Міністерство освіти і науки України
ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут економіки, управління, права та інформаційних технологій

М А Т Е Р І А Л И

науково-практичної конференції
за підсумками проходження виробничої практики
здобувачів вищої освіти
спеціальності
126 Інформаційні системи та технології
Випуск IX

кафедра інформаційних систем та технологій

10 жовтня 2024 року

Полтава – 2024

Редакційна колегія:

Уткін Ю. В. – к.т.н., доцент, завідувач кафедри інформаційних систем та технологій, доцент кафедри;
Поночовний Ю. Л. – д.т.н., с.н.с., професор кафедри;
Копішинська О. П. – к.ф.-м.н., доцент, професор кафедри;
Одарущенко О. М. – д.т.н., професор, професор кафедри;
Вакуленко Ю.В. – к.с.-г.н., доцент, доцент кафедри;
Слюсар В. І. – д.т.н., професор, професор кафедри;
Слюсарь І. І. – к.т.н., доцент, доцент кафедри;
Протас Н. М. – к.с.-г.н., доцент, доцент кафедри;
Дегтярьова Л.М. – к.т.н., доцент, доцент кафедри;
Одарущено О.Б. – к.т.н., доцент, доцент кафедри
Флегантов Л.О. – к.ф.-м.н., доцент, професор кафедри

Матеріали науково-практичної конференції за підсумками проходження виробничих практик здобувачів вищої освіти спеціальності 126 Інформаційні системи та технології, кафедра інформаційних систем та технологій Полтавського державного аграрного університету, 10 жовтня 2024. Вип. IX. Полтава: ПДАУ, 64 с.

У збірнику надруковані матеріали досліджень, оприлюднених на науково-практичній конференції за підсумками проходження здобувачами вищої освіти виробничої практики «Організаційно-аналітична практика» та «Комплексна практика з фаху» за освітньо-професійною програмою «Інформаційні управляючі системи» спеціальності 126 Інформаційні системи та технології кафедри інформаційних систем та технологій Полтавського державного аграрного університету. У публікаціях зроблені узагальнення теоретичних знань та практичних навичок, набутих під час практики на базі підприємств, організацій.

Відповідальність за зміст та редакцію тез несуть автори та наукові керівники.

© *Полтавський державний аграрний університет* (*ПДАУ*)
© *Кафедра інформаційних систем та технологій*

ЗМІСТ

Коряк Владислав, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: д.т.н., професор Поночовний Юрій

ОПТИМІЗАЦІЯ БІЗНЕС-ПРОЦЕСІВ ПІДПРИЄМСТВА ЧЕРЕЗ ВПРОВАДЖЕННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

В умовах стрімкого розвитку інформаційних технологій інтеграція сучасних інформаційних систем стала необхідною для забезпечення конкурентоспроможності та підвищення ефективності бізнес-процесів. ТОВ «ВАК», як компанія, що спеціалізується на телекомунікаційних послугах і технічному обслуговуванні, активно використовує цифрові інструменти для оптимізації своєї діяльності. Це дослідження присвячене аналізу впливу інформаційних систем управління (CRM і ERP) на організацію бізнес-процесів та підвищення продуктивності підприємства.

CRM (Customer Relationship Management, система управління взаємовідносинами з клієнтами) – це програмне забезпечення, яке допомагає організаціям перетворювати потенційних клієнтів на постійних, залучати нові ліди та підтримувати відносини з наявними клієнтами, охоплюючи всі етапи взаємодії. Основними завданнями CRM-системи є розвиток відносин із клієнтами, підвищення їхньої лояльності, збільшення ймовірності успішних угод та зростання прибутків.

Для досягнення цих цілей CRM-система зберігає та обробляє великі обсяги даних, пов’язаних з управлінням відносинами з клієнтами: інформацію про клієнтів та партнерів, історію комунікацій, документи, комерційні пропозиції, розклад працівників, показники ефективності тощо. Завдяки єдиному інформаційному середовищу, актуальні дані доступні всім підрозділам, що працюють з клієнтами. Це не лише спрощує взаємодію із замовниками, але й сприяє тісній співпраці між командами продажів, маркетингу та обслуговування клієнтів (рисунок 1).

Рисунок 1 – CRM-система

Планування ресурсів підприємства (ERP) – це програмне забезпечення, яке допомагає організаціям управляти щоденними операціями, такими як бухгалтерія, закупівлі, проєктне управління, управління ризиками, дотримання нормативних вимог і логістичні процеси. Повноцінне ERP-рішення також включає інструменти для управління ефективністю підприємства, що дозволяють планувати, прогнозувати фінансові результати, звітувати та складати бюджет.

ERP-системи інтегрують різні бізнес-процеси та забезпечують обмін даними між ними. Завдяки збору транзакційної інформації з різних джерел, ERP-системи усувають дублювання даних і гарантують їхню цілісність, використовуючи єдину базу даних, яка є "єдиним джерелом правди."

Сьогодні ERP-системи є життєво важливими для управління тисячами підприємств різного розміру в усіх галузях. Для цих організацій ERP-система настільки ж незамінна, як електроенергія, без якої неможливо виконувати основні операції (рисунок 2).

Рисунок 2 – ERP системи управління

Ці системи дозволяють оптимізувати діяльність підприємства, спрощуючи управління взаємодією з клієнтами, ведення фінансової звітності та організацію внутрішніх процесів. Практика довела, що інтеграція таких систем є ключовою для підвищення продуктивності компанії, скорочення витрат на обслуговування та забезпечення прозорості фінансових операцій. Особливо важливою є автоматизація процесів, таких як управління клієнтськими запитами, технічна підтримка та моніторинг мережі, що значно покращує якість обслуговування.

Практичний досвід роботи з інформаційними системами показав ефективність їхньої інтеграції в щоденну діяльність компанії. Впровадження CRM-систем дозволяє автоматизувати процеси взаємодії з клієнтами, зберігати історію запитів та оперативно на них реагувати. ERP-системи забезпечують контроль за фінансовими операціями, що прискорює обробку рахунків, управління замовленнями та планування ресурсів. Системи

моніторингу мережі показали, як швидко можна виявляти та усувати технічні несправності, забезпечуючи безперебійну роботу підприємства.

Результати дослідження свідчать, що впровадження інформаційних систем є невід'ємною частиною сучасного бізнесу. Вони сприяють зниженню витрат на управління, підвищують якість обслуговування клієнтів і дозволяють ефективніше використовувати ресурси компанії. Однак для збереження їхньої ефективності важливо регулярно оновлювати та адаптувати системи до нових викликів, таких як кіберзагрози.

На основі проведеного аналізу рекомендується подальша модернізація програмно-апаратного забезпечення для підвищення стабільності систем. Також слід посилити заходи кібербезпеки, запровадивши додаткові механізми захисту даних. Використання хмарних технологій дозволить компанії розширити доступ до систем з будь-якого місця, підвищуючи гнучкість роботи співробітників. Варто також розглянути впровадження інструментів штучного інтелекту для автоматизації аналітики та управління процесами, що допоможе швидше реагувати на ринкові зміни.

Отже, інформаційні системи є потужним інструментом для покращення діяльності підприємства, але їхня ефективність залежить від постійної модернізації та впровадження новітніх технологічних рішень.

Список використаних джерел:

1. Телекомунікаційна компанія ТОВ "ВАК". URL: https://vak.com.ua/

2. Інформаційні потоки в логістиці. URL: https://pidru4niki.com/15970122 /logistika/informatsiyni_potoki.

Костов Михайло, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий курівник: д.т.н., професор Поночовний Юрій

СИСТЕМНИЙ АНАЛІЗ В УПРАВЛІННІ ПІДПРИЄМСТВОМ

Системний аналіз в управлінні підприємством є ключовим інструментом для забезпечення ефективності та стійкості будь-якої організації, особливо в сучасних умовах, коли бізнес-процеси стають дедалі складнішими, а конкуренція на ринку зростає. Зокрема, для ТОВ «ЄВРОБУС ПОЛТАВА», системний аналіз дозволяє не тільки оцінити поточний стан справ на підприємстві, але й сформувати обґрунтовані прогнози щодо майбутнього розвитку, що є важливим для забезпечення довгострокової стійкості компанії.

Виконуючи індивідуальне завдання, спрямоване на аналіз інформаційних систем, які використовуються на підприємстві, була здійснена глибока оцінка різних аспектів роботи ТОВ «ЄВРОБУС ПОЛТАВА». Особлива увага приділялася функціональним можливостям існуючих систем, їх взаємодії між собою, а також їхній здатності задовольняти потреби компанії у швидкому і точному обміні інформацією.

Результати аналізу показали, що інформаційні системи, які використовуються на підприємстві, в цілому відповідають основним вимогам

сучасного бізнесу. Зокрема, автоматизація бізнес-процесів дозволила значно скоротити час на виконання рутинних завдань, зменшити кількість помилок при обробці даних, а також підвищити загальну ефективність роботи. Водночас, було виявлено, що деякі з систем, які використовуються, не забезпечують належного рівня інтеграції, що може призводити до ускладнень в управлінні інформаційними потоками.

У процесі аналізу також було встановлено, що інтеграція інформаційних систем залишається важливою проблемою для підприємства. Наявність різних платформ і рішень, що використовуються для виконання різних завдань, створює певні труднощі при об'єднанні даних, що в свою чергу може призвести до затримок в ухваленні управлінських рішень. Наприклад, недостатня інтеграція систем управління проектами та фінансового обліку може призводити до складнощів у плануванні ресурсів і контролі витрат.

Окрім того, аналіз показав, що частина програмного забезпечення потребує модернізації або навіть заміни, оскільки воно не повністю відповідає сучасним вимогам. Це стосується як забезпечення належного рівня інформаційної безпеки, так і підтримки нових стандартів обміну даними, що є критично важливим для підприємства, яке прагне залишатися конкурентоспроможним на ринку. Важливо відзначити, що без своєчасного оновлення інформаційних систем підприємство ризикує втратити свою ринкову частку через нездатність швидко адаптуватися до змінних умов.

Додатково, системний аналіз включав оцінку кадрового потенціалу підприємства в контексті його здатності ефективно використовувати існуючі інформаційні системи. Було встановлено, що, хоча рівень кваліфікації співробітників є достатнім для виконання поточних завдань, існує необхідність у постійному підвищенні їхнього професійного рівня. Це зумовлено швидкими темпами розвитку інформаційних технологій, що вимагає від співробітників підприємства постійного вдосконалення своїх знань і навичок. Навчання і підвищення кваліфікації персоналу стають невід'ємною частиною стратегічного планування в області управління інформаційними системами.

На основі проведеного аналізу було розроблено ряд рекомендацій щодо вдосконалення інформаційних систем підприємства. Зокрема, пропонується розглянути можливість впровадження єдиної платформи для управління всіма аспектами діяльності підприємства, що дозволить забезпечити повну інтеграцію різних модулів і значно спростить процеси управління. Такий підхід не тільки зменшить витрати на обслуговування різних систем, але й підвищить швидкість обміну інформацією між різними відділами підприємства, що в кінцевому підсумку призведе до підвищення загальної ефективності роботи.

Іншою важливою рекомендацією є посилення заходів з інформаційної безпеки. З огляду на зростаючу загрозу кібератак і витоків даних, важливо забезпечити належний рівень захисту інформаційних систем підприємства. Це може включати як впровадження нових технологій захисту, так і регулярне проведення аудитів інформаційної безпеки з метою виявлення і усунення

потенційних вразливостей. Окрім цього, необхідно активно впроваджувати політику інформаційної безпеки на всіх рівнях організації, щоб забезпечити розуміння важливості захисту даних серед співробітників і мінімізувати людський фактор як одну з найбільших загроз для безпеки.

Таким чином, системний аналіз, виконаний у рамках індивідуального завдання, дозволив виявити ключові аспекти, які потребують уваги та можуть стати основою для подальшого розвитку підприємства. Зокрема, важливість подальшого вдосконалення інтеграції інформаційних систем, модернізації програмного забезпечення та підвищення кваліфікації персоналу стала очевидною. Крім того, пропозиції щодо впровадження нових рішень у сфері інформаційних технологій та підвищення рівня інформаційної безпеки дозволять ТОВ «ЄВРОБУС ПОЛТАВА» залишатися конкурентоспроможним і забезпечити стійкий розвиток у майбутньому.

Список використаних джерел::

1. Петренко П.П. Управління інформаційними системами в умовах цифрової трансформації. Харків: ХНУ, 2020. 214 с.

2. Іванов І.І., Сучасні підходи до системного аналізу на підприємствах ІТ-сфери. Київ: КНУ, 2021. 312 с.

3. Іванова І. Управління бізнес-процесами в організації, Львів: Новий Світ-2000, 2019. 144 с.

Кривий Ілля, здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник: д.т.н., професор Поночовний Юрій

АНАЛІЗ МОЖЛИВИХ ДЖЕРЕЛ І КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Аналіз можливих джерел і каналів витоку інформації є важливим етапом у забезпеченні безпеки будь-якої організації, особливо в умовах сучасного розвитку технологій і зростання обсягів даних. Витоки інформації можуть призвести до фінансових втрат, шкоди репутації компанії, порушення прав клієнтів та конфіденційності. Для того, щоб попередити такі інциденти, необхідно розуміти, які канали і джерела можуть стати потенційними загрозами.

Одним із найбільш поширених джерел витоку інформації є внутрішній персонал компанії. Співробітники мають доступ до великої кількості конфіденційних даних, що робить їх потенційними джерелами витоків. Це може бути ненавмисний витік, коли працівник випадково розголошує інформацію через неуважність або недостатню обізнаність із безпековими процедурами. Іншою причиною може стати навмисний витік, коли співробітник свідомо передає конфіденційні дані третім особам, наприклад, конкурентам або зацікавленим особам, можливо, внаслідок конфлікту з роботодавцем або за фінансову винагороду [1]. Особливо небезпечним є те,

що внутрішній персонал часто має широкий доступ до критичних систем і даних, що ускладнює виявлення витоків на ранній стадії.

Окрім внутрішніх загроз, важливими є також зовнішні атаки. Хакери та кіберзлочинці постійно шукають уразливі місця в IT-системах компаній, щоб отримати доступ до конфіденційних даних [1]. Це можуть бути як цілеспрямовані атаки, коли кіберзлочинці свідомо атакують певну компанію, так і масові атаки на вразливі системи, в ході яких злочинці шукають слабкі місця в системах захисту. Найбільш поширеними методами є фішингові атаки, зараження шкідливим програмним забезпеченням, використання уразливостей програмного забезпечення або атак через соціальну інженерію. Важливим аспектом є те, що технології зламу та доступу до даних постійно удосконалюються, що робить захист системи надзвичайно складним завданням.

Окрім явних джерел витоку, варто звернути увагу на недостатню захищеність партнерських відносин і постачальників. Багато компаній передають частину своїх операцій стороннім організаціям, таким як постачальники хмарних послуг, аутсорсингові IT-компанії або маркетингові агентства. Ці компанії, в свою чергу, можуть мати доступ до конфіденційних даних клієнтів або внутрішніх систем, що створює додатковий ризик витоку. Якщо ці партнери або постачальники не дотримуються належних стандартів кібербезпеки, це може стати слабкою ланкою в загальному ланцюзі безпеки. Крім того, складність у контролі за безпекою партнерів може призвести до витоку інформації через їхні системи.

Важливим фактором є також неправильне управління доступом до даних. У багатьох організаціях спостерігається проблема надлишкового доступу, коли співробітники мають більше прав доступу, ніж це необхідно для виконання їхніх обов’язків. Це може призвести до того, що певні дані можуть бути доступними великій кількості осіб, що підвищує ризик витоку. Недостатнє використання політики поділу прав доступу та багатофакторної автентифікації також збільшує ризики. Наприклад, відсутність контролю за тим, хто і коли отримує доступ до певної інформації, може призвести до втрати контролю над конфіденційними даними.

Окрім цього, варто згадати про людський фактор. Незважаючи на всі технічні засоби захисту, людські помилки залишаються однією з головних причин витоків. Недостатня обізнаність співробітників про загрози кібербезпеки, недотримання інструкцій з використання корпоративних ресурсів або недбалість у роботі з конфіденційною інформацією може призвести до серйозних наслідків. Наприклад, випадкове відправлення конфіденційного документа на неправильну електронну адресу, розкриття паролів або використання незахищених каналів для передачі даних – усе це типові помилки, що призводять до витоків.

Крім того, зростає кількість атак на мобільні пристрої та інші носії інформації. Сучасні смартфони, планшети та інші гаджети використовуються для зберігання та передачі корпоративної інформації, що створює додаткові ризики [2]. Використання незахищених мереж Wi-Fi, ненадійних додатків або

слабких паролів може призвести до того, що дані будуть викрадені з таких пристроїв. Втрата або крадіжка самого пристрою також може стати джерелом витоку, якщо дані на ньому не зашифровані [2].

Усі ці аспекти свідчать про те, що витік інформації може статися з різних джерел та каналів. Для мінімізації ризиків необхідно впроваджувати комплексні заходи з кібербезпеки, які включатимуть як технічні рішення (таким як шифрування, моніторинг систем та багатофакторна автентифікація), так і навчання персоналу основам інформаційної безпеки.

Список використаних джерел:

1. Богуш В.М., Богуш В.В., Бровко В.Д., Основи кіберпростору, кібербезпеки та кіберзахисту. К: Ліра-К, 2021, 472 с.
2. Когут Ю. Кібербезпека та ризики цифрової трансформації компанії. К: Сідкон, 2021. 327 с.

Макаренко Станіслав, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к. т. н. доцент Дегтярьова Лариса

АНАЛІЗ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ПДАУ

Аналіз системи захисту корпоративної мережі Полтавський державний аграрний університет, включає кілька ключових аспектів, що спрямовані на забезпечення безпеки даних і ресурсів університету.

Перш за все, важливою є архітектура мережі. Внутрішня мережа університету, що включає ресурси, такі як сервери, бази даних і системи управління навчальним процесом (наприклад, MOODLE), повинна бути ізольована від зовнішніх загроз за допомогою мережевих екранів (firewalls). Це дозволяє захистити критичні ресурси від несанкціонованого доступу. Для доступу до інтернету і взаємодії з зовнішніми партнерами використовуються демілітаризовані зони (DMZ), де розміщуються веб-сервіси університету, що забезпечує додатковий рівень безпеки.

