Міністерство освіти і науки України

Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)
напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)
спеціальність *Кібербезпека*
(код і назва спеціальності)
освітній рівень *магістр*
(назва освітнього рівня)
кваліфікація *Професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Дослідження методів захисту інформаційних ресурсів підприємства при використанні хмарних технологій***

Виконавець: студент 6 курсу, групи 125м-16-1

(підпис) **Журавель Владислав Костянтинович** (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	к.т.н., доц. Флоров С.В.		
розділів:			
спеціальний	к.т.н., доц. Флоров С.В.		
економічний	к.е.н., доц. Волотковская Ю.А.		
Рецензент			
Нормоконтроль	к.т.н., доц. Галушко О.М.		

Дніпро 2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій

д.т.н., проф_____Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра
спеціальності *Кібербезпека*
(код і назва спеціальності)

студенту 125м-16-1 Журавель Владислав Костянтинович
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***«Дослідження методів захисту інформаційних ресурсів підприємства при використанні хмарних технологій»***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від «____» _____ №_____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***Безпека інформації, що передається зберігається та оброблюється при використанні хмарних обчислень***

Предмет досліджень ***Методи забезпечення інформаційної безпеки при використанні хмарних сервісів***

Мета НДР ***Підвищення інформаційної безпеки підприємств що обробляють інформацію за допомогою хмарних технологій***

Вихідні дані для проведення роботи ***результати та матеріали з виробничої, переддипломної практики та курсового проекту з комплексних систем захисту інформації***

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна ***полягає в дослідженні методів забезпечення інформаційної безпеки на підприємствах, де використовуються сучасні хмарні сервіси***

Практична цінність ***полягає в протидії загрозам несанкціонованого доступу до інформації, що оброблюється за допомогою хмарних обчислень та при взаємодії локальної корпоративні мережі зі хмарою.***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати повинні відповідати вимогам Закону України «Про інформацію», Закону України «Про захист персональних даних», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», «Положення про технічний захист інформації в Україні», що затверджено указом Президента України від 27 вересня 1999 р. №1229/99, НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», «Про вищу освіту», Закону України «Про освіту», «Положення про організацію навчального процесу у вищих навчальних закладах», що затверджено наказом Міністерства освіти України від 2 червня 1993 р. №161, нормативних документів з технічного захисту інформації, державних стандартів України в галузі інформаційної безпеки та інших законів України, що стосуються забезпечення безпеки інформації.

Результати досліджень мають бути подані у вигляді, що дозволяє безпосереднє використання для створення засобів захисту інформації в системах хмарних обчислень.

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)

1 Провести аналіз основних властивостей хмарних технологій.	«11» вересня 2017 р.
2 Провести аналіз моделей обслуговування та розгортання хмарних технологій.	«22» жовтня 2017 р.
3 Дослідити методи забезпечення інформаційної безпеки при використанні хмарних сервісів служби на рівні провайдера та користувача.	«2» листопада 2017 р.
4 Побудувати модель загроз для підприємства, де використовують технологію хмарних обчислень.	«28» листопада 2017 р.
5 Розглянути функціональні послуги безпеки, що реалізують різні компоненти хмарної служби G Suite Enterprise.	«24» травня 2017 р.
6 Оформлення пояснювальної записки дипломної роботи	«10» січня 2018 р.

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***від реалізації результатів роботи очікується завдяки поліпшення бізнес процесів підприємства при одночасному підвищенні рівня захисту інформаційних активів.***

Соціальний ефект ***від реалізації результатів роботи очікується позитивним завдяки створенню умов для реалізації можливостей працівникам підприємства ,підвищити продуктивність праці та її комфортність***

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення «ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення» та «Методичні вказівки. Загальні вимоги до оформлення магістерських дипломних робіт і дипломних проектів спеціалістів для студентів галузей знань 1701 «Інформаційна безпека» та 0509 «Радіотехніка, радіоелектронні апарати та зв'язок»

Завдання видав _____ С.В. Флоров
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ В.К. Журавель
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ДЕК _____

РЕФЕРАТ

Пояснювальна записка: с., рис., табл., 4 додатка, джерела.

Об’єкт дослідження: безпека інформації, що передається, зберігається та оброблюється при використанні хмарних обчислень.

Мета роботи: підвищення інформаційної безпеки підприємств, що обробляють інформацію за допомогою хмарних та взаємодіє з нею

Методи дослідження: аналіз, синтез, дедукція, системний аналіз, структурний аналіз, методи порівняння та спостереження.

У спеціальній частині було досліджено методи забезпечення інформаційної безпеки при використанні хмарної служби G Suite Enterprise на рівні центру обробки даних та на рівні кінцевого користувача, побудована модель загроз для підприємства, де використовують технологію хмарних обчислень, обрані функціональні профілі захищеності від несанкціонованого доступу для захисту інформації, що реалізують різні компоненти хмарної служби G Suite Enterprise

У економічному розділі наведено порівняння витрат на впровадження хмарної служби G Suite Enterprise у порівнянні з аналогічною локальною інфраструктурою.

Практичне значення роботи полягає в дослідженні ефективності протидії загрозам несанкціонованого доступу до інформації, що оброблюється за допомогою хмарних обчислень та при взаємодії локальної корпоративні мережі зі хмарою

Наукова новизна роботи полягає в дослідженні методів забезпечення інформаційної безпеки на підприємствах, де використовуються сучасні хмарні сервіси

Напрямки подальших досліджень полягають у детальному аналізі існуючої нормативно-правової бази України і світу, стосовно застосування хмарних технологій на підприємствах різної форми власності.

Ключові слова: ХМАРНІ ОБЧИСЛЕННЯ, ХМАРНІ ТЕХНОЛОГІЙ, SAAS, IAAS, PAAS, G SUITE ENTERPRISE, ІНФОРМАЦІЙНА БЕЗПЕКА.

РЕФЕРАТ

Пояснительная записка: с., рис., табл., 4 приложения, 43 источников.

Объект исследования: безопасность передаваемой информации, хранимой и обрабатываемой при использовании облачных вычислений. Цель работы: повышение эффективности обеспечения информационной безопасности предприятий, обрабатывающих информацию с помощью службы G Suite Enterprise.

Методы исследования: анализ, синтез, дедукция, системный анализ, структурный анализ, методы сравнения и наблюдения.

В специальной части были исследованы методы обеспечения информационной безопасности при использовании облачной службы G Suite Enterprisena уровне центра обработки данных и на уровне конечного пользователя, составлена модель угроз для предприятия, где используют технологию облачных вычислений, избраны функциональные профили защищенности от несанкционированного доступа для защиты информации, которую реализуют различные компоненты облачной службы G Suite Enterprise. В экономическом разделе приведено сравнение расходов на внедрение облачной службы G Suite Enterprise по сравнению с аналогичной локальной инфраструктурой.

Практическое значение работы состоит в исследовании эффективности противодействия угрозам несанкционированного доступа к информации, обрабатываемой с помощью облачных вычислений и при взаимодействии локальной корпоративные сети с облаком. Научная новизна работы заключается в исследовании методов обеспечения информационной безопасности на предприятиях, где используются современные облачные сервисы. Направления дальнейших исследований заключаются в детальном анализе существующей нормативно-правовой базы Украины и мира, касательно применения облачных технологий на предприятиях различной формы собственности.Ключевые слова: ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ, ОБЛАЧНЫХ ТЕХНОЛОГИЙ, SAAS, IAAS, PAAS, G SUITE ENTERPRISEИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

ABSTRACT

Explanatory note: p., figures, tables, 4 supplements, 43 sources.

Object of research: the security of transmitted information is stored and processed when using cloud computing.

The purpose of the work: to increase the effectiveness of information security of enterprises that process information through cloud computing by G Suite Enterprise.

Methods of research: analysis, synthesis, deduction, system analysis, structural analysis, methods of comparison and observation.

In the special part, methods have been investigated to provide information security when using the G Suite Enterprisecloud service at the data center level and at the end user level, a model of threats for the enterprise using cloud computing, a functional security profile from unauthorized access to protect information, Which implement various components of the G Suite Enterprisecloud service

The economic section provides a comparison of the costs of implementing the G Suite Enterprisecloud service over a local infrastructure that is an analogue of G Suite Enterprise.

The practical significance of the work is to investigate the effectiveness of countering threats to unauthorized access to information processed using cloud computing and when local corporate networks interact with the cloud.

The scientific novelty of the work is to research methods for providing information security in enterprises where modern cloud services are used

The directions of further research consist in a detailed analysis of the existing legal and regulatory framework of Ukraine and the world regarding the application of cloud technologies at enterprises of different forms of ownership.

Key words: CLOUD COMPUTING, CLOUD, SAAS, IAAS, PAAS, G SUITE ENTERPRISE, INFORMATION SECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

SAAS – програмне забезпечення як сервіс
PAAS – програмне забезпечення як сервіс
IAAS – програмне забезпечення як сервіс
КС – комп'ютерна система
ЛОМ – локальна обчислювальна мережа
МК – мобільні користувачі
МП – мобільні пристрої
НД ТЗІ – нормативний документ технічного захисту інформації
ОС – операційна система
ПБ – політика безпеки
ПК – персональний комп'ютер
ПЗ – програмне забезпечення
ПЕОМ – персональна електронно-обчислювальна машина
РС – робоча станція
AVAPI – Antivirus Application Programming Interface
CA – Certificate Authority
PKI – Public Key Infrastructure
SMS – System Management Server
SP – Service Pack
SUS –Software Update Services
TLS – Transport Layer Security
UPN – User Principal Name

ЗМІСТ

ВСТУП

Розвиток глобальної мережі Інтернет та всеохоплююче її використання у різних сферах життя та комерційної діяльності людей призводить до збільшення обсягів інформації, що циркулює та оброблюється.

Хмарні технології створюють базу в інфраструктурі нового покоління, яка дозволяє створити потужну інформаційно-телекомунікаційну систему з новою архітектурою та можливостями. Доволі великий відсоток коштів підприємства та організації використовують на експлуатацію та технічне обслуговування локальних інформаційних систем, хмарні технології дозволяють пришвидшити процес розробки та випуску програмних продуктів на ринок та збільшити ефективності праці підприємства шляхом організації прозорого документообігу та спільної праці над проектами.

Швидке зростання хмарних технологій надає величезний потенціал для підвищення ефективності функціонування інформаційної системи, скорочення витрат на її обслуговування, технічне забезпечення та швидке розгортання філіалів для підприємств різної форми власності. Основними особливостями хмарних технологій є можливість масштабування інфраструктури для зберігання даних та динамічне керування потужностями, що звільнить користувача від управління складною технологією.

Використання хмарних технологій має широкий спектр переваг, однак досі залишається відкритим процес формування нормативно-правової платформи врегулювання взаємодії постачальника послуг та користувача.

Метою дипломної роботи є підвищення ефективності забезпечення інформаційної безпеки підприємств, що обробляють інформацію за допомогою хмарних обчислень службою G Suite Enterprise.

Для досягнення зазначеної мети дипломної роботи поставлені окремі завдання:

– провести аналіз основних властивостей хмарних технологій;

– провести аналіз моделей обслуговування та розгортання хмарних технологій;

– сформувати висновки щодо переваг і недоліків кожної моделі обслуговування хмарних технологій;

– дослідити методи забезпечення інформаційної безпеки при використанні хмарної служби G Suite Enterprisена рівні центру обробки даних та на рівні користувача;

– побудувати модель загроз для підприємства, де використовують технологію хмарних обчислень.

РОЗДІЛ 1.
ОСОБЛИВОСТІ ХМАРНИХ ТЕХНОЛОГІЙ
1.1 Побудова хмарних обчислень

Хмарні обчислення передбачають зручний доступ до загального пулу сконфігурованих обчислювальних ресурсів, таких як мережі передачі даних, сервери, пристрої зберігання даних, додатки та сервіси, що можуть бути швидко надані і звільнені за мінімальних експлуатаційних витрат та взаємодії з постачальником цих послуг [1].

Хмарні обчислення – це нова парадигма, що припускає розподілену і видалену обробку і зберігання даних. Хмара – це не що інше, як великий центр обробки даних (ЦОД) або мережа взаємопов'язаних між собою серверів.

Самі розробники хмарних технологій визначають їх як інноваційну технологію, яка надає динамічно масштабовані обчислювальні ресурси і програми через інтернет в якості сервісу під керуванням постачальника послуг.

На сьогодні великі обчислювальні хмари будуються з тисяч серверів, розміщених у центрах обробки даних та забезпечують обчислювальними ресурсами десятки тисяч додатків, якими одночасно користуються мільйони користувачів по всьому світу. Хмарні технології стали зручним інструментом для підприємств, яким дорого утримувати власні сервери планування ресурсів підприємства, системи управління взаємовідносинами з клієнтами або інші сервери, що вимагають придбання і налаштування додаткового обладнання.

Зростаюча популярність хмарних технологій пояснюється їх можливістю застосування для вирішення великого спектру завдань і дозволяють економити на обслуговуванні, персоналі та інфраструктурі. Хмарний технології дозволяють стандартизувати програмне забезпечення та використовувати його на комп’ютерах підприємства, навіть якщо на них встановлено різні операційні системи, а для співробітників підприємства, що перебувають поза офісом, значно спрощують доступ до даних компанії.

Хмарні обчислення, у сучасному розумінні з'явилися відносно недавно, але слід зауважити, що їх історичним прообразом є технологія розподілених обчислень. Розподілені обчислення дозволяють вирішити трудомісткі обчислювальні завдання, використовуючи множину комп'ютерів об'єднаних у паралельну обчислювальну систему. Їх сутність полягає у тому, що для вирішення ресурсномісткої задачі використовуються потужності декількох персональних комп'ютерів. Такий відхід було вперше використаний у 1973 році Джоном Шохом та Джоном Хаппом з каліфорнійського науково-дослідного центру Xerox PARC, що написали програму, яка вночі запускалася у локальну мережу і змушувала працюючи комп'ютери виконувати певні обчислення. Ще одним відомим проектом, що використовує розподілені обчислення є SETI@home, метою якого був пошук позаземного розумного життя шляхом аналізу даних з радіотелескопів [4].

Хмарні обчислення визначаються Національним інститутом стандартів і технології США (NIST) як «модель для зручного, на вимогу, мережевого доступу до загального сховища даних з налаштованим обчислювальними ресурсами (наприклад, до мереж, серверів, систем зберігання, додатків і послуг), який може бути здійснений швидко, при мінімальній необхідності в управлінні і взаємодії з постачальником послуг » [1].

Завдяки консолідації ресурсів з боку постачальника хмарних технологій і мінливому характеру звернень з боку споживачів, хмарні обчислення дозволяють економити використовуючи менші апаратні ресурси, ніж у ситуації, коли б було потрібно виділити відповідні апаратні потужності для кожного споживача, а за рахунок автоматизації процедур виділення ресурсів істотно знижуються витрати на абонентське обслуговування.

Кінцевому споживачу, використання хмарних технологій дозволяють отримати послуги з високим рівнем доступності ресурсів та низькими ризиками непрацездатності, забезпечує можливість швидкого масштабування обчислювальної системи завдяки відсутності необхідності створення, обслуговування і модернізації власної апаратної інфраструктури.

Добавлено примечание ([V1]): http://www.popmech.ru/technologies/9137-s-miru-po-nitke-superkompyuter/

Добавлено примечание ([V2]): Що за маячня?

