час тестування виправлення помилки на сервері сталась зупинка бази даних, та її пошкодження без можливості відновлення її працездатності. Відновлення можливе лише як копія поточної робочої бази. Після проведення копіювання бази даних, роботи по тестування продовжились. З розробниками провели бесіду про зберігання даних на серверах. Слід розуміти шо помилка була прогнозованою, ми мали змогу бачити її темпи

росту. Тестування продовжувалось, але людський фактор призвів до того що весь сервер на якому проводились тестування було втрачено. Втрачено дисковий масив без можливості відновлення (відновлення було можливе, але на це були потрібен час, та після відновлення не гарантувало працездатність). В зв'язку з тим що серверне обладнання з підрозділів було переміщено до Дата Центру, то мались технічна можливість реалізовувати відновлення працездатності сервера.

Був проведено попередній аналіз. Повна резервна копія сервера, знаходилась на видаленій площадці. Повний розмір резервної копії складає приблизно 15 Тбайт в зжатому вигляді . Якщо брати швидкість 1 Гбіт/с каналу L2 та 30% загрузку каналу, то тільки на копіювання необхідно приблизно 2 доби. Це якщо не буде розривів каналів зв’язку. Але, це не гарантує шо після того як резервна копія буде розвернута, то сервер зможе працювати. Проте файл резервної копії бази даних займає приблизно 6 Тбайт, та знаходиться в тому ж Дата Центрі в локальної мережі. Топ то можливе копіювання значно швидше без можливості втрати зв’язку по локальної мережі.

Було запропоновано два шляхи:

- Починаємо копіювати повну резервну копію сервера з видаленої площадки, щоб потім можливо її було розгорнути.
- Починаємо розгортання нового сервера, на технічних можливостях які здобули за рахунок переміщення техніки з підрозділів, для того щоб на ньому розгорнути тільки базу даних для продовження тестування.

Під час розгортання резервного сервера, почалось копіювання резервної копії бази даних. Це дозволило скоротити час простою. На момент закінчення копіювання, програмне забезпечення має бути встановлене та налаштоване. Ліцензійність не беремо до уваги, так як є тимчасові ліцензії, які дозволяють користуватися програмним забезпеченням. На час тестування, нам вистачить тимчасових ліцензій.

За основу був взятий другий варіант, розгортання нового сервера. В процесі нарад з компанією постачальником програмного забезпечення з’ясувалось шо потрібне встановлювати таке саме програмне забезпечення, як на головному сервері. Складність складається в тому, шо будо встановлено застаріле програмне забезпечення, яке зникло з масового обігу (просторів інтернету). Після аналізу репозиторіїв з програмним забезпеченням які є в відділі інформаційних технологій, стало зрозуміло шо програм інсталяторів програмного забезпечення немає. Почався пошук програм інсталяторів по можливим каналам та персональним зв’язкам. Нам вдалося знайти всі необхідні інсталятори програмного забезпечення, інсталювати новий сервер. Через деякий час скінчилось копіювання резервної копії бази даних. Нам вдалось відновити роботу бази даних приблизно за 6 годин, та продовжити тестування виправлення помилки.

Після успішного тестування виправлення помилки настав час проведення робіт на робочій базі. Були розроблено плани, та етапи. Ці плани та етапи були основані на попередньому опите, якій ми отримали під час тестування. Всі роботи були заплановані на нічній час. Підрозділи з цілодобовим чергуванням мали інструкції як користуватися паперовими носіями в разі необхідності. Зі сторони відділу інформаційних технологій були підготовлені резервні потужності та перелік програм інсталяторів. Були розміщені різні копії, для різних варіантів розгортання. Перед початком проведення виправлення помилки, були зроблені повні резервні копії баз даних.

Перший етап пройшов дуже гарно, без зауважень. Під час другого етапу стався технічний інцидент, який поставив під сумнів подальшу працездатність всієї медичної інформаційної системи. Виявилась помилка яка призвела до виходу з ладу дискової системи (практично така, як під час першого тестування на тестовому сервері). Це почалось в тій момент, коли зв'язок з командної підтримки був обмежений

(технічно). Був розпочатий план по розгортанню резервного сервера для проведення робіт по відновленню бази даних. Після того як з’явився зв'язок з командою розробників з’ясувалося що на сервері, окрім основної бази в якій виправляли помилку, є ще бази даних, які приймають участь в роботі медичної системи. Також є налаштування для правильної роботи медичної системи які ніхто не пам’ятає, немає записів як треба проводити налаштування, немає резервних копій.

В зв’язку з новими фактами, роботи проводилися в двох напрямах, підготовка для розгортання з резервної копії, та спроби відновити працездатність існуючої. Власними силами, адміністратори другої лінії технічної підтримки змогли повернути сервер до робочого ладу. Це зайняло багато часу, але вдалось вкластися в технологічне вікно. Подальші етапи пройшли без помилок та форс мажорних обставин.

Цей приклад наведений про то шо в компанії, були зроблені наперед правильні кроки по агрегації потужностей, на базі Дата Центру, шо надало можливість оперативно проводити дії з відновлених робіт.

3.2. Стратегії масштабування та ризик-менеджмент медичного бізнесу.

Навесні 2022 року, було прийнято рішення про відкриття двох тимчасових підрозділів в м. Львів та Івано-Франківськ. Це були невеликі підрозділи для наших працівників, які були змушені тимчасово перебувати за межами своїх домівок.

Критерії від бізнесу. Тиждень на відкриття. Повинні працювати всі сервіси крім місцевої телефонії. SLA не нижчі 90%.

Технічне забезпечення цих підрозділів було здійснено за рахунок раніше закритих підрозділів. (один підрозділ переїхав до корпусу В на Севастопольської площі, інший був закритий тому шо був не рентабельний ще до початку воєнних дій). Адміністратор другої лінії технічної підтримки, було командировано на виконання цього завданя. Це було обумовлено тим шо одним співробітником можливо закрити декілька задачі:

- Налаштування мережевого обладнання для роботи з медичною інформаційною системою, поштою, папки загального користування то шо (робота другої лінії технічної підтримки).
- Налаштування робочих місць користувачів, принтерів, касового місця то шо (робота першої лінії технічної підтримка)
- Допомога медичним інженерам по встановленню медичного обладнання та підключення його до мережі.