Захист від загроз є наступним важливим аспектом. Це включає встановлення антивірусного програмного забезпечення на всіх робочих станціях і серверах для захисту від шкідливих програм. Використання систем виявлення і запобігання вторгненням (IDS/IPS) дозволяє моніторити трафік і виявляти підозрілі дії або вторгнення, що допомагає попередити можливі атаки. Міжмережеві екрани також грають ключову роль у розмежуванні доступу до мережевих сегментів і фільтрації вхідного та вихідного трафіку, що знижує ризик проникнення небажаного трафіку в мережу.

Контроль доступу до ресурсів мережі є ще одним критично важливим аспектом. Ідентифікація і аутентифікація користувачів, зокрема використання двофакторної аутентифікації, забезпечує захищений доступ до критичних систем. Налаштування доступу на основі ролей (RBAC) дозволяє забезпечити користувачам доступ лише до тих ресурсів, які їм необхідні для виконання

своїх обов'язків, що зменшує ймовірність випадкового або навмисного порушення безпеки.

Захист даних в мережі передбачає використання шифрування для зберігання конфіденційних даних та їх передачі через мережу. Це забезпечує додатковий рівень захисту від перехоплення або несанкціонованого доступу до інформації. Крім того, регулярне створення резервних копій важливих даних і їх зберігання у віддалених безпечних місцях дозволяє забезпечити збереження інформації у разі технічних збоїв або атак.

Моніторинг і аудит є невід'ємною частиною підтримки безпеки мережі. Ведення журналів подій і їх регулярний аналіз дозволяє виявляти аномальну активність, яка може вказувати на спробу проникнення або інші загрози. Постійний моніторинг мережевої інфраструктури також допомагає виявляти і усувати вразливості, забезпечуючи стабільну роботу мережі [1-3].

Політики безпеки грають важливу роль у захисті мережі. Встановлення чітких правил і процедур для захисту інформаційних ресурсів є необхідною умовою для забезпечення безпеки. Крім того, регулярне навчання співробітників основам інформаційної безпеки та найкращим практикам роботи з інформаційними системами дозволяє підвищити загальний рівень обізнаності і готовності до захисту.

Нарешті, важливо мати розроблений і випробуваний план реагування на інциденти. Наявність чіткого плану дій на випадок порушення безпеки або кібератаки допомагає швидко відновити роботу мережі та мінімізувати збитки. Формування спеціалізованої команди для реагування на інциденти безпеки є ключовим елементом в ефективному усуненні загроз.

Додаткові заходи включають сегментацію мережі, що дозволяє ізолювати критичні ресурси і знизити ризик поширення загроз у разі порушення безпеки. Використання віртуальних локальних мереж (VLANs) для розділення ресурсів логічно, навіть якщо вони фізично підключені до однієї інфраструктури, забезпечує підвищений контроль над трафіком і знижує ризик атак. Політика мінімальних привілеїв, що передбачає надання користувачам і службам доступу тільки до тих ресурсів, які їм необхідні для роботи, також значно знижує ризики.

Шифрування трафіку між сегментами мережі і під час передачі даних через інтернет є обов’язковим для захисту конфіденційної інформації. Управління вразливостями включає регулярне сканування мережі на наявність слабких місць і оперативне їх усунення, а контроль і моніторинг трафіку дозволяють своєчасно виявляти та реагувати на підозрілу активність. Навчання персоналу основам інформаційної безпеки також залишається критично важливим, оскільки людський фактор може бути найбільш вразливим місцем в будь-якій системі безпеки.

Таким чином, комплексний підхід до захисту корпоративної мережі ПДАУ, що включає всі ці аспекти, є необхідним для захисту від сучасних загроз і забезпечення безперебійної роботи організації.

Щоб посилити захист корпоративної мережі Полтавського державного аграрного університету, можна розглянути кілька додаткових заходів. По-

перше, доцільно впровадити регулярне тестування безпеки мережі за допомогою проведення аудиту та пентестів для виявлення можливих вразливостей. По-друге, варто забезпечити автоматизоване оновлення всіх систем і програмного забезпечення, щоб мінімізувати ризики, пов'язані з експлуатацією застарілих версій. Крім того, слід розглянути можливість застосування штучного інтелекту для виявлення аномалій у мережевому трафіку, що дозволить оперативніше реагувати на потенційні загрози. Нарешті, регулярне навчання співробітників з актуальних питань інформаційної безпеки допоможе підвищити загальну стійкість організації до кібератак.

Список використаних джерел::

1 Применение IPS/IDS. URL: https://xakep.ru/2012/10/29/ids-ips/ .

2. Чунарьова А.В., Юдін О.К. Підсистеми моніторингу функціонування корпоративних мереж // Захист інформаційно-комунікаційних систем: науково-практична конференція, 26 - 28 травня 2009, Київ. К.: НАУ, 2009. С. 59-60.

3. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ, 2020. С. 119-125.

Туманевич Олександр, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Дегтярьова Лариса

ОБРАЗ ОПЕРАЦІЙНОЇ СИСТЕМИ ТА ІНСТРУМЕНТИ ДЛЯ ЙОГО СТВОРЕННЯ

Операційна система (ОС) є основою функціонування комп'ютерних систем, забезпечуючи управління апаратними ресурсами, виконання програм та зручність користувачів. В умовах стрімкого розвитку інформаційних технологій та зростання вимог до безпеки й продуктивності, створення якісного образу операційної системи стає критично важливим завданням. Образ ОС, як інтегральне представлення налаштувань, конфігурацій та програмного забезпечення, дозволяє забезпечити швидке розгортання робочих середовищ, зберігаючи консистентність та зменшуючи ризик помилок. Тому дослідження методів та інструментів для створення образів ОС є актуальним питанням як для IT-професіоналів, так і для освітніх установ, які готують фахівців у цій галузі.

В умовах глобалізації та цифровізації, ефективне управління інформаційними ресурсами стає ключовим чинником успіху для бізнесу, освіти та державного управління. Одним із важливих аспектів цього управління є створення та підтримка образів операційних систем, які дозволяють стандартизувати робочі середовища, спростити управління ними та зменшити витрати на технічну підтримку. Зокрема, використання образів

ОС є важливим у середовищах, де потрібно швидко та ефективно розгортати нові робочі станції, забезпечуючи при цьому надійність та безпеку систем.

Особливо актуальною ця проблема стає у світлі останніх змін у сфері кібербезпеки. Вразливості операційних систем та необхідність їх оперативного оновлення підкреслюють важливість створення якісних та безпечних образів ОС, які можна швидко розгорнути на великій кількості пристроїв. Крім того, зростаюча популярність віртуалізації та хмарних технологій відкриває нові горизонти для використання образів ОС, зокрема у сфері мобільних та розподілених обчислень [1].

Під час літньої практики в Навчально-науковому центрі інформаційно-комунікаційних освітніх технологій та освіти дорослих Полтавського державного аграрного університету було проведено глибоке дослідження методів та інструментів для створення образів операційних систем.

Основною метою було ознайомлення з сучасними підходами до створення, налаштування та розгортання образів ОС на прикладі реальних задач, що постають перед установами освіти та бізнесу.

Вивчення інструментів таких, як Microsoft Deployment Toolkit (MDT), Acronis True Image та Clonezilla, дало змогу проаналізувати їх переваги та недоліки у різних умовах використання. Зокрема, Microsoft Deployment Toolkit (MDT) виявився ефективним засобом для автоматизації процесу розгортання операційних систем у великих мережах. Його використання дозволяє стандартизувати процес розгортання, зменшити ризик помилок та забезпечити високий рівень контролю над налаштуванням ОС.

Acronis True Image була протестована для створення резервних копій та клонування системних дисків, що дозволяє швидко відновлювати робочі середовища у разі системних збоїв або атак зловмисників. Цей інструмент має потужний функціонал для управління резервними копіями, що є важливим для забезпечення безперервності роботи інформаційних систем.

Clonezilla – це безкоштовний інструмент для клонування та створення образів дисків, який показав свою ефективність у малих та середніх мережах. Незважаючи на простоту використання, Clonezilla забезпечує високу швидкість та надійність клонування, що робить його привабливим вибором для багатьох системних адміністраторів.

На базі досвіду, отриманого під час практики, було розроблено рекомендації щодо впровадження зазначених інструментів у практичну діяльність освітніх закладів та підприємств. Особлива увага приділялася питанням налаштування безпеки та автоматизації процесів розгортання ОС, що дозволяє мінімізувати людський фактор та підвищити ефективність управління IT-інфраструктурою [2-4].

На основі проведеного дослідження можна зробити висновок, що використання сучасних інструментів для створення та управління образами операційних систем є важливою складовою успішного функціонування інформаційних систем в умовах сучасного світу. Використання Microsoft Deployment Toolkit для автоматизації процесу розгортання ОС у великих

організаціях значно підвищує ефективність роботи IT-відділів, зменшує ризик виникнення помилок та забезпечує стандартизацію процесів.

З метою підвищення рівня підготовки студентів у галузі IT, пропонується включити в навчальні програми курси з використання інструментів для створення образів ОС, зокрема MDT, Acronis True Image та Clonezilla. Це дозволить студентам отримати практичні навички, які будуть корисними у їхній майбутній професійній діяльності.

Крім того, рекомендується подальше дослідження можливостей впровадження відкритих рішень, таких як Clonezilla, у великих організаціях. Це може сприяти зниженню витрат на програмне забезпечення, підвищенню рівня безпеки та гнучкості в управлінні IT-інфраструктурою.

Список використаних джерел:

1.Каплун В.А., Майданюк В.П. Захист операційних систем: навч. посіб. Вінниця: ВНТУ, 2023. 11-20 с.

2. Використання Microsoft Deployment Toolkit. URL: https://learn.microsoft.com/ru-ru/mem/configmgr/mdt/use-the-mdt .

3. Використання Acronis True Image. URL: https://uk.wikipedia.org/wiki/Acronis_True_Image.

4. Використання Clonezilla. URL: https://uk.wikipedia.org/wiki/Clonezilla.

Вернигора Антон, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ОБҐРУНТУВАННЯ ВИБОРУ ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ РЕАЛІЗАЦІЇ ЗАХИСТУ ВІД ВИТІКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ

Захист інформації від витоку через технічні канали є важливим аспектом інформаційної безпеки, який набуває все більшого значення в умовах зростання кіберзагроз і цифрової трансформації [2]. Витік інформації може призвести до серйозних фінансових втрат, зниження конкурентоспроможності та шкоди репутації організації [3]. Тому вибір ефективних технічних засобів захисту є ключовим завданням для забезпечення безпеки даних.

Першим етапом у процесі забезпечення захисту є ідентифікація можливих технічних каналів, через які може відбуватися витік інформації. Основними видами технічних каналів є акустичні канали, через які звукові хвилі можуть передавати інформацію на відстань; вібраційні канали, які використовують вібрації, що передаються через будівельні конструкції, такі як стіни, підлога або стеля; електромагнітні випромінювання, через які інформація може витікати через електромагнітні поля, що створюються електронними пристроями, такими як комп'ютери, монітори, клавіатури та інше обладнання; і, нарешті, оптичні канали, де використовуються оптичні прилади для зчитування інформації, наприклад, за допомогою камер або лазерів [1]. Для ефективного захисту важливо провести детальний аналіз

наявних технічних каналів, які можуть становити загрозу витоку інформації. Це дозволить обрати оптимальні методи захисту.

Після ідентифікації технічних каналів витоку необхідно оцінити рівень загрози, яку вони становлять для організації. Цей етап включає аналіз потенційних наслідків витоку інформації через кожен із каналів, оцінку ймовірності реалізації тієї чи іншої загрози, а також визначення рівня ризику, пов'язаного з кожним технічним каналом, і встановлення пріоритетів для вжиття заходів захисту. Такий підхід дозволяє зосередити зусилля на найбільш критичних загрозах і вибрати технічні засоби, що найбільше підходять для конкретної організації [5].

На основі оцінки ризиків здійснюється вибір технічних засобів захисту, які можуть включати екранування приміщень, використання спеціальних матеріалів для захисту від електромагнітних випромінювань. Екранування може бути застосоване до стін, підлоги, стелі, а також до окремих пристроїв. Засоби захисту акустичних каналів можуть включати звукоізоляцію, використання спеціальних акустичних матеріалів, а також активні системи шумозаглушення. Для захисту від несанкціонованого доступу через електромагнітні та оптичні канали важливим є використання криптографічних засобів захисту, що передбачає шифрування даних на різних етапах їх обробки та передачі [2]. Крім того, системи контролю доступу забезпечують обмеження доступу до приміщень, де обробляється конфіденційна інформація, а також до обладнання, яке може бути джерелом витоку. Вибір конкретних технічних засобів повинен ґрунтуватися на умовах, потребах та можливостях організації, що дозволяє забезпечити оптимальний рівень захисту.

Після вибору технічних засобів їх необхідно правильно впровадити в інфраструктуру організації. Це включає монтаж обладнання відповідно до інструкцій виробника та вимог безпеки, проведення тестів на ефективність засобів захисту, що дозволяє переконатися, що всі системи працюють належним чином і забезпечують необхідний рівень захисту, а також регулярний аудит і моніторинг систем захисту, адже загрози можуть змінюватися, і важливо своєчасно оновлювати засоби захисту, щоб вони залишалися ефективними.

Одним із ключових завдань є забезпечення балансу між високим рівнем захисту і безперебійною роботою організації. Важливо, щоб впроваджені технічні засоби захисту не впливали негативно на продуктивність і не створювали перешкод для виконання основних функцій організації [4]. Це дозволить забезпечити безпеку інформації без шкоди для ефективності бізнес-процесів.

Захист від витоку інформації через технічні канали є комплексним завданням, яке вимагає системного підходу. Вибір відповідних технічних засобів захисту, їх правильне впровадження та регулярний моніторинг ефективності є основою успішної стратегії інформаційної безпеки. Це забезпечить захист конфіденційної інформації, запобігає фінансовим втратам та збереже репутацію організації на належному рівні [1].

Список використаних джерел:

1. The prospective mathematics teachers' thought processes and views about using problem-based learning in statistics education URL: https://www.researchgate.net/publication/373961544_Challenges_and_opportunities_of_modernity_a_comprehensive_system_of_information_protection/fulltext/65059f4cca19e8355c95f48e/Challenges-and-opportunities-of-modernity-a-comprehensive-system-of-information-protection.pdf
2. Канали витоку інформації URL: https://uk.wikipedia.org/wiki/Канали_витоку_інформації
3. Як правильно інвестувати в кібербезпеку: стратегії та основні ризики URL: https://eska.global/blog/yak-pravilno-investuvati-v-kiberbezpeku-strategiya-ta-osnovni-riziki
4. Методи та засоби захисту інформації: Конспект лекцій / Викладач В.І. Стаценко. Друге навчальне видання. Дніпро. URL: https://files.fti.dp.ua/wp-content/uploads/tainacan-items/2456/14592/metody-ta-zasoby-zakhystu-informatsii_.pdf
5. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. URL: https://www.kmu.gov.ua/npas/32791826

Корецька Діана, здобувачка вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий курівник: д.т.н., професор Поночовний Юрій

КРИТЕРІЇ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНИХ РЕСУРСІВ У ФІНАНСОВОМУ СЕКТОРІ: БАЛАНСУВАННЯ МІЖ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ ТА ПІДТРИМКОЮ БЕЗПЕРЕБІЙНОЇ РОБОТИ БАНКІВСЬКИХ СИСТЕМ

У сучасному фінансовому секторі питання захищеності інформаційно-технологічних ресурсів є надзвичайно актуальним. Зі зростанням цифровізації та використанням інформаційних технологій, банки і фінансові установи стикаються з підвищеними ризиками кібератак, що можуть мати катастрофічні наслідки для економіки, довіри клієнтів та стабільності фінансової системи в цілому. У цьому контексті балансування між забезпеченням високого рівня захищеності та підтримкою безперебійної роботи банківських систем стає складним завданням, що вимагає ретельного аналізу та впровадження відповідних критеріїв захищеності.

З розвитком інформаційних технологій банки значно розширили свій спектр послуг, включаючи електронні платіжні системи, онлайн-банкінг, мобільні додатки та інші інноваційні сервіси. Однак, такі технологічні інновації відкрили нові можливості для кіберзлочинців, які використовують вразливості в IT-системах для несанкціонованого доступу до конфіденційної інформації, фінансових ресурсів та інших критичних даних. Згідно з дослідженнями, кількість кібератак на фінансові установи зростає з кожним роком, і їх складність також збільшується [1]. Це підкреслює необхідність

розробки ефективних механізмів захисту інформаційно-технологічних ресурсів у фінансовому секторі, що забезпечать безперервну роботу банківських систем.

Одним із ключових аспектів забезпечення безпеки інформаційно-технологічних ресурсів є визначення чітких критеріїв захищеності. До них належать:

– Конфіденційність: забезпечення захисту інформації від несанкціонованого доступу. В фінансовому секторі конфіденційність є одним із головних пріоритетів, оскільки втрати даних клієнтів можуть призвести до серйозних репутаційних збитків та фінансових санкцій. Використання технологій шифрування, контроль доступу та регулярний моніторинг є важливими заходами для підтримки конфіденційності даних [2].

– Цілісність: гарантування, що дані залишаються незмінними та достовірними протягом усього процесу обробки. Цілісність інформації є критично важливою, оскільки помилки або навмисні зміни в даних можуть призвести до неправильних фінансових операцій та недовіри клієнтів. Використання технологій хешування, контроль версій та резервне копіювання є ключовими для забезпечення цілісності [3].

– Доступність: забезпечення безперебійного доступу до інформації та ресурсів для авторизованих користувачів. Доступність є важливою для безперервної роботи банківських систем, особливо у випадку обробки платіжних транзакцій, коли навіть короткочасні переривання можуть мати серйозні наслідки. Використання резервних систем, реплікація даних та забезпечення стійкості до відмови допомагають підтримувати високу доступність [4].

– Автентифікація та авторизація: забезпечення того, щоб доступ до інформаційних ресурсів мали тільки авторизовані користувачі. Надійні механізми автентифікації, такі як двофакторна автентифікація, біометрія або використання токенів, допомагають знизити ризик несанкціонованого доступу [5].

– Моніторинг та аудит: регулярний контроль та аналіз дій у системах дозволяє своєчасно виявляти загрози та порушення. Це допомагає знизити ризики, пов'язані з кібератаками та внутрішніми загрозами [5].

Одним із ключових викликів у сфері захищеності інформаційно-технологічних ресурсів є необхідність балансування між високим рівнем безпеки та підтримкою безперебійної роботи банківських систем. Це завдання стає особливо актуальним у контексті необхідності швидкої обробки великої кількості транзакцій та надання послуг в режимі 24/7.