Добавлено примечание ([V3]): Технологій чи Обчислень?????

Універсальність доступу забезпечується широкою доступністю послуг і підтримкою безлічі термінальних пристроїв: персональних комп'ютерів, мобільних телефонів, смартфонів, інтернет-планшетів тощо.

1.2 Які технології можна назвати хмарними

Національним інститутом стандартів і технологій США було виділено п'ять основних принципів побудови хмарної моделі [1]:

– самообслуговування за вимогою. Споживач самостійно визначає і змінює у односторонньому порядку потребу у обчислювальних ресурсах та їх параметри, наприклад: серверний час, швидкість доступу та обробки даних, обсяг збережених даних без безпосередньої взаємодії з представником постачальника послуг хмарних технологій;

– універсальність доступу. Послуги хмарних обчислень мають бути доступні споживачам незалежно від термінального пристрою, що використовуються;

– об'єднання ресурсів. Постачальник послуг поєднує ресурси для обслуговування великої множини споживачів в єдиний пул для динамічного перерозподілу обчислювальних потужностей між ними в умовах швидкоплинних змін попиту на обчислювальні потужності. При цьому споживачі контролюють лише основні параметри наданих послуг (обсяг даних, швидкість доступу), але фактичний розподіл ресурсів, що надаються споживачеві, здійснює постачальник (в окремих випадках споживач може безпосередньо керувати деякими фізичними параметрами перерозподілу, наприклад обирати бажаний центр обробки даних з міркувань географічного розташування);

– еластичність масштабування. Послуги можуть бути надані, розширені і звільнені у автоматичному режимі в будь-який момент, без витрат часу та ресурсів на взаємодію з представником постачальника послуг хмарних технологій;

Добавлено примечание ([V4]): Коректність перекладу: «On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.»

– облік споживання. Постачальник послуг автоматично обчислює спожиті обчислювальні ресурси на певному рівні абстракції: обсяг збережених даних, пропускна здатність, кількість користувачів, кількість транзакцій тощо і на основі цих даних оцінює обсяг наданих споживачам послуг.

1.2.1 Універсальність доступу

Хмарні обчислення відокремлюють обчислювальні ресурси від споживачів, тому їм не потрібно самостійно їх підтримувати та обслуговувати. Наслідком цього є необхідність доступу за допомогою мережі інтернет до територіально розподілених центрів обробки інформації [6].

Добавлено примечание ([V5]): https://remonsinnema.com/cloud-2/cloud-computing/broad-network-access/

(2)

У загальному випадку, комп'ютерна мережа являє собою сукупність двох або більше комп'ютерів, з'єднаних один з одним з метою обміну інформацією. Міжнародним комітетом зі стандартизації (ISO) та міжнародною організацією із стандартизації у сфері електричних, електронних і суміжних технологій (IEC) визначили базову модель взаємодії відкритих систем – OSI, яка складається з наступних 7 рівнів :

1) фізичний рівень;
2) канальний рівень;
3) мережевий рівень;
4) транспортний рівень;
5) сеансовий рівень;
6) рівень відображення;
7) прикладний рівень.

Найнижчий рівень моделі – фізичний, призначений безпосередньо для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів у кабель і відповідно їхній прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів. На цьому рівні визначені електричні, процедурні і функціональні специфікації для середовища передачі даних, в тому числі роз'єми і призначення контактів, рівні напруги, синхронізацію зміни напруги, кодування сигналу. В сучасних мережах використовуються три

основні типи середовища передачі: мідний кабель, оптичне волокно та бездротове середовище передачі.

В залежності від типу середовища передачі, тип сигналу, за допомогою якого здійснюється передача даних є різним. Так, для мідного кабелю, біти даних представляють собою електричні імпульси, для оптичного кабелю – світлові імпульси, а у разі використання бездротових з'єднань сигнали є електромагнітними хвилями.

Канальний рівень пов’язаний з локальною доставкою кадрів між пристроями в одній і тій же локальній мережі. Дані, що були отримані з фізичного рівня, упаковуються у кадри даних, перевіряються на цілісність, за необхідності виправляються наявні помилки, та відправляються на мережевий рівень

Мережевий рівень відповідає за встановлення з’єднання та маршрутизацію пакетів даних від джерела до вузла призначення через одну або більше мереж, шляхом адресації хостів з використанням протоколу IP.

Транспортний рівень надає послуги передачі без помилок, втрат і дублювання в тій послідовності, у який вони були передані. Цей рівень визначає механізм передачі й не має значення звідки й куди та які саме дані передаються.

Сеансовий рівень забезпечує механізми для відкриття, закриття, управління сеансом, обміну інформацією та синхронізацією завдань. Сеанс складається з запитів і відповідей, що з’являються між взаємодіючими додатками.

Рівень відображення відповідає за кодування і декодування даних, перетворення протоколів та стиснення і розпакування даних. Отримані з прикладного рівня запити додатків, він перетворює у формат для передачі у мережі й відповідно отримані з мережі дані у формат, зрозумілий додаткам.

Прикладний рівень забезпечує взаємодію користувача і мережі, дозволяє додаткам користувача доступ до мережевих служб, відповідає за передачу службової інформації та надає додаткам інформацію про помилки.

Більшість додатків, що призначені для обміну даними по мережі використовують протокол передачі гіпертекстових документів (HTTP), але деякі додатки додатково використовують інші протоколи поверх протоколу HTTP для формування веб-служб. Консорціум Всесвітньої павутини (W3C) визначає веб-службу як програмну систему, що застосовується для підтримки взаємодії типу машина-машина. Можна вирізнити два основні класи веб-служб: ті, що засновані на SOAP [8] – протоколі обміну структурованими повідомленнями в розподілених обчислювальних системах, та ті, що засновані на REST [9] – особливому підході до архітектури мережевих протоколів, який забезпечує доступ до інформаційних ресурсів.

Добавлено примечание ([V6]): https://uk.wikipedia.org/wiki/SOAP

Простий протокол доступу до об’єктів (SOAP) заснований на форматі XML у якості формату повідомлень та зазвичай використовує протокол HTTP для передачі повідомлень. SOAP утворює основу цілого набору специфікацій, що зазвичай називають стеком WS-*. Мова опису веб-сервісів (WSDL) та інструментарій для опису веб-сервісів (UDDI) дозволяють відкривати веб-служби, що пропонують певну послугу використовуючи реєстр UDDI, а потім зв’язатися з ним за допомогою WSDL, без попереднього ознайомлення з прикладним програмним інтерфейсом (API) замовника. Через складність стеку WS-*, SOAP додає велику кількість накладних витрат, тому спостерігається тенденція переходу до більш простих реалізацій.

Використання архітектурного стилю REST дозволяє враховувати масштабованість веб-служби та використовує тільки HTTP-методи, що значно спрощує інтерфейс та дозволяє використовувати одночасно XML та JavaScript Object Notation (JSON) у якості формату повідомлень. Стосовно хмарних технологій, спостерігається поступове зменшення популярності SOAP на користь REST.

1.2.2 Самообслуговування за вимогою

Хмарні обчислення надають ресурси на вимогу, тобто, коли вони потрібні споживачу. Це стає можливим завдяки самообслуговуванню і автоматизації, споживач сам виконує всі дії, необхідні для модернізації наданих йому послуг, замість того, щоб звертатися до постачальника послуг або IT-відділу своєї компанії. Запит споживача автоматично обробляється хмарною інфраструктурою, без втручання посередників [5].

Для реалізації самообслуговування, постачальник повинен мати інфраструктуру для автоматичних запитів споживачів. Зазвичай, ця інфраструктура має віртуальний характер, що дозволяє різним споживачам використовувати одне й теж апаратне забезпечення.

Автоматизація самообслуговування вимагає від постачальника хмарних послуг високого рівня планування. Так, споживач може запросити нову віртуальну машину у будь-який час, та очікує, що вона запрацює за кілька хвилин, але постачальнику хмарних послуг може знадобитися значно більший проміжок часу для отримання фізичного обладнання для центру обробки даних. Тому необхідно постійно стежити за тенденціями використання обчислювальних ресурсів та своєчасно планувати оновлення та модернізацію обладнання.

Постачальник хмарних технологій не може вимагати спеціалізованих знань від споживача, бо у традиційній IT-структурі компанії, відповідні спеціалісти заздалегідь прогнозують очікуваний рівень навантаження на обчислювальні ресурси підприємства. Але для споживача хмарних послуг таке прогнозування є неприйнятним. Відповідно, кінцевий користувач хмарного сервісу не має піклуватися про розподіл навантаження та інші технічні параметри. Замість цього, постачальник хмарних обчислень має надати зрозумілий інтерфейс користувача за замовчанням, а при необхідності забезпечити доступ для IT-фахівця споживача для перегляду та зміни відповідних технічних параметрів наданої хмари.

Високий рівень автоматизації, необхідний для роботи з хмарою, означає, що для користувача немає ніякої можливості для перевірки кожної окремої ситуації та прийняття зваженого рішення для запиту на основі його контексту. Замість цього рішення мають бути своєчасно формалізовано у вигляді обмеженого набору політик, що автоматично виконуються хмарною інфраструктурою.

1.2.3 Спільне використання обчислювальних потужностей

Об’єднання ресурсів, спільне використання обчислювальних потужностей призводить до збільшення коефіцієнта використання ресурсів, відповідно використовуючи віртуальну інфраструктуру та динамічний перерозподіл обчислювальних потужностей дозволяє заощадити певну частину коштів за рахунок збільшення кінцевих користувачів [10].

Об’єднання ресурсів на програмному рівні, накладає відповідні обмеження на розробників програмного забезпечення, що мають передбачити можливість одночасного використання програмного продукту одночасно кількома користувачами.

Коли кілька споживачів використовують одні й ті самі ресурси, виникає питання, як саме має розраховуватися вартість отриманий послуг. Білінгова та дозуюча інфраструктури автоматично збирають інформацію про кожного споживача. Для цього кожному запиту має бути встановлено відповідний ідентифікатор транзакції, що також пов’язаний з відповідним споживачем хмарних технологій. Ідентифікатор транзакції передається всім використаним компонентам для розрахунку загальною вартості наданих послуг. Розмір плати може залежати від технічних характеристик наданого обладнання: центрального процесору, обсягу пам’яті, пропускної здатності мережі, кількість одночасно оброблюваних запитів, кількість одночасно працюючих користувачів.

1.2.4 Масштабування за потребою

Оскільки споживачі хмарних послуг очікують отримувати обчислювальні ресурси у будь-якій кількості і у будь-якій час, хмара повинна повсякчас мати змогу для швидкого масштабування вгору й вниз, як того вимагає поточне навантаження. Слід мати на увазі, що масштабування вниз так само важливо, як і масштабування вгору, для відповідного розподілу навантаження та зберігання вільних ресурсів [11].

Різне програмне забезпечення, що працює у хмарі, мають різні моделі робочого навантаження. Через ці відмінності, високі робочі навантаження у деяких додатках, буде збігатися з низьким навантаженням у інших. Саме тому об'єднання ресурсів призводить до підвищення коефіцієнта використання ресурсів та економії.

Для досягнення цієї економії хмарна інфраструктура повинна мати можливість для швидкого масштабування. У загальному випадку, масштабування – це здатність системи збільшувати продуктивність пропорційно до збільшення апаратного забезпечення. У масштабованій хмарі, можна просто додати нове обладнання при збільшенні попиту на нього, забезпечуючи забезпечувати продуктивність додатків на необхідному рівні.

Спираючись на те, що ресурси у системі, як правило, мають певний рівень службового навантаження, важливо зрозуміти, який саме відсоток від загального обчислювального ресурсу доступно для користувача. Вимірювання додаткового збільшення продуктивності шляхом додавання одиниці апаратного забезпечення, в порівнянні з раніше доданим забезпеченням ресурсу називається коефіцієнтом масштабування.

Але існує це один спосіб погляду на масштабованість: вертикальна та горизонтальна масштабованість. Вертикальна масштабованість передбачає збільшення або зменшення продуктивності одного вузла в системі, шляхом зміни його апаратного забезпечення. Але існує межа того, як сильно можна змінити продуктивність вузла, через обмеження операційної системи на об'єм оперативної пам'яті, сталу кількість фізичних портів, відповідність роз'єму

процесору й материнської плати тощо. Горизонтальна масштабованість спрямована на зміну кількості вузлів у системі, що дозволяє обійти обмеження вертикальної масштабованості. Горизонтальна масштабованість дозволяє використовувати обладнання загального призначення, не використовуючи дороге спеціалізоване апаратне забезпечення.

1.2.5 Плачу за те що споживаю

Для оперативного масштабування вгору чи вниз, потрібно постійно аналізувати поточний попит на обчислювальні ресурси хмари, тобто навантаження на центральний процесор, оперативну пам'ять та пропускну здатність мережі, щоб переконатися, що споживачі не відчують вичерпності цих ресурсів [12].

Щоб зменшити власні ризики, споживачі підписують з постачальником хмарних технологій угоду про рівень обслуговування (SLA), що має гарантувати відповідність послуг, що надаються і мають надаватися поставником хмарних обчислень. Одна з найбільш важливих послуг у SLA є доступність. Хоча апаратне забезпечення, як правило, дуже надійне, воно теж може бути виведене з ладу, тому угода про рівень обслуговування має передбачати дії поставника хмари на цей випадок. Наприклад, це може бути реалізована реплікація даних до територіально відокремлених центрів обробки даних, що може гарантувати, що принаймні у одному з цих центрів інформація буде доступна для споживача..

1.3 IaaS, PaaS і SaaS як моделі обслуговування

На сьогодні можна вирізнити три основні моделі обслуговування хмарних технологій [1]:

інфраструктура як послуга (Infrastructure as a Service, скор. IaaS);

платформа як послуга (Platform as a service, скор. PaaS);

– програмне забезпечення як послуга (software as a service, скор. SaaS).

Інфраструктура як послуга надає споживачеві набір фізичних ресурсів, таких як сервери, мережеве обладнання та накопичувачі. Замість того, щоб купувати власне апаратне та програмне забезпечення, серверні стійки, інше обладнання, виділяти окреме приміщення та забезпечувати необхідні мікрокліматичні умови, споживач просто в міру необхідності купують ці ресурси (і в подальшому відмовляються від них) у поставника хмарних послуг.

За концепцією IaaS споживач купує лише ті обчислювальні потужності, які необхідні йому для виконання конкретних завдань. До складу додаткових послуг IaaS може входити під`єднання будь-якого фізичного обладнання користувача до хмарної платформи і його розміщення в мережі центрів обробки даних. Споживачу при цьому не надається керування базовою інфраструктурою хмари, але він має контроль над операційними системами, системами зберігання даних, додатками та може мати певний обмежений контроль над мережевими компонентами. У цьому випадку захист платформ і додатків забезпечує сам споживач, а провайдер хмари повинен організувати захист інфраструктури, а для надання ресурсів на вимогу зазвичай використовується віртуалізація.

Найпоширенішою формою використання моделі IaaS є віртуальні виділені сервери (VPS). VPS – це віртуальний сервер, що емулює звичайний фізичний комп’ютера із власною операційною системою. Віртуальні сервери використовують виділені їм обчислювальні ресурси фізичного серверу з повністю ізольованим від інших серверів програмним забезпеченням [15].