Всі роботи були виконані вчасно, без затримок. Відбувалися в такому порядку:

- Все мережеве обладнання яке повинне було встановлено в нових підрозділах, було налаштоване в Києве.
- Після приїзду на підрозділ, адміністратор проводив підключення мережевого обладнання до обладнання провайдерів.

- Після перевірки, шо на мережеве обладнання подається канал зв’язку від провайдера, проводились налаштування по побудові каналів зв'язку з Дата Центром.
- Поки адміністратори другої лінії видалено налаштовують канали зв’язку, проводились роботи по налаштуванню робочих місць на місцях (силами командированого адміністратора).
- Після всіх налаштувань, проводилась перевірка доступності всіх сервісів.

Висновок: На прикладі цих двох підрозділів було протестовано ряд нових видів підключень, які дали змогу в майбутньому (на прикладі підрозділу в м. Ірпінь) надавати змогу видаленої роботи користувачів і підрозділів. Також була протестована робота без локального розміщення серверів.

В червні місяці 2022 року, бізнес повідомив про відкриття стоматологічного підрозділу. ІТ відділу була поставлена задача відкрити підрозділ як можливо швидше, так як медичне обладнання все стояло. Завдяки стандартам, які почали з’являтися в відділі інформаційних технологій, підрозділ почав робити через 1,5 доби повністю забезпеченим доступами до всіх сервісів. Після відкриття, були зроблені певні коригування в стандарті по відкриттю нових підрозділів. Це стосувалось тестування локальної мережі перед початком встановленням техніки. Також були внесені нові умови по термінам відкриття підрозділу. Ці умови були узгоджені з представниками бізнесу, та прийняті до виконання.

В березні місяці 2023 року, почалися роботи по завершенню ремонтних робіт в підрозділі на пр. Бажана.

Перед початком монтажних робіт підрядниками, відділом інформаційних технологій, був проведений аналіз по перегляду первинних планів по розміщенню обладнання, цілей, етапів робіт:

- Було проведено декілька навчальних нарад з метою підвищення рівня обізнаності адміністраторів стосовного умов розміщення мережевого обладнання в мережевих шафах на поверхах.
- Проведені наради стосовно ролі даного підрозділу в іт інфраструктурі компанії. Це підрозділ який працює цілодобово, має незалежні генератори та розвинену інфраструктуру. Було запропоновано зробити третьою резервну площадку з повним резервуванням по сервісам.
- Проведена повна інвентаризація залишків мережевого обладнання. Складений перелік техніки для відкриття підрозділу. Перелік враховував попередній досвід оптимізації комутаційних, серверних кімнат.

За результатами цих нарад було обрано наступний напрям руху:

1. Даний підрозділ розглядати як сховище для резервних копій, так як карта ризиків дає дуже негативний результат в разі руйнування будівлі (буде дуже проблематично дістатися до серверів під час руйнування будівлі, є 100% впевненість шо неможливо буде відновити дані з цих серверів та на момент відновлення, інформація може бути вже не актуальна)
2. Повний перегляд розміщення мережевого обладнання в стійках на поверхах і серверній кімнаті.
3. Складання плану адресації
4. Вибір двох надійних провайдерів. Результат вибору повинен базуватись на за результатами моніторингу та можливістю надавати прямій канал зв’язку з опорних точок, де є резервування по електроживленню і підключенню.
5. Мережеве обладнання встановлювати те яке раніше стояло на підрозділі (перед початком ремонтних робіт, на підрозділі було замінено все мережеве обладнання на нове)

6. Зробити єдиний телефонний сервер між підрозділами (пр. Бажана – Севастопольська площа).

Після переробки проектної документації по розташуванню обладнання, вдалося вивільнити близько 30% мережевого обладнання. При кінцевій інсталяції ця цифра зросла до 40% за рахунок того шо не всі кабінети були заповнені технікою та багато портів були переведені в резерв за рахунок того шо техніка була встановлена в іншому місці. Було обрано двох провайдерів інтернет, які за результатами моніторингу показали самий більший UpTime роботи каналів зв'язку. Під час технічного відкриття питань до відділу інформаційних технологій не було. Всі сервіси працювали. Також під час запуску даного підрозділу було впровадження сервісу телефонії, який був побудований на єдиному сервері. Цез значно підвищило комунікацію між підрозділами (наприклад, між базами швидкої допомоги).

Висновки: Як шо до проектуванню мережевої інфраструктури були залучені адміністратори відділу інформаційних систем, то вдалось би отримати значну економіє на прокладанні локальної мережі. Початок переходу на сервісну модель обслуговування, показав перспективності розвитку.

Під час закінчення ремонтних робіт в підрозділі на пр. Бажана, почалися роботи по проведенню ремонтних робіт на новому підрозділі яке розташоване в готеле «Славутич» (на цих двох підрозділах ремонтні роботи були розпочати ще до початку воєнних дій та були на різних стадіях готовності).

Враховуючи попередні домовленості, адміністратори другої лінії технічної підтримки були залучені до проектування серверної кімнати ще на етапі проектної документації та прокладання локальної мережі. Це дало змогу:

- Відмовитись від великих серверних стійок та перейти на мережеві шафи

- Перенести розташування мережевих шаф на стіни, замість розташування посеред кімнати
- Вивільнити багато вільного місця (приблизно 70%).
- Провести нараду з медичними інженерами про додаткові порти для медичного обладнання.
- Провести радіо розвідку для більш оптимального розташування точок доступа WiFi для більш рівномірного покриття, та мати відповідну документацію.
- Після проведення прокладання локальної мережі, провести тестування, на відповідність пропускної швидкості та категоричності.
- Знизити вимоги до охолодження серверної кімнати, так як в неї немає критичного серверного обладнання.
- Відкрити підрозділ вчасно, без затримок.

Висновки: під час відкриття нового підрозділу, з застосуванням нових стандартів, дозволило заощадити близько 70% вільної площини. Підвищило комунікацію за рахунок використання сервісу телефонії, сервісу печаті. Почали з’являтися проекти и паспорти локальної мережі, системи WiFi. Почались комунікації з медичними інженерами на предмет прокладки комунікацій під медичне обладнання. Бізнес почав прислуховуватися до порад відділу інформаційних технологій, так як відділ почав показувати економічну ефективність та надійність.