З одного боку, впровадження жорстких заходів безпеки може сповільнювати роботу системи та ускладнювати доступ до неї. Наприклад, багаторівнева автентифікація може затримувати час доступу до системи, що може бути критичним під час термінових операцій. З іншого боку, зниження рівня захисту для підвищення швидкодії може призвести до збільшення ризиків кібератак та витоків даних.

Забезпечення ефективного балансування між цими двома аспектами вимагає комплексного підходу. Наприклад, використання адаптивних систем захисту, що можуть автоматично змінювати рівень захищеності залежно від контексту, може бути ефективним рішенням. Такі системи можуть підвищувати рівень захисту під час виявлення підозрілої активності та знижувати його, коли ризики мінімальні, що забезпечує як безпеку, так і ефективність роботи.

Захищеність інформаційно-технологічних ресурсів у фінансовому секторі є критично важливою для підтримки довіри клієнтів та стабільності банківської системи. Розробка та впровадження чітких критеріїв захищеності, що враховують конфіденційність, цілісність, доступність, автентифікацію та моніторинг, є ключовим завданням для банківських установ. Водночас, досягнення оптимального балансу між забезпеченням безпеки та підтримкою безперебійної роботи системи вимагає ретельного планування та впровадження адаптивних підходів. Цей баланс є важливою складовою стратегії кібербезпеки, що дозволяє банкам ефективно протистояти сучасним загрозам та зберігати свою конкурентоспроможність у цифровому середовищі.

Список використаних джерел:

1. Огляд подій в сфері кібербезпеки, липень 2023. URL: https://www.rnbo.gov.ua/files/НКЦК/2023/Cyber%20digest_July_2023_UA.pdf

2. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

3. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах : навч. посіб. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с.

4. Коханський М. Методи масштабування реляційних баз даних: переваги, недоліки та кейси використання. URL: https://dou.ua/forums/topic/45890/

5. Що таке двофакторна автентифікація або 2FA? URL: https://experience.dropbox.com/uk-ua/resources/what-is-2fa

Радченко Владислав, здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник: д.т.н., професор Поночовний Юрій

ПРОЕКТУВАННЯ ГРАФІЧНОГО ІНТЕРФЕЙСУ ФОРМ КОРИСТУВАЦЬКОГО ДОДАТКУ З ОБСЛУГОВУВАННЯ ЗАМОВЛЕНЬ

В сучасних умовах швидкого розвитку інформаційних технологій та глобалізації ринку використання інформаційно-пошукових систем стає критично важливим для ефективного функціонування підприємств і організацій [1]. Ці системи забезпечують доступ до великих обсягів даних, що

дозволяє компаніям отримувати актуальну інформацію, приймати обґрунтовані рішення й підтримувати конкурентоспроможність на ринку. Інформаційні системи також сприяють підвищенню продуктивності, оптимізації внутрішніх процесів та покращенню якості послуг.

Метою даного дослідження є розробка та оцінка ефективності графічного інтерфейсу користувача для додатку з обслуговування замовлень, який забезпечує зручність використання та високу продуктивність.

Основні принципи розробки інтерфейсу користувача такі як, контроль користувача інтерфейсу, що забезпечує можливість користувачу контролювати процеси в додатку [2]. Зменшення завантаження пам'яті користувача, спрощує інтерфейс для зменшення навантаження на пам'ять користувача. Послідовність інтерфейсу користувача, забезпечує послідовні дії і елементи інтерфейсу для полегшення роботи з додатком.

Головне вікно програми відображає дані про замовлення, документи та товарно-транспортні накладні (ТТН) [3]. Головне меню містить пункти:

- Операції
- Довідники
- Звіти
- Діаграми
- Допомога

Функціональність додатку

1. Операції з даними

- Додавання, редагування та видалення замовлень, документів і ТТН.
- Пошук за заданим параметром та можливість скасування пошуку.

2. Візуалізація даних

- Відображення статистики у вигляді звітів і діаграм.
- Аналіз даних по замовленнях та їх виконанні.

3. Оптимізація роботи з додатком

- Мінімізація навантаження на пам'ять користувача.
- Автоматичний розрахунок суми замовлення та інтеграція з іншими елементами додатку.

Розроблений графічний інтерфейс користувача забезпечує зручний доступ до основних операцій: додавання замовлень, документів і ТТН, а також пошуку й редагування записів. Форми додавання та редагування даних побудовані таким чином, щоб мінімізувати навантаження на пам'ять користувача та спростити процес взаємодії з системою. Особлива увага приділена відображенню статистики у вигляді звітів і діаграм, що дозволяє користувачам аналізувати дані по замовленнях та їх виконанні.

Розробка графічного інтерфейсу користувача для додатку з обслуговування замовлень сприяє оптимізації внутрішніх процесів підприємства, підвищенню продуктивності та покращенню якості послуг. Використання інформаційних систем дозволяє компаніям залишатися конкурентоспроможними та приймати обґрунтовані рішення на основі актуальних даних.

Список використаної літератури

1. Ситнік Б. Т. Основи інформаційних систем і технологій : навчальний посібник, Б. Т. Ситнік. Харків : УкрДУЗТ, 2019. 176 с.
2. Павлиш В., Гліненко Л., Шаховська Н. Основи інформаційних технологій і систем. Львів: Львівська політехніка, 2018. 612 с.
3. С. В. Приймак, М. Т. Костишина, Д. В. Долбнєва, Фінансова звітність підприємств: Навчально–методичний посібник. Львів: Ліга-Прес, 2016. 268 с.

Лелюх Вадим, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

АНАЛІЗ ВИДІВ МОЖЛИВОГО ЗБИТКУ, ЩО НАНОСИТЬСЯ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ ПІДПРИЄМСТВА

Злом системи – це несанкціонований доступ до комп'ютерних систем або мереж зловмисниками з метою отримання конфіденційної інформації, пошкодження систем, викрадення даних або нанесення інших збитків. Для корпоративних мереж, таких як у Новосанжарському управлінні Полтавської філії Полтавського обласного центру зайнятості, злом системи може призвести до серйозних наслідків, зокрема витоку персональних даних громадян.

1. Основні шляхи здійснення злому. Існує кілька основних методів, які зловмисники використовують для злому системи:

Фішинг: Цей метод полягає у відправці співробітникам або користувачам підприємства підроблених електронних листів чи повідомлень, що імітують офіційні джерела. Отримувачі можуть несвідомо надати свої облікові дані або клікнути на шкідливе посилання, що дозволяє зловмиснику отримати доступ до системи.

Брутфорс (перебір паролів): Цей метод полягає в тому, що зловмисник систематично перебирає різні комбінації паролів, поки не знайде правильну. Слабкі або легко передбачувані паролі є особливо вразливими до таких атак.

Експлойти вразливостей: Кожне програмне забезпечення має певні вразливості, які можуть бути використані для отримання доступу до системи. Зловмисники використовують спеціальні програми, щоб знаходити та експлуатувати ці вразливості, отримуючи несанкціонований доступ.

Мережеві атаки: Використання протоколів передачі даних або відкритих портів мережі може бути експлуатоване для перехоплення даних або зломів. Наприклад, атаки типу «людина посередині» (Man-in-the-Middle) дозволяють зловмисникам перехоплювати та змінювати інформацію, що передається між користувачами та системою [1].

2. Наслідки витоку даних. Одним з найбільш критичних наслідків злому є витік даних користувачів. Для підприємств, таких як центри зайнятості, персональні дані, зокрема імена, прізвища, дати народження, ідентифікаційні номери, адреси, номери телефонів тощо, можуть бути викрадені та використані зловмисниками для шахрайства або інших злочинних дій.

Використання даних для шахрайства: Отримавши доступ до особистої інформації громадян, зловмисники можуть використовувати її для створення фальшивих документів, оформлення кредитів або інших фінансових зобов'язань на ім'я жертви.

Шантаж та вимагання викупу: Зловмисники можуть погрожувати підприємству або жертвам витоку оприлюдненням або продажем конфіденційної інформації на чорному ринку, вимагаючи викуп за її збереження.

Втручання у приватне життя: Викрадені персональні дані можуть бути використані для стеження за особами або втручання в їхнє приватне життя. Це може включати як створення профілів жертв для маніпуляцій, так і переслідування в реальному житті [2].

3. Економічні та репутаційні наслідки включають:

Фінансові втрати: Витік даних може призвести до значних фінансових втрат для підприємства. Це можуть бути витрати на відновлення системи після злому, а також витрати, пов'язані з судовими позовами або штрафами за недотримання законів про захист даних.

Втрати репутації: Після витоку персональних даних, довіра клієнтів та партнерів до підприємства може значно знизитися. Особливо це стосується організацій, які обробляють особисті дані громадян. Репутаційні втрати можуть вплинути на подальше функціонування організації, оскільки громадяни можуть неохоче співпрацювати з підприємством, яке втрачає їхні дані [3].

4. Юридичні наслідки. Втрата або витік персональних даних може мати серйозні юридичні наслідки. У багатьох країнах існують закони, що регулюють захист персональних даних, наприклад, Загальний регламент щодо захисту даних (GDPR) в Європейському Союзі. У разі порушення вимог цих законів підприємства можуть отримати штрафи або зазнати інших санкцій з боку державних органів.

Судові позови: Жертви витоку даних можуть подати до суду на підприємство за недбале поводження з їхніми даними. Це може призвести до додаткових фінансових втрат у вигляді компенсацій постраждалим.

Державні санкції: Регулюючі органи можуть накладати штрафи або обмеження на діяльність підприємства, яке допустило витік даних. Це може включати як фінансові санкції, так і тимчасове або постійне позбавлення права обробляти персональні дані [4].

5. Способи запобігання злому та витоку даних. Щоб запобігти злому системи та витоку даних, підприємствам необхідно впроваджувати комплекс заходів інформаційної безпеки:

Посилення політики паролів: Використання складних паролів та регулярне їх оновлення може значно знизити ризик злому через перебір паролів. Крім того, бажано впроваджувати двофакторну автентифікацію для додаткового захисту облікових записів.

Оновлення програмного забезпечення: Регулярне оновлення операційних систем, антивірусного ПЗ та інших компонентів системи дозволяє

закривати вразливості, через які зловмисники можуть отримати доступ до системи.

Шифрування даних: Використання шифрування під час передачі та зберігання даних робить їх непридатними для використання зловмисниками навіть у разі перехоплення або викрадення.

Підвищення обізнаності співробітників: Регулярне навчання персоналу основам інформаційної безпеки, зокрема розпізнаванню фішинг-атак та правильному поводженню з конфіденційною інформацією, може значно знизити ризики злому.

Моніторинг активності мережі: Постійний моніторинг активності у мережі дозволяє швидко виявляти підозрілі дії та реагувати на них до того, як буде завдано серйозної шкоди [5].

Злом системи та втрата даних користувачів – це серйозна загроза для будь-якої організації, яка обробляє персональні дані. Для уникнення таких інцидентів необхідно впроваджувати ефективні заходи безпеки, постійно моніторити стан мережі та навчати співробітників основам інформаційної безпеки.

Список використаних джерел:

1. Байковський О.Ф**.** *Інформаційна безпека: Навчальний посібник*. Київ: КНТ, 2012. 234 с.
2. Тимощук О.В. *Інформаційна безпека в корпоративних мережах*. Харків: ХНЕУ, 2014. 134 с.
3. Петренко Л.А., Мельник П.І. *Захист інформації у комп'ютерних системах та мережах*. Київ: Видавничий дім "Кондор", 2011. 45 с.
4. Рибак А.І. *Основи кібербезпеки: Підручник*. Львів: ЛНУ імені Івана Франка, 2018. 112 с.
5. Закон України "Про захист персональних даних". Відомості Верховної Ради України, 2010, № 34. 34 с.
6. Петренко А.І. *Інформаційні технології та безпека даних*. Київ: НАУ, 2015. 111 с.

Руцький Андрій, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології,
Науковий керівник: д. т. н., професор Поночовний Юрій

ВИКОРИСТАННЯ БАГАТОЯДЕРНОСТІ ЕОМ ДЛЯ ПАРАЛЕЛЬНИХ ТА РОЗПОДІЛЕНИХ ОБЧИСЛЕНЬ

Сучасні електронні обчислювальні машини (ЕОМ) зазнали значних змін протягом останніх десятиліть, і однією з головних інновацій є впровадження багатоядерних процесорів [1]. В умовах зростаючої складності обчислювальних задач, необхідності швидкої обробки даних та оптимізації роботи з великими масивами інформації, багатоядерність стала ключовим рішенням для підвищення продуктивності обчислювальних систем. Це дозволило використовувати паралельні обчислення, які відіграють важливу

роль у сучасній обробці даних, комп'ютерному моделюванні, машинному навчанні та багатьох інших областях науки й техніки.

Паралельні обчислення – це процес виконання кількох обчислень одночасно, розподіляючи завдання між кількома обчислювальними ядрами або процесорами. У традиційних однопроцесорних системах завдання виконуються послідовно, що обмежує продуктивність системи, оскільки швидкість виконання завдань залежить від одного процесора. Введення багатоядерних процесорів дозволило розв'язувати цю проблему, оскільки тепер різні ядра можуть одночасно виконувати різні завдання, що прискорює обробку даних та підвищує ефективність.

Сучасні процесори можуть містити від двох до десятків ядер, кожне з яких здатне виконувати свою власну програму або частину завдання. Це дозволяє розподіляти обчислювальні навантаження на кілька ядер, що дає змогу використовувати паралелізм на рівні інструкцій, даних та задач. У багатоядерних процесорах існує кілька ключових підходів до паралельних обчислень [2]:

1. Паралелізм на рівні інструкцій (ILP) – кожне ядро може виконувати кілька інструкцій одночасно, підвищуючи продуктивність за рахунок розподілу інструкцій між ядрами.

2. Паралелізм на рівні даних (DLP) – дані можуть бути розділені на частини та оброблятися одночасно різними ядрами, що особливо корисно для масивних обчислень, таких як обробка зображень, відео або наукові обчислення.

3. Паралелізм на рівні задач (TLP) – кожне ядро може виконувати окрему задачу, що робить цей підхід ефективним для багатозадачності.

Багатоядерні процесори забезпечують низку переваг:

1. Підвищення продуктивності – основна перевага полягає в тому, що багатоядерні системи дозволяють паралельно виконувати кілька завдань, скорочуючи час їх виконання.

2. Зниження енергоспоживання – багатоядерні процесори споживають менше енергії на одиницю обчислень у порівнянні з однопроцесорними системами. Це особливо важливо для мобільних пристроїв.

3. Масштабованість – зростання кількості ядер дозволяє системам адаптуватися до збільшених обчислювальних навантажень без значного підвищення споживання ресурсів.

Незважаючи на очевидні переваги, існують і певні виклики при розробці та використанні багатоядерних систем [3]:

1. Складність програмування – програмування для багатоядерних систем потребує від розробників спеціальних навичок та розуміння паралельних алгоритмів. Не всі задачі можуть бути легко розпаралелені.

2. Управління синхронізацією – обробка кількох завдань одночасно вимагає синхронізації між ядрами, що може призвести до виникнення проблем із гонкою даних або взаємними блокуваннями.

3. Обмеження масштабованості – ефективність використання багатоядерних систем не зростає лінійно з кількістю ядер. Наприклад, згідно з

законом Амдала, прискорення виконання програми обмежене часткою завдань, які можна розпаралелити.

Багатоядерні процесори широко використовуються в різних областях, таких як:

1. Наукові обчислення – паралельні обчислення дозволяють вирішувати складні математичні моделі та симуляції (наприклад, кліматичні моделі, симуляції фізичних процесів).

2. Обробка великих даних – багатоядерні процесори ефективно використовуються в аналізі великих обсягів даних у таких галузях, як бізнес-аналітика, машинне навчання та штучний інтелект.

3. Комп'ютерні ігри та віртуальна реальність – багатоядерні процесори дозволяють покращувати графіку, фізичні симуляції та реакцію ігор у реальному часі.

Використання багатоядерних процесорів для паралельних обчислень є важливим досягненням у галузі комп'ютерної техніки. Це дозволяє суттєво підвищити продуктивність сучасних ЕОМ, одночасно знижуючи енергоспоживання. Проте, для ефективної роботи таких систем необхідно враховувати складність програмування, синхронізації та масштабування. Перспективи розвитку багатоядерних систем залишаються значними, оскільки нові методи та алгоритми дозволяють ще більше розширити можливості паралельних обчислень.

Список використаних джерел:

1. McCool M., Reinders J., Robison A. Структуроване паралельне програмування: Шаблони для ефективних обчислень. Сан-Франциско: Morgan Kaufmann, 2012. 400 с.

2. Herlihy M., Shavit N. Мистецтво багатопроцесорного програмування. Сан-Франциско: Morgan Kaufmann, 2012. 508 с.

3. Culler D., Singh J. Паралельна архітектура комп'ютерів: апаратно-програмний підхід. Сан-Франциско: Morgan Kaufmann, 1998. 1056 с.

Ціпановська Дар'я, здобувачка вищої освіти СВО «Бакалавр»,
спеціальність 126 Інфрмаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ОСНОВИ ВЕБ-ДИЗАЙНУ

Веб-дизайн – це мистецтво та наука створення візуально привабливих і зручних для користувача веб-сайтів. Це не просто створення красивих картинок, а й забезпечення ефективної взаємодії користувача з цифровим продуктом.

Чому веб-дизайн важливий? Перше враження формує перше враження у відвідувача. Добре продуманий дизайн робить сайт інтуїтивно зрозумілим і легким у навігації. Він може збільшити конверсію, тобто перетворити відвідувачів на клієнтів. У сучасному світі веб-дизайн є одним з ключових

факторів успіху будь-якого бізнесу, тому сьогодні розберемо основні поняття веб-дизайну[1].

Головним ключем дизайну є аналіз цільовою аудиторії та конкурентів. Потрібно дослідити нішу проєктів, потреби клієнтів, бажання та їхні болі, проаналізувати сайти конкурентів, соціальні мережі та послуги, сильні та слабкі сторони, візуал, відгуки клієнтів.

Типографіка[2]:

– міжлітерну відстань потрібно збільшувати у великих букв, не потрібно збільшувати у маленьких;

– розмір тексту для контенту 14-22px, для заголовків 24px;

– вирівнювання тексту по лівому краю, іноді невеликі уривки тексту можна вирівняти по центру, але варто уникати вирівнювання по правому краю;

– оптимальна довжина рядка від 40 до 85 символів;

– прибирати “звисаючі” прийменники;

– текст на фотографіях потрібно розміщувати акуратно, не закриваючи змісту фото;

– поділ тексту на абзаци + відступи в один порожній рядок між ними;

– міжрядкова відстань +8-10 px від розміру шрифту;

– для набору довгого тексту краще вибирати шрифти із засічками (антиква – serif);

– створення контрастів та акцентів у тексті для привернення уваги.