Віртуальні сервери розгортаються і управляються хостом – фізичним сервером на якому вони встановлені. Кожен віртуальний сервер має власну операційну систему, яка є основою для встановлення інших програм. Загалом віртуальний сервер ідентичний виділеному фізичному серверу, хоча його продуктивність іноді може бути дещо нижчою через спільне використання фізичних ресурсів з іншими серверами [16].

Обчислювальні ресурси для віртуального сервера надаються фізичним сервером, на якому він розміщений. Хост використовує програмне забезпечення, що називається гіпервізором та слугує для розгортання та керування віртуальними виділеними серверами, а також для надання їм ресурсів, які знаходяться під його контролем. Поняття гіпервізор, як правило, використовують для позначення фізичних хостів, на яких встановлені гіпервізори (і підконтрольні їм віртуальні сервери). На рисунку 1.1 наведено узагальнену структуру організації віртуальних серверів.

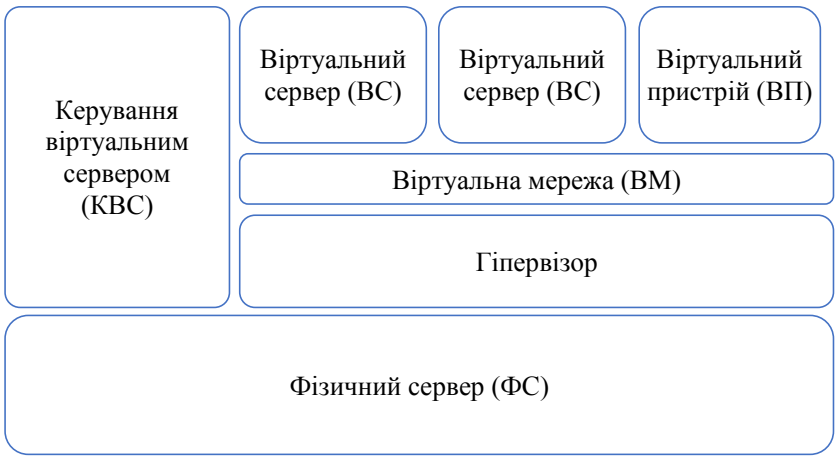

Рисунок 1.1 – Узагальнена структура організації віртуальних серверів

При розгортанні нового віртуального виділеного сервера хост виділяє для цього сервера пам’ять, процесорні ядра та мережеве підключення. Гіпервізор у свою чергу планує розподіл процесів між віртуальними та фізичними ядрами. Оскільки одне і теж саме фізичне ядро може одночасно використовуватися кількома віртуальними серверами. Ключовою відмінністю між різними гіпервізорами полягає саме у методах планування розподілу процесів [17].

Гіпервізор Kernel-Based Virtual Machine (KVM) – це інфраструктура віртуалізації, вбудована в ядро Linux. При активації KVM фізичний сервер з операційно. системою Linux перетворюється на гіпервізор, що дає змогу почати розміщення віртуальних серверів.

Використання KVM значно спрощує процес розгортання, через відсутність необхідності створювати або емулювати ядра, які використовуються для віртуального хостингу.

Одним з найпоширеніших гіпервізорів є гіпервізор Xen. На відміну від KVM, Xen використовує мікроядро, що надає усі необхідні інструменти для підтримки віртуальних серверів без необхідності внесення змін в ядро хоста.

Xen використовує два різні методи віртуалізації:

– паравіртуалізація, використання цього методу усуває необхідність емулювати апаратні засоби, але вимагає внесення змін до операційної системи віртуальних серверів;

– віртуалізація з апаратною підтримкою, гіпервізор використовує спеціальні апаратні засоби для ефективної емуляції віртуального сервера, що усуває необхідність змінювати операційні системи.

Гіпервізор ESXi є автономним гіпервізором корпоративного рівня, що розробляється компанією VMware. Особливістю ESXi є те, що він не вимагає встановлення операційної системи на хості. ESXi надзвичайно продуктивний завдяки відсутності посередників між апаратними засобами і віртуальними серверами.

Ще одним популярним способом віртуалізації серверів Windows є використання гіпервізору Hyper-V. Hyper-V переважно вибирають розробники, що працюють у середовищі Windows, так як він вбудований у Windows Server починаючи з версії Windows Server 2008, а також доступний як автономний сервер без необхідності встановлення Windows Server.

Якщо створити фізичну мережу з наведених на рисунку 1.3 вузлів зі спільним доступом до пристрою зберігання даних та організувати керування цією інфраструктурою, забезпечити фільтрацію та кешування, а роботу віртуальних серверів динамічно розподіляти між вузлами в залежності від їх завантаженості, то у результаті отримаємо віртуальну інфраструктуру, що може називатися хмарою. Узагальнену структуру такої хмари наведено на рисунку 1.4.

Окрім віртуалізації для реалізації моделі IaaS використовується автоматичне управління, що забезпечує динамічний розподіл ресурсів без участі персоналу постачальника послуг, система автоматично може збільшувати або зменшувати кількість віртуальних серверів, обсяг дискового простору для зберігання даних та змінювати пропускну здатність каналів зв'язку мережі. Віртуалізація та автоматичне управління забезпечують ефективне використання обчислювальних ресурсів і зниження вартості оренди моделі IaaS.

Платформа як послуга дозволяє споживачу використовувати хмарну інфраструктуру для розміщення власного програмного забезпечення для подальшого його використання та модифікації, уникаючи витрат на обслуговування відповідної інфраструктури і сервісів для розробки, тестування, розгортання і розміщення додатків. Як правило, системи PaaS є повноцінним середовищем розробки і розгортання в хмарі з ресурсами, які дозволяють надавати будь-які додатки, від простих хмарних додатків, до просунутих хмарних додатків промислового класу.

Як і IaaS, PaaS включає інфраструктуру: сервери, сховище даних та мережеве обладнання, а також проміжне програмне забезпечення, засоби розробки, служби системи управління базами даних тощо. Модель PaaS призначена для підтримки повного життєвого циклу веб-додатків: розробки, тестування, розгортання, управління та оновлення.

Програмне забезпечення як послуга передбачає доступ до додатків як до сервісу, тобто додатки постачальника запускаються в хмарі і надаються користувачам на вимогу як послуга. Користувач отримує доступ до програмного забезпечення на віддалених серверах, за допомогою мережі Інтернет, а оновлення та керування ліцензіями виконується постачальником хмарних послуг.

Програмне забезпечення що надається є доступим на різноманітних клієнтських пристроях за допомогою, наприклад веб-браузера. Керування базовою інфраструктурою хмари, мережами, серверами, операційними

системами покладається цілком на постачальника, а користувачу надається можливість змінювати обмежений набір параметрів самого додатку.

При використанні цієї моделі обслуговування, споживач сплачує лише за фактичне використання наданого програмного забезпечення або взагалі воно надається безкоштовно. Багато додатків розповсюджуються на умовах місячної підписки, що дає певну перевагу над класичним програмним забезпеченням у разі їх тимчасового або періодичного використання.

Щоб краще зрозуміти, що включає в себе кожна з моделей обслуговування, розглянемо рисунок 1.5, що ілюструє склад кожної моделі у повірянні з традиційним рішенням [18].

Рисунок 1.5 – Склад моделей обслуговування хмарних технологій у порівнянні з локальним рішенням

1.4 Типи розгортання хмарних технологій

За типами розгортання хмари поділяють на приватні, комунальні, публічні та гібридні [1].

Приватні хмари – модель розгортання хмарної інфраструктури, при якій обчислювальні ресурси хмари доступні тільки однієї організації, але споживачів у такої хмари може бути декілька, наприклад, різні підрозділи. Особливістю цієї моделі розгортання є те, що приватна хмара знаходиться в межах корпоративної мережі, тому організація може керувати хмарою самостійно або доручити цю задачу іншому підприємству. Інфраструктура може розміщуватися або в приміщеннях підприємства, або у зовнішнього оператора чи частково на підприємстві та частково у зовнішнього оператора. Ідеальним варіантом розгортання приватної хмари є розгортання на території організації. Це забезпечує детальний контроль над різними ресурсами хмари та спрощує її обслуговування і контроль.

Добавлено примечание ([V7]): http://www.treolancloud.ru/knowledge/articles/modeli_razvertyvaniya_oblaka_i_ih_osobennosti/

Зважаючи на те, що підприємство власноруч займається установкою і підтримкою хмари, вартість і складність розгортання такої хмари можуть значно перевищувати вартість експлуатації хмар розгорнутих за іншими моделями.

При використанні приватної хмари гарантується високий рівень безпеки, завдяки відсутності прямого виходу хмари до мережі Інтернет та розміщення в ній інфраструктури тільки однієї організації. Це відмінний варіант для компаній з високими вимогами до конфіденційності даних, що розміщуються в хмарі, наприклад різних фінансових, державних компаній.

Громадською хмарою називають інфраструктуру яка слугує для використання конкретною множиною споживачів, що мають спільні задачі.

Наприклад. громадською хмарою можна вважати об’єднання приватних хмар різних підрозділів одного підприємства або різних підприємств

Публічні хмари – модель розгортання хмарної інфраструктури, при якій обчислювальні ресурси хмари доступні безлічі споживачів і організацій, але при цьому технологія віртуалізації забезпечує сегментацію віртуальних машин різних споживачів, тобто віртуальні машини різних організацій знаходяться на одному фізичному обладнанні, але повністю відокремлені один від одного. На відміну від приватних хмар, публічні завжди знаходяться за межами корпоративної мережі підприємства.

Користувачі публічних хмар не мають можливості керувати або обслуговувати хмару, а вся відповідальність покладена на власника цієї хмари. Постачальник хмарних послуг приймає на себе обов'язки по інсталяції, управлінню, наданню та обслуговуванню програмного забезпечення, інфраструктури додатків або фізичної інфраструктури. Споживачі платять тільки за ресурси, які вони використовують.

Послуги, що надаються публічними хмарами у більшості випадків є стандартизованими, виходячи з умов найбільш поширених випадків використання. Відповідно у споживача є менше можливостей по вибору конфігурації в порівнянні з системами, у яких повнота керування надана самому споживачу. Оскільки споживачі слабо контролюють або взагалі не контролюють інфраструктуру, процеси, що вимагають дотримання суворих заходів безпеки і відповідальності нормативним вимогам повністю лягають на постачальника хмарних послуг.

Гібридна хмара – модель розгортання хмарної інфраструктури, як комбінації приватної і публічної хмари. Поєднання цих двох моделей дозволить організації, яка вже побудувала свою приватну хмару, використовувати обчислювальні ресурси публічної хмари, тобто можливість при необхідності розширити власну інфраструктуру за рахунок ресурсів публічної хмари.

1.5 Висновки до першого розділу

Хмарні технології розробляються протягом багатьох років та є поєднанням декількох ключових технологій, які багатьма розглядаються як наступний етап розвитку IT-архітектури підприємств.

Впровадження хмарних технологій дозволяє відмовитися від застарілого локального інфраструктурного підходу до запуску сервісів у сфері інформаційно-комунікаційних технологій та мають практичні переваги:

– швидкість отримання доступу до необхідних додатків;

– динамічна зміна обчислювальної потужності залежно від потреб споживача;

– стандартизовані платформи для розробки власних додатків та сервісів;

– зменшення потреби у збільшенні обчислювальної потужності власних серверів.

Але використання хмарних технологій призводить до необхідності вирішення поставником відповідних проблем, що наведені у таблиці 1.1:

Таблиця 1.1 – Основні проблеми, що виникають при використанні хмарних технологій

Добавлено примечание ([V8]): Убрать

Проблема	Зміст проблеми
Інформаційна безпека	Дані споживача перебувають у хмарі. Постачальник хмарних послуг несе повну відповідальність за забезпечення безпеки даних, що розміщено у ЦОД споживачем.
Цілісність даних	Технологія хмарних обчислень базується на використанні гетерогенних мереж. Постачальник має забезпечити повноцінне виконання транзакцій в інформаційних сховищах.

Продовження табл. 1.1

Проблема	Зміст проблеми
Надійність	Постачальник хмарних послуг повинен забезпечити повну працездатність доданків і сервісів у умовах пікових навантажень, а при необхідності масштабувати обчислювані ресурси, відповідно до потреб споживача.
Обслуговування	На постачальника хмарних послуг лягає відповідальність на забезпечення безперервності ведення бізнесу споживача та послуг резервування і відновлення даних.
Утилізація інформації	Забезпечення поставником достовірної утилізації інформації споживача та неможливість повторного використання інформації споживача, іншими споживачами.

Розподіл відповідальності між споживачем та поставником хмарних послуг відрізняється в залежності від моделі обслуговування:

– при використанні моделі SaaS на споживача покладається відповідальність лише за збереження конфіденційності автентифікаційних даних, а постачальник хмарних послуг забезпечує всі рівні захисту;

– модель PaaS передбачає покладання відповідальності за забезпечення захисту додатку, що ним розробляється, захист платформ та інфраструктури забезпечує постачальник;

– при обслуговуванні за моделлю IaaS повнота відповідальності надається споживачеві, за виключенням захисту інфраструктури, що забезпечується постачальником хмарних послуг.

Відповідно, у SaaS споживач несе відповідальність лише за дані, що завантажуються у хмару, а за їх збереження відповідає постачальник. Це дає споживачу сподівання на порядність постачальника та забезпечення ним більшого рівня безпеки інформації у порівнянні з використанням моделей

PaaS та IaaS. Але у цьому випадку споживач не має можливостей для впливу на перелік засобів дотримання інформаційної безпеки. Це може стати перепоною для великих корпорацій, що звикли самостійно здійснювати контроль над власною інфраструктурою.

Модель PaaS, що є основою для міграції у хмару, не має чітко визначеного розмежування обов'язків, оскільки у подібній системі виникає два типи контролю доступу: споживач – додаток, що забезпечує споживач та додаток – сервер, що забезпечується постачальником хмарних послуг.

Модель IaaS дає клієнтові найбільшу свободу над керуванням обладнанням, засобами віртуалізації, операційними системами, програмним забезпеченням тощо. Але одночасно забезпечення інформаційної безпеки лягає на споживача та залежить від професіоналізму його IT-служби, від якої і буде залежати ступінь захисту. Постачальник забезпечує лише безперервність роботи наданого обладнання.

РОЗДІЛ 2.
ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ G SUITE ENTERPRISE

2.1 Послуги, що надаються підписникам G Suite Enterprise

G Suite Enterprise– це хмарне рішення Компанії Google, що дозволяє отримати доступ до засобів Office практично звідусіль завдяки мережі інтернет, а також надає можливість загального доступу до файлів і інші можливості для корпоративних клієнтів.

Використання G Suite Enterprise дозволяє для організацій будь-якого розміру користуватися популярними продуктами Google для спільної роботи (Обмін повідомленнями: Gmail, Календар, Контакти, Групи, Пошук, Перекладач, Сейф, Hangouts), не встановлюючи їх на сервери організації, а отримуючи доступ до служб через інтернет на основі щомісячної оплати.