Під час технічного відкриття підрозділу в готелі «Славутич» стало відомо, шо буде переїзд стоматологічного підрозділу в інше місце. По факту це був переїзд в існуючий бізнес, де було встановлено все медичне обладнання.

Завдання перед відділом інформаційних технологій полягало в тому щоб надати доступи до сервисів в Дата Центрі з нової локації. Було прийнято рішення провести налаштування обладнання яке є в наявності на складі, для економії часу на локації. Обладнання яке буде зняте з існуючого підрозділу пройде технічне обслуговування, потім буде переміщено на

склад. Перед тим як проводити монтаж мережевого обладнання, було проведено існуючої локальної мережі на відповідність. Такий підхід надав наступні переваги:

- Час переключення каналів зв’язку в Дата Центр становив приблизно 20 хвилин.
- Час простою при проведенні робіт з монтажу мережевого обладнання 1,5 години. Топ то сумарний час простою при комутації – до 2х годин, проти 2 тижнів які були озвучені за старими стандартами.
- Проведення сканування локальної мережі виявило що де кілько портів не відповідають вимогам, де які не працюють. Це зекономило час при встановлені техніки на робочі місця, так як не витрачався час на з’ясування причин непрацездатності сервісів.
- Показало бізнесу в необхідності тестування локальної мережі перед придбанням приміщень з ремонтом, який унеможливлює прокладання нової або ремонт існуючої.
- Складання карти мережі та підтвердження існуючої значно скорочує час встановлення техніки.

Висновки: початок демонтажу техніки на існуючому підрозділі почався о 8-00 годині ранку. Об 14-00 на новому підрозділі закінчили встановлення техніки, та тестування каналів зв'язку. Топ то, при застосуванні єдиних стандартів для всіх підрозділів, документування всіх налаштувань, використання однотипного обладнання від одного бренду, стандартизовані сервіси, це все призводить до скорочення часу на розгортання техніки та каналів зв’язку з Дата Центром для надання сервісів. Замість 2 тижнів – 1 доба.

Висновок з висновків: При використані Дата Центрів (основного та резервного), необхідно розуміти шо ключовою точкою відмово стійкості є Дата Центри (основний та резервний). Слід розробляти окремі SLA для підрозділів та Дата Центрів. Наприклад, на підрозділі достатньо мати «теплий склад» з комп'ютерів для робочих місць, а на складі тримати

декілька примірників мережевого обладнання. В разі якщо виходить зі строю комп'ютер на робочому місці, то адміністратори першої лінії проводять видалени заміну без залучення адміністраторів другої лінії технічної підтримки. В разі якщо виходить з ладу мережеве обладнання, тоді зі складу береться аналогічний примірник, на нього заливається резервна копія конфігурації. Після чого це обладнання доставляється на підрозділ. Допускається втрата всього мережевого обладнання, тому шо його можливе оперативно замінити на аналогічне. В цьому питанні, буде довше проводитись фізичне з'єднання, ніж повернення працездатності сервісів. При цьому всі дані будуть доступні з других підрозділів. Сервіси будуть доступні через мобільну мережу передачі даних або видалений доступ.

В разі якщо в Дата Центрі вийде з ладу мережеве обладнання, то це буде відчутно на всій мережі підрозділів. Тому на Дата Центрах потрібно встановлювати обладнання яке має резервування. Також необхідно враховувати ризики фізичної втрати всього Дата Центру. Для цього на резервній площадці потрібно мати актуальну копію всіх даних, які можуть бути оперативно використані при відсутності основного майданчику.

В зв’язку з переміщенням великої кількості техніки, з’явилась технічна необхідність в веденні обліку комп’ютерної, серверної, мережевої техніки. Ця необхідність включала в себе:

- Кількісний склад, скільки техніки взагалі є
- Модельний ряд, які моделі техніки у нас є в наявності
- Стан, в якому стані знаходиться техніка, була в використанні чи ні
- Гарантійна-експлуатаційні, знаходиться лі на гарантії, знята з виробництва.

Ці властивості надали можливості розділити техніку за наступними напрямками:

- Холодний склад, це та техніка яка не приймала участі в оперативній роботі, або знята з використання ввиду того шо закінчились її експлуатаційні терміни або не має застосуванні в поточної роботі або нова техніка яка знаходиться на зберіганні. Зазвичай це складські запаси які розташовані на відстані від оперативного складу, терміни доставки обладнання становить 1-2 добу.
- Теплий склад, це та техніка яка приймає участь в оперативній роботі, та може використана у разі якщо проходить масовий вихід з ладу техніки. Зазвичай, терміни поставки такої техніки зі складу до 6 годин.
- Гарячий склад, це техніка яка знаходиться в оперативної роботі, може бути використана в будь який момент. Техніка знаходиться в безпосередньої близькості від чергових адміністраторів відділу інформаційних технологій, має кількісні показники по знаходженню на складах.

Для підтримки рівня SLA не нижче 95% на підрозділах, для першої лінії технічної підтримки, були розміщені додаткові комплекти картриджів для принтерів, комплекти клавіатур і мишок та за можливістю комп'ютери (моноблоки) та принтери. Ці одиниці техніки, користувачі можуть змінити самостійно. Не доцільне розміщення додаткових комплектів мережевого обладнання, так як:

- Специфічне. Під кожен сервіс або задачу треба свій набір обладнання.
- Коштовне. За рахунок того шо обладнання відмово стійке коштує дорого.
- Монтується в мережеву стійку. Для заміни потребує специфічних знань та навичок. Звичайний користувач не може замінити.
- Всі налаштування, та резервна копія налаштувань знаходиться на центральному сервері з котрого проводиться оновлення обладнання.
- Вихід з ладу значно рідше ніж звичайних робочих станцій або принтерів.

Тому доцільніше на гарячому складі тримати де кілько повних комплектів техніки.

В разі підтвердження від адміністраторів другої лінії технічної підтримки, виходу з ладу мережевого обладнання, простіше перемістити обладнання адміністраторам другої лінії для проведення налаштувань. За час проведення робіт з копіюванням нових налаштувань на мережеве обладнання, вирішується питання хто буде їхати на підрозділ. Після узгодження всіх питань, бізнесу було повідомлено через який час буде відновлено роботу підрозділу.