Шрифти та гарнітура. Шрифт - це набір малих і великих символів, розділових знаків, цифр і спецсимволів одного розміру і товщини для окремої гарнітури.

Гарнітура - це "комплект" шрифтів, що мають загальні стильові ознаки та принципи побудови знаків.

Види гарнітур: гротески, антикви, брускові, рукописні, декоративні.

Колірне коло. Колірне коло - це діаграма, яка відображає взаємозв'язки між різними кольорами і колірними схемами:

– первинні - червоний, синій, жовтий;

– вторинні - кольори, які виходять в результаті змішування двох первинних кольорів, - помаранчевий, зелений, фіолетовий;

– третичні - кольори, які виходять в результаті змішування первинного та вторинного кольорів, - жовтий + помаранчевий, червоний + помаранчевий, червоний + фіолетовий, синій + фіолетовий, синій + зелений, жовтий + зелений.

Колірні схеми бувають трьох видів:

– компліментарна – кольори, які розташовані в колі один навпроти одного. наприклад, помаранчевий та синій;

– тріадна – кольори, що утворюють на колі рівносторонній трикутник. наприклад, зелений, помаранчевий та фіолетовий;

– аналогова – кольори, які розташовані у сусідніх чи близьких секторах один одного.наприклад, зелений, жовтий та жовтооранжевий.

Робота з кольором. В дизайні сайта потрібно використовувати не більше 3-4 кольорів (+чорний і білий). Обов'язково один колір має бути контрастним. Потрібно слідкувати за тим, щоб об'єкти були контрастними [3].

Початок ознайомлення з проєктом розпочинається із заповнення брифу і обговорення деталей. Бриф - це основа, на якій створюється весь сайт, тому слід попередити замовника, що заповнювати бриф потрібно максимально детально і розгорнуто. Бриф зазвичай створюється на платформі Google Forms і надсилається через посилання кожному клієнту, який бажає замовити розробку сайту.

За допомогою вивчення брифу веб-дизайнер може зануритись у філософію і стилістику бренду, сформулювати ціну і визначитися із стратегією розробки сайту. Питання у бриф слід додавати з різних галузей: від стилістики бренду до брендбуку і контенту.

Приклади питань у брифі: тип сайту(лендинг, багатосторінковий сайт, інтернет-магазин), назва і позиціонування бренду(для кого, чим займаються), опис послуги чи продукту, конкуренти, цільова аудиторія, переваги перед конкурентами, наявність брендбуку побажання по кольорам, обажання по анімації, ціль розробки сайту, емоції, які мають виникати від перегляду сайту, приклади сайтів, які подобаються.

Окремі SEO-спеціалісти займаються пунктом налаштувань SEO на сайтах, але на етапі створення сайту веб-дизайнер має робити базове SEO – налаштування: опис і адрес сторінок, налаштування сторінки заголовок H1(головний заголовок, який використовується на сайті лише один раз. Він має містити основний запит для пошуку, використовуйте не більше 12 слів або 70 символів). Опис кожної сторінки слід робити унікальним. він відображається в пошуку під заголовком сайту (160-180 символів). Вказати ключові слова для сайту, за якими сайт можуть знайти у пошуку, не слід додавати дуже багато ключових слів, слід зосередитися на декількох. Вказати зрозумілий URL, щоб людина могла запам'ятати адрес сайту або сторінки (adres.com.ua/dostavka). Встановити фавікон для сайту (фото біля назви вкладки в браузері і пошуку) [4].

Основи веб-дизайну включають різні аспекти, спрямовані на створення зручних, привабливих і функціональних веб-сайтів. Веб-дизайн – це не лише візуальне оформлення, а й грамотна організація контенту, інтуїтивна навігація, адаптивність під різні пристрої та швидке завантаження сторінок.

Список використаних джерел:

1. Круг, С. Не змушуйте мене думати! Посібник із веб-юзабіліті. Манн: Іванов і Фербер, 2015. 216 с.
2. Зельдман, Д. Веб-дизайн: книга Джеффрі Зельдмана. К.: Вільямс, 2009. 432 с.
3. Папанек, В. Дизайн для реального світу: екологія людини і соціальні зміни. К.: Лібрика, 2020. 336 с.
4. Норман, Д. Дизайн звичайних речей. К.: Видавництво Старого Лева, 2019. 384 с.

Бережна Аміна, здобувачка вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: д.т.н., професор Поночовний Юрій

СИСТЕМНИЙ АНАЛІЗ УПРАВЛІНСЬКИХ ПРОБЛЕМ НА ПІДПРИЄМСТВІ

Системний аналіз управлінських проблем є ключовим елементом забезпечення ефективного функціонування підприємства. В умовах глобалізації та цифровізації роль інформаційних систем (ІС) значно зросла, оскільки вони дозволяють інтегрувати процеси, оптимізувати ресурси та підвищувати рівень безпеки. У цьому контексті, системний аналіз управлінських проблем спрямований на виявлення недоліків у функціонуванні підприємства, розробку ефективних рішень та підвищення конкурентоспроможності.

Сучасні підприємства стикаються з численними викликами, зокрема швидкими змінами в технологіях, глобальною конкуренцією, необхідністю автоматизації бізнес-процесів та забезпечення інформаційної безпеки. Успішний аналіз управлінських проблем неможливий без комплексного підходу, який враховує як технологічні, так і організаційні аспекти. Зростання кількості зовнішніх і внутрішніх загроз для ІС підкреслює важливість створення ефективної системи управління ризиками та безпеки.

Інформаційна система є центральним елементом в управлінні підприємством, оскільки забезпечує:

- автоматизацію бізнес-процесів: дозволяє швидко обробляти великі обсяги даних, виконувати бухгалтерські операції, управляти проєктами та взаємодіями з клієнтами.
- оптимізацію ресурсів: CRM- та ERP-системи сприяють раціональному використанню фінансових, людських і матеріальних ресурсів.
- моніторинг продуктивності: відстеження виконання завдань, якості обслуговування та продуктивності співробітників.
- забезпечення звітності: формування аналітичних і фінансових звітів для внутрішнього та зовнішнього використання.

У контексті системного аналізу управлінських проблем широко використовуються такі системи:

- CRM-системи (Customer Relationship Management): управління взаємодіями з клієнтами, аналіз продажів і поведінки споживачів.
- ERP-системи (Enterprise Resource Planning): інтеграція процесів підприємства, оптимізація ресурсів і управління виробничими циклами.
- Системи бізнес-аналітики (BI-системи): обробка великих обсягів даних для прийняття стратегічних рішень.
- Інструменти моніторингу безпеки: забезпечують контроль доступу до інформації, моніторинг активності користувачів і запобігання загрозам.

Безпека є критично важливим аспектом функціонування ІС. Основні загрози поділяються на:

- Зовнішні загрози: кібератаки, віруси, фішинг, DDoS-атаки. Для їхнього запобігання використовуються антивірусні програми, фаєрволи, шифрування даних та двофакторна аутентифікація.
- Внутрішні загрози: недбалість або зловмисні дії працівників. Контроль доступу та моніторинг активності дозволяють мінімізувати такі ризики.

Основні методи забезпечення безпеки:

- шифрування даних для захисту від несанкціонованого доступу.
- регулярне резервне копіювання інформації.
- впровадження систем контролю доступу для обмеження доступу до критично важливих даних.

Ефективність інформаційної системи оцінюється за такими критеріями:

- стійкість до зовнішніх загроз: здатність протидіяти кібератакам.
- контроль внутрішніх загроз: ефективність моніторингу та управління доступом.
- надійність резервного копіювання: швидкість і точність відновлення роботи після збоїв.

Системний аналіз управлінських проблем дозволяє підприємству досягти стратегічних цілей через оптимізацію бізнес-процесів, ефективне використання ресурсів та мінімізацію ризиків. Інформаційні системи відіграють центральну роль у цьому процесі, забезпечуючи автоматизацію, інтеграцію та захист ключових процесів. Зростання загроз вимагає постійного вдосконалення безпеки ІС. Використання сучасних технологій, таких як CRM, ERP та BI-системи, дозволяє не лише підвищити ефективність управління, а й створити конкурентні переваги на ринку. Загалом, впровадження системного аналізу та інтеграція інформаційних систем є невід'ємною складовою успішного управління підприємством у сучасному світі.

Список використаних джерел:

1. Бебик, В.М. Інформаційні системи в управлінні підприємствами. Київ: Видавничий дім «КМ Академія», 2020. 250 с.
2. Вітлінський, В.В., Наконечний, С.І. Інформаційні технології в менеджменті. Київ: Центр учбової літератури, 2019. 280 с.
3. Системний аналіз управлінських проблем. URL: https://studfile.net/preview/7639460/page:5/

Горб Денис, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.с.-г.н., доцент Протас Надія

ІНТЕГРАЦІЯ ТА АНАЛІЗ ДАНИХ GPS-ТРЕКІНГУ З ІНШИМИ СИСТЕМАМИ УПРАВЛІННЯ ПІДПРИЄМСТВА

Із розвитком технологій моніторингу та контролю за транспортними засобами, зокрема через системи GPS-трекінгу, багато підприємств впроваджують сучасні методи відстеження транспорту, що забезпечують доступ до детальної інформації про місцезнаходження та стан рухомих

об’єктів. Однак, щоб максимізувати користь від таких систем, важливо не лише отримувати дані, але й інтегрувати їх з іншими інформаційними системами підприємства, такими як ERP (системи управління ресурсами), CRM (системи управління взаємовідносинами з клієнтами) та системи аналітики бізнесу. Така інтеграція дає змогу використовувати дані GPS-трекінгу для комплексного аналізу та ухвалення рішень, які підвищують ефективність операційних процесів та сприяють конкурентоспроможності компанії.

Інтеграція даних GPS-трекінгу з іншими інформаційними системами на підприємстві дозволяє автоматизувати та оптимізувати значну частину процесів управління ресурсами, зменшуючи вплив людського фактора та знижуючи ймовірність помилок. Основні цілі інтеграції включають:

1. Оптимізація логістики та зниження витрат: завдяки GPS-трекінгу та ERP-системам компанія може не лише відстежувати маршрути транспортних засобів, а й оптимізувати їх, виходячи з даних про час поїздок, швидкість та витрати палива. Така інтеграція дозволяє уникати заторів, скоротити час доставлення та оптимізувати витрати.

2. Підвищення якості обслуговування клієнтів: завдяки інтеграції GPS-трекінгу з CRM-системою компанія може надавати клієнтам актуальну інформацію про час прибуття товарів або послуг. Це особливо важливо для компаній, що займаються доставкою та обслуговуванням, оскільки своєчасна інформація про доставку підвищує рівень задоволеності клієнтів.

3. Підтримка стратегічного планування та ухвалення рішень: інтеграція даних GPS-трекінгу з системами бізнес-аналітики (BI) дозволяє керівництву аналізувати великі обсяги інформації для визначення найбільш ефективних шляхів розвитку підприємства. Наприклад, можна аналізувати середню витрату палива на маршруті, час затримки в дорозі та стан транспортних засобів, щоб приймати більш обґрунтовані рішення щодо технічного обслуговування або планування маршрутів.

Інтеграція даних GPS-трекінгу з ERP-системою є одним із найбільш перспективних напрямків, оскільки ERP охоплює широкий спектр операційних процесів підприємства, зокрема управління ресурсами, закупівлями, складами та логістикою. Через поєднання ERP та GPS-трекінгу можна автоматизувати облік пересування транспортних засобів, контролювати витрати пального та час виконання завдань.

Одним із ключових завдань інтеграції є відстеження та зменшення витрат. Дані про місцезнаходження та швидкість транспортних засобів, що надходять від GPS-систем, можуть автоматично передаватися в ERP для аналізу витрат на паливо та технічне обслуговування, що сприяє зниженню загальних операційних витрат. Завдяки цьому підприємство може, наприклад, прогнозувати витрати на основі аналізу минулих маршрутів та визначати оптимальні шляхи для майбутніх поїздок.

Інтеграція GPS-трекінгу з CRM-системою є важливим кроком для компаній, які надають послуги з доставки, технічного обслуговування чи перевезення клієнтів. Така інтеграція дозволяє відстежувати стан замовлення у

режимі реального часу та оперативно інформувати клієнтів про місцезнаходження їхнього замовлення або час прибуття.

Наприклад, при наданні послуг технічного обслуговування інтеграція GPS з CRM-системою дозволяє диспетчеру бачити, де знаходяться технічні працівники, і спрямовувати їх до клієнтів, що потребують обслуговування. Це допомагає оперативніше реагувати на виклики клієнтів, забезпечуючи їм швидке та якісне обслуговування. Крім того, на основі таких даних можна аналізувати затримки, переглянути маршрути та вносити корективи, які покращать загальний рівень обслуговування клієнтів.

Інтеграція GPS-трекінгу з системами аналітики бізнесу (BI) дозволяє отримати важливу інформацію для ухвалення стратегічних рішень. Компанії, що мають доступ до детальних звітів про переміщення транспортних засобів, витрати на паливо, час простою та інших показників, можуть проводити глибокий аналіз для покращення операційної діяльності.

Наприклад, система бізнес-аналітики може використовувати GPS-дані для аналізу продуктивності кожного транспортного засобу, враховуючи такі фактори, як середня швидкість, частота зупинок та тривалість простоїв. Це дозволяє визначити слабкі місця в операційних процесах та вжити заходів для їх усунення. Така інформація корисна для довгострокового планування, оскільки вона дозволяє оцінити ефективність різних маршрутів і коригувати плани для досягнення більшої ефективності.

Інтеграція GPS-трекінгу з іншими системами управління підприємством має і певні виклики. Одним із головних є технічна сумісність систем, адже не всі системи легко інтегруються між собою. Виникає потреба у використанні проміжного програмного забезпечення або API для синхронізації даних між різними платформами.

Іншим важливим аспектом є безпека даних. Інтеграція може призвести до виникнення ризиків несанкціонованого доступу до інформації про пересування транспорту чи взаємодії з клієнтами. Тому важливо забезпечити належний захист даних та використовувати засоби аутентифікації та шифрування, щоб уникнути витоку інформації.

Також варто згадати питання масштабування, оскільки обсяги даних, які зберігаються та обробляються, постійно зростають. Для великих компаній із численним автопарком необхідні потужні системи зберігання даних, що дозволяють обробляти великі обсяги інформації у режимі реального часу.

Інтеграція GPS-трекінгу з іншими управлінськими системами підприємства є важливим кроком для підвищення ефективності та прозорості операційної діяльності компанії. Вона дозволяє оптимізувати логістичні процеси, покращити обслуговування клієнтів, а також забезпечує керівництво інформацією, необхідною для ухвалення стратегічних рішень.

Крім того, інтеграція з системами ERP, CRM та бізнес-аналітики сприяє автоматизації значної частини операцій, що дозволяє компанії уникати помилок, пов'язаних з людським фактором, та знижувати витрати. Однак для успішної інтеграції необхідно враховувати технічні, організаційні та безпекові аспекти, забезпечуючи сумісність систем та належний рівень захисту даних.

Завдяки впровадженню таких інтегрованих рішень компанія отримує можливість гнучко реагувати на зміни в ринковому середовищі, підвищуючи власну конкурентоспроможність та створюючи додаткову цінність для клієнтів.

Список використаних джерел:

1. Інтеграція GPS-трекінгу в транспортний менеджмент. URL: https://wezom.com.ua/ua/blog/integratsiya-gps-trekingu-v-transportniy-menedzhment
2. CRM I ERP. URL: https://cleverbox-crm.com/blog/CRM-i-ERP-u-chomu-riznytsia.html

Горда Віталіна, здобувачка вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Дегтярьова Лариса

ОБГРУНТУВАННЯ НЕОБХІДНОСТІ ЗАБЕЗПЕЧЕННЯ СВОЄЧАСНОГО КОПІЮВАННЯ, АРХІВУВАННЯ ТА РЕЗЕРВУВАННЯ ДАНИХ

У сучасному світі, де інформаційні технології відіграють значну роль у всіх сферах діяльності, дані стали одним із найцінніших активів для організацій та окремих осіб. Від бізнесу до урядових установ, від освіти до охорони здоров’я – у всіх цих галузях вони допомагають приймати обґрунтовані рішення, оптимізувати процеси та покращувати якість послуг.

Однак, зростання обсягів даних і їх значення супроводжується значними ризиками втрати та пошкодження інформації. Збої в роботі обладнання, програмні помилки, кіберзлочини та людські помилки можуть призвести до серйозних наслідків, таких як фінансові втрати, порушення безперервності бізнесу та пошкодження репутації. У контексті цих ризиків, забезпечення своєчасного зберігання даних стає надзвичайно важливим.

В цієї тези є мета розглянути основні аспекти та необхідність впровадження стратегій копіювання, архівування та резервування даних. А також проведення дослідження існуючих методів їх захисту, аналіз переваг їх застосування та визначення кращих практик для мінімізації ризиків втрати інформації.

Для глибшого розуміння слід розглянути основні поняття, пов'язані з цими процесами.

Копіювання – це створення копії файлів на іншому пристрої або в хмарі на випадок втрати або пошкодження основного пристрою. Власне, його суть в тому, що при виникненні проблем з інформацією на основному комп'ютері, копія не постраждає [1]. Воно може здійснюватися вручну або автоматизовано, що забезпечує регулярне оновлення копій.

Архівування – стискання одного або багатьох файлів з метою зменшення обсягу даних при їх зберіганні на носіях інформації або при передачі їх по каналах зв’язку, у т.ч. і в мережі *Інтернет*, та розміщення стислих файлів в

одному архівному [2]. Ця інформація зазвичай не є активно використовуваною, до спеціалізованих систем зберігання для довгострокового зберігання та захисту. Архівування допомагає звільнити ресурси основних систем, зменшуючи навантаження на них, а також зберігає історичні дані для подальшого аналізу.

Резервування – це процес створення резервних копій, що дозволяє відновити їх у разі втрати чи пошкодження оригінальних даних. Резервні копії можуть зберігатися локально або в хмарі, забезпечуючи додатковий рівень захисту та доступності.

Існує кілька ключових причин, чому організації повинні забезпечувати своєчасне проведення дій по збереженню своїх даних. Як було згадано раніше, незалежно від того, чи це випадкове видалення файлів, апаратний збій або кібератака, втрата даних може мати серйозні наслідки для компанії. Кіберзлочинці постійно вдосконалюють свої методи атак. Файли можуть бути пошкоджені через віруси, шкідливе програмне забезпечення або навіть через помилки користувачів. Маючи резервні копії, організації можуть відновити пошкоджені файли без значних втрат часу, ресурсів та мінімізувати збитки.