Організації, що придбали підписку на G Suite Enterprise отримують такі переваги :

– використання всієї потужності сучасних інформаційних технологій без необхідності вкладатися в створення власної мережевої інфраструктури, розгортати і супроводжувати складне програмне забезпечення;

– можливість перекласти рутинні роботи щодо створення резервної копії даних, встановлення оновлень безпеки на корпорацію Google і зосередити зусилля IT-підрозділів на стратегічних завданнях;

– оплата послуг за принципом оренди: перенесення витрат на програмне забезпечення з капітальних в операційні, прогнозованість платежів;

– знайомі користувачам інструменти роботи, швидке розгортання і використання співробітниками, низькі витрати на навчання кінцевих користувачів;

– краща в галузі система забезпечення безпеки і приватності даних: вбудовані антивірус і антиспам, відсутність перлюстрації пошти, відповідність

стандарту ISO/IEC 27001, ISO/IEC 27017 та ISO/IEC 27018 і вимогам Європейського Союзу в галузі безпеки;

– прозора система оновлення ПЗ, інформування про нововведення, завжди актуальні версії програмного забезпечення;

– можливості збереження поточних інвестицій в IT за рахунок коштів інтеграції та реалізації гібридних моделей;

– фінансова відповідальність Google: гарантії доступності сервісу 99,9% часу.

Кожен план G Suite Enterprise містить набір окремих служб. У таблиці 2.1 наведено служби, доступні в кожному з планів G Suite Enterprise

Таблиця 2.1 – Порівняння планів G Suite Enterprise

	G Suite Enterprise	G Suite Business	G Suite Basic
Обмін повідомленнями: Gmail, Календар, Контакти	✓	✓	✓
Дані для зберігання і диск взаємодії, документи, відеокімнати	✓	✓	✓
Веб-форуми та спільних поштових скриньки, бізнес-групи	✓	✓	✓
Пошук повідомлень і документів в домен для зберігання пошт, Сейф	✓	✓	✓ *
Інших служб Google: Blogger, YouTube, і т. д.	✓	✓	✓
Універсальний підказку системи та пошук вмісту у різних послуг (G) люкс: хмара пошуку *	✓		

Корпоративний Gmail – це рішення для обміну повідомленнями з поширеними можливостями у вигляді хмарної служби. Воно надає користувачам доступ до електронної пошти, календаря, контактів і завдань з персональних комп’ютерів, мобільних пристроїв і через Інтернет.

Організації, підписані на Корпоративний Gmail, зберігають контроль над службами обміну повідомленнями, які пропонуються користувачам, але позбавляються від операційних витрат на локальне серверне програмне забезпечення. При використанні планів G Suite Enterprise, електронна пошта розміщується на серверах, які одночасно підтримують кілька клієнтів. Ці сервери розміщені в центрах обробки даних Google і доступні для користувачів на широкому спектрі пристроїв в корпоративній мережі або через Інтернет.

Google Sites дозволяє організаціям створювати власні сайти для співпраці в команді або над проектом і керувати ними. Крім того, можливо розгортання в інтрамережі порталу організації для поширення інформації та новин по всій організації [21] .

Зовнішні користувачі успадковують права користувача з Каталогу G Suite Enterprise, який запросив їх до спільної роботи. Це означає, що якщо організація створює сайт, який використовує корпоративні компоненти, то зовнішньому користувачу надаються права на використання або перегляд цих компонентів в сімействі веб-сайтів, в яке він запрошений. Хоча зовнішніх користувачів можна запрошувати як додаткових учасників проекту для виконання повного спектра завдань на сайті, у них не буде точно таких же можливостей, що і у співробітників організації.

Google Диск для бізнесу – приватне інтернет-сховище в хмарі для співробітників компанії. Воно дозволяє з легкістю зберігати робочі файли на декількох пристроях, обмінюватись файлами з колегами по бізнесу і спільно редагувати документи у реальному часі за допомогою сервісу Google Документи та синхронізувати файли за допомогою програми для синхронізації Google Диск для бізнесу.

Додаток Hangouts дозволяє відправляти і приймати повідомлення, спілкуватися в голосовому чаті, а також безкоштовно проводити індивідуальні та групові відеозустрічі. Ця служба надає користувачам доступ до відомостей про присутність, забезпечує обмін миттєвими повідомленнями, аудіо- та

відеодзвінки, повнофункціональні зборів по мережі і широкі можливості проведення веб-конференцій. Служба Hangouts для бізнесу розміщена на мультітенантних серверах, які підтримують декількох клієнтів одночасно. Ці сервери розміщені в центрах обробки даних Google доступні з ряду пристроїв користувачів через корпоративну мережу або Інтернет [23].

Служба Google Документи дозволяє відкривати документи Word, Excel, O і PowerPoint в веб-браузері. Завдяки цій службі працювати з офісними файлами і надавати до них спільний доступ набагато простіше, адже це можна робити скрізь, де є підключення до Інтернету, і практично з будь-якого пристрою. Клієнти G Suite Enterprisez можуть переглядати, створювати і редагувати файли на ходу [24].

Корпоративна приватна корпоративна соціальна мережа Google+, що дозволяє співробітникам підвищити продуктивність, дозволяючи їм легко працювати разом, швидше приймати рішення, а також самостійно організувати групи для вирішення будь-якого бізнес-завдання. Це новий спосіб взаємодії, який покращує узгодженість і гнучкість компанії, скорочує час робочих циклів, підвищує задоволеність співробітників і покращує відносини з клієнтами і партнерами,

Сьогодні практично всі організації прагнуть до того, щоб самостійно налаштовувати і контролювати функції, що забезпечують безпеку хмарних сервісів. Йдеться про компоненти, що відповідають за електронну пошту, календар, управління контентом, організацію спільної роботи і об'єднані комунікації.

Компанії потрібно надавати доступ користувачам до документів та відомостей, які сьогодні розміщуються в самих різних місцях і доступ до яких здійснюється з величезної кількості пристроїв і платформ. Важко заперечувати очевидні переваги такого підходу для користувачів, проте він серйозно ускладнює завдання управління безпекою. Кожний кінцевий пристрій являє собою потенційну точку атаки і додатковий актив, за безпеку якого відповідають фахівці. Кожен день в світі зростає кількість загроз, з якими

стикаються організації. Вони повинні управляти потенційними ризиками, що виникають в результаті випадкової втрати користувачем пристрою або компрометації конфіденційної інформації. Саме тому компаніям потрібно хмарна служба з надійними вбудованими засобами безпеки, функції яких можна налаштовувати відповідно до потреб бізнесу. Розширення функцій віддаленого доступу для підтримки передових практик забезпечення безпеки – складна і дорога задача, якщо в компанії розгорнуті лише локальні IT-сервіси.

Поряд з великою кількістю переваг хмарного рішення, перед провайдером такого сервісу стоїть складне завдання управління безпекою. Компанія Googlet використовує методики, процеси і технології, що дозволяють забезпечити безпеку G Suite Enterprise, кожен аспект яких призначений для захисту конфіденційності ваших даних.

Навіть якщо ви зберігаєте ваші дані в хмарі Google, ви є їх власником, ви можете завантажити копію ваших даних у будь-який час, за будь-якої причини. Жодні дані споживачів не зберігаються протягом більш ніж 180 днів після того, як їх підписка або контракт скасовано або зупинено.

Споживач зберігає повний контроль над доступом до власних даних, що зберігаються у хмарі. Інженери Google не мають постійного доступу до будь-яких даних в службі G Suite Enterprise, а дані споживачів повністю ізольовані від співробітників корпорації і Google не використовує ці дані для маркетингових цілей. У рідкісному випадку, коли інженеру служби Google потрібен доступ до даних, споживач має схвалити його доступ.

Для захисту від несанкціонованого доступу G Suite Enterprise дозволяє реалізувати багатофакторну автентифікацію. Налаштування параметрів перевірки автентичності надають споживачу повний контроль над тим, як користувачі отримують доступ і використовують G Suite Enterprise. Споживач можете контролювати, як користувачі отримують доступ до інформації з певних пристроїв або в певних місцях, або їх комбінації, наприклад, обмежити

доступу з загальнодоступних комп'ютерів або з використанням відкритої мережі Wi-Fi.

Шифрування захищає дані споживача на серверах, а шифрування при надсиланні за допомогою TLS захищає дані під час передачі між споживачем і Google.

Механізм запобігання втрати даних у G Suite Enterprise дозволяє споживачам зупинити витік даних, не впливаючи на продуктивність праці. Використовуючи вбудовані шаблони, споживачу надається можливість налаштовувати і виконувати політики запобігання втрати даних. Споживач також можете визначити і адаптувати правила і політики до потреб власної організації, наприклад, обмежити доступ співробітників організації від обміну особистою інформацією (PII) з зовнішніми сторонами, при цьому дозволяючи використання PII всередині підприємства. Крім того, використовуючи можливості управління правами на доступ до даних, споживач може обмежити перегляд для окремих одержувачів або обмежити відправку і друк документів.

На рівні обслуговування споживач обирає регіон або регіони, де знаходиться центр обробки даних, у якому зберігаються його дані і резервні копії. Також Google надає інформацію в режимі реального часу і попередження про операції обслуговування, надійності і часу безвідмовної роботи для моніторингу даних споживача.

G Suite Enterprise реєструє події активності користувачів і адміністраторів в службах що входять до цього сервісу . Також журнали відстежують будь-які дії, що виконуються інженером підтримки Google Всі журнали зберігаються централізовано і доступні протягом 90 днів. Споживач може в будь-який час перевірити журнали в Центрі безпеки та відповідності за допомогою веб-інтерфейсу або API керування діяльністю G Suite Enterprise. API-інтерфейс управління забезпечує безпрецедентний рівень видимості у всіх транзакціях користувачів і адміністраторів в G Suite Enterprise і з дозволу споживача, може використовуватися іншими постачальниками програмного

забезпечення для інтеграції даних активності G Suite Enterprise в їх рішення по забезпеченню безпеки і відповідності вимогам і звітності.

У Центрі безпеки та відповідності споживач може створювати докладні звіти, які допоможуть йому зрозуміти, як співробітники отримують доступ і використовують дані підприємства, використовуючи пошук по користувачу, файлу або іншому ресурсу в що розташовані в службах G Suite Enterprise.

Споживачу надається можливість налаштувати політики виявлення аномалій безпеки, щоб попередити про підозрілу активність. Наприклад, попередження буде надіслано, якщо сеанс користувача буде виконаний поверх анонімного проксі, при використанні інтернет-провайдера, якого користувач раніше не використовував, було кілька невдалих спроб входу в систему тощо. Ці політики можуть контролювати багато показників і використовують машинне навчання. Споживач може налаштувати параметри повідомлень і навіть закрити доступ для користувачів на основі результатів політики. Для подальшого підвищення прозорості політик, є можливість візуалізувати використання організацією G Suite Enterprise і інших хмарних сервісів, щоб максимізувати інвестиції в IT.

Корпорація Google впроваджує суворі процедури безпеки у своїх центрах обробки даних, які важко скомпрометувати. Центри даних Google мають кілька рівнів фізичної безпеки, щоб запобігти доступу неавторизованих людей до фізичних серверів. Забезпечення безпеки починається з багатофакторної аутентифікації, 24-годинного моніторингу і включає біометричне сканування для доступу до центру обробки даних.

Співробітники піддаються суворим перевіркам, а поділ ролей не дозволяє співробітникам з фізичним доступом до серверів знати місце розташування конкретних даних клієнта. У деяких випадках сервери можуть бути встановлені в шафах, що замикаються та мають постійне відеоспостереження.

Центри обробки даних Google також забезпечують високу надійність. Google підтримує кілька центрів обробки даних в кожному регіоні і гарантує,

що дані споживачів зберігаються в декількох центрах обробки даних. В окремих центрах обробки даних використовуються системи пожежогасіння, сейсмічна арматура і резервні системи вироблення електроенергії, щоб гарантувати, що фізичні дані захищені від втрат або збоїв.

Однією з найсерйозніших проблем безпеки є захист користувачів від невідомих атак. G Suite Enterprise захищає користувачів від хакерів шляхом інтеграції у сервіси захисту від спаму, фішингу та інших загроз за допомогою технологій IRM и DLP. Але те, що дійсно привабливе в цій функції, це те, що вона забезпечує захист навіть від зовсім нових, невідомих атак типу «вразливість нульового дня». Вкладення, виявлені як шкідливі, видаляються і знешкоджуються, що дозволяє отримувати повідомлення електронної пошти з майже нульовою затримкою, а якщо вкладення вважається безпечним, воно вставляються назад в повідомлення.

Крім можливостей активного захисту, G Suite Enterprise, ці технології надають багаті функції для звітності та відстеження, які допоможуть споживачу дізнатися, хто або що у організації націлений на атаку і які види атак використовуються і куди мають бути спрямовані ресурси безпеки.

Традиційні засоби IT-безпеки забезпечують обмежений захист від складних кібератак, коли були викрадені облікові дані користувача. Технології IRM и DLP забезпечують простий і швидкий спосіб для аналізу подій, що відбуваються у мережі підприємства, шляхом виявлення підозрілих дій користувачів і пристроїв, таких як активні атаки, аномальні логіни, спільне використання паролів і інші відомі вразливості.

Мобільні пристрої, такі як смартфони та планшети, все частіше використовуються для доступу до робочої електронної пошти, календарів, контактів і документів підприємства. Іншими словами, вони відіграють велику роль в забезпеченні того, щоб співробітники виконували свою роботу в будь-який час, з будь-якого місця.

Оскільки все більше підприємств використовують підхід «використовуй власний пристрій для роботи» до телефонів і планшетів, захист корпоративних

даних на мобільних пристроях стає головною проблемою. Використання G Suite Enterprise дозволяє розділити свої особисті і корпоративні додатки, використовуючи функції управління мобільними пристроями в різноманітних смартфонах і планшетах, включаючи пристрої на таких операційних системах як iOS, Android і Windows Phone.

Щоб гарантувати, що корпоративна електронна пошта і документи синхронізуються тільки на телефонах і планшетах співробітників компанії, G Suite Enterprise дозволяє застосувати політику безпеки на пристроях до того, як вони зможуть підключитися до G Suite Enterprise.

Якщо мобільний пристрій співробітника було втрачено або викрадено, для запобігання доступу неавторизованих користувачів до корпоративної електронної пошти та даних підприємства, дані компанії можуть бути стерті. У будь-який час споживач можете бачити, які пристрої підключені до G Suite Enterprise і ідентифікувати пристрої, які були заблоковані.

Google адаптує G Suite Enterprise відповідно до стандартів і правил, які застосовуються до вашої галузі та регіону. G Suite Enterprise забезпечує комплексне рішення по забезпеченню відповідності даних, яке задовольняє нормативним вимогам і вимогам внутрішньої відповідності.

Стандарти нормативного регулювання G Suite Enterprise перевіряється незалежно, щоб допомогти споживачам відповідати вимогам, зазначеним в ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, Типових положеннях Європейського союзу (ЄС), Договорі про переносимості та підзвітності медичного страхування (HIPAA BAA) і Федеральному законі про управління інформаційною безпекою FISMA) тощо.

В угоді про обробку даних для G Suite Enterprise детально описується конфіденційність, безпека і обробка даних споживачів, що допомагає відповідати місцевим нормам та міжнародним зобов'язанням щодо дотримання конкретних галузевих стандартів.

Організації повинні зберігати і захищати найважливіші дані і мати простий спосіб для пошуку того, що має значення. G Suite Enterprise допомагає

ефективно управляти вашими даними, надаючи можливість керувати даними підприємства і погоджувати їх з вимогами підприємства про дотримання організаційної структури. Використання машинного навчання в G Suite Enterprise, дозволяє ефективно використовувати кореляції в даних і пропонувати інтелектуальні рішення, які охоплюють імпорт, збереження, захист та видалення даних.