Висновок: Ведення типів складів, надало можливості:

- Оперативно відслідковувати залишки
- Формувати потреби в запчастинах, техніці.
- Фінансово оцінити кількісні показники залишків на холодному складі, шо призвело до появи «Мертвого складу». Мертвий склад це склад техніки яка є новою не вживаною, та є поняття того шо на момент того как виникне в ней потреба вона буде морально і фізично застаріла. Використання недоцільне.

До початку воєнних дій, відділом інформаційних технологій була впроваджена система Help Desk. Основна задача цієї системи полягала в тому шо би реєструвати та аналізувати всі заявки які поступали з боку користувачів на роботу інформаційних систем. За результатами роботи даної системи були зрозумілі основні напрями за якими необхідно було проводити роботи по оптимізації та перехід на сервісні моделі обслуговування. На приклад, як шо раніш не працювало будь яка програма або були проблеми з каналами зв’язку у всьому були винні адміністратори першої та другої лінії. Після впровадження Help Desk почали розділяти заявки від користувачів. Більшість заявок була адресована медичним системам та системам обліку. Кількість заявок

стосовно не працюючого мережевого обладнання або серверного становила близько 20%.

Після аналізу заявок стало зрозуміло шо є проблема з друком на підрозділах. Часто поступали скарги на те шо під час прийому не друкують принтера. Було запропоновано зробити сервіс який буде базуватися на двох серверах для балансування загрузки та відмово стійкості. Після впровадження, заявки знизились на 80%, налаштування нового принтера робиться автоматично, навантаження по встановленню нового принтера першою лінією технічної підтримки на 90%.

Основним здобутком впровадження Help Desk для другої лінії технічної підтримки стало зрозуміло де є технічні моменти які треба проаналізувати та вдосконалити, а де «Людський фактор». Стало зрозуміло шо треба зменшувати «Людський фактор» за рахунок впровадження стандартів та інструкцій. Також треба підвищувати знання персоналу, через навчання.

В зв’язку з тим шо, під час оперативного переміщення техніки з підрозділів в Дата Центр та другу резервну площадку, ряд серверів були розміщені фізично дуже близько, знаходяться в одній мережі. Це призводило до перенасиченості та надмірності. В деяких моментах, наприклад з телефонією, це приводило до колізій та помилок в роботі. Було прийнято рішення про трансформацію однотипних серверів в сервіси.

Приклад: На кожному підрозділі був свій домен контроллер. При переміщенні всіх серверів до Дата Центру необхідність в такій кількості на однієї локації відпала. Замість 22 треба було 4. Тому було прийнято рішення про видалення зайвих серверів. Це дало:

- Зростання вільного простору за рахунок вилучення серверів
- Зменшення часу на обслуговування
- Зменшення розміру резервної копії
- Зменшення часу відновлення всього домену у разі катастрофи.
- Зменшення часу на встановлення оновлень.

За рахунок того шо з’явились вільні ресурси, стало можливе впровадження нових проектів без придбання та залучення нових ресурсів. Більшість проектів може бути реалізоване за власний рахунок.

На базі застарілої техніки з’явилась можливість відточувати свої знання та створювати віртуальні лабораторії.

Впровадження стандартизації в роботі відділу інформаційних технологій дозволило провести скорочення адміністраторів першої лінії. За рахунок того шо було скорочено персонал але не був скорочено фонд оплати праці, всі працівники мали підвищену заробітну плату відносно інших працівників компанії. Скорочення працівників не вплинуло на якість роботи сервісів та роботу першої лінії технічної підтримки, так як більшість монотонної роботи була скорочена. З’явилась автоматизація більшості процесів.

1.1. Людський.

1.1.1. Людський фактор. Слід розуміти що, при будь якому випадку як шо буде персональна загроза або загроза для сім’ї

або рідним, співробітник буде думати про забезпечення безпеки для себе і своїх рідних. Тому слід будувати систему таким чином, щоб вона могла працювати незалежно, без втрачання персоналу.

1.1.2. Компетенція. Необхідно враховувати шо технології потребують певних знань та навичок. Чим більше практики, тим менше часу простою внаслідок виходу з ладу техніки. Слід точно розуміти границі своїх можливостей компетенцій та аутсорсовії. Під час воєнних дій може скластися ситуація коли аутсорсні компетенції будуть недоступні. Визначення компетенцій повинно базуватися не тільки на закритті поточних питань, але на вирішені нетипових ситуацій ті прогнозуванням на майбутню перспективу.

1.1.3. Нестача кваліфікованого персоналу може стати перепоною в обслуговуванні техніки, наданні консультацій користувачам стосовно роботи програм. Слід чітко розуміти шо не кваліфікований персонал це потенційна точка загрози яка має підвищені права. Це може спричини більші руйнування системи, ніж простої системи.

1.2. Обладнання

1.2.1. Повна втрата обладнання внаслідок бойових дій або вибухової хвилі. Необхідно тримати холодний запас техніки та запчастин для відновлених робіт.

1.2.2. Обслуговування техніки або програмного забезпечення може бути припинено або надаватись не своєчасно. Тому необхідно заздалегідь створити резерв з примірниками програмного забезпечення, надрукувати інструкції шо робити з програмним забезпеченням на випадок не доступності обслуговуючого персоналу (бажано з малюнками)

1.2.3. Заміна запчастин може бути ускладнена з відсутністю поставок та роботи обслуговуючих компаній. Тому слід створити резерви, які треба розподілити між різними (географічно) майданчиками. Бажано надрукувати покрокові інструкції по заміні запчастин, для того щоб не кваліфікований персонал зміг провести ремонтні роботи.

1.3. Аутсорсові послуги. Під час активних бойових дій більшість аутсорсових послуг буде недоступна. Тому треба подбати про те щоб були інструкції як треба діяти при певних умовах коли потрібні аутсорсові послуги.

1.4. Компанія.

1.4.1. Закриття підрозділів внаслідок руйнувань або скорочення. Необхідно розуміти де розташувати персонал, шо з ним робити дали (звільняти, переводити на другі посади)

1.4.2. Закриття компанії в наслідок банкрутства або повного руйнуванні інфраструктури. Необхідно знайти тимчасовий варіант співпраці з співробітниками до нового їх працевлаштування.