Є кілька методів та технологій, які можна застосувати для забезпечення копіювання, архівування та резервування даних.

Локальне копіювання передбачає зберігання резервних копій на внутрішніх носіях, таких як жорсткі диски або сервери. Віддалене копіювання включає зберігання копій на віддалених серверах або в хмарі, що забезпечує додатковий рівень захисту від локальних незгод. Тлумачення того, що таке хмарні сервіси, може бути наступним: це онлайн-платформи, пов'язані з наданням користувачам постійного доступу до віддалених інтернет-ресурсів [3]. Сучасні системи резервування та архівування дозволяють автоматизувати ці процеси.

Щоб гарантовано забезпечити захист даних, важливо дотримуватися певних практик та рекомендацій. Розробка чітких політик і процедур для копіювання, архівування та резервування є критично важливою для забезпечення систематичності та узгодженості в управлінні даними.

Важливо не лише створювати резервні копії, але й регулярно перевіряти їх на предмет цілісності та можливості відновлення. Тестування допомагає виявити потенційні проблеми та забезпечити, що файли можуть бути без проблем відновлені у разі необхідності.

Шифрування копій є важливим для захисту даних від несанкціонованого доступу. Це гарантує, що навіть у випадку втрати чи крадіжки носія, вони залишаються захищеними від зловмисників.

Існує безліч реальних прикладів, коли своєчасне резервування інформації допомогло вчасно відновити інформацію після втрати.

У 2017 році Україна стала жертвою кібератаки, відомої як «*Petya*». Багато державних установ і компаній постраждали від втрати даних. Однією з них, яка змогла оперативно відновити свою інформацію, була Державна фіскальна служба України, завдяки регулярному резервуванню.

Банк «ПриватБанк» є прикладом організації, яка інвестує в системи резервування і відновлення після збоїв. У 2018 році, після серйозної технічної проблеми, банку вдалося швидко відновити всі операції завдяки регулярному проведенню дій по збереженню даних, що дозволило уникнути значних фінансових втрат і зберегти довіру клієнтів.

У 2020 році одна з великих медичних клінік в Україні постраждала від збою в системі інформаційних технологій. Завдяки наявності резервних копій даних вона змогла відновити медичні записи пацієнтів і уникнути серйозних затримок у лікуванні та діагностиці.

Відомі українські роздрібні мережі, такі як «Фора» та «АТБ», також часто стають об'єктами атак або технічних збоїв. Наявність резервних копій дозволяє їм швидко відновити інформацію про транзакції, запаси товарів і інші важливу інформацію, що важлива для безперебійної роботи магазинів.

Ці випадки демонструють, наскільки важливо інвестувати в надійні системи копіювання та архівування даних, щоб мінімізувати ризики втрати інформації і забезпечити стабільність бізнес-процесів.

На основі проведеного дослідження та аналізу можна зробити кілька важливих висновків. По-перше, це показує, що компанії, які систематично впроваджують практики резервування та архівування даних, значно знижують ризики фінансових втрат і порушень операційних процесів. По-друге, застосування сучасних технологій, таких як хмарні сервіси та автоматизовані системи архівування, забезпечує не тільки захист від фізичних пошкоджень, але й від кібератак і вірусів. Крім того, важливою є регулярна перевірка цих копій на можливість відновлення, що гарантує їх ефективність у критичних ситуаціях. Отже, інтеграція цих практик у стратегію управління даними є необхідною умовою для збереження інформаційної безпеки та стабільності організації.

Список використаних джерел:

1. Для чого потрібно резервне копіювання даних?: веб-сайт. URL: https://technari.com.ua/ua/services/about-company/articles/what-is-backup/.
2. Архівація інформації.: веб-сайт. URL: https://www.pharmencyclopedia.com.ua/article/2884/arxivaciya-informacii#:~:text=archivation%20—%20архівація)%20—%20стискання%20одного,файлів%20в%20одному%20архівному%20файлі.
3. Хмарні сервіси.: веб-сайт. URL: https://www.miyklas.com.ua/p/informatica/7-klas/sluzhbi-internetu-16659/khmarni-servisi-onlain-perekladachi-385018/re-61185e80-05e4-44d0-93aa-9f481489eb48#:~:text=Хмарні%20сервіси%20—%20це%20сервіси%2C%20пов,віддалене%20опрацювання%20та%20зберігання%20даних.

Григорчук Владислав, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий курівник: к.ф.-м.н., доцент Флегантов Леонід

ШЛЯХИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ

Інформаційна сфера, як системоутворюючий фактор життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових національної безпеки України [1]

У сучасному інформаційному середовищі захист інформації є однією з найактуальніших проблем для організацій будь-якого рівня. З ростом цифрових технологій, збільшенням обсягів даних та розвитком кіберзагроз, надійний захист інформації став життєво важливим.

1. Фізичний захист є першою лінією оборони від несанкціонованого доступу до інформаційних систем та обладнання.

Системи контролю доступу: Це технології, які обмежують доступ до критичних приміщень або систем. Вони можуть включати електронні замки, карткові системи, біометричні сканери (відбитки пальців, райдужна оболонка ока).

Огородження території: важливо мати огорожу та охоронну службу, що забезпечує контроль за доступом до об'єкта. Відеоспостереження дозволяє оперативно реагувати на загрози.

Захист обладнання: використання сейфів, стійких до злому, та спеціальних приміщень для зберігання важливих матеріалів.

2. Технічний захист передбачає використання технологій для захисту інформації від кіберзагроз.

Шифрування даних: це процес перетворення інформації в недоступну форму, що ускладнює її несанкціонований доступ. Шифрування важливе як для зберігання, так і для передачі даних.

Брандмауери і антивірусні програми: вони забезпечують фільтрацію трафіку та захист від шкідливих програм, які можуть викрасти або знищити інформацію.

Системи виявлення та запобігання вторгнень (IDS/IPS): ці системи аналізують трафік і можуть виявляти та блокувати атаки в реальному часі.

3. Організаційний захист Організаційний захист має на меті забезпечення ефективної політики безпеки на рівні організації.

Політики безпеки інформації: важливо розробити та впровадити внутрішні документи, які регламентують доступ до інформації, обробку даних та дії в разі інцидентів.

Навчання співробітників: регулярні тренінги підвищують обізнаність персоналу про ризики та способи їх запобігання, зменшуючи ймовірність випадкових помилок.

Аудити та оцінка ризиків: проведення регулярних перевірок системи безпеки дозволяє виявити вразливості та розробити стратегії їх усунення.

4. Правовий захист інформації передбачає дотримання норм законодавства та укладення відповідних угод.

Законодавство щодо захисту персональних даних: Організації повинні дотримуватись законів, що регулюють обробку персональних даних, таких як GDPR у Європі або національне законодавство в Україні.

Угоди про конфіденційність: важливо укладати угоди з партнерами, які регламентують обробку та захист інформації, що передається.

Правовий контроль: регулярні перевірки дотримання законодавчих вимог забезпечують правову безпеку організації.

5. Моніторинг і готовність до реагування на інциденти – критично важливі елементи системи захисту інформації.

Моніторинг систем: постійний моніторинг допомагає виявляти аномалії, що можуть свідчити про спробу несанкціонованого доступу.

Плани реагування на інциденти: наявність чітких планів та процедур дозволяє швидко реагувати на загрози та зменшити їх наслідки.

Тестування на проникнення: проведення регулярних тестів на проникнення виявляє потенційні вразливості, дозволяючи своєчасно вжити заходів.

Новітні тренди в кібербезпеці:

– Захист на основі штучного інтелекту: використання алгоритмів машинного навчання для виявлення аномалій у трафіку та поведінці користувачів. Це дозволяє швидше реагувати на загрози. Наприклад, системи, які аналізують величезні обсяги даних в реальному часі, можуть ідентифікувати потенційні атаки ще до їх реалізації [2].

– Zero Trust Architecture (ZTA): модель безпеки, яка передбачає, що жоден користувач або система не можуть бути автоматично визнані надійними. Кожен запит на доступ перевіряється незалежно від його джерела. Цей підхід зменшує ризики внутрішніх загроз і покращує контроль за доступом [3].

– Кібергігієна: поняття, яке включає в себе найкращі практики, які користувачі повинні дотримуватись для захисту своїх особистих і корпоративних даних. Це охоплює такі речі, як створення складних паролів, регулярне оновлення програмного забезпечення та обережність у використанні публічних Wi-Fi мереж.

– Розширена безпека в хмарі: з ростом популярності хмарних технологій, багато організацій реалізують нові засоби захисту для даних, зокрема шифрування, контроль доступу та моніторинг активності [4].

Управління ризиками:

– Аналіз ризиків: регулярне оцінювання потенційних загроз і вразливостей допомагає організаціям створити дієві стратегії захисту. Рекомендується використовувати такі моделі, як OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) для систематизації оцінки ризиків [2].

– Бізнес-процеси і безпека: впровадження концепції безпеки в бізнес-процеси є ключовим. Це включає в себе створення безпечних каналів для обробки інформації та захисту даних на всіх етапах їхнього життєвого циклу.

Захист інформації на об’єкті є багатогранним завданням, що вимагає інтеграції фізичних, технічних, організаційних і правових заходів. Тільки комплексний підхід дозволить забезпечити надійний захист інформації, запобігти її витоку та зберегти довіру клієнтів і партнерів. Сучасні загрози вимагають від організацій постійного вдосконалення методів захисту та адаптації до нових викликів. Це дозволить не лише забезпечити інформаційну безпеку, а й створити здорове середовище для розвитку бізнесу.

Список використаних джерел:

1. Основи інформаційної системи та захисту URL: https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf
2. Кібербезпека та штучний інтелект URL: Cybersecurity Insiders
3. Zero Trust Architecture модель безпеки URL: https://www.trendmicro.com//what-is/what-is-zero-trust/zero-trust-architecture.html
4. Кібергігієна що таке кібергігієна URL: https://www.nist.gov/itl/publications/cyber-hygiene-guide
5.Управління ризиками URL: https://biz.ligazakon.net/news/230512_upravlnnya-rizikami-nformatsyno-bezpeki-v-kompan

Майборода Віталіна, здобувачка вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Дегтярьова Лариса

МОДЕРНІЗАЦІЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ, АПАРАТНОГО ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Модернізація мережевого обладнання, апаратного та програмного забезпечення є однією з ключових задач, з якими стикаються підприємства, що спеціалізуються на ремонті комп'ютерів. В умовах швидкого розвитку інформаційних технологій і збільшення потреб у обробці та зберіганні даних, оновлення технічної бази стає не просто бажаним, а необхідним кроком для забезпечення конкурентоспроможності та ефективності роботи. У невеликих підприємствах, таких як ФОП «Ремонт комп'ютерів та периферійного устаткування», на якому була пройдена практика, проблеми із застарілим обладнанням можуть призвести до зниження продуктивності, зростання витрат на обслуговування та втрат клієнтів через незадовільний рівень обслуговування.

Застаріле мережеве обладнання може значно обмежити можливості малого бізнесу. Витрати на підтримку та ремонт такого обладнання зростають, а його продуктивність і надійність залишають бажати кращого. Оновлення технічної бази дозволяє не лише підвищити ефективність роботи підприємства, але й забезпечити стабільну і безперебійну роботу інформаційних систем [1]. У цьому контексті підприємства з обмеженими ресурсами повинні ретельно підходити до вибору нового обладнання,

обираючи такі рішення, які забезпечать максимальну вигоду за мінімальних витрат.

Модернізація підприємства ФОП «Ремонт комп'ютерів та периферійного устаткування» може включати заміну старих комутаторів і маршрутизаторів стандарту Fast Ethernet на сучасні рішення з підтримкою Gigabit Ethernet. Крім того, варто звернути увагу на впровадження систем безпеки, таких як фаєрволи та захищені VPN-з'єднання, що дозволять підвищити рівень захисту даних. Програмне забезпечення також відіграє критично важливу роль: використання сучасних операційних систем і антивірусних програм сприяє підвищенню продуктивності та безпеки роботи.

Апаратне та програмне забезпечення, яке використовується на малих підприємствах, має відповідати сучасним стандартам безпеки та ефективності. Вибір правильних рішень дозволяє знизити витрати на енергоспоживання, покращити управління ресурсами та забезпечити надійний захист від кіберзагроз [2]. Це означає, що модернізація апаратного забезпечення повинна враховувати не лише поточні потреби підприємства, а й можливості для подальшого розвитку і розширення бізнесу.

Причини, що спонукають підприємства до модернізації, часто пов'язані з проблемами, які виникають через використання застарілого обладнання. На прикладі підприємства, де була пройдена практика, очевидно, що старі комутатори та маршрутизатори вже не можуть забезпечити достатню швидкість і надійність з'єднання для ефективної роботи. Крім того, вони стають вразливими до кіберзагроз, що ставить під загрозу безпеку даних клієнтів.

Застарілі системи не здатні забезпечити необхідний рівень захисту даних та ефективності обробки інформації. Їх заміна на новіші моделі дозволяє не лише підвищити продуктивність, але й знизити ризики, пов’язані з безпекою [3]. Це твердження ще раз підкреслює необхідність оновлення технічної бази, зокрема на підприємствах, які працюють з великими обсягами інформації та даними клієнтів.

Для невеликих ФОП, що займаються ремонтом комп'ютерів, підходящими оновленнями апаратного та програмного забезпечення є придбання сучасних настільних комп'ютерів з потужними процесорами і великим обсягом оперативної пам'яті, а також впровадження актуальних версій операційних систем і антивірусних програм. Оновлення програмного забезпечення має включати інструменти для діагностики і ремонту, які полегшать процес роботи і дозволять швидше вирішувати проблеми клієнтів [4].

Під час виробничої практики на базі ФОП «Ремонт комп'ютерів та периферійного устаткування» було проаналізовано стан програмного і апаратного забезпечення підприємства. Виявлено, що єдиний комп'ютер на підприємстві працює на застарілому обладнанні, що потребує оновлення: заміна процесора, збільшення оперативної пам'яті до 16 ГБ, встановлення SSD для підвищення продуктивності. Також було запропоновано оптимізувати

програмне забезпечення, зокрема інтегрувати RemOnline з іншими системами для покращення управління бізнес-процесами.

Отже, модернізація мережевого обладнання, апаратного та програмного забезпечення є ключовим фактором для забезпечення ефективності та безпеки роботи підприємств у сфері ремонту комп'ютерів. Вона дозволяє не лише покращити продуктивність, але й забезпечити надійний захист даних, що є критично важливим в умовах сучасного цифрового світу.

Список використаних джерел:

1. Петренко І. В. Мережеві технології для малого бізнесу: проблеми та перспективи // Журнал "Інформаційні системи". 2023. № 2. С. 45–50.

2. Іваненко А. М., Сидоренко В. П. Вибір апаратного та програмного забезпечення для малих підприємств // Монографія "Сучасні тенденції в управлінні ІТ-ресурсами". Київ: Технопрес, 2022. С. 132–148.

3. Савченко О. Л. Забезпечення безпеки даних на малих підприємствах: сучасні виклики та рішення // Журнал "Кібербезпека і захист інформації". 2023. № 3. С. 60–67.

4. Семенов, Р. Г. (2022). "Оптимізація ІТ-інфраструктури для малих підприємств". Київ: Видавництво "Бізнес".

Насоненко Олександр, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к. т. н. доцент Дегтярьова Лариса

АНАЛІЗ СПЕЦІАЛІЗОВАНИХ ЗАСОБІВ ДЛЯ БОРОТЬБИ З ВІРУСАМИ, НЕСАНКЦІОНОВАНИМИ РОЗСИЛКАМИ ЕЛЕКТРОННОЇ ПОШТИ, ШКІДЛИВИМИ ПРОГРАМАМИ

На сучасному підприємстві питання кібербезпеки займають одне з ключових місць, оскільки навіть невеликий витік даних чи зараження системи може призвести до серйозних наслідків. Протягом моєї літньої практики я ознайомився з різними засобами, що застосовуються для боротьби з вірусами, несанкціонованими розсилками електронної пошти та шкідливими програмами. В цьому звіті буде детально проаналізовано спеціалізовані програми, які використовуються на підприємстві для забезпечення безпеки.

Для аналізу було використано захист від вірусів ESET NOD32 Antivirus.

ESET NOD32 Antivirus [1] є одним із найпопулярніших антивірусних рішень, яке використовується на підприємстві для захисту від вірусів та інших видів шкідливого програмного забезпечення. Основні переваги ESET NOD32 включають в себе:

1. Висока швидкість сканування: Завдяки оптимізованому алгоритму сканування програма мінімально впливає на продуктивність системи, що є важливим фактором для забезпечення безперебійної роботи підприємства.

2. Проактивний захист: ESET NOD32 використовує технології евристичного аналізу для виявлення нових загроз, навіть якщо вони ще не були внесені до баз даних вірусів.

3. Легка інтеграція та централізоване управління: Програма легко інтегрується в існуючу IT-інфраструктуру підприємства, а централізована консоль управління дозволяє адміністратору контролювати стан безпеки на всіх робочих станціях.

На підприємстві ESET NOD32 встановлено на кожному комп'ютері та сервері. Окрім цього, регулярно проводяться автоматизовані оновлення вірусних баз, що дозволяє завжди бути готовими до нових загроз. Для підвищення рівня захисту, підприємство також налаштувало автоматичне сканування всіх підключених пристроїв та завантажених файлів, що мінімізує ризик зараження системи.

Для боротьби з несанкціонованими розсилками можна використовувати SpamAssassin, який є відомим рішенням для фільтрації спаму, що використовується на підприємстві для забезпечення чистоти електронної пошти. Основні переваги цього програмного забезпечення включають:

1. Гнучкість налаштувань: SpamAssassin [2] дозволяє створювати та налаштовувати правила фільтрації спаму відповідно до потреб підприємства. Це забезпечує більш ефективний захист, адаптований до конкретних умов.

2. Висока точність фільтрації: Завдяки використанню різних методів аналізу, включаючи перевірку заголовків, аналіз тексту та оцінку ймовірності, SpamAssassin має високу точність у виявленні спаму, знижуючи кількість помилкових спрацьовувань.

3. Можливість інтеграції з іншими системами: Програма легко інтегрується з поштовими серверами та іншими засобами захисту, що використовуються на підприємстві, що дозволяє створити єдину систему безпеки електронної пошти. На підприємстві SpamAssassin використовується як на основному поштовому сервері, так і на клієнтських комп'ютерах, що забезпечує двоетапну фільтрацію вхідних повідомлень. Це зменшує кількість несанкціонованих розсилок, які доходять до кінцевих користувачів, а також запобігає можливим фішинговим атакам.