При експоненційному збільшенні обсягу електронних даних важлива дисципліна в життєвому циклі даних, включаючи збереження і видалення. Архівування G Suite Enterprise дозволяє зберігати дані в усіх службах цього сервісу. Дані також можуть бути імпортовані з локальних рішень або зі сторонніх джерел, таких як соціальні мережі тощо.

G Suite Enterprise може реалізувати єдину політику зберігання і не допускати її зміни або відключення, а також допомагає розширити докладні політики на рівні елементів або папок для Gmail і на рівні сайту для Google Sites і Google Диск для бізнесу.

Під час ситуацій внутрішнього розслідування, що вимагають збереження даних, споживач можете встановити утримання для всіх поштових скриньок або сайтів SharePoint. Вміст залишається у Exchange і SharePoint, а співробітники не піддаються впливу. Вони можуть продовжувати створювати, редагувати і видаляти контент, не знаючи, що поштову скриньку призупинено. Замість того, щоб дані переміщалися в різних внутрішніх і зовнішніх середовищах, він залишається в Office 365, який захищений суворої хмарної безпекою Google.

Сервіс Пщщпду eDiscovery допомагає ефективно організувати пошук і зменшити обсяг даних, знаходячи дублікати файлів, відновлюючи потоки електронної пошти. Споживач може використовувати машинне навчання для подальшого скорочення обсягів даних, навчаючи систему інтелектуальному вивченню та аналізу великих, неструктурованих наборів даних і даних, що швидко втрачають актуальність.

За допомогою аудиту G Suite Enterprise реєструє події активності користувачів і адміністраторів. Звіт про діяльність G Suite Enterprise дозволяє досліджувати активність користувачів, використання файлів або інших ресурсів в в усіх службах.

Крім того, API керування забезпечує безпрецедентний рівень видимості всіх транзакцій користувачів і адміністраторів в G Suite Enterprise. API дозволяє організаціям і іншим постачальникам програмного забезпечення інтегрувати дані про діяльність G Suite в свої рішення щодо забезпечення безпеки та відповідності вимогам і звітності.

2.2 Забезпечення інформаційної безпеки служби G Suite Enterprise

G Suite Enterprise– це надійно захищена служба, розроблена відповідно до життєвого циклу розробки систем безпеки Google , розгорнута за моделлю SaaS і включає практичний досвід розробки корпоративного програмного забезпечення та керування онлайновими службами.

На рівні служби G Suite Enterprise використовується підхід поглибленого захисту, у якому функції безпеки та передові робочі методики задіяно на кількох рівнях: фізичному, логічному і на рівні даних. Крім того, служби містить засоби керування корпоративного класу для користувачів і адміністраторів, що додатково посилює захист середовища.

2.2.1 Методи забезпечення інформаційної безпеки при використанні служби G Suite Enterprise на рівні центрів обробки даних.

Центр обробки даних – це місце, де розташовані прикладні програми та пов'язані з ними дані клієнта. Корпорація Google використовує регіональну стратегію розміщення центрів обробки даних. Вибір основного сховища для даних клієнта залежить від того, яку країну або регіон вказав адміністратор клієнта при початковій установці служб. Всі клієнти в регіоні можуть

переглянути розташування центрів обробки даних і відповідних служб. Корпорація Google реплікує дані клієнтів принаймні в двох центрах обробки даних в будь-який момент часу, щоб запобігти збою або локальній аварійній ситуації.

Рисунок 2.1 – Глобальна карта розміщення центрів обробки Google

Якщо з якої-небудь причини робота центру обробки даних припинена, втрата даних не відбувається, так як прикладна програма і пов'язані з нею дані клієнта також доступні в другому або третьому центрі обробки даних. Користувачі можуть не отримувати повідомлення при відпрацюванні відмови. У деяких службах відпрацювання відмови може не призводити до порушення роботи служби. Клієнтам слід припускати, що в будь-який момент часу їх дані можуть оброблятися в одному або декількох центрах обробки даних в регіоні. Але при вході на портал веб-служб з іншого регіону все переглянуті веб-сторінки розміщуються в центрі обробки даних цього регіону.

Узагальнена схема взаємодії між користувачами, підприємством і центрами обробки при використанні G Suite Enterprise зображено на рисунку 2.2.

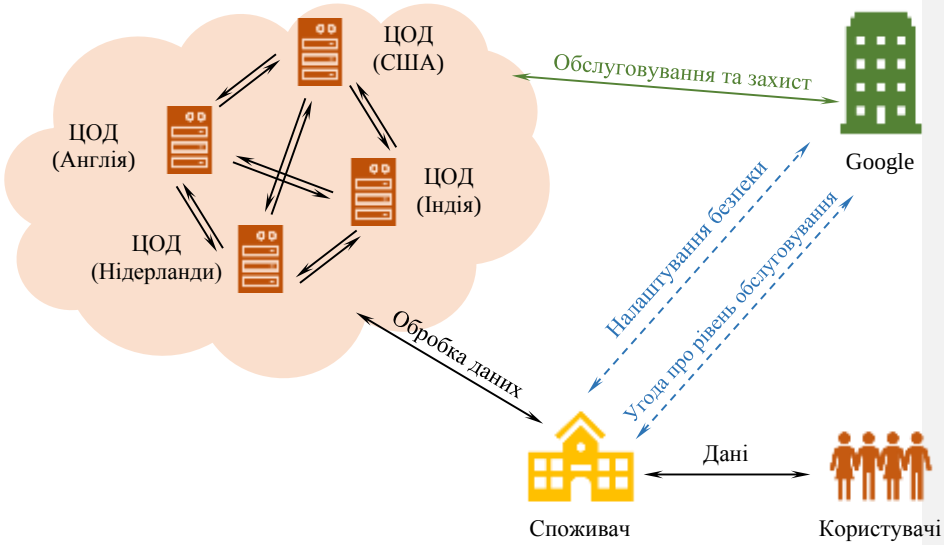

Рисунок 2.2 Узагальнена схема взаємодії між користувачами, підприємством і центрами обробки при використанні G Suite Enterprise

Дані G Suite Enterprise зберігаються в мережі центрів обробки даних компанії Google, які знаходяться під управлінням служби Google Cloud Platform Services. Ці центри обробки даних гарантують надання послуг і захист інформації від стихійних лих або несанкціонованого доступу. Персонал має доступ до центрів обробки даних протягом 24 годин тільки для виконання робочих завдань. Іншими словами реалізовано поділ за ролями, завдяки якому персонал, що має фізичний доступ до місця зберігання даних, жодним чином не може визначити розташування конкретних даних клієнтів. Контроль фізичного доступу здійснюється за допомогою численних процедур аутентифікації і забезпечення безпеки, наприклад використовуються бейджи і смарт-карти, біометричне сканування, багатофакторна автентифікація, в будівлі присутні співробітники локальної служби безпеки, ведеться постійне відеоспостереження. Центри обробки даних обладнані датчиками руху, системами відеоспостереження та сигналізації. Безпеку даних та серверів в

разі стихійних лих забезпечують сейсмостійкі стійки, а також автоматичні системи протипожежної безпеки та пожежогасіння [29].

Відповідальність співробітників забезпечується цілим набором системних процедур, включаючи використання унікальних імен користувачів, засобів управління доступом до даних і аудиту. На відміну від загальних імен користувачів, таких як "Гість" або "Адміністратор", задля забезпечення відповідальності використовуються унікальні імена користувачів, які дозволяють співвідносити дії користувача з конкретним співробітником, так зване "зв'язування".

Корпорація Google вкрай жорстко контролює надання конкретних ролей співробітникам. Доступ співробітників до IT-систем, в яких зберігаються дані клієнтів, суворо контролюється за допомогою управління доступом на основі ролей (RBAC) і процедур блокування. Контроль доступу являє собою автоматизований процес, заснований на принципах поділу обов'язків і надання мінімально необхідних привілеїв. Цей процес гарантує, що інженер, що запитує доступ до таких IT-систем, відповідає необхідним вимогам, що охоплюють в тому числі перевірку благонадійності, контроль відбитків пальців, обов'язкове навчання заходам безпеки і утвердження прав доступу. Крім того, рівень доступу періодично переглядається, щоб гарантувати доступ до систем тільки тих користувачів, які дійсно потребують цього для вирішення робочих завдань.

Фізичний доступ до центрів обробки даних G Suite Enterprise контролюється за допомогою дворівневої системи перевірки справжності, що включає в себе пристрій зчитування карт проксі-доступу, необхідний жетон доступу по карті, і біометричний зчитувач геометрії долоні та ока.

Процес превентивного захисту передбачає перегляд допусків і дій оператора або адміністратора і зачіпає як персонал, так і процедури допуску до виконання необхідних робіт. Обнуляються дозволи служб для адміністраторів, помилки в службі усуваються точно в строк при наданні допуску та підвищенні привілеїв інженера, це гарантує, що всі необхідні

заходи будуть вжиті в потрібний час, сегрегується поштове середовище серед співробітників і середовище допусків в робочу зону. Службовці, які не пройшли перевірку основних даних, автоматично позбавляються прав доступу з високими привілеями. Результати ретельних перевірок основних даних службовців затверджуються в ручному режимі.

Щокварталу співробітники служби безпеки Google відправляють звіт уповноваженим фахівцям, що мають право затверджувати доступ до центру обробки даних. Цей звіт містить список співробітників, що мають доступ до центрів обробки даних в даний час. Уповноважені фахівці перевіряють користувачів в списку на предмет необхідності продовження їх доступу та наявності у них мінімального рівня доступу, достатнього для виконання їх робочих обов'язків.

Така перевірка охоплює відомості про освіту, працевлаштування та несудимість кандидата. Крім стандартної перевірки анкетних даних, яка застосовується до всіх нових співробітників корпорації Google, нові і поточні співробітники, що мають доступ до даних клієнтів або керують ключовими засобами фізичного і логічного доступу, в обов'язковому порядку проходять перевірку за:

- списками експортного контролю (список управління з контролю за іноземними активами (OFAC),
- список бюро промисловості та безпеки (BIS)
- списком осіб, позбавлених права заняття певних посад, відділу Міністерства оборони США по регулюванню зовнішньої торгівлі (DDTC).

Адміністратори баз даних Google за визначенням мають доступ до всіх ресурсів в базі даних, включаючи дані клієнтів. Використання даних клієнтів допускається тільки з метою надання послуг. Таким чином, корпорація Google суворо забороняє доступ до даних клієнтів з іншою метою. В рамках надання послуг адміністратори баз даних можуть звертатися до даних клієнтів для

виконання певних дій, таких як налаштування бази даних або перенесення клієнтів з однієї бази даних в іншу..

Дані клієнта – це всі дані, включаючи текстові і звукові файли, файли програм і файли зображень, які зберігаються у центрі обробки даних в процесі використання служб. Дані клієнта не включають в себе дані адміністраторів, дані про платежі і оперативну інформацію про служби. Контент – це підмножина даних клієнта, що в загальному випадку є конфіденційною інформацією і, як правило, не передається в незашифрованому вигляді. Зокрема, до контенту відносяться тексти повідомлень і вкладення електронної пошти Gmail, зміст файлів Google Sites, текст бесід з використанням миттєвих повідомлень, голосові бесіди тощо. У таблиці 2.2 описані рівні доступу для різних типів адміністраторів і даних.

Таблиця 2.2 – Рівні доступу для різних типів адміністраторів і даних.

Адміністратор	Дані клієнта (виключаючи контент)	Контент
Оперативна група (тільки кваліфікований персонал)	Так, при необхідності	Так, як виняток
Організація, що забезпечує підтримку	Так, тільки при необхідності у відповідь на запит в службу підтримки	Ні
Інженери	Немає прямого доступу. Дані можуть передаватися в ході усунення неполадок.	Ні

Партнери	З дозволу клієнта	З дозволу клієнта
Інші співробітники Google	Ні	Ні

Мережі в центрах обробки даних розділені на сегменти, що забезпечує фізичну ізоляція критично важливих внутрішніх серверів і пристроїв зберігання даних від загальнодоступних інтерфейсів, а засоби безпеки прикордонних маршрутизаторів дозволяють виявляти спроби вторгнення і ознаки уразливості системи (рисунок 2.4).

Підключення клієнтів до G Suite Enterprise відбувається по протоколу Transport Layer Security (TLS), що забезпечує безпеку при доступі клієнті до веб-служб зі своїх комп'ютерів, підключених до Інтернету, а запити на доступ потрапляють до центру обробки даних компанії Google. Підключення шифруються з використанням стандартного протоколу безпеки TLS.

Протокол TLS гарантують безпечне підключення клієнтів до сервера, конфіденційність і цілісність даних, що передаються між комп’ютером користувача і центром обробки даних. Клієнти можуть налаштовувати параметри протоколу TLS між і зовнішніми серверами як для вхідної, так і для вихідної пошти. За замовчуванням цей параметр включений.

Окрім шифрування даних при передачі між комп’ютером клієнта та центром обробки даних за допомогою протоколу TLS, статичні дані, тобто ті, що не передаються у даний момент в екосистемі Google підписуються спеціальним криптографічним ключем, а дані шифруються під час запису на диск. На додаток до цього криптографічні ключі зберігаються в ОЗУ рівно стільки, скільки вони потрібні. Дистанційні підключення і всі інші способи зв'язку між дата-центрами шифруються за умовчанням. Одна з причин

масштабованості і низької вартості G Suite Enterprise полягає в тому, що ця служба є багатокористувачевою, тобто дані різних клієнтів розміщені на одних і тих же апаратних ресурсах. Зберігання та обробка даних кожного клієнта здійснюється окремо за допомогою Google Directory і інших засобів, спеціально розроблених для створення, контролю і забезпечення безпеки багатокористувацьких середовищ. Google Directory ізолює клієнтів, використовуючи зони безпеки. Такий підхід не дозволяє одним клієнтам отримати доступ до даних інших клієнтів або поставити під загрозу безпеку цієї інформації. За додаткову плату можна придбати версію Office 365, яка забезпечує зберігання даних на спеціально виділеному обладнанні.

Коли клієнти видаляють дані або припиняють користуватися службою Office 365, вони можуть зберегти дані локально і назавжди видалити їх з серверів Google. Корпорація Google дотримується стандартів щодо перезапису ресурсів сховища до повторного використання, а також фізичного знищення списаного обладнання, несправні диски та обладнання розмагнічується і видаляється.

Забезпечення безпеки в G Suite Enterprise– це безперервний процес, а не просто послідовність певних дій. Досвідчений і добре навчений персонал постійно тестує, обслуговує і удосконалює засоби безпеки. Компанія Google прагне підтримувати актуальний рівень програмних і апаратних технологій, використовувати надійні процеси розробки, побудови, експлуатації та підтримки. Як приклад подібних процесів можна навести життєвий цикл розробки безпечних додатків, процеси регулювання трафіку, превентивного захисту, виявлення і усунення прогалин в системі безпеки.

Регулювання трафіку з метою запобігання атак типу «відмова в обслуговуванні (DoS)», виконується службою Gmail, що відстежує базові показники використання і регулює стандартні сплески трафіку таким чином, щоб це не позначалося на роботі користувачів. Трафік регулюється з того моменту, коли він перевищив стандартні показники, і до тих пір, поки використання не нормалізується.

Превентивний захист, як оборонна стратегія, спрямований на прогнозування і проактивний захист від вторгнень та вимагає постійного вдосконалення вбудованих засобів безпеки: сканування портів і усунення виявлених проблем, виявлення вразливостей периметра, оновлення операційних систем для інсталяції актуальних версій засобів забезпечення безпеки, виявлення і запобігання розподілених атак типу «відмова в обслуговуванні» (DDOS), а також багатофакторну аутентифікацію при наданні доступу до служби.