1.4.3. Невиплата заробітної плати. Потрібно розглянути альтернативні шляхи підвищення залученості персоналу в робочій процес щоб таким чином зберегти кадри.

Таблиця 4. Перелік ризиків, вплив на роботу та план реагування на ризики.

№	Ризик	1-й План дій	2-й План дій	Вплив на роботу	Тригер
1	Відмова каналу зв'язку на підрозділі одного провайдера	Перехід на резервний	Перехід на L2	Середній	Повідомлення моніторингу зі сторони Хмарного Дата Центру
2	Відмова двох каналів доступу до інтернет на підрозділі	Перехід на L2 якщо заведене, Якщо ні, перехід на паперові носії	Чекаємо на відновлення зв'язку	Важливій	Повідомлення моніторингу зі сторони Хмарного Дата Центру, Повідомлення моніторингу каналів зв'язку з Дата Центру або резервного майданчику.
3	Відмова каналу зв'язку в Дата Центрі одного провайдера	Перехід на резервний	Перехід на L2	Середній	Повідомлення моніторингу зі сторони Хмарного Дата Центру
4	Відмова двох каналів доступу до інтернет в Дата Центрі	Перехід на L2	Чекаємо на відновлення зв'язку	Важливій	Повідомлення моніторингу зі сторони Хмарного Дата Центру, Повідомлення моніторингу каналів зв'язку з Дата Центру або резервного майданчику.
5	Відмова всіх каналів зв'язку в Дата Центрі	Перехід роботи на резервний майданчик	Починати розгортати резервні копії в Хмарному Дата Центрі	Критичній	Повідомлення про відсутність сервісів від моніторингу, находження скарг через Help Desk
6	Відмова каналу зв'язку в резервному майданчику одного з провайдерів	Перехід на резервний	Перехід на L2	Середній	Повідомлення моніторингу зі сторони Хмарного Дата Центру

7	Відмова двох каналів доступу до інтернет в резервному майданчику	Перехід на L2	Починати розгортати резервні копії в Хмарному Дата Центрі	Важливій	Повідомлення моніторингу зі сторони Хмарного Дата Центру, Повідомлення моніторингу каналів зв'язку з Дата Центру або резервного майданчику.
8	Відмова всіх каналів зв'язку в резервному майданчику та Дата Центрі	Перевірка на фізичну цілісність майданчиків	Починати розгортати резервні копії в Хмарному Дата Центрі	Критичній	Повідомлення про відсутність сервісів від моніторингу, находження скарг через Help Desk
9	Вихід з ладу мережевого обладнання на підрозділі	Провести дії по відновленню працездатності	Підготувати та встановити резервне обладнання	Середній	Повідомлення про відсутність сервісів від моніторингу, находження скарг через Help Desk
10	Вихід з ладу мережевого обладнання в Дата Центрі	Перевести роботу на резервне обладнання	Підготувати та встановити резервне обладнання	Середній	Повідомлення про відсутність сервісів від моніторингу
11	Вихід з ладу мережевого обладнання на резервній площадці	Провести дії по відновленню працездатності	Підготувати та встановити резервне обладнання	Середній	Повідомлення про відсутність сервісів від моніторингу
12	Вихід з ладу серверного обладнання в Дата Центрі	Перевести роботу на резервне обладнання	Підготувати та встановити резервне обладнання відновитись з резервної копії	Критичній	Повідомлення про відсутність сервісів від моніторингу, находження скарг через Help Desk
13	Вихід з ладу серверного обладнання на резервній площадці	Провести дії по відновленню працездатності	Підготувати та встановити резервне обладнання відновитись з резервної копії	Критичній	Повідомлення про відсутність сервісів від моніторингу, находження скарг через Help Desk

14	Підтвердження фізичне руйнування Дата Центру і резервного майданчику	Починати розгортати резервні копії в Хмарному Дата Центрі	Готувати нову інфраструктуру на базі існуючого обладнання на складі.	Критичній	Повідомлення про відсутність сервісів від моніторингу, находження скарг через Help Desk, голосові повідомлення від керівництва
15	Кібер загроза (шифрування даних)	Перевірка та відновлення з архівів	Встановлення нової інфраструктури	Критичній	Находження скарг через Help Desk
16	Втрата системного адміністратора 2-й лінії	Перекладання обов'язків на іншого адміністратора	Пошук аутсорсового спеціаліста	Середній	Голосове або письмове повідомлення (персональне, керівництво) про втрату адміністратора.
17	Вихід з ладу одного з двох джерел безперебійного живлення серверного обладнання розташованого на резервному майданчику	Перевести роботу на другий	Перевести роботу від електромережі, підготувати срочну заміну	Не критичній	Повідомлення від моніторингу або усне повідомлення від системних адміністраторів 1й лінії
18	Вихід з ладу одного з дисків в дискової полиці в Хмарному Дата Центрі	Попередити технічну службу Хмарного Дата Центру про необхідність заміни	Перевести критичні сервіси на інші потужності	Не критичній	Повідомлення від моніторингу або письмове повідомлення від технічної підтримки Хмарного Дата Центру

3.3 Роль персоналу та управління людьми для оптимізації роботи Дата Центру медичного закладу

Управління командою системних адміністраторів є важливим аспектом забезпечення безперебійної та ефективної роботи інформаційної інфраструктури. Ось декілька методів та підходів, які були застосовані для управління командою системних адміністраторів другої лінії технічної підтримки IT відділу :

- Чіткі та прозори зони відповідальності : Для кожного з адміністраторів були визначені свої зони відповідальності та SLA по сервісам які вони підтримують. Також були визначені перелік документів які повинні бути заповнені.
- Ефективний комунікація: Була забезпечена відкрита комунікація як всередині команди так і с зовнішніми користувачами. Проводились регулярні оперативні збори, вся інформація була доступна по всім каналам зв’язку.
- Навчання та розвиток: Одним із важливих напрямів було застосування безперервного процесу навчання через виробничу необхідність, через власний приклад. Були організовані тренінги, на яких члени команди ділилися власним опитом та інструментарієм. Одним з головних здобутків, це те шо системні адміністратори почали візуалізувати інформацію та спілкуватися на зрозумілому рівні
- Розподіл завдань: Під час складних часів коли вимикалось світло, було важливо правильно розподіляти цілі та задачі між членами команд. Були враховані професійні можливості, звички та особливості спеціаліста як людини, які потім дали змогу більш точно розподіляти завдання та отримувати гані результати.
- Створення процедур та документації: Для забезпечення стабільності в роботі, почали розроблятися стандарти та процедури. На базі цих

стандартів та процедур почали з’являтися документи та регламенти, які змогли забезпечити економію часу на виконання завдань, за рахунок того шо вся інформація знаходиться в одному місті, має логічну структуру, постійно оновлюється.