Для захисту від шкідливих програм розглянуто ПЗ Malwarebytes [3].

Malwarebytes є потужним інструментом для захисту від шкідливих програм, який використовується на підприємстві як додатковий рівень безпеки. Його основні переваги:

1. Висока ефективність у боротьбі з рідкісними загрозами: Malwarebytes спеціалізується на виявленні загроз, які можуть бути пропущені стандартними антивірусами, таких як руткіти, шпигунські програми та інші складні види шкідливого програмного забезпечення.

2. Регулярні оновлення: Програма регулярно оновлює свої бази даних, що дозволяє бути в курсі нових методів атак. Простота використання: Malwarebytes має зручний інтерфейс, що робить її легкою у використанні як для IT-спеціалістів, так і для звичайних користувачів.

На підприємстві Malwarebytes інтегрована з основною антивірусною системою і використовується для щоденного сканування комп'ютерів. Це дозволяє забезпечити глибоке сканування системи на наявність шкідливих програм та своєчасно видаляти загрози. Окрім цього, Malwarebytes

використовується для аналізу підозрілих файлів та процесів, які можуть бути загрозою для безпеки підприємства.

Використання спеціалізованих програм, таких як ESET NOD32 Antivirus, SpamAssassin та Malwarebytes, дозволяє підприємству підтримувати високий рівень кібербезпеки. Завдяки комплексному підходу до захисту, який включає антивірусний захист, фільтрацію спаму та боротьбу зі шкідливими програмами, підприємство може ефективно протистояти різним загрозам, забезпечуючи стабільну та безпечну роботу всіх інформаційних систем.

Список використаних джерел::

1. ESSENTIAL SECURITY ESET NOD32 Antivirus. URL: https://help.eset.com › uk-UA
2. Антиспам SpamAssassin. URL: https://uh.ua/ua/kb/hosting/bezopasnost/spamassistent.html
3. Malwarebytes Огляд 2024: Безпечна безкоштовна версія? URL: https://uk.wizcase.com/antivirus/malwarebytes/

Рибка Анастасія, здобувачка вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ТЕХНОЛОГІЯ ЗАСТОСУВАННЯ МЕРЕЖІ ІНТЕРНЕТ У СУЧАСНИХ БІЗНЕС-ПРОЦЕСАХ

Сучасний бізнес вже не може існувати без використання Інтернету. Це стало невід'ємною частиною будь-якої діяльності, незалежно від розміру компанії або галузі. Інтернет надає можливість ефективніше взаємодіяти з клієнтами, оптимізувати внутрішні процеси та забезпечувати швидкий доступ до необхідної інформації. Компанії створюють свої вебсайти та використовують Інтернет для розміщення реклами товарів і послуг. Використання Інтернет-технологій для оптимізації інформаційних і комерційних процесів на підприємствах сприяло появі численних методів отримання прибутку через мережу Інтернет.

Насамперед одним із ключових аспектів застосування Інтернету у бізнесі є комунікація. Засоби комунікації, такі як соціальні медіа, чат-боти та персоналізовані рекомендації, дозволяють сучасним підприємствам налагоджувати більш ефективний та індивідуалізований контакт з клієнтами, що формує клієнто-орієнтовану економіку [1]. Крім того, Інтернет дозволяє ефективно впроваджувати CRM-системи для управління відносинами з клієнтами. Завдяки інтеграції з веб-платформами, CRM-системи дозволяють автоматично оновлювати дані, аналізувати поведінку клієнтів і планувати маркетингові кампанії.

Інтернет дозволяє компаніям автоматизувати чимало внутрішніх процесів. Наприклад, системи управління підприємством (ERP), які працюють на базі Інтернету, дозволяють інтегрувати різні підрозділи компанії,

забезпечуючи єдиний доступ до даних. Це сприяє зменшенню кількості помилок, пришвидшує прийняття рішень та покращує координацію між відділами. Інтернет також дозволяє використовувати хмарні рішення для зберігання даних та їх обробки.. Завдяки ним підприємство не лише знижує витрати на підтримку власних серверів, але й забезпечує доступ до інформації з будь-якої точки світу, що є особливо важливим для компаній з розгалуженою мережею офісів. Найбільш поширеними хмарними платформами є Amazon Web Services, Microsoft Azure та Google Cloud Platform

Технології Інтернету дозволяють реалізувати різноманітні стратегії онлайн-маркетингу. Він включає в себе використання різних цифрових каналів, таких як соціальні мережі, електронна пошта, контекстна реклама, SEO (пошукова оптимізація), контент-маркетинг та багато іншого. Інтернет дозволяє в умовах жорсткої конкуренції здійснювати так званий індивідуальний маркетинг, тобто пропонувати товари і послуги, максимально адаптовані до потреб конкретного споживача [2]. Більшість підприємств використовують SMS-розсилки, які дозволяють компанії швидко повідомляти клієнтів про нові пропозиції, акції та важливі оновлення, що допомагає підтримувати високий рівень взаємодії та лояльності. Власний сайт також є ключовим елементом стратегії онлайн-маркетингу, оскільки забезпечує централізовану платформу для представлення продуктів і послуг. Сайт оснащений зручними функціями для онлайн-замовлень та зворотного зв'язку, що спрощує процес взаємодії з компанією. Соціальні мережі, такі як Facebook та Instagram теж грають важливу роль у маркетинговій стратегії підприємства. Через ці платформи компанія активно взаємодіє з аудиторією, публікуючи контент, що відображає новини, акції, та інші важливі оновлення.

Застосування Інтернету в бізнесі відкриває нові можливості, але й створює ризики, зокрема кіберзагрози. Зі зростанням цифровізації збільшується кількість кібератак, що можуть призвести до крадіжки даних і порушення роботи компанії. Для захисту необхідно впроваджувати заходи кібербезпеки: антивірусні програми, аудити систем та навчання персоналу.

Інтернет став важливим елементом сучасного бізнесу, надаючи можливості для покращення ефективності компаній. Він дозволяє швидше та ефективніше спілкуватися з клієнтами, знижуючи витрати на традиційні методи комунікації і покращуючи обслуговування. Оптимізація внутрішніх процесів через онлайн-платформи знижує витрати і підвищує продуктивність, а електронна комерція розширює ринки збуту, підвищуючи конкурентоспроможність. Проте, з розширенням використання Інтернету виникають нові виклики, особливо у сфері кібербезпеки та захисту даних. Важливо враховувати ці ризики і впроваджувати заходи безпеки, такі як регулярний аудит систем, оновлення програмного забезпечення та навчання персоналу, щоб мінімізувати загрози і забезпечити стабільний розвиток бізнесу.

Список використаних джерел:

1. Вербівська Л.В., Буринська О.І. Використання цифрових технологій у підприємницькій діяльності. *Економіка та суспільство*. 2024. № 61.
2. Антонів Є. Використання можливостей інтернету у підприємницькій діяльності: матеріали VIII Всеукр. студ. наук.-техн. конф. Тернопіль: ТНТУ, 2015. Т. 2. 26-27 с.

Срібна Єва, здобувачка вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ЗАСТОСУВАННЯ ЛОМ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ОХОРОНИ

Локальна обчислювальна мережа (ЛОМ) – це система, яка об’єднує пристрої в межах конкретного регіону, охоплюючи від кількох до тисячі комп'ютерів однієї організації [1].

На підприємствах ЛОМ є важливим елементом у сучасних системах відеоспостереження та охорони. Вона забезпечує ефективну передачу, обробку та зберігання даних з камер спостереження, датчиків та інших пристроїв безпеки, що сприяє підвищенню рівня безпеки і оптимізації управління системами охорони.

Завдяки ЛОМ забезпечується швидка та надійна передача відео та даних між камерами спостереження, серверами для обробки інформації та моніторинговими точками. Використання сучасних мережевих протоколів, таких як Ethernet, дозволяє передавати відео високої чіткості без затримок.

Системи відеоспостереження генерують великі обсяги даних, які потребують зберігання для подальшого аналізу та перегляду. ЛОМ дає змогу використовувати мережеве сховище даних (NAS) і сервери для централізованого зберігання відеозаписів, що забезпечує швидкий та зручний доступ до них.

Завдяки ЛОМ відеоматеріали з камер спостереження можуть бути негайно надіслані на сервери для аналізу і обробки. Це дозволяє застосовувати програмне забезпечення для розпізнавання облич, виявлення підозрілої поведінки та виконання різноманітних аналітичних завдань.

LOM також дозволяє інтегрувати системи відеоспостереження з іншими системами безпеки, такими як сигналізація, контроль доступу та пожежна безпека, забезпечуючи комплексний підхід до управління безпекою об’єкта.

Основні компоненти для систем відеоспостереження та охорони на підприємстві включають:

1. Камери спостереження: Наприклад, IP-камери, які підключаються до ЛОМ і передають відео через мережу, можуть мати різні функції, такі як роздільна здатність, кут огляду, нічне бачення та вбудована аналітика.

2. Мережеве обладнання: Комутатори, маршрутизатори та точки доступу використовуються для побудови локальної мережі (LAN),

забезпечуючи з’єднання між камерами, серверами та моніторинговими точками.

3. Сервери та сховища даних: Сервери обробляють відео та інші дані, а NAS забезпечує зберігання відеозаписів. RAID-масиви гарантують надійність і безпеку зберігання даних.

4. Програмне забезпечення: Системи управління відеоспостереженням дозволяють контролювати камери, переглядати та аналізувати відеоматеріали, створювати оповіщення та інтегруватися з іншими системами безпеки. Наприклад, на ТОВ «Завод Укрбудмаш» використовується програмне забезпечення Luxriot Evo, яке забезпечує реальний час аналітики, відстежуючи як рухомі, так і нерухомі об’єкти, і залишається ефективним при зміні умов навколишнього середовища [2].

LOM забезпечує високу швидкість передачі даних, що дозволяє переглядати відео в реальному часі без затримок – це критично важливо для оперативного реагування на інциденти. Мережа легко адаптується до нових пристроїв, що дозволяє інтегрувати додаткові камери і обладнання без значних витрат, що є особливо важливим для великих об’єктів з розгалуженою інфраструктурою.

Таким чином, ЛОМ забезпечує централізоване управління всіма пристроями в системі відеоспостереження та безпеки, спрощуючи адміністрування та моніторинг. Сучасні системи безпеки на базі ЛОМ пропонують швидку передачу даних, миттєву обробку відео, централізоване зберігання та можливості для аналізу, що дозволяє підприємствам створювати надійні та адаптивні системи безпеки, що відповідають сучасним вимогам. Впровадження передових технологій у ЛОМ підвищує рівень захисту об’єктів і поліпшує управління безпекою.

Список використаних джерел:

1. ЛОМ. Що це таке? URL: https://os.eco/uk/blog/blog-lvc/.

2. Багатофункціональна система LUXRIOT. URL: https://www.konicaminolta.ua/uk-ua/software/videosolution/luxriot.

Щербина Ілля, здобувач вищої освіти СВО «Бакалавр», спеціальність 126 Інформаційні системи та технології
Науковий керівник : к.т.н. , доцент Одарущенко Олена

ЕРГОНОМІКА (ЮЗАБІЛІТІ) ВЕБ-САЙТУ

Юзабіліті (ергономічність) веб-сайту – одна з основних характеристик, що визначає його зручність для кінцевих користувачів. Сайт «Компанії «Надежда» відповідає вимогам сучасного веб-дизайну, забезпечуючи високий ступінь зручності та доступності для різних категорій користувачів.

Домашня сторінка «Компанії «Надежда» надає користувачам швидкий доступ до основної інформації про діяльність компанії, продукти та послуги. Важливими аспектами є розташування меню та основних розділів, що відображаються у верхній частині сторінки.

Меню розділів представлено чітко та логічно, що дозволяє користувачам швидко знаходити потрібну інформацію та мінімізує час пошуку. Кнопки, що забезпечують перехід до різних сторінок, добре помітні, а контрастні кольори використовуються для того, щоб зробити їх більш привабливими та легшими для навігації порівняно з типовим фоном. Це підвищує ефективність роботи користувачів, особливо тих, хто вперше заходить на сайт.

Веб-сайт приватного підприємства розроблений у приємних кольорах, щоб не надавати користувачам занадто багато непотрібної інформації. Простий дизайн дозволяє користувачам зосередитися на головному і не відволікатися на другорядні елементи. Важливо також відзначити, що веб-сайт використовує адаптивний дизайн, що означає, що його можна використовувати на різних розмірах екранів, у тому числі на мобільних пристроях. Враховуючи, що все більше людей користуються інтернетом через смартфони та планшети, це значно підвищує доступність та зручність користування сайтом.

Великі блоки тексту та зображень, що відображають основні послуги та переваги компанії, дозволяють користувачам з першого погляду зрозуміти, що пропонує «Компанія «Надежда».

Кожен блок добре виділений на сторінці і підкріплений відповідними зображеннями, які підвищують видимість тексту. Візуальні елементи гармонійно поєднуються з текстовими, привертаючи увагу користувача і збільшуючи ймовірність того, що він залишиться на сайті довше.

Інформаційна архітектура сайту розроблена таким чином, щоб задовольнити потреби різних груп користувачів. Наприклад, розділи скрапленого газу та нафтопродуктів розділені таким чином, щоб клієнти, які цікавляться певним видом продукції, могли швидко перейти до відповідного контенту.

Функціонал сайту доповнюють інтегровані інструменти зворотного зв'язку на різних рівнях.

Наприклад, контактна форма внизу сторінки дозволяє користувачам легко зв'язатися з представником компанії, не залишаючи сторінки, на якій вони перебувають. Це підвищує зручність взаємодії та скорочує час, який витрачається на відповіді на запитання та вирішення проблем. Інтеграція цього функціоналу зворотного зв'язку демонструє орієнтацію компанії на клієнтоорієнтований підхід.

З технічної точки зору, сайт створено відповідно до найсучасніших вимог щодо швидкості завантаження сторінок та оптимізації контенту.

Завдяки цьому користувачі можуть переміщатися по сайту без затримок, що дуже важливо для користувачів з повільним інтернет-з'єднанням. Стиснення зображень, ефективне використання кешу браузера та оптимізація коду зменшили час завантаження, що позитивно вплинуло на загальний користувацький досвід.

Веб-сайт інтегрований із соціальними мережами, дозволяючи користувачам легко переходити на сторінки компанії на таких популярних платформах, як Facebook, Instagram і YouTube. Це дає їм більше можливостей

для взаємодії з клієнтами та доступу до останніх новин компанії, акцій та інших важливих оновлень. Соціальні кнопки розміщуються у верхній частині сторінки і стають доступними одразу після завантаження сайту, допомагаючи поширювати контент компанії в інтернеті.

Ще одним важливим аспектом є багатомовна підтримка. Це демонструє готовність компанії розширювати свою клієнтську аудиторію, надаючи інформацію різним мовним групам. Такий підхід не тільки підвищує доступність інформації, але й покращує міжнародну репутацію компанії.

З точки зору безпеки, сайт оснащений SSL-сертифікатом, який гарантує безпечний обмін даними між користувачем і сервером. Це важливо для захисту конфіденційної інформації, особливо форм зворотного зв'язку, де користувачі вводять свої персональні дані. Безпечне з'єднання створює довіру до сайту і показує, що компанія піклується про безпеку своїх клієнтів.

Адаптивний дизайн забезпечує високу якість перегляду на мобільних пристроях. Користувачі можуть переглядати контент сайту без втрати функціональності та зручності.

Інтерфейс мобільної версії сайту інтуїтивно зрозумілий, а основні кнопки залишаються доступними для натискання на невеликих екранах, що підвищує загальну зручність використання. Крім того, сайт швидко завантажується, що також важливо для мобільного юзабіліті.

Крім того, на сайті розміщена карта мережі АЗС BVS, яка полегшує навігацію і дозволяє клієнтам швидко знайти найближчу заправку.

Відгуки користувачів, розміщені на сайті, також сприяють підвищенню довіри до компанії, що важливо для створення позитивного іміджу.

Загалом, сайт «Компанії «Надежда» вирізняється продуманою структурою, вдосконаленою ергономікою та простотою використання. Це сприяє підвищенню задоволеності та лояльності користувачів до компанії, забезпечуючи максимально приємний досвід для всіх категорій користувачів.

Список використаних джерел:

1. Компанія «Надежда» веде свою діяльність з 1988 року: https://www.oil.pl.ua/about-us/

2. Грицунов О. В.Інформаційні системи та технології: навч. посіб. для студентів за напрямом підготовки «Транспортнітехнології». Харк. нац. акад. міськ. госп-ва. Х.: ХНАМГ, 2010. 222 с.

3. Структура інформаційної системи: https://pidru4niki.com/13761025/informatika/struktura_informatsiynoyi_sistemi#google_vignette

Юдінцов Даніїл, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: д.т.н., професор Поночовний Юрій

ШЛЯХИ ВДОСКОНАЛЕННЯ РЕКЛАМНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

Рекламна діяльність, так само як і будь-яка інша діяльність, реалізується з урахуванням відповідних методів і певних правил. Вона може складатися з операцій, а також часткових процесів, тобто можна сказати, що вона виконується за технологією, ефективність якої, як правило, залежить від якості її попередньої підготовки (планування та виконання) [1]. При дослідженні роботи підприємства були виявлені проблеми знаходження інформації про його діяльність. Це пов'язано з тим, що компанія не дуже вдало працює в рекламній сфері України. В сьогоднішніх умовах нестабільної ринкової економіки і розвитку підприємств в цілому, дуже важко знайти інформацію про такі підприємства. Для того, щоб розв'язувати цю проблему потрібно розширення інформаційного простору діяльності підприємства. Тобто підприємство повинно, проводити цілісну рекламну компанію, що до своєї діяльності.

Для цього рекомендується наступні кроки:

– створення власних курсів по типу Prometheus, які допомагають клієнтам ефективніше використовувати продукти чи послуги компанії;

– створення заходів в соціальних мережах компанії, де клієнти можуть обмінюватися досвідом та ідеями;

– реалізацію соціальних ініціатив, які відповідають цінностям цільової аудиторії;

– участь у галузевих виставках та конференціях, допоможе збільшити впізнаваність бренду та налагодити нові контакти;

– розвиток клієнтського сервісу з використанням вебчатів;

– тестування нових продуктів підприємства, яка дозволяє клієнтам тестувати нові продукти перед їх офіційним запуском;

– бонуси(це можуть бути знижки) за досягнення, допустимо винагородження клієнтів за досягнення певних цілей, покупок тощо;

– впровадження свого відео-каналу, де будуть навчальні відео про використання продуктів, інтерв'ю з експертами в галузі;

– покращення видимості сайту підприємства в результатах пошуку;

– впровадження конкурсів, допустимо: «Найкреативніші ідеї від користувачів».