У G Suite Enterprise триває розвиток автоматизованих систем, які дозволяють виявляти аномальну і підозрілу поведінку і миттєво реагувати на неї з метою усунення ризику безпеки. Компанія Google постійно удосконалює високоефективні системи автоматичного розгортання виправлень, які вирішують проблеми, виявлені системами моніторингу, без втручання людини. Це значно підвищує рівень безпеки і гнучкість служби. У G Suite Enterprise проводяться тести на захист від несанкціонованого доступу, мета яких – постійне поліпшення процедур реагування на інциденти. Результати цих тестів дають фахівцям з безпеки можливість створювати систематизовані, повторювані і оптимізовані покрокові процеси реагування на інциденти і автоматизувати ці процеси.

2.2.2 Безпека на рівні споживача.

Кожна служба пропонує індивідуалізовані функції безпеки, якими управляє клієнт. Елементи управління дозволяють забезпечувати відповідність нормативним вимогам, надавати співробітникам організацій доступ до служб і контенту, налаштовувати захист від спаму і шкідливих програм, а також шифрувати дані за допомогою ключа.

Додатково до описаних надійних функцій шифрування в G Suite Enterprise забезпечуються необхідною гнучкістю при виборі елементів, які потрібно зашифрувати. Включивши спеціалізовані служби шифрування G Suite Enterprise, споживач отримує можливість шифрувати електронну

переписку з користувачами поза підприємством. Адміністратори можуть задавати алгоритми шифрування для шифрування і підписування документів.

G Suite Enterprise Message Encryption забезпечує конфіденційні бізнес-зв'язки з підвищеною безпекою, що дозволяє користувачам надсилати та отримувати зашифровані електронні листи так само легко, як і звичайний електронний лист безпосередньо з їх настільних комп'ютерів. Електронна пошта може бути зашифрована без придбання складного обладнання та програмного забезпечення, налаштування або підтримки, що допомагає мінімізувати капіталовкладення, звільнити IT-ресурси та пом'якшити ризики обміну повідомленнями. Електронну пошту можна надіслати на будь-яку електронну адресу в Інтернеті, включаючи такі популярні сервіси як outlook.com, Yahoo! та Gmail [33].

Впровадження та захист даних із Gmail Message Encryption усуває загрози, які можуть виникнути через різні форми цифрового перехоплення. Це вірно для електронних листів, що надсилаються всередині та зовні компанії. У той же час будь-який необґрунтований доступ до електронних повідомлень запобігається через політику, властиву самим повідомленням електронної пошти. Це пом'якшує ризик втрати даних як свідомо, так і несвідомо, і забезпечує можливість запобігання втратам даних.

Коли користувач Gmail надсилає повідомлення електронної пошти, яке відповідає правилу шифрування, повідомлення надсилається HTML-вкладенням. Одержувач відкриває вкладення HTML у повідомленні електронної пошти, та виконує вставлені вказівки для входу, відкриття та читання зашифрованого повідомлення на порталі G Suite Enterprise Message Encryption. Процес входу допомагає забезпечити, щоб лише передбачувані одержувачі могли переглядати зашифровані повідомлення.

Наступна схема зображує робочий цикл, за допомогою якого служба шифрування повідомлень О захищає зашифровані електронні листи від сторонніх користувачів, одночасно забезпечуючи простий доступ для вповноважених одержувачів.:

Добавлено примечание ([ФСВ9]):

Добавлено примечание ([ФСВ10R9]):

1) Користувач Gmail надсилає повідомлення одержувачу.

2) Повідомлення фільтрується на основі правил, визначених адміністратором, які визначають умови для шифрування.

3) Повідомлення зашифровано за допомогою Google Message Encryption.

4) Зашифроване повідомлення доставляється в папку "Вхідні" одержувача.

5) Одержувач відкриває вкладення HTML та підключається до порталу шифрування Google Message Encryption

6) Одержувач виконує перевірку автентичності шляхом входу чи вводу одноразового паролю.

7) Повідомлення розшифровано. Отримувач переглядає повідомлення та відправляє відповідь у шифрованому вигляді.

Наочно, це проілюстровано на рисунку 2.5.

Зміст і послуги G Suite Enterprise захищаються на рівні центру обробки даних, рівні зберігання та передачі. Поряд з цим важливо розуміти, які користувачі отримують доступ до даних і які операції можуть виконувати. Тому клієнти G Suite Enterprise, яким необхідні методи суворої аутентифікації, отримують можливість ретельно контролювати доступ і використання служби IT-фахівцями та кінцевими користувачами.

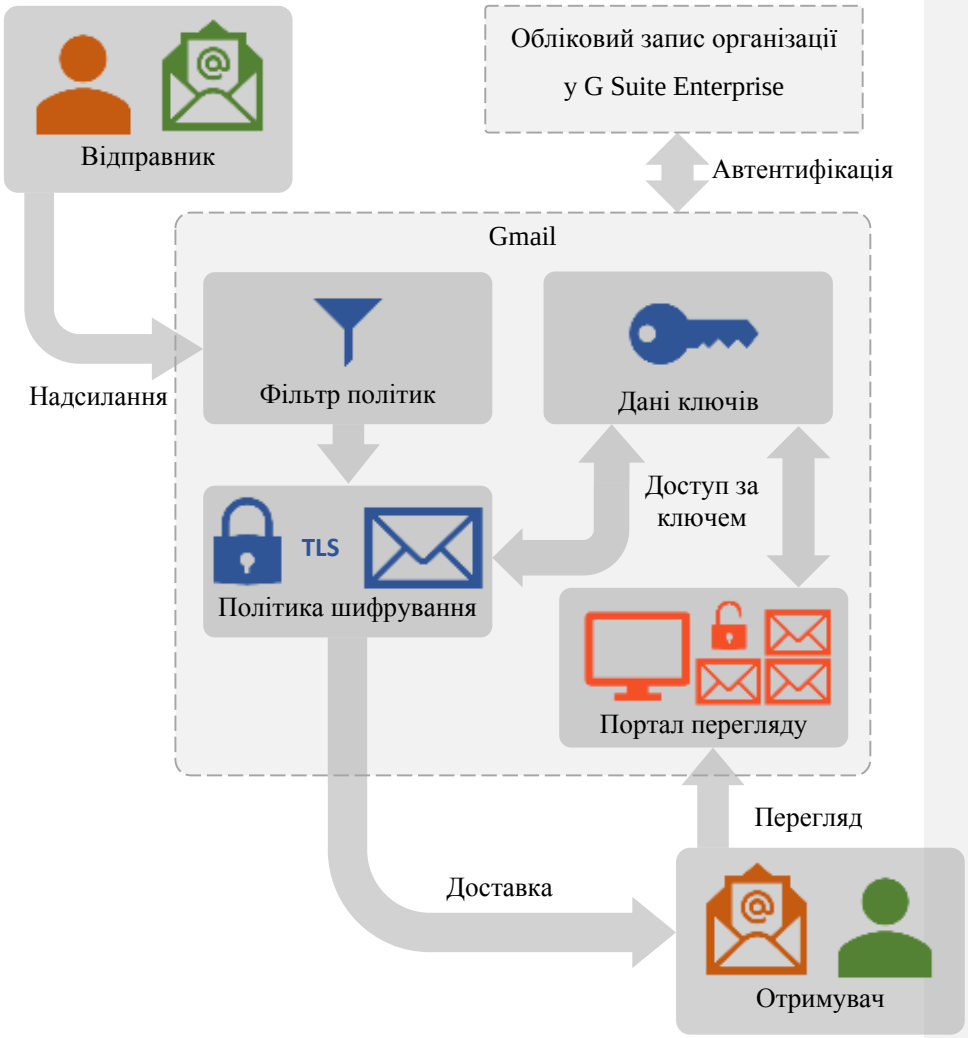

Рисунок 2.5 – Схема робочого циклу шифрування повідомлень у G Suite Enterprise

Адміністратори можуть створювати додаткові механізми аутентифікації, наприклад:

– Двофакторну перевірку автентичності;

– спосіб управління доступом з боку клієнта, що дозволяє організаціям контролювати, як користувачі будуть отримувати доступ до інформації з різних пристроїв або з різних місць, або з урахуванням цих двох

чинників (наприклад, обмеження доступу з загальнодоступних комп'ютерів або через публічні мережі Wi-Fi);

– контроль доступу на основі ролей.

Двофакторна перевірка справжності підвищує рівень безпеки в середовищі з безліччю пристроїв, орієнтованої на хмарні технології. Компанія Google пропонує рішення для двухфакторной перевірки автентичності з можливістю аутентифікації по телефону, а також підтримує рішення сторонніх розробників. При двофакторній перевірці автентичності з використанням телефону користувач отримує ПІН-код у смс-повідомленні чи голосовому виклику і вводить його в якості другого пароля при вході в службу [32].

G Suite Enterprise пропонує ряд функцій відповідності нормативним вимогам: запобігання втрати даних (DLP), виявлення електронних даних (eDiscovery), а також інструменти проведення аудиту і звітності. Все більше користувачів використовують ці можливості, оскільки вони прості і не впливають на продуктивність [34].

Шкідливі програми і атаки можуть організувати діри в системі безпеки, однак набагато більші ризики в багатьох організаціях пов'язані з помилками користувачів. Gmail використовує технологію запобігання втрати даних (DLP), за допомогою якої здійснюється ідентифікація, моніторинг і захист конфіденційних даних. Ця технологія дозволяє виявляти ризики для даних і керувати ними. За допомогою технології DLP можна виявити конфіденційну інформацію в електронному повідомленні, наприклад номер соціального страхування або кредитної картки, і попередити користувача за допомогою повідомлення перш, ніж він відправить подібний лист. У розпорядження адміністраторів наданий широкий спектр функцій управління, що дозволяють встановлювати обмеження у всій організації.

Наприклад, можна просто попередити користувача про те, він збирається переслати конфіденційні дані, можна змусити користувача пройти авторизацію перед відправкою або заблокувати відправку. Функція DLP

дозволяють переглядати повідомлення та вкладення, а також формувати докладні звіти про те, які дані відправляються і ким.

Політика захисту від втрати даних визначає наступне:

1) де потрібно захищати контент);

2) коли і як захищати дані за допомогою правил, що складаються з наступних елементів:

– умови застосування правила до контенту (наприклад, пошук тільки контенту з номерами соціального страхування, доступ до якого відкритий для користувачів не з вашої організації);

– дії, які зазвичай автоматично застосовує при виявленні контенту, відповідного заданим умовам (наприклад, блокування доступу до документа і відправка електронного повідомлення користувачу і співробітникові, відповідальному за забезпечення відповідності вимогам).

Наприклад, можна створити політику захисту від втрати даних, яка допомагає знаходити інформацію, що потрапляє під дію акта про передачу і захисту даних установ охорони здоров'я (HIPAA). Ця політика допоможе захистити дані HIPAA на всіх сайтах Google Sites і Google Диск), виявляючи всі документи з подібною конфіденційною інформацією, доступ до яких надано користувачам не з вашої організації (умови), а потім блокуючи доступ до цього документа і відправляючи повідомлення (дії). Ці вимоги зберігаються у вигляді окремих правил і групуються в політику захисту від втрати даних, щоб спростити управління і створення звітів.

Політика захисту від втрати даних може знаходити і захищати конфіденційну інформацію в G Suite Enterprise незалежно від того, чи зберігається ця інформація в Gmail, Google Sites або у Google Диск. Споживач може налаштувати захист для всіх сайтів і поштових скриньок або тільки для деяких з них.

Правила застосовують вимоги підприємства до даних, що зберігаються. Політика містить одне або кілька правил, а кожне правило складається з умов і дій. При дотриманні заданих умов дії правила виконуються автоматично.

Правила в кожній політиці застосовуються послідовно починаючи з найпріоритетніших.

Правила також дозволяють повідомляти користувачів (за допомогою підказок політик і по електронній пошті) і адміністраторів (за допомогою звітів про інциденти, що відправляються по електронній пошті) про те, що той чи інший елемент контенту потрапив під дію правила.

Умови визначають, до яких типів даних буде застосовано дію. Наприклад, можна виключити з пошуку елементи контенту з номерами паспортів, що містять десять або менше таких номерів і доступні людям за межами організації.

Умови пов'язані з контентом, наприклад з важливими типами конфіденційної інформації, а також контекстом, таким як користувачі, яким надано доступ до документа. За допомогою умов можна призначати різні дії для різних рівнів ризику. Наприклад, обмін конфіденційними даними всередині організації представляє менший ризик і вимагає менше дій, ніж надання доступу до них людям за її межами.

Кожен тип конфіденційних даних визначається за допомогою таких методів:

- ключові слова;
- внутрішні функції для перевірки контрольних сум або структури;
- оцінка регулярних виразів для виявлення збігів з шаблонами;
- аналіз іншого вмісту.

Це допомагає забезпечити високу точність і знизити кількість помилкових спрацьовувань, які можуть перешкодити роботі співробітників.

Якщо вміст відповідає умові правила, застосовуються дії, щоб автоматично захистити документ або контент.

Доступні такі дії:

1) Блокування доступу до контенту. В контексті вмісту сайту це означає блокування доступу до документа для всіх користувачів, крім головного адміністратора групи веб-сайтів, власника документа і користувача,

який вніс останню зміну. Ці користувачі можуть видалити конфіденційні відомості з документа або виконати інші дії. Коли документ знову буде відповідати вимогам, вихідні дозволи будуть відновлені автоматично. При блокуванні доступу документ відображається в бібліотеці на сайті зі спеціальним значком підказки політики.

Для електронної пошти це дія забороняє відправку відповідного повідомлення. Залежно від того, як налаштоване правило захисту від втрати даних, відправник отримає звіт про не доставлення або (якщо в правилі налаштоване повідомлення) підказку політики та / або повідомлення по електронній пошті.

2) Сповіщення та перевизначення користувачів. За допомогою сповіщень і перевизначень можна розповісти користувачам про політиків захисту від втрати даних і про те, що відповідність вимогам не буде заважати їх роботі. Наприклад, якщо користувач намагається надати доступ до документа, який містить конфіденційну інформацію, політика захисту від втрати даних може як відправити йому повідомлення по електронній пошті, так і вивести в контексті бібліотеки документів підказку, яка дозволяє перевизначити політику при наявності вагомої ділової причини.

Повідомлення електронної пошти може містити повідомлення для користувача, який відправив контент, поділився ним або вніс в нього останні зміни. Якщо мова йде про вміст сайту, повідомлення також може бути відправлено головному адміністратору групи веб-сайтів і власнику документа. Крім того, є можливість додати в повідомлення електронної пошти потрібних одержувачів або видалити їх звідти.

3) Звіти про інциденти. У разі збігу з правилом відправляється звіт з докладними відомостями про інцидент особи, відповідальної за відповідність вимогам (або будь-якого іншого користувача). Звіт містить інформацію про об'єкт, який потрапив під дію правила, фактичне елементі контенту, а також імені користувача, яким останнім вносив до нього зміни. Для повідомлень

електронної пошти звіт також містить у вигляді вкладення вихідне повідомлення, для якого спрацювала політика захисту від втрати даних.