- Використання управлінських інструментів: Для контролю роботи систем була заведена система моніторингу та HelpDesk. Завдяки цьому спростилися задачі по працездатності системи та терміни виконання завдань системними адміністраторами.
- Мотивація та визнання: Для підвищення продуктивності команди, були розроблені та запропоновані керівництву ряд заходів, такі як KPI, премії, то що. В середині команди регулярно проводились порівняльні заходи, які визначали прогресуючий ріст системних адміністраторів і команди в цілому.
- Управління стресом: Головною проблему в роботі команди були повітряні тривоги в розрізі безпеки своїх сімей. Для того щоб зменшити емоційне напруження, дозволявся гібридний режим роботи. Після закінчення визначних етапів, проводились неформальні зустрічі на яких промовлялися всі негативні емоції. Це стосувалось і роботи всередині колективу.
- Відкрите співробітництво: Дуже приймалося коли в команді співробітники ділилися інформацією, опитом, допомагали колегам по роботі на добровольчих засадах. Це стосувалось не тільки робочих питань, а також сімейних.
- Врахування думки команди: Кожен член команди, повинен мав бути свою думку. Всі думки обговорювалися. Всі думки розкладались на карті ризиків перед імплантаціями. Як що у системного адміністратора не хватало опиту, то йому розповідали та ділилися опитом члени команди, які його мали.
- Управління командою системних адміністраторів вимагає збалансованого підходу, який поєднує технічні знання з навичками

управління та комунікації. Використовуючи ці методи, ви зможете забезпечити ефективну та продуктивну роботу вашої команди адміністраторів.

Всього виявлено 320 віртуальних серверів які є в наявності в компанії. На кожен сервер повинно витрачатися не менше як 1 години впродовж місяця на перегляд подій та здоров’я системи. Топ то маємо що в місяць адміністратор повинен витратити 320 годин часу на огляд серверів. Приймаємо шо в місяць приблизно 4 тижня по 40 годин, топ то 160 годин в місяць. З цього виходить шо нам потрібно мати 2 адміністратора які будуть тільки займатися серверами переглядаючи їх здоров’я. Так як адміністратори займаються розгортанням нових сервісів, налаштуванням та іншими завданнями нам потрібно шо найменш 4 адміністратора тільки на віртуальні сервери. Якщо провести скорочення серверів по підрозділам, тоді число серверів скоротиться до 260 шт. шо може зменшити кількість адміністраторів до 2х. Один адміністратор працює, на іншого відкрита вакансія. Економічний ефект крім скорочення ліцензій на 3 600 000у.грн. складає: 2 адміністратора по 36 000 у.грн. в місяц = 72 000у.грн. без рахувань забезпечення робочим місцем та пр.

3.4. Економічний ефект імплементації запропонованих інновацій.

Таблиця 6. Економічний ефект по поточним підрозділам при оптимізації розміщення серверів та сервісів

№	Найменування	Кіл-ть, шт	Ціна у.грн.	Кількість підрозділів	Всього у.грн.
1	Ліцензія на Windows для Домен контролеру	1	50 000	18	900 000
2	Ліцензія на Windows дляСерверу резерних коп	1	50 000	18	900 000
3	Ліцензія на Windows для Серверу збереженя даних	1	50 000	20	1 000 000
4	Сервер телефонії	1	40 000	20	800 000
5	**Всього по підрозділу**		**190 000**		
6	**Всього по підрозділам**				**3 600 000**

Таблиця 7. Економічний ефект при відкритті нових підрозділів

№	Найменування	Кіл-ть, шт	Ціна у.грн.	Кількість підрозділів	Всього у.грн.
1	Ліцензія на Windows для Домен контролеру	1	50 000	4	200 000
2	Ліцензія на Windows дляСерверу резерних копії	1	50 000	4	200 000
3	Ліцензія на Windows для Серверу збереженя даних	1	50 000	4	200 000
4	Сервер телефонії	1	40 000	4	160 000
5	Фізичний сервер	1	480 000	4	1 920 000
6	Дискова полиця	1	440 000	4	1 760 000
7	Джерело безперебійного живлення	2	50 000	4	400 000
8	**Всього по підрозділу**		**1 160 000**		
9	**Всього по підрозділам**				**4 840 000**

Таблиця 8. Економічний ефект від додаткових заходів

№	Найменування	Кіл-ть, шт	Ціна у.грн.	Кількість підрозділів	Всього у.грн.
1	Адміністратори 1й лінії	5	20 000		**100 000**
2	Адміністратори 2й лінії	2	36 000		**72 000**
1	Мертвий склад	1	4 800 000		**4 800 000**

ВИСНОВКИ

1. Проведення стратегічних сесій. Це дало змогу відслідковувати напрями за якими потрібно рухатися зараз та планувати подальші стратегічні кроки. Ці сесії стали більш реалістичними та деталізованими, направлені в першу чергу на збереження того шо є, максимальне використання наявних запасів ті технологій.
2. Введення матричної системи взаємодії між адміністраторами першої та другої ліній технічної підтримки та керівництвом компанії і відділу інформаційних технологій.
3. За рахунок оптимізації серверних, комутаційних кімнат та оптимізації роботи складу:

- «Мертвий склад» на понад 4 800 000 у.грн.
- З’явились поняття Холодного, Теплого, Гарячого складів, розташуванню обладнання.
- Резерв по серверному обладнанню
- Виведення з роботи застарілого серверного обладнання
- Створення полігону для тестування та прогнозування роботи мережевого та серверного обладнань.
- З’явився додатковий вільний простір до 30% від загального

4. Завдяки оптимізації розміщенню серверів в Хмарному Дата Центрі, та скороченню кількості віртуальних серверів, вдалося отримати резерв по серверним потужностям до 20%.
5. Середній SLA по мережевому та серверному обладнанню складає не нижче 90%
6. Застосовані нові принципи стандартизації та єдиних термінів, найменувань то шо.
7. За рахунок скорочення віртуальних серверів, змогли провести глобальні оновлення систем безпеки та встановити необхідні оновлення на мережеву інфраструктуру та серверну.