Ці рішення допоможуть покращити рекламну діяльність підприємства. В результаті цих впроваджень можна побачити такі позитивні чинники:

– збільшення продажів;

– зростання обізнаності про товари і послуги компанії;

– покращення іміджу компанії;

– підвищення лояльності у наявних клієнтів;

– підтримка виходу нових продуктів на ринок.

Для покращення рекламної стратегії рекомендується [2]:

– аналіз даних та покращення показників ефективності. Необхідно визначити які планові показники були досягнуті, а які ні та висунути гіпотези про причини недосягнення планових показників;

– використання нових рекламних каналів. Це дозволить знайти нових потенційних клієнтів та збільшити впізнаваність бренду;

– збільшення рекламного бюджету. Це дозволить охопити більшу кількість зацікавленої аудиторії;

– використання інновацій в рекламній діяльності. Наприклад, технології інтерактивної взаємодії, віртуальної реальності, тривимірне зображення рекламної інформації тощо.

Планування рекламної діяльності є важливим етапом у формуванні загальної стратегії бізнесу і повинно бути інтегровано з усіма розділами бізнес-плану підприємства. Це дозволяє чітко визначити місце реклами у комплексі маркетингових комунікацій і забезпечити узгодженість між рекламними кампаніями та іншими елементами стратегії. Зокрема, рекламна діяльність повинна відповідати конкретній ціновій та товарній політиці компанії. Це включає визначення цільової аудиторії, яка найбільше зацікавлена у пропонованих товарах або послугах, а також розробку повідомлень, які відображають унікальні переваги продуктів чи послуг і відповідають споживчим очікуванням. Крім того, реклама повинна бути узгоджена з організацією продажу товарів, включаючи вибір каналів розподілу, структуру ціноутворення і спеціальні акції. Це забезпечить синергію між рекламними зусиллями та процесами продажу, що, своєю чергою, сприятиме досягненню високих результатів у просуванні товарів і послуг на ринку. Включення реклами в загальний бізнес-план також дозволяє здійснювати ефективний моніторинг і оцінку результатів рекламних кампаній, вносячи необхідні корективи на основі отриманих даних. Це допомагає підприємству адаптувати свою маркетингову стратегію відповідно до змін на ринку, потреб споживачів та конкурентних умов, забезпечуючи тим самим сталий розвиток і успішну реалізацію бізнес-цілей.

Отже, основу рекламної діяльності підприємства, як цілісної системи, складає програма організації управління рекламною діяльністю відповідно до якої виділено основні блоки організації управління рекламною діяльністю в підприємстві: дослідження, планування рекламних заходів, тактичні рішення, оперативний контроль, оцінка ефективності рекламних заходів [3]. Підприємство ТОВ «КвартСофт АГРО» може здійснювати ефективну рекламну стратегію, яка задовольнятиме компанію новими клієнтами, які свою чергу задовольнятимуть потреби користувачів, зацікавлених у агробізнесі.

Список використаних джерел:

1. Vynohradova O. V. Organization of advertising activities at production enterprises. Economy. Management. Business. 2021. № 1. URL: https://doi.org/10.31673/2415-8089.2021.011015.

2. Kurylo L., Pichyk N. Advertising activity of the enterprise and

directions of its improvement. International scientific journal "Internauka". Series: "Economic Sciences". 2017. No. 4(48). URL: https://doi.org/10.25313/2520-2294-2021-4-7112

3. Шульга О. А. Управління рекламно-інформаційною діяльністю підприємства. Підприємництво і торгівля. 2023. № 38. С. 84–93. URL: https://doi.org/10.32782/2522-1256-2023-38-11

Юхименко Євгеній, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к. т. н. доцент Дегтярьова Лариса

ХАРАКТЕРИСТИКА ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ НА ПІДПРИЄМСТВАХ

Технічні засоби охорони на підприємстві є ключовими компонентами для забезпечення безпеки активів і працівників. Вони включають широкий спектр інструментів та рішень, що забезпечують захист від несанкціонованого доступу, крадіжок, вандалізму та інших загроз. Це комплексний підхід, що охоплює фізичний, технічний захист, моніторинг та сигналізацію. Важливою частиною забезпечення безпеки є правильна інтеграція цих систем для створення єдиного захисного середовища.

Основні методи захисту даних які використовують на підприємстві можна розділити на такі категорії:

1. Фізичний захист

Передбачає заходи, які запобігають несанкціонованому доступу до серверів, комп’ютерів та інших носіїв інформації:

Контроль доступу та використання систем контроль (СКД Система Контролю Доступа)

Система контролю доступу (СКД) - це сукупність технічних і програмних засобів, призначених для обмеження і контролю доступу до приміщень, зон, інформації або інших ресурсів. Вона використовується для забезпечення безпеки, ідентифікації осіб і реєстрації їхнього доступу. Основними елементами СКД є електронні замки, картки доступу, біометричні датчики, камери спостереження, а також програмне забезпечення для управління доступом і моніторингу [1,2].

Електронні замки які керуються через картки доступу, або біометричні дані які внесені до бази;

Карткові системи доступу: Видаються спеціальні картки які використовуються для входу як на територію так і в приміщення;

Турнікети та шлагбауми задача яких контролювати фізичний доступ до території і приміщення. Оснащенні картковою системою для пропуску працівників.

Відеоспостреження, виконується завдяки камерам спостереження, включаючи інфрачервоні камери для нічного бачення, камери з функцією PTZ (поворот, нахил, масштабування) та відеореєстратори (DVR/NVR), забезпечують моніторинг важливих зон.

Записуючі пристрої зберігають відео для подальшого аналізу і можуть бути інтегровані з системами оповіщення для швидкого реагування на загрози.

Постійна охорона території та приміщення, виконується завдяки охоронцям які забезпечують контроль над територією, перевіряють автомобілі працівників, патрулюють територію та реагують на будь-які підозрілі активності.

Це дозволяє вчасно виявити і запобігти потенційним загрозам. Технічний захист включає використання апаратного та програмного захисту.

Шифрування даних завдяки використання алгоритмів шифрування для захисту даних під час зберігання та передачі. Наприклад шифрування файлів на дисках або використання протоколів SSL/TLS допомагає захисту даних через мережу.

Мережевий захист використовує систему виявлення та запобігання вторгнень (IDS/IPS) контролюють мережевий трафік, виявляють і блокують небезпечні дії, атаки та інші загрози. Вони можуть бути інтегровані з іншими системами для забезпечення комплексного захисту.

Антивірусне програмне забезпечення задача якого інсталяція та регулярне оновлення антивірусних програм для захисту від вірусів, прикладом таких антивірусних програм ESET NOD32 Antivirus, Malwarebytes [1].

Контроль доступу завдяки якому впроваджена система управління доступом (PBAC) вона дозволяє обмежити доступ до конфіденційних даних лише авторизованим користувачам.

2. Системи охоронної сигналізації:

Датчики рух які виявляють будь який рух на площі встановлення, в результаті чого активують сигналізацію;

Датчики відкриття дверей і вікон: Спрацьовують світлові покажчики на панелі у охорони при кожному їх відкритті;

Центральна панель сигналізації у якій інтегровані всі датчики та контроль взаємодії з охоронною службою.

У разі активації система передає сигнал на пульт охорони або на мобільні пристрої відповідальних осіб для оперативного реагування. Це може включати автоматичне викликання правоохоронних органів у разі серйозної загрози [3].

Така різнопланова система технічних засобів захисту підприємства від різних видів загроз, підтримує високий рівень безпеки як персоналу так і даних.

Всі ці засоби взаємодіють між собою, створюючи єдину інтегровану систему безпеки, як дозволяє запобігати різноманітні ситуації.

Сучасні технічні засоби охорони дозволяють підприємствам підтримувати високий рівень безпеки завдяки інтеграції фізичних, технічних та моніторингових систем.

Залежно від специфіки підприємства, ці системи можуть бути адаптовані для врахування особливих потреб і вимог.

Інтеграція фізичних засобів контролю доступу, відеоспостереження, шифрування даних та систем охоронної сигналізації створює єдине захисне

середовище, що забезпечує комплексний захист як фізичних активів, так і інформаційних ресурсів.

Важливою частиною інтеграції є постійний моніторинг і оновлення систем для забезпечення їхньої ефективності у відповідь на нові загрози.

Регулярний аудит і тестування систем безпеки допомагають виявляти слабкі місця і впроваджувати необхідні вдосконалення, що дозволяє підприємству зберігати високий рівень захисту у будь-яких умовах.

Список використаних джерел:

1. Савченко, О. О. Системи контролю доступу: технічні рішення та практика впровадження. Київ: Політехніка, 2020. 368 с.
2. Система контролю доступу (СКД) - URL: Wikipedia - Access Control
3. Ковальчук І.І. "Системи охоронної сигналізації та моніторинг на підприємствах" // Львів: ЛНУ ім. Івана Франка, 2020.

Шкурба Анастасія, здобувачка вищої освіти СВО «Бакалавр»,
спеціальність «Інформаційні системи та технології»
Науковий керівник: к.с.-г.н., доцент Протас Надія

РОЗРОБКА КОМПЛЕКСУ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ

Аналіз загроз та ризиків інформаційної безпеки на підприємствах є ключовим елементом для забезпечення стабільної та безпечної роботи інформаційних систем. З огляду на стрімкий розвиток технологій та підвищену кількість кібератак, необхідність у систематичному моніторингу та оцінці стану захисту інформації стає пріоритетом для будь-якої організації. Метою даного дослідження є проведення попереднього аналізу загроз інформаційної безпеки в межах IT-інфраструктури підприємства та оцінка ефективності існуючих заходів захисту, враховуючи обмежений доступ до критично важливих систем.

Перший етап аналізу полягав у дослідженні поточного стану захисту робочих станцій і мережевих компонентів, з якими здійснювалась безпосередня робота. Було перевірено налаштування антивірусного програмного забезпечення, зокрема ESET Endpoint Security, і виявлено, що на ряді комп'ютерів відсутні актуальні оновлення, що могло становити потенційну загрозу для безпеки системи. Наступним важливим аспектом став аналіз системи резервного копіювання даних, частина якої була перевірена. Встановлено, що процес резервного копіювання даних, реалізований за допомогою Veeam Backup & Replication, не завжди виконувався згідно з розкладом через періодичні відключення серверів, спричинені перебоями в електропостачанні. Це могло підвищувати ризик втрати даних у разі аварійної ситуації, що підкреслює важливість резервних джерел живлення і регулярної перевірки налаштувань системи резервного копіювання. Додатково було виявлено потенційні загрози через неналежне управління доступом до

корпоративних ресурсів. У процесі аналізу з'ясувалося, що частина користувачів мала доступ до даних і ресурсів, до яких їм не слід було мати доступу, через помилки в налаштуваннях Microsoft Active Directory. Хоча змінювати ці налаштування самостійно не дозволялося, акцентувалась необхідність регулярного перегляду і коригування прав доступу для запобігання можливим інцидентам, пов'язаним із безпекою.

Після проведення аналізу загроз і ризиків наступним ключовим етапом стала розробка комплексного плану дій у випадку інцидентів інформаційної безпеки. Метою цього плану є не тільки підготовка до оперативного реагування на можливі атаки чи витоки даних, але й мінімізація їх негативних наслідків для підприємства. Першочергово розроблялися чіткі інструкції та процедури реагування, які визначають, що вважається інцидентом безпеки і які дії необхідно вжити у разі його виникнення. Наприклад, при виявленні таких загроз, як програми-вимагачі або зловмисне програмне забезпечення, важливо мати детальні покрокові інструкції для ізоляції заражених систем, оцінки масштабу загрози та інформування відповідальних осіб. Другим важливим аспектом стала чітка ідентифікація відповідальних осіб та розподіл ролей у разі виникнення інциденту. Формування команди реагування є критичним кроком: до її складу можуть входити спеціалісти з інформаційної безпеки, системні адміністратори та представники керівництва. Кожен член команди повинен чітко розуміти свою роль. Наприклад, одна особа може відповідати за технічне усунення проблеми, інша – за комунікацію з постраждалими сторонами або зовнішніми організаціями. Крім того, важливим є документування всіх дій під час реагування, що дозволить не лише відслідковувати хід інциденту, а й використовувати ці дані для покращення процедур і навчання персоналу. Всі виявлені вразливості мають бути зафіксовані для подальшого вдосконалення плану. Наприклад, можна розглянути гіпотетичний сценарій витоку конфіденційної інформації через шкідливе ПЗ, отримане в результаті фішинг-атаки. У такій ситуації план дій передбачає першочергове підтвердження факту зараження за допомогою антивірусного моніторингу, такого як ESET Endpoint Security. Після підтвердження активності зловмисного програмного забезпечення, інфіковані системи ізолюються від мережі для запобігання його поширенню. Далі проводиться детальний аналіз масштабів інциденту та оцінка можливого компрометаційного ризику для критичних даних. Паралельно проінформуються відповідальні особи через внутрішні канали зв’язку, такі як електронна пошта або спеціалізовані платформи, а також керівництво підприємства для координації подальших дій та забезпечення необхідної підтримки.

Після визначення масштабу інциденту та його впливу на інформаційні системи підприємства, необхідно вжити заходів для відновлення роботи і захисту даних. Одним із першочергових завдань є перевірка і відновлення системи резервного копіювання за допомогою Veeam Backup & Replication. Це дозволить відновити втрачені або пошкоджені дані, при цьому необхідно перевірити резервні копії на наявність потенційного зараження, щоб уникнути

повторного інфікування після відновлення. Якщо інцидент вплинув на клієнтів чи партнерів підприємства, необхідно своєчасно повідомити їх про факт інциденту та заходи, що були вжиті для його усунення. Після повного вирішення проблеми важливо провести постінцидентний аналіз, щоб зрозуміти, що стало причиною порушення безпеки, як відбувався витік інформації і які заходи можна вжити для уникнення подібних ситуацій у майбутньому.

Для підвищення інформаційної безпеки підприємства рекомендується реалізувати низку організаційних заходів. План захисту, розроблений на основі практичного досвіду, включає впровадження політики інформаційної безпеки, яка охоплює всі аспекти захисту даних: від управління доступом до процедур реагування на інциденти. Важливо визначити відповідальних осіб за реалізацію політики та забезпечити їх підготовку. Політика має містити детальні інструкції щодо обробки конфіденційних даних, методів захисту від шкідливого програмного забезпечення та попередження фішинг-атак. Крім того, необхідно впровадити регулярні тренінги для всіх співробітників, які допоможуть розпізнавати фішинг-повідомлення, створювати надійні паролі та безпечно користуватися корпоративними ресурсами. Такі тренінги можуть бути організовані за допомогою платформ, як-от KnowBe4 чи Cofense, і адаптовані під специфіку підприємства. Управління доступом слід поліпшити шляхом впровадження двофакторної аутентифікації для критичних систем і даних, а також регулярного перегляду прав доступу, щоб забезпечити доступ до конфіденційної інформації лише уповноваженим особам. Для забезпечення безпеки даних слід запровадити регулярне резервне копіювання, зберігаючи копії у захищених хмарних сховищах, таких як Google Cloud Storage або AWS S3, з можливістю швидкого відновлення. Процеси резервного копіювання мають постійно тестуватися для перевірки їх надійності.

Розробка та впровадження плану реагування на інциденти стане основою для швидкого і ефективного розв'язання проблем безпеки. Він має включати покрокові інструкції для аналізу інцидентів, відновлення роботи систем і належної комунікації як із внутрішніми відділами, так і з партнерами підприємства. Інтеграція зазначених заходів у загальну стратегію інформаційної безпеки підвищить стійкість підприємства до потенційних загроз, забезпечивши надійний захист корпоративних даних та безперервність бізнес-процесів у разі інцидентів.

Список використаних джерел:

1. Top 5 Methods of Protecting Data. URL: https://www.titanfile.com/blog/5-methods-of-protecting-data/ .
2. Veeam Backup & Replication Overview. URL: https://www.veeam.com/backup-replication.html
3. KnowBe4 Security Awareness Training. URL: https://www.knowbe4.com/security-awareness-training/ .

4. Microsoft Active Directory: Overview. URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services
5. ESET Endpoint Security for Business. URL: https://www.eset.com/us/business/endpoint-security/
6. AWS S3 Cloud Storage Overview. URL: https://aws.amazon.com/s3/
7. Cofense Phishing Defense. URL: https://cofense.com/phishing-defense/
8. Google Cloud Storage Features. URL: https://cloud.google.com/storage

Бойко Євгеній, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: д.т.н., професор Поночовний Юрій

ОСОБЛИВОСТІ ДІАГНОСТИКИ ТА УСУНЕННЯ НЕСПРАВНОСТЕЙ У СМАРТФОНАХ

Дослідження у напрямку діагностики та усунення несправностей у смартфонах є актуальними в сучасних умовах, оскільки смартфони стали невід'ємною частиною нашого життя. Люди постійно використовують їх для комунікації, роботи, розваг та інших щоденних завдань. Зважаючи на таку популярність, збільшення кількості користувачів смартфонів зумовлює й зростання кількості технічних проблем, які виникають у процесі експлуатації. Сучасні смартфони є складними електронними пристроями з багатьма компонентами, включаючи процесори, екрани, камери, модулі зв'язку та акумулятори. Тому діагностика та усунення несправностей, пов'язаних з їхньою роботою, потребують детальних знань та спеціальних навичок.

Технічний прогрес призводить до того, що смартфони стають дедалі складнішими, інтегруючи нові функції й можливості. Це, у свою чергу, робить процес ремонту більш складним, оскільки фахівці повинні мати справу з новими технологіями та системами. Крім того, ускладнення конструкції та інтеграція все більшої кількості функцій у смартфони роблять самостійний ремонт практично неможливим для пересічного користувача. Професійні сервіси, які займаються ремонтом смартфонів, часто стикаються з новими викликами, пов'язаними з діагностикою та усуненням несправностей.

Враховуючи, що вартість смартфонів постійно зростає, а багато користувачів не можуть собі дозволити часту зміну пристроїв, зростає попит на якісний ремонт. Усунення несправностей стає більш економічно доцільним вибором для багатьох користувачів, що підвищує значення розуміння технологій діагностики й ефективних методів ремонту.

Діагностика смартфонів – це перший та найважливіший етап усунення несправностей. Основна мета діагностики – виявити, в чому полягає проблема, і визначити, чи пов'язана вона з апаратними компонентами пристрою або з програмним забезпеченням [1]. Апаратні проблеми можуть включати несправності екрану, акумулятора, камер, мікрофона, динаміків, модулів зв’язку (Wi-Fi, Bluetooth) або системних плат. Програмні несправності часто

пов'язані з зависанням операційної системи, збоями у встановлених додатках, вірусами або пошкодженими файлами.

Процес діагностики включає кілька етапів:

1. Візуальний огляд для перевірки зовнішніх пошкоджень, таких як тріщини на екрані, деформації корпусу або пошкодження портів.

2. Використання спеціального програмного забезпечення для тестування функцій смартфона: перевірки стану акумулятора, діагностики сенсорних панелей, камер, мікрофона та динаміків.

3. Апаратне тестування за допомогою мультиметрів або спеціальних тестерів для визначення електричних проблем у системній платі або шлейфах.

Особливості діагностики апаратних несправностей залежать від конструкції смартфона. У сучасних пристроях компоненти дуже компактні, часто інтегровані в одну плату, що ускладнює ремонт. Наприклад, при пошкодженні екрана зазвичай потрібно замінити цілий модуль, який включає скло, сенсор та дисплей. Або при несправності акумулятора важливо враховувати, що більшість сучасних смартфонів мають нерозбірні корпуси, і для заміни батареї потрібно розбирати пристрій спеціальним інструментом [2].

Програмні несправності часто вимагають перепрошивки смартфона або скидання налаштувань до заводських. Якщо проблеми виникають через віруси або збій у системних файлах, то вирішити їх можна за допомогою спеціальних інструментів для відновлення операційної системи, таких як завантаження офіційних прошивок або відновлення через комп'ютер.

Усунення апаратних несправностей вимагає наявності спеціальних знань та інструментів. Наприклад, для заміни дисплея або акумулятора необхідно мати набір викруток, пінцетів, присосок, іонізуючі паяльники та інші інструменти для роботи з мікросхемами. Заміна пошкоджених деталей вимагає обережності, оскільки внутрішні компоненти дуже мініатюрні і тендітні.

Крім фізичного ремонту, важливою складовою є правильне складання пристрою після ремонту. Часто після заміни екрана або акумулятора можуть виникнути проблеми з герметичністю корпусу, що впливає на захист від вологи та пилу.

Програмне забезпечення також може вимагати складних операцій для відновлення його нормальної роботи. Якщо смартфон перестає коректно працювати через системні збої, такі як проблеми з оновленнями, пошкодження системних файлів або віруси, необхідно використовувати спеціальні програми для перепрошивки або повного скидання налаштувань. У деяких випадках може бути корисно виконати "чисте" встановлення операційної системи або звернутися до розробників програмного забезпечення для отримання допомоги.

Дана тема є важливою, оскільки смартфони стали дуже важливою частиною сучасного суспільства. Розуміння методів діагностики та процесів ремонту дозволяє не лише збільшити термін служби пристроїв, але й забезпечити безперебійну роботу важливих цифрових сервісів та комунікацій.

Дослідження особливостей діагностики та усунення несправностей у смартфонах виявляє важливість ретельного аналізу як апаратних, так і

програмних компонентів. Процес діагностики вимагає комплексного підходу, починаючи з візуальної перевірки стану пристрою і закінчуючи використанням спеціального програмного забезпечення для тестування його функцій. Проблеми з апаратними компонентами часто потребують заміни цілих модулів через інтегровану структуру сучасних смартфонів, а пошкодження програмного забезпечення потребує використання інструментів для відновлення операційної системи.

Усунення несправностей передбачає не лише професійні знання, але й спеціалізовані інструменти, адже ремонт смартфонів вимагає делікатної роботи з дрібними і складними компонентами. Важливим фактором також є правильне складання пристрою після ремонту, що впливає на його довговічність і стійкість до зовнішніх впливів.

Таким чином, успішна діагностика та ремонт смартфонів сприяють продовженню їхнього терміну служби і забезпечують користувачам надійну роботу пристроїв у повсякденному житті.

Список використаних джерел:

1. Петров В.В. Діагностика та ремонт мобільних пристроїв: методи та інструменти. К.: Техніка, 2021. 320 с.

2. Смирнов А.С. Сучасні підходи до усунення несправностей смартфонів / Електроніка та обслуговування. 2023. №5. С. 45-52.

Вовнянко Іван, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: д.т.н., професор Поночовний Юрій

ДОСЛІДЖЕННЯ ВПЛИВУ ТЕМПЕРАТУРНИХ КОЛИВАНЬ НА ЕЛЕКТРОННІ КОМПОНЕНТИ ТАКТИЧНИХ НАВУШНИКІВ

Вплив температурних коливань на електронні компоненти є важливою і актуальною проблемою для сучасних електронних пристроїв, включаючи тактичні навушники. Сучасні технології використовуються в різних умовах експлуатації, що включає екстремальні температури, як в умовах високих, так і низьких температур. Це особливо важливо для тактичних навушників, які застосовуються в умовах військових операцій, спортивних заходів на відкритому повітрі та інших середовищах, де температурні умови можуть варіюватися.

Температурні коливання можуть суттєво вплинути на функціональність і довговічність електронних компонентів сучасних пристроїв, таких як тактичні навушники. Тактичні навушники, включаючи моделі як Sordin Supreme Pro X, використовуються в умовах, де температура може варіюватися від екстремально низьких до високих значень.

Ці навушники часто застосовуються в військових операціях, спортивних заходах на відкритому повітрі та інших середовищах, де важливо забезпечити їх надійність в умовах змінних температур [1]. Низькі температури можуть

викликати конденсацію вологи, яка впливає на електричні з'єднання та може привести до короткого замикання або корозії.
Зниження температури може також уповільнити роботу електронних компонентів або зробити їх менш чутливими до фізичних пошкоджень.

Дослідження впливу температури на електронні компоненти тактичних навушників є критично важливим. Це дослідження допоможе в [2]:

– оцінці впливу температури на продуктивність навушників: аналіз того, як різні температури впливають на функціональність навушників, допоможе виявити потенційні проблеми і забезпечити оптимальні умови для їхньої роботи;

– розробці рекомендацій для користувачів: надання порад для користувачів про те, як правильно використовувати навушники в умовах змінних температур, щоб забезпечити їх тривалу експлуатацію;

– покращенні конструкції і матеріалів: результати дослідження можуть допомогти в розробці більш стійких до температурних коливань компонентів і конструкцій, що підвищить надійність продукту.

Для вивчення впливу температурних коливань на електронні компоненти можуть бути використані різні методи:

– лабораторні випробування: тестування компонентів навушників при різних температурних режимах для оцінки їхньої продуктивності і надійності;

– моделювання: використання комп'ютерних моделей для симуляції впливу температури на електронні компоненти, що дозволяє прогнозувати їхню поведінку в різних умовах;

– аналіз матеріалів: оцінка матеріалів, з яких виготовлені компоненти, для визначення їхньої стійкості до температурних коливань і їхнього впливу на загальну надійність навушників.

Це дослідження має потенціал значно покращити якість та надійність тактичних навушників, забезпечуючи їхню ефективну експлуатацію в екстремальних умовах.

Розуміння того, як різні температури впливають на навушники, дозволяє не лише виявити потенційні проблеми, але й розробити рекомендації для користувачів, які допоможуть забезпечити тривалу експлуатацію пристроїв у різних умовах. Також результати дослідження можуть бути використані для вдосконалення конструкції і вибору матеріалів, щоб підвищити стійкість навушників до температурних змін. Лабораторні випробування, комп'ютерне моделювання та аналіз матеріалів мають цінну інформацію для покращення якості та надійності тактичних навушників, що є важливим для їх ефективного використання в екстремальних умовах.

Список використаних джерел:

1. Electronics Tutorials (ресурси та інформацію про електроніку, включаючи аспекти впливу температури на електронні компоненти). URL: www.electronics-tutorials.ws;

2. IEEE Spectrum (новітні дослідження та інновації в області електроніки, включаючи вплив температури на компоненти). URL: www.spectrum.ieee.org;
3. EDN Network (статті та дослідження про електронні компоненти та їх поведінку при різних умовах, включаючи температурні коливання). URL: www.edn.com.

Матюшко Денис, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: д.т.н., професор Поночовний Юрій

МЕТОДИ ТЕСТУВАННЯ І ДІАГНОСТИКИ ФУНКЦІОНАЛЬНИХ ВУЗЛІВ СМАРТФОНА

Смартфони стали важливою частиною нашого повсякденного життя, і їхній ринок швидко розвивається. З новими моделями та технологіями, що з'являються постійно, необхідність у ефективних методах тестування та діагностики функціональних вузлів смартфонів стає все більш актуальною. Важливість теми обумовлена кількома факторами:

1. Зростання складності технічних компонентів: сучасні смартфони мають все більше складних компонентів, таких як процесори з кількома ядрами, складні дисплеї з високою роздільною здатністю, камери з багатьма датчиками тощо. Це робить діагностику і ремонт більш складними і вимагає спеціалізованих методів тестування для точного визначення причин несправностей;
2. Збільшення вартості ремонту: оскільки сучасні смартфони використовують дорогі компоненти і технології, точна діагностика є критично важливою для уникнення непотрібних витрат на ремонт або заміну частин. Неправильна діагностика може призвести до додаткових витрат і втрати часу.
3. Потреба в швидкому обслуговуванні: в умовах конкурентного ринку споживачі очікують швидкого і якісного обслуговування. Ефективні методи тестування і діагностики дозволяють технікам швидше виявляти і усувати проблеми, що сприяє зменшенню часу ремонту і підвищенню задоволеності клієнтів;
4. Еволюція програмного забезпечення: оновлення програмного забезпечення смартфонів можуть впливати на роботу функціональних вузлів. Це створює потребу в розробці і впровадженні нових методів тестування для забезпечення сумісності та належної роботи після оновлень;
5. Зростання кількості самостійних користувачів: з ростом доступності інформації та інструкцій користувачі все частіше намагаються самостійно вирішувати проблеми з їхніми пристроями.

Дослідження методів тестування і діагностики функціональних вузлів смартфонів є важливим для підвищення ефективності обслуговування і ремонту. Розробка нових і вдосконалення існуючих методів допоможе забезпечити швидке і точне визначення причин несправностей, що в свою чергу підвищить якість обслуговування і задоволеність споживачів.

З огляду на швидкий розвиток технологій і постійні інновації в сфері мобільних пристроїв, ця тема залишається надзвичайно актуальною і важливою для фахівців у галузі ремонту та обслуговування смартфонів.

Смартфони сьогодні є складними багатофункціональними пристроями, що об'єднують різноманітні технології і компоненти в одному компактному корпусі. Технічна складність сучасних смартфонів вимагає ефективних методів тестування та діагностики для забезпечення їх належної роботи. У цьому контексті важливо розглянути основні методи тестування і діагностики функціональних вузлів смартфона, їх переваги та обмеження, а також практичне застосування.

Тестування та діагностика смартфонів охоплюють визначення працездатності та функціонування ключових компонентів, таких як процесор, дисплей, акумулятор, камери і комунікаційні модулі. Апаратне тестування включає фізичну перевірку компонентів на наявність фізичних ушкоджень і тріщин, а також вимірювання параметрів з використанням спеціалізованих інструментів, таких як мультиметри і осцилографи. Програмне тестування використовує діагностичні програми для оцінки продуктивності різних модулів, включаючи стрес-тести і перевірки швидкості, а також може включати оновлення прошивки для усунення програмних проблем. Інтерактивне тестування перевіряє функціональність пристрою в реальному часі, тестуючи камери, сенсорний екран, кнопки та порти, а також моделює різні умови, такі як температура і вологість, для виявлення можливих проблем [1].

Методи тестування і діагностики мають свої переваги та обмеження. Сучасні програмні методи забезпечують швидке виявлення проблем без необхідності візуальної перевірки або розбирання пристрою, а апаратні інструменти гарантують точність вимірювань. Комбінація апаратних і програмних методів дозволяє отримати всебічну картину стану пристрою. Проте вартість спеціалізованих інструментів може бути високою, що створює проблеми для невеликих ремонтних майстерень, а також точне тестування і діагностика вимагають певних знань і навичок, що може бути складно для новачків.

Практичне застосування цих методів в сервісних центрах і при самостійних ремонтах користувачів допомагає швидко і точно визначати проблеми і забезпечувати якісний ремонт, підвищуючи загальну продуктивність і надійність смартфонів.

Методи тестування та діагностики функціональних вузлів смартфона відіграють критичну роль у забезпеченні їхньої ефективної роботи. Різноманітні методи, як апаратні, так і програмні, дозволяють точно виявляти і усувати проблеми, що виникають в пристроях [2]. Сучасні інструменти і діагностичні програми забезпечують швидкість і точність у перевірці компонентів, таких як процесори, дисплеї, акумулятори і комунікаційні модулі.

Разом з тим, важливо враховувати і деякі обмеження, такі як вартість спеціалізованого обладнання та необхідність спеціальних знань для

ефективного використання методів. В умовах швидкого розвитку технологій та зростання складності смартфонів, удосконалення методів тестування і діагностики є важливим для забезпечення високої якості обслуговування і ремонту.

Застосування розроблених методів у практичній діяльності допомагає не лише виявляти дефекти і несправності, але і забезпечувати швидкий та ефективний ремонт, що підвищує загальну продуктивність і надійність сучасних смартфонів.

Список використаних джерел:

1. Тестування та діагностика смартфонів. Вебсайт: URL: https://dialogue.techtoday.in.ua/testm/

2. Смирнов А.С. Сучасні підходи до усунення несправностей смартфонів. Електроніка та обслуговування. 2023. №5. С. 152.

Гавриленко Максим, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.ф.-м.н., доцент Флегантов Леонід

ІНТЕГРАЦІЯ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ СИСТЕМАМИ В УМОВАХ ГІБРИДНОЇ ІТ-ІНФРАСТРУКТУРИ

Гібридні ІТ-інфраструктури, що поєднують локальні і хмарні ресурси, дозволяють підприємствам бути більш гнучкими і ефективними. Однак інтеграція цих різних компонентів може бути складною і вимагати значних зусиль для забезпечення безперебійної роботи і безпеки. Зростаюча популярність хмарних рішень і зміни в ІТ-ландшафті роблять цю тему особливо актуальною.

Основні моделі хмарних послуг включають SaaS (Software as a Service), PaaS (Platform as a Service) і IaaS (Infrastructure as a Service). Кожна з цих моделей має свої переваги та обмеження. SaaS пропонує готові до використання програми, PaaS забезпечує платформи для розробки та розгортання додатків, а IaaS надає базову інфраструктуру, таку як віртуальні машини та системи зберігання даних. Хмара може забезпечити масштабованість, високу доступність та зниження витрат на апаратне забезпечення [1, с 34-37]. Проте, є й потенційні ризики, такі як проблеми з безпекою даних, зменшена контрольованість над системами та залежність від постачальника послуг, залежність від каналів зв’язку, а недостатньо спланована міграцій в хмару може підвищити витрати без підвищення продуктивності систем.

На практиці це включає налаштування інтеграційних рішень між локальними і хмарними системами, використання інструментів для моніторингу ресурсів і управління ними. Важливо також забезпечити високу доступність і відмовостійкість систем, а також реалізувати політики безпеки для захисту даних у гібридному середовищі.

Під гібридною хмарою прийнято називати таку модель побудови IT-інфраструктури, яка поєднує в собі приватні, публічні хмари та локальні датацентри [2]. При створенні такої інфраструктури слід чітко розуміти та враховувати багато чинників та ретельно планувати таку діяльність. У табл. 1 надано порівняння основних показників ефективності для локальної, хмарної та гібридної інфраструктур. Інтеграція та управління інформаційними системами в умовах гібридної IT-інфраструктури є складним, але важливим завданням. Успішне впровадження таких систем дозволяє підприємствам максимально ефективно використовувати доступні ресурси, знижувати витрати і забезпечувати високу доступність та безпеку даних. Проте для досягнення цих цілей необхідно враховувати численні технічні та організаційні аспекти, що потребують глибоких знань та практичних навичок у сфері IT-управління.

Гібридні інфраструктури ідеально підходять для компаній різного масштабу, від стартапів до великих корпорацій, завдяки їхній гнучкості та здатності вирішувати різноманітні завдання. Вони сприяють цифровій трансформації, дозволяючи компаніям поетапно впроваджувати нові IT-рішення, зберігаючи при цьому ключові системи в приватній інфраструктурі.

Таблиця 1 – Порівняння показників ефективності для різних інфраструктур

Показник	Опис	Локальна інфраструктура	Хмарна інфраструктура	Гібридна інфраструктура
Економія витрат на апаратне забезпечення	Зменшення витрат на фізичні сервери та обладнання	Високі витрати на обладнання	Відсутні витрати на обладнання	Часткова економія завдяки хмарі
Продуктивність	Використання ресурсів для забезпечення стабільної роботи	Висока, залежить від обладнання	Залежить від пропускної здатності інтернету	Оптимальна за рахунок балансування ресурсів
Безпека даних	Захист конфіденційних даних та систем від несанкціонованого доступу	Високий рівень за внутрішніми стандартами	Потребує спеціальних заходів безпеки	Потребує інтеграції політик безпеки для обох типів систем
Масштабованість	Можливість швидкого збільшення обчислювальних ресурсів	Обмежена потужностями обладнання	Висока, автоматична	Висока за рахунок хмарних компонентів
Доступність	Відсоток часу, протягом якого система доступна для користувачів	Висока, але залежить від технічного обслуговування	Висока, залежить від постачальника	Дуже висока завдяки резервуванню даних

Для підприємств, що працюють з конфіденційними даними, гібридні хмари дозволяють захищати чутливу інформацію в приватній хмарі, залишаючи решту даних у публічній. Крім того, гібридні хмари оптимальні для організації резервного копіювання, тестування нових проектів і швидкого масштабування ресурсів у пікові періоди. Вони також підвищують ефективність IoT-пристроїв, дозволяючи обробляти дані локально, а зберігати їх у публічних хмарах. Завдяки таким можливостям, гібридні хмари є універсальним рішенням для багатьох бізнес-задач.

Список використаних джерел:

1. Джордж Риз. Облачные вычисления / пер. с англ О. Кокорева . Санкт-Петербург: БХВ-Петербург, 2011, 281 стр. ISBN 978-5-9775-0630-4
2. Гібридна хмара: чим корисна для бізнесу та які задачі виконує.: веб-сайт. URL: https://hub.kyivstar.ua/articles/gibrydna-hmara-chym-korysna-dlya-biznesu-ta-yaki-zadachi-vykonuye