При створенні політики захисту від втрати даних спочатку потрібно зрозуміти, яким даним потрібно забезпечити безпеку. Можна використати в якості основи шаблон, щоб не створювати новий набір правил з нуля і не з'ясовувати, які типи інформації повинні бути включені за замовчуванням. Потім можна додати або змінити ці вимоги для точної настройки правила відповідно до вимог організації.

Заздалегідь настроєний шаблон політики допоможе виявляти певні типи конфіденційної інформації або навіть персональні дані для конкретного регіону. Щоб спростити пошук і захист поширених типів конфіденційної інформації, включені в G Suite Enterprise шаблони політик вже містять найпоширеніші типи конфіденційної інформації, необхідні для початку роботи.

Політику захисту від втрати даних можна в будь-який момент відключити. При цьому будуть відключені всі містяться в ній правила. Крім того, кожне з них можна відключити окремо, змінивши його статус у редакторі.

Після створення і включення політик захисту від втрати даних потрібно переконатися, що вони працюють за планом і допомагають забезпечувати відповідність вимогам. Звіти політики захисту від втрати даних дозволяють швидко переглянути число збігів з політиками і правилами, а також кількість помилкових спрацьовувань і перевизначень. Для кожного звіту можна відфільтрувати збіги по розташуванню, часовому інтервалу або за конкретною політикою, правилом або дією.

За допомогою звітів захисту від втрати даних можна отримати важливі дані, а також:

– зосередитися на певних періодах часу і визначити причини стрибків і тенденцій;

– виявити бізнес-процеси, які порушують політики відповідності вимогам вашої організації;

– визначити вплив політик захисту від втрати даних на роботу організації.

Документи на всіх сайтах Google Sites або у Google Диск постійно змінюються – їх безперервно створюють, редагують, спільно використовують, переміщують тощо. Це означає, що документи в будь-який момент можуть порушити політику захисту від втрати даних або знову почати відповідати їй. Користувач може викласти на сайт групи документ, який не містить конфіденційної інформації, але потім інший співробітник може змінити цей файл і додати в нього такі відомості.

З цієї причини політики захисту від втрати даних регулярно перевіряють документи на збіги з політиками в фоновому режимі. Це можна представити як асинхронну оцінку політики.

У міру того як користувачі додають або редагують документи на своїх сайтах, пошукова система сканує вміст, щоб його можна було знайти пізніше. В цей час вміст також сканується на предмет наявності конфіденційної інформації та наданого до нього доступу. Всі знайдені конфіденційні відомості безпечно зберігаються в індексі пошуку, щоб вони були доступні тільки команді відповідності вимогам, а не звичайним користувачам. Кожна включена політика захисту від втрати даних працює у фоновому режимі – асинхронно, регулярно перевіряючи вміст на збіги з політикою і застосовуючи дії для захисту цих відомостей від ненавмисного розголошення [35].

Нарешті, документи можуть не тільки порушити політику захисту від втрати даних, але і знову почати відповідати їй. Якщо користувач додає в документ конфіденційну інформацію, політика захисту від втрати даних може автоматично заблокувати доступ до документа. Але якщо потім користувач видалить конфіденційну інформацію, застосоване раніше дію буде скасовано при наступній оцінці політики.

Політики аудиту G Suite Enterprise дають клієнтам можливість реєструвати в журналі такі події, як перегляд, редагування та видалення вмісту електронних повідомлень, документів, списків завдань, списків проблем, дискусійних груп і календарів подій. При включенні аудиту до складу політики управління інформацією адміністратори можуть отримувати дані аудиту і узагальнювати використання інформації. За допомогою цих звітів можна буде визначити, як використовується інформація, управляти відповідністю нормативним вимогам і аналізувати проблемні області.

Звіти журналу аудиту можна використовувати, щоб переглянути дані в журналів аудиту для колекції сайтів. Можна сортувати, фільтрувати й аналізувати дані для визначення користувачів, які отримали доступ до сайтів, списки, бібліотеки, типи вмісту, елементи списків і файлів бібліотеки в колекції сайтів. Наприклад, можна визначити, який вміст видалено.

Відомості про те, хто виконував певні дії із вмістом у колекції сайтів, можуть мати критично важливе значення для виконання організацією вимог, таких як дотримання правових норм і керування записами.

Події, доступні у звітах журналу аудиту у Google Sites:

- редагування й завантаження документів, перегляд елементів у списках або перегляд властивостей елемента
- редагування елементів;
- узяття файлів на редагування та повернення їх із редагування;
- переміщення та копіювання елементів в інше розташування в колекції сайтів;
- видалення й відновлення елементів;
- зміни типів вмісту та стовпців;
- запити пошуку;
- зміни облікових записів і дозволів користувачів;
- зміни настройок аудиту та видалення подій журналу аудиту;
- події робочих циклів;

– налаштовані події [37].

Підприємству може бути потрібно зберігати або архівувати вміст, включаючи повідомлення електронної пошти, вкладення і документи, протягом певного періоду часу для виконання ділових, юридичних або нормативних вимог. При наявності обгрунтованих передумов для судових позовів організаціям потрібно зберігати електронні дані (включаючи пошту), пов'язані зі справою, з метою виявлення електронних даних. Якщо необхідно зберігати тільки вміст поштових скриньок, можна використовувати зберігання на місці або зберігання для судового розгляду. Щоб зберігати вміст поштових скриньок і контент на сайтах Google Sites і Google Диск, використовується центр виявлення електронних даних в G Suite Enterprise. Щоб зберегти весь вміст в організації, включаючи вміст поштових скриньок, загальних папок і сайтів, використовуються політики збереження, які можна створювати і контролювати за допомогою Центру відповідності вимогам G Suite Enterprise

Добавлено примечание ([ФСВ11]): 17 -31. Устал!

Залежно від політики організації щодо виявлення електронних даних, можна вжити таких заходів щодо збереження електронної пошти:

– користувачам можна порекомендувати зберігати пошту, не видаляючи повідомлення. Однак користувачі все ж можуть видаляти електронну пошту навмисно або випадково.

– можуть бути припинені механізми автоматичного видалення, наприклад управління записами обміну повідомленнями. Це може привести до того, що в поштових скриньках користувачів буде накопичуватися великий обсяг електронної пошти, через що продуктивність їх роботи може знижуватися. Призупинення автоматичного видалення також не заважає користувачам вручну видаляти електронну пошту.

– у деяких організаціях електронна пошта копіюється або переміщається в архів, що дозволяє запобігти її видалення, зміни або підміни. Це веде до підвищення витрат, обумовлених необхідністю ручного копіювання або переміщення повідомлень в архів або впровадження сторонніх продуктів для збору і зберігання електронної пошти поза Exchange.

Відсутність можливості зберігання електронного листування може піддати організацію юридичним і фінансовим ризикам, наприклад до критичного аналізу процесів виявлення та зберігання записів в організації, несприятливим остаточним рішенням, санкцій або штрафів. За допомогою зберігання на місці і зберігання для судового розгляду можна вирішувати такі завдання:

– поміщати поштові скриньки користувачів на зберігання і зберігати їх елементи без змін.

– зберігати елементи поштових скриньок, віддалені вручну або автоматично, наприклад службою управління записами повідомлень.

– використовувати зберігання на місці на основі запитів для пошуку і зберігання елементів, які відповідають певним умовам.

– зберігати елементи нескінченно або протягом заданого періоду часу.

– встановлювати кілька заборон на видалення для різних справ або розслідувань.

– приховувати заборони на видалення від користувача, так як робота служби управління записами повідомлень не переривається.

– включати пошук з виявленням електронних даних на місці для елементів, поміщених на зберігання.

Якщо поштова скринька користувача поміщається на зберігання на місці або зберігання для судового розгляду, а відповідна обліковий запис G Suite видаляється, поштовий ящик стає неактивним, тобто видаленим з можливістю відновлення. У неактивних поштових скриньках можна зберігати вміст поштових скриньок користувачів після їх звільнення з організації. Елементи в неактивному поштовій скриньці зберігаються протягом всього терміну зберігання, який був заданий до того, як ящик став неактивним. Це дозволяє адміністраторам, співробітникам, відповідальним за забезпечення відповідності вимогам, і співробітникам, керуючим записами, використовувати функцію виявлення електронних даних на місці, щоб

отримати доступ до вмісту неактивного поштової скриньки і пошуку в ньому. Неактивні поштові ящики не можуть отримувати електронну пошту і не відображаються у спільній адресній книзі організації та інших списках.

2.3 Побудова моделі загроз

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів. Впливи, які призводять до зниження цінності інформаційних ресурсів, називаються несприятливими. Потенційно можливий несприятливий вплив називається загрозою [42].

Автоматизована система являє собою організаційно-технічну систему, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію. Прийнято розрізняти два основних напрями захисту інформації в автоматизованій системі – це захист автоматизованої системи і оброблюваної інформації від несанкціонованого доступу і захист інформації від витоку технічними каналами: оптичними, акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наводів.

Захист інформації, що обробляється в автоматизованій системі, полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації і автоматизованої системи в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і автоматизованої системи, що її обробляє.

Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно автоматизованої системи і повинні враховуватись у моделі загроз, наприклад:

– зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів автоматизованої системи;

– наслідки помилок під час проектування та розробки компонентів автоматизованої системи (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) автоматизованої системи під час експлуатації;

– навмисні дії (спроби) потенційних порушників [43].

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

– дії, що призводять до відмови автоматизованої системи (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи автоматизованої системи (окремих компонентів, обладнання, програмного забезпечення тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

– неумисне зараження програмного забезпечення комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в автоматизованій системі розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження і використання забороненого політикою безпеки програмного забезпечення (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

– наслідки некомпетентного застосування засобів захисту;

– інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи автоматизованої системи (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

– порушення фізичної цілісності автоматизованої системи (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення автоматизованої системи (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);

– порушення режимів функціонування автоматизованої системи (обладнання і програмного забезпечення);

– впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу автоматизованої системи;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам’яті, зовнішніх накопичувачів;

– одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;

– неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, аналіз трафіку тощо;

– впровадження і використання забороненого політикою безпеки програмного забезпечення або несанкціоноване використання програмного забезпечення, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

– інші.

Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів обчислювальної системи, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози називається атакою.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані: конфіденційності, цілісності та доступності інформації, а також порушення спостережності та керованості автоматизованої системи.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації або видалення. Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного проміжку часу. Автоматизована система зберігає спостережність, якщо зберігається можливість фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою

запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії [43].

Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації.

Розглянемо згідно з завданнями роботи була розроблена модель потенційних загроз інформації, що обробляється за допомогою хмарних технологій (таблиця 2.5).

Таблиця 2.5 – Потенційні загрози інформації, що обробляється за допомогою хмарних технологій.

Джерело	Природа	Загроза	Наслідки порушення	Вразливість
Зовнішнє стихійне	Об’єктивна	Стихійні явища	ЦД	Стихійні явища
Зовнішнє техногенне	Об’єктивна	Збої та відмови системи електроживлення	ЦД	Техногенні аварії. Диверсія.
Внутрішнє техногенне	Об’єктивна	Збої та відмови апаратних ресурсів центру обробки даних	ЦД	Порушення умов експлуатації. Диверсія.
Внутрішнє техногенне	Об’єктивна	Збої, відмови та пошкодження носіїв інформації центру обробки даних	ЦД	Порушення умов експлуатації. Диверсія.

Внутрішнє техногенне	Об’єктивна	Збої та відмови програмного забезпечення	ЦД	Впровадження нової версії програмного забезпечення. Халатність та помилки при тестуванні нового програмного забезпечення.

Продовження табл. 2.5

Джерело	Природа	Загроза	Наслідки порушення	Вразливість
Внутрішнє техногенне	Об’єктивна	Відмова в доступі санкціонованому користувачу в результаті помилки у програмному забезпеченні	Д	Впровадження нової версії програмного забезпечення. Халатність та помилки при тестуванні нового програмного забезпечення.
Зовнішнє антропогенне	Суб’єктивна (Навмисна/ ненавмисна)	Ураження програмного забезпечення комп’ютерними вірусами	КЦД С	Помилки при налаштуванні антивірусного програмного забезпечення.
Внутрішнє антропогенне	Суб’єктивна (Навмисна/ ненавмисна)	Несанкціоноване внесення змін до технічних засобів, в програмне забезпечення, що призводять до зміни режиму роботи чи відмови	КЦД С	Службова недбалість. Диверсія.
Внутрішнє антропогенне	Суб’єктивна (Навмисна/ ненавмисна)	Порушення адміністратором безпеки реалізації розмежування доступу	КЦД С	Помилка адміністратора. Диверсія.
Внутрішнє антропогенне	Суб’єктивна (Ненавмисна)	Втрата атрибутів розмежування доступу	КЦД	Помилка адміністратора.

Продовження табл. 2.5

Джерело	Природа	Загроза	Наслідки порушення	Вразливість
Внутрішнє антропогенне	Суб'єктивна (Навмисна)	Неправомірне впровадження і використання забороненого програмного забезпечення	КЦД С	Диверсія. Недосконаліть механізмів розмежування доступу.
Зовнішнє антропогенне	Суб'єктивна (Навмисна)	Використання з корисливою метою персоналу центру обробки даних	КЦД С	Вербування працівників центру обробки даних.
Зовнішнє антропогенне	Суб'єктивна (Навмисна)	Несанкціонований доступ до приміщення центру обробки даних	КЦД С	Порушення процедури надання допусків на виконання необхідних робіт. Вербування працівників центру обробки даних.
Зовнішнє антропогенне	Суб'єктивна (Навмисна)	Вербування працівників закладу	КЦД С	Шантаж. Залякування.
Зовнішнє / Внутрішнє антропогенне	Суб'єктивна (Навмисна)	Розкрадання матеріальних носіїв інформації	КЦ	Порушення процедури надання допусків на виконання необхідних робіт. Халатність локальної служби безпеки.

Продовження табл. 2.5

Джерело	Природа	Загроза	Наслідки порушення	Вразливість
Внутрішнє антропогенне	Суб'єктивна (Ненавмисна)	Ненавмисне псування матеріальних носіїв інформації	Д	Порушення процедури надання допусків на виконання робіт. Недостатня кваліфікація персоналу.
Зовнішнє техногенне	Суб'єктивна (Навмисна)	Розвідка, аналіз трафіка	КЦД	Перехоплення інформації, що пересилається. Збої у роботі механізмів забезпечення шифрування.
Зовнішнє техногенне	Суб'єктивна (Навмисна)	Підміна (імітація) центру обробки даних із підробкою мережних адрес тих об'єктів, що атакують	КЦД	Фальсифікація (підробка мережних адрес IP-адреси, повторне відтворення повідомлень, недостатня ідентифікація та автентифікація)
Зовнішнє техногенне	Суб'єктивна (Навмисна)	Підміна маршруту до центру обробки даних	КЦД	Зміна параметрів маршрутизації й змісту інформації, що передається, внаслідок збою у роботі програмного забезпечення контролю за маршрутом повідомлень чи фільтрації пакетів.

Продовження табл. 2.5

Джерело	Природа	Загроза	Наслідки порушення	Вразливість
Зовнішнє техногенне	Суб’єктивна (Навмисна)	Читання залишкової інформації із оперативної пам'яті із зовнішніх запам'ятовуючих пристроїв	К	Збої у роботі програмного забезпечення віртуалізації серверів
Зовнішнє антропогенне	Суб’єктивна (Ненавмисна)	Вилучення серверів з центру обробки даних представниками спецслужб	КЦД С	Зберігання забороненої інформації на серверах
Зовнішнє антропогенне	Суб’єктивна (Ненавмисна)	Неавторизоване переглядання документів на пристрої віддаленого чи мобільного співробітника	К	Втрата чи викрадення мобільного пристрою

2.4 Побудова моделі порушника

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної автоматизованої системи.

Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце тощо. По відношенню до автоматизованої системи порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони) [43].

Модель порушника повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності для автоматизованої системи;

– категорії осіб, з числа яких може бути порушник.;

– припущення про кваліфікацію порушника;

– припущення про характер його дій.

Метою порушника можуть бути:

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами автоматизованої системи, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– перший рівень визначає найнижчий рівень можливостей ведення діалогу з автоматизованій системі – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням автоматизованої системи, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення автоматизованої системи, аж до включення до складу автоматизованої системи власних засобів з новими функціями обробки інформації.

За рівнем знань про автоматизовану систему усіх порушників можна класифікувати як таких, що:

– володіють інформацією про функціональні особливості автоматизованої системи, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації автоматизованої системи;

– володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

– використовують виключно агентурні методи одержання відомостей;

– використовують пасивні технічні засоби перехоплення інформаційних сигналів;

– використовують виключно штатні засоби автоматизованої системи або недоліки проектування для реалізації спроб несанкціонованого доступу;

– використовують способи і засоби активного впливу на автоматизовану систему, що змінюють конфігурацію системи (підключення

додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального програмного засобу тощо).

За місцем здійснення дії можуть класифікуватись:

– без одержання доступу на контрольовану територію організації;

– з одержанням доступу на контрольовану територію, але без доступу до технічних засобів автоматизованої системи;

– з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів автоматизованої системи;

– з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, відповідних адміністраторів тощо);

– з одержанням доступу до засобів адміністрування автоматизованою системою.

2.5 Функціональні профілі захищеності від несанкціонованого доступу для захисту інформації, що реалізують різні компоненти хмарної служби G Suite Enterprise

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації.

Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів:

– загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності.

– загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності.

– загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності.

– ідентифікація і контроль за діями користувачів, керованість становлять предмет послуг спостереженості і керованості.

Розглянемо функціональні послуги безпеки, що реалізують різні компоненти хмарної служби G Suite Enterprise(таблиця 2.6)

Таблиця 2.6 – Функціональні послуги безпеки, що реалізують різні компоненти хмарної служби G Suite Enterprise.

Компоненти хмарної служби G Suite Enterprise	Функціональні послуги безпеки
Корпоративний Gmail	КД-2, КА-2, КВ-2, ЦД-1, ЦО-2, ДР-2, ДС-2, ДВ-2, НР-3, НИ-3, НО-2, НЦ-1
Google Sites	КД-2, КА-2, КВ-2, ЦД-1, ЦА-1, ЦО-2, ДР-2, ДС-2, ДВ-2, НР-2, НИ-3, НО-3, НЦ-1
Google Диск	КД-2, КА-2, КВ-2, ЦД-1, ЦА-1, ЦО-2, ДР-2, ДС-2, ДВ-2, НР-1, НИ-3, НО-2, НЦ-1

Skype для бізнесу Online	КД-2, КА-2, КВ-2, ЦД-1, ДС-2, ДВ-2, НР-1, НИ-3, НО-2, НЦ-1, НВ-1
Google Документи	КД-2, КА-2, КВ-2, ЦО-1, ДЗ-1, ДВ-2, НР-2, НИ-3, НО-1, НЦ-1

Опис вимог до функціональних послуги безпеки, що реалізує комплекс засобів захисту (КЗЗ) різних компонентів хмарної служби G Suite Enterprise:

1) Критерії конфіденційності:

– КД-2. Базова довірча конфіденційність. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

– КА-2. Базова адміністративна конфіденційність. Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і

захищеного об'єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

– КВ-2. Базова конфіденційність при обміні. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається. Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження. Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

2) Критерії цілісності:

– ЦД-1. Мінімальна довірча цілісність. Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

– ЦА-1. Мінімальна адміністративна цілісність. Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

– ЦО-1. Обмежений відкат. Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу

або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

– ЦО-2. Повний відкат. Доповнює рівень ЦО-1 можливістю авторизованому користувачу або процесу відкатити або відмінити всі операції, виконані над захищеним об'єктом за певний проміжок часу.

3) Критерії доступності:

– ДР-2. Недопущення захоплення ресурсів. Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів КС. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу і довільним групам користувачів. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку окремого користувача і довільних груп користувачів.

– ДС-3. Стійкість без погіршення характеристик обслуговування. Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів системи. Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги. Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування. КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента.

– ДЗ-1. Модернізація. Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації системи. Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію. Модернізація не повинна призводити до

необхідності ще раз проводити інсталяцію програмного забезпечення або до переривання виконання КЗЗ функцій захисту.

– ДВ-2. Автоматизоване відновлення. Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція. Після відмови або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ має бути здатним виконати їх і повернути службу до нормального функціонування. Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести службу до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути службу до нормального функціонування.

4) Критерії спостереженості:

– НР-1. Зовнішній аналіз. Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події.

– Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту.

– НР-2. Захищений журнал. Доповнює рівень НР-1. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані

відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

– НР-3. Сигналізація про небезпеку. Доповнює рівень НР-2. КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій

– НИ-1. Зовнішня ідентифікація і автентифікація. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.

– НИ-3. Множинна ідентифікація і автентифікація. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищених механізмів двох або більше типів. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

– НО-1. Виділення адміністратора. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

– НО-2. Розподіл обов'язків адміністраторів. Доповнює рівень НО-1. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

– НО-3. Розподіл обов'язків на підставі привілеїв. Доповнює рівень НО-2. Політика розподілу обов'язків повинна визначати множину ролей користувачів.

– НЦ-1. КЗЗ з контролем цілісності. Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ. В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести службу до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

– НВ-1: Автентифікація вузла. Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

Висновки до другого розділу

G Suite Enterprise може ефективно використовуватися організаціями, які є представниками практично будь-якій галузі, в тому числі із суворим нормативним регулюванням.

Оскільки G Suite Enterprise побудовано на моделі обслуговування SaaS, то корпорація Google контролює і захищає інфраструктуру, операційні системи вузлів і додатки та забезпечує захист даних в центрах обробки даних, а також при передачі між центром обробки даних і клієнтом.

На клієнта покладається керування доступом, забезпечення захисту своїх автентифікаційних даних, в тому числі налаштовує набір доступних додатків, що доступні в хмарній службі.

У свою чергу корпорація Google гарантує:

1) Конфіденційність. Google не сканує дані споживачів з метою створення рекламних кампаній чи аналізу. Дані споживачів не змішуються, а зберігаються окремо. Споживач може у будь-який час повністю видалити свої дані.

2) Прозорість. Споживачу відкрита інформація про те, де саме зберігається його інформація, а також хто має доступ до його даних і на якому рівні. Клієнти завжди отримують інформацію про зміни у питаннях безпеки та конфіденційності даних.

3) Безпека. Цілодобовий контроль за центрами обробки даних. Логічна ізоляція даних споживача. Суворе дотримання розділення внутрішньої обробки даних у центрі обробки даних від зовнішніх мереж. Шифрування при збереженні та передачі даних. Безпечний доступ через ідентифікацію. Захист від втрати даних. Антивірус та захист від спаму.

4) Безперервність. Центри обробки даних доступні 99,9% часу. Фінансові гарантії. Резервування ресурсів. Автоматизовані системи контролю та відновлення. Цілодобова підтримка клієнтів.

Корпорація Google рекомендує розробити політики оцінки, прийняття і використання хмарних служб, щоб звести до мінімуму виникнення невідповідностей і вразливостей, якими можуть скористатися зловмисники. Споживачу потрібно переконатися, що в організації оновлені і впроваджені політики управління даними і безпеки:

- політики щодо посвідчень;
- політики щодо даних;
- політики щодо відповідності вимогам і документації.

РОЗДІЛ 3.
ВИЗНАЧЕННЯ ВИТРАТ НА ВПРОВАДЖЕННЯ G SUITE ENTERPRISEНА ПІДПРИЄМСТВІ У ПОРІВНЯННІ З ЛОКАЛЬНОЮ ІНФРАСТРУКТУРОЮ

3.1 Розрахунок поточних витрат на впровадження G Suite Enterprise на підприємстві.

Впровадження на підприємстві G Suite Enterprise дозволяє уникнути капітальних витрат на відповідне апаратне і програмне забезпечення, оскільки все необхідне апаратне і програмне забезпечення надається корпорацією Google в оренду на умовах місячної або річної підписки на відповідні пакети сервісів.

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

За методикою Gartner Group до поточних (експлуатаційних) варто відносити наступні витрати:

- вартість Upgrade-відновлення й модернізації системи ($С_в$);
- витрати на керування системою в цілому ($С_к$);
- витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ – "активність користувача").

Під "витратами на керування системою" маються на увазі витрати, пов'язані з керуванням і адмініструванням серверів та інших компонентів сервісів G Suite Enterprise. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата обслуговуючого персоналу;
- аутсорсинг (тобто залучення сторонніх організацій для виконання деяких видів обслуговування);
- навчальні курси й сертифікація обслуговуючого персоналу;

– технічне й організаційне адміністрування й сервіс.

Вартість забезпечення роботи користувача відбита в понятті "активність користувача". За даними аналітичних компаній, основні фактори, що впливають на підсумкову вартість володіння інформаційними технологіями, на 75% обумовлені проблемами кінцевого користувача. Ця стаття витрат, за даними Gartner Group, має найбільшу вагу в сукупній вартості системи інформаційної безпеки. У ній виділяють наступні під статті витрат:

– пряма допомога й додаткові настроювання;
– формальне навчання;
– розробка додатків;
– робота з даними;
– неформальне навчання;
– futz-фактор (параметр, що визначає обсяг витрат, пов'язаних з наслідками некомпетентних дій користувача). Ці витрати зв'язані, наприклад, з участю адміністратора в налагодженні робочої станції, з наданням допомоги користувачеві або з консультаціями.

У загальному випадку поточні (експлуатаційні) витрати розраховуються за формулою:

$$C = C_в + C_к + C_{ак}\text{ , грн.} \quad (3.1)$$

де, $C_в$ – витрати на Upgrade-відновлення й модернізацію системи хмарних обчислень;

$C_к$ – витрати на керування хмарною системою;

$C_{ак}$ – витрати, викликані активністю користувачів G Suite Enterprise.

Витрати на Upgrade-відновлення й модернізацію системи хмарних обчислень ($C_в$) при використанні G Suite Enterprise складатимуть 0 грн., оскільки витрати по відновленню й модернізації включені у вартість підписки.

Витрати на керування хмарною системою ($C_к$) у загальному випадку складають:

$$C_к = C_н + C_а + C_з + C_{єв} + C_о + C_{тос}\text{, грн.} \quad (3.2)$$

де, $С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів;

$С_а$ – річний фонд амортизаційних відрахувань;

$С_з$ – річний фонд заробітної плати інженерно-технічного персоналу;

$С_{єв}$ – вартість електроенергії, що споживається апаратурою;

$С_о$ – витрати на залучення сторонніх організацій;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс.

Витрати на навчання адміністративного персоналу й кінцевих користувачів ($С_н$) з використанням безкоштовних онлайн-тренінгів складатимуть 0 грн.

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів у вигляді програмного забезпечення, оскільки при використанні G Suite Enterprisевідсутні капітальні інвестиції, то річний фонд амортизаційних відрахувань складатиме 0 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складатиме:

$$С_з = З_{осн} + З_{дод}\text{ , грн.} \qquad (3.3)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн. на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

До річного фонду заробітної плати додається єдиний внесок на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

З 1.01.2016 р. єдиний соціальний внесок для всіх категорій платників на території України складає 22% від заробітної плати (у тому числі від понаднормових робіт).

Відповідно, за формулою 3.3 розрахуємо річний фонд заробітної плати інженерно-технічного персоналу, що складається з 1 людини:

$$С_з = (3200 \cdot 12 + (3200 \cdot 12) \cdot 0,1) \cdot 1,22 = 51\,532,8 \text{ грн.}$$

Вартість електроенергії, що споживається апаратним забезпеченням протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн.,} \qquad (3.4)$$

де, Р – встановлена потужність апаратного забезпечення, кВт;

Fр – річний фонд робочого часу системи (визначається виходячи з режиму роботи системи).

Оскільки впровадження технології хмарних обчислень не потребує наявність окремих локальних серверів, то вартість електроенергії складає 0 грн.

Витрати на залучення сторонніх організацій ($С_о$) та витрати на технічне й організаційне адміністрування та сервіс ($С_{тос}$) не передбачені.

Визначимо витрати на керування хмарною системою за формулою 3.2:

$$С_к = 0 + 0 + 51\,532,8 + 0 + 0 + 0 = 51\,532,8 \text{ грн}$$

Витрати викликані активністю користувачів системи хмарних обчислень ($С_{ак}$) можна орієнтовно визначити так:

$$С_{ак} = N \cdot С_{міс} \cdot Г, \text{ грн,} \qquad (3.4)$$

де, N – кількість користувачів хмарного сервісу;

$С_{міс}$ – вартість річної підписки на хмарні сервіси G Suite Enterprise, дол. США;

Г – офіційний курс гривні щодо долару США (станом на 13.06.2017).

Для подальших розрахунків, кількість користувачів складатиме 30 чол., а курс долару США – 26,0071 грн за 1 долар США (станом на 13.06.2017).

Витрати викликані активністю користувачів системи хмарних обчислень за формулою 3.4:

$$С_{ак} = 30 \cdot 125 \cdot 26,0071 = 97\,526,63 \text{ грн.}$$

Поточні (експлуатаційні) витрати на впровадження G Suite Enterprise, для підприємства з 30 працівниками за формулою 3.1, складатимуть:

$$C = 0 + 51\,532{,}8 + 97\,526{,}63 = 149\,059{,}43 \text{ грн.}$$

3.2 Розрахунок витрат на впровадження локальної інфраструктури на підприємстві, що є аналогом G Suite Enterprise.

3.2.1 Капітальні витрати

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту локальної інфраструктури (розробка схем пристроїв, політики функціонування системи тощо);

– витрати на залучення зовнішніх консультантів;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення;

– вартість створення основного й додаткового програмного забезпечення;

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Проектні капіталовкладення в апаратне забезпечення та придбання ліцензійного основного й додаткового програмного забезпечення визначаються на основі цін, наведених у прайс-листах відповідних фірм, інших довідкових матеріалів або за фактичними витратами.

Витрати на навчання технічних фахівців і обслуговуючого персоналу приймаються за фактичними затратами організації.

Витрати на інтеграцію системи у вже існуючу корпоративну систему визначаються у відсотках до сумарної вартості обладнання та програмного забезпечення. (7-8%).

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта локальної інфраструктури складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{ грн.} \quad (3.5)$$

де, $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, грн.;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення, грн.;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, грн.;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, грн.;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн.;

$К_{н}$ – витрати на встановлення обладнання та налагодження локальної інфрастуртури, грн.

Вартість закупівель ліцензійного основного й додаткового програмного забезпечення ($К_{зпз}$), відображено у таблиці 3.1:

Таблиця 3.1 – Вартість закупівель ліцензійного основного й додаткового програмного забезпечення

Найменування програмного забезпечення	Ціна, грн	Кількість ліцензій, шт	Вартість, грн
Microsoft Windows