8. Керуючись на інформацію зі моніторингових серверів, було проведення скорочення провайдерів інтернету з 17 до 2х. Були побудовані нові лінії зв’язку до опорних пунктів провайдерів які мають резервування по електроживленню та підключенню до інтернет.
9. Були побудовані пункти Незламності в яких був наданий інтернет для потреб населення під час необхідності.
10. Так як з’явилась вільна техніка, почали розвиватися нові проекти.
11. Завдяки впровадженню роботи по збору та категоризації заявок від користувачі про недоступність сервісів, стало зрозуміло що в більшості випадків винне не серверне або мережеве обладнання, а налаштування програмного забезпечення.
12. Почався перехід від серверної моделі, коли під кожну роль інсталювався відповідний віртуальний сервер, до сервісної. Це коли надається сервіс для використання. Сервери інсталюються тоді коли це технічно необхідно.
13. Почалась проводитись мережева сегментація, яка змогла підвищити безпеку, зробити прогнозованість роботи мережі.
14. Оптимізація кількості серверів дала змогу збільшити вільного простору та зменшити кількість часу на обслуговування.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Карен Фелан, книга «Вибачте, я зруйнувала вашу компанію». Коли бізнес-консультанти – проблема, а не рішення», видавництво «Наш формат», 2021, 216 с. ISBN 978-617-7866-92-2;
2. Свен Карлссон, Йонас Лейонхуфвуд, книга «Spotify навиворіт. Як шведський стартап здійснив Музичну революцію», видавництво «Yakaboo Publishing», 2021, 296 с., ISBN 978-617-7544-89-9
3. Марк Рендольф, книга «Netflix. Ця ідея Ніколи НЕ спрацює», видавництво «Форс», 2020, 320 с., ISBN 978-966-993-204-4
4. Тімур Ворона, книга «Дмитро Дубілет. Бізнес на здоровому глузді. 50 Ідей, як досягти свого», видавництво «BookChef», 2020, 300 с., ISBN 978-966-993-251-8
5. Стівен Кові, книга «7 звичок Надзвичайно ефективних людей», видавництво «Клуб сімейного дозвілля», 2012, 384 с., ISBN 978-966-14-2945-0
6. Віл Сторр, книга «Наука сторітелінгу. Чому історії впливають на нас і як ними впливати на інших», видавництво «Наш формат», 2022, 224 с., ISBN 978-617-7973-73-6
7. Олександра Фідкевич, книга «Як начинити гадюку салом. Рецепт створення бізнесу на творчості», видавництво «#книголав», 2023, 256 с., ISBN 978-617-8012-87-8
8. Річ Карлгаард, книга «Людський фактор. Секрети тривалого успіху видатних компаний», видавництво «#книголав», 2017, 336 с., ISBN 978-966-97610-7-1
9. Леррі Вайдел, книга «Серійній переможець: п'ять Дій для створення вашого циклу успіху», видавництво «# кніголав», 2018, 256 с., ISBN 978-617-7563-31-9
10. Філіп Котлер, Гарі Армстронг, книга «Основи маркетингу», видавництво «Вільямс», 2020, 880 с., ISBN 978-617-7812-04-2

11. Олівер Беркмен, книга «Тайм-менеджмент для смертних», видавництво «Лабораторія», 2021, 176 с., ISBN 978-617-8053-05-5
12. Деніел Ґоулман, Енні Маккі, Річард Бояціс, книга «Емоційний інтелект лідера», видавництво «Наш формат», 2019, 288 с., ISBN 978-617-7682-91-1
13. Джордж Ґілдер, книга «Життя після Google. Занепад великих Даних і становлення блокчейн-економіки», видавництво «BookChef», 2021, 320 с., ISBN 978-966-993-573-1
14. Ерін Меєр, книга «Культурна карта, бар'єри міжкультурного спілкування в бізнесі», видавництво «Наш формат» 2020, 224 с. ISBN 978-617-7863-29-7
15. Кітамі Масао, книга «Самурай без меча. Перемагай не силою зброї, а силою розуму», видавництво «Сварог», 2020, 192 с., ISBN 978-611-01-1829-3
16. Фрідріх Глазл, книга «Конфлікт менеджменту. Довідник для керівників та консультантів», видавництво «АДЕФ-Україна», 2020, 528 с., ISBN 978-617-7736-47-8
17. Джошуа Купер Ремо, книга «Сьоме чуття. Влада, багатство и виживання в Епоха мереж», видавництво «Yakaboo Publishing», 2018, 284 с., ISBN 978-617-7544-05-9
18. Тоні Шей, книга «Доставка щастя», видавництво «Видавництво Старого Лева», 2016, 288 с., ISBN 978-617-67-9255-0
19. Брайан Меркант, книга «Девайс №1. Таємна історія iPhone», видавництво «BookChef», 2018, 512 с., ISBN 978-617-7559-05-3
20. Сьюзі Уелч, Джек Уелч, книга «Сам собі MBA. Про бізнес без цензури», видавництво «Наш формат», 2018, 200 с., ISBN 978-617-7388-91-2
21. Сатья Наделла, книга «Натисніть «Оновити». Подорож у пошуках душі Microsoft та кращий майбутнього для кожного», видавництво «КМ-Букс», 2019, 280 с., ISBN 978-966-948-086-6

22. Кріс Гільбо, книга «Пасивний заробіток. Як перетворити ідею на гроші за 27 днів», видавництво «Наш формат», 2018, 240 с., ISBN 978-617-7682-42-3
23. Гарі Вайнерчук, книга «Вони всіх Зробили!», видавництво «Віват», 2019, 288 с., ISBN 978-966-982-059-4
24. Рогіт Бгаргава, книга «неочевидності як Передбачити майбутнє аналізуючи тренді», видавництво «Фактор», 2019, 288 с., ISBN 978-966-942-984-1
25. Джон Каррейра, книга «Дурна Кров», видавництво «Форс Україна», 2019, 464 с., ISBN 978-617-7561-15-5
26. Юрген Аппель, книга «Менеджмент 3.0. Agile-менеджмент. Лідерство та управління командами», видавництво «Фабула», 2019, 432 с., ISBN 978-617-09-5264-6
27. Пітер Ф. Друкер, книга «Виклики для менеджменту XXI століття», видавництво «Країна Мрій», 2020, 240 с., ISBN 978-966-948-377-5
28. Лоїс Френкел, книга «Чемні дівчата не займають просторих кабінетів», видавництво «# кніголав», 2022,448 с., ISBN 978-617-8012-57-1
29. Любомир Остапів, книга «Війна та бюджет», видавництво «Yakaboo Publishing», 2022, 312 с., ISBN 978-617-7933-64-8
30. Сава Лібкін, Антон Фрідлянд, книга «Бізнес по-Одеський. Як побудувати мережу, не втративши себе», видавництво «BookChef» ;2021;270 с.;ISBN 978-966-993-700-1
31. Максим Роменський, книга «Переговори з дельфінами», видавництво «Фабула», 2021, 176 с., ISBN 978-617-09-6152-5
32. Пасічник В.В. , Пасічник О.В. , Басюк Т.М. , Думанський Н.О., книга «Основи інформаційних технологій», видавництво «Новий світ-2000», 2020, 390 с., ISBN 978-966-418-121-8
33. Андрій Лунтовський, Ігор Мельник, книга «Комп'ютерні мережі та телекомунікації», видавництво «Університет ""Україна""», 2007, 274 с., ISBN 978-966-388-146-1

34. Андрій Лунтовський, Ігор Мельник, книга «Проектування та дослідження комп'ютерних мереж», видавництво «Університет "Україна"»,2010, 362 с., ISBN 978-966-388-315-1
35. Б.Ю. Жураковський, І.О. Зенів, книга «КОМП'ЮТЕРНІ МЕРЕЖІ», видавництво «КПІ ім. Ігоря Сікорського», 2020, 336 с.
36. TDMUV, Принципи побудови і призначенння компютерних мереж, URL: https://tdmuv.com/kafedra/internal/informatika/classes_stud/uk/nurse/and/03.%D0%9F%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D0%B8%20%D0%BF%D0%BE%D0%B1%D1%83%D0%B4%D0%BE%D0%B2%D0%B8%20%D1%96%20%D0%BF%D1%80%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BA%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D1%85%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6.htm
37. UA5.ORG, Обладнання для побудови комп'ютерних мереж, URL: https://ua5.org/lan/2297-obladnannya-dlya-pobudovy-kompyuternyh-merezh.html
38. UA5.ORG, Який комутатор вибрати для бізнес-мережі, URL: https://ua5.org/lan/2872-yakyj-komutator-vybraty-dlya-biznes-merezhi.html
39. DELTAHOST, Яку ОС вибрати для сервера?, URL: https://deltahost.ua/ua/yaku-os-vibrati-dlya-servera.html
40. Dell, Серверні операційні системи, URL: https://www.dell.com/support/contents/uk-ua/article/product-support/self-support-knowledgebase/enterprise-resource-center/server-operating-system-support
41. HyperNet, Вимоги до серверної (серверному приміщенню, апаратної), URL: https://shop.hypernet.com.ua/trebovaniya-k-servernoy-komnate/
42. E Server, Як правильно облаштувати серверну кімнату, URL: https://e-server.com.ua/uk/poradi/jak-pravilno-oblashtuvati-servernu-kimnatu

43. Аріна Оголь, eSputnik, SWOT-аналіз із прикладами, URL: https://esputnik.com/uk/blog/swot-analiz-iz-prikladami
44. Дія.Бізнес,Що таке SWOT аналіз?, URL: https://business.diia.gov.ua/handbook/marketing/so-take-swot-analiz
45. Vector, Керувати хаосом командної роботи. Чим займається проєктний менеджер в IT та як ним стати (курси, поради, книжки), URL: https://vctr.media/ua/keruvati-haosom-komandnoyi-roboti-chim-zajmayetsya-proyektnij-menedzher-v-it-ta-yak-nim-stati-134556/
46. Будуй СВОЄ!, РИЗИК-МЕНЕДЖМЕНТ І ОЦІНКА РИЗИКІВ. НА СТОРОЖІ ЗАХИСТУ ВАШОГО БІЗНЕСУ, URL: https://buduysvoe.com/publications/ryzyk-menedzhment-i-ocinka-ryzykiv-na-storozhi-zahystu-vashogo-biznesu
47. Mind, Як перетворити ризики в можливості з IT-системою для бізнесу LIGA360, URL: https://mind.ua/publications/20226255-yak-peretvoriti-riziki-v-mozhlivosti-z-it-sistemoyu-dlya-biznesu-liga360
48. Go it, Project Manager в IT: обов`язки, переваги та шлях до кар`єрного успіху, URL: https://goit.global/ua/articles/project-manager-v-it/
49. Редакція IT STEP Academy, IT Step, Бізнес Аналітик в IT - все про професію, URL: https://kiev.itstep.org/blog/business-analyst-in-it-all-about-the-profession
50. Марія Бровінська, Dev.UA, Бізнес-аналітик в IT: хто він, що робить і як ним стати, URL: https://dev.ua/news/biznes-analityk
51. Бушуєв С.Д., Шкуро М.Ю. , Козир Б.Ю. Проактивне управління проектами забезпечення енергоефективності муніципальної інфраструктури. Вісник НТУ «ХПІ». Сер. Стратегічне управління, управління портфелями, програмами та проектами. Харків : НТУ «ХПІ», 2019. № 1 (1326). С. 3 – 10.
52. Лепський В.В. Ідентифікація цінностей стейкхолдерів проектів проектно-орієнтованого медичного закладу. Вісник ЧДТУ : зб. наук. пр. Черкаси : ЧДТУ, 2017. № 3. С. 44 – 51.

53. Данченко О. Б. Огляд сучасних методологій управління ризиками в проектах. Управління проектами та розвиток виробництва: зб. наук. пр. Луганськ : СНУ ім. В.Даля, 2014. №1(49). С. 16 – 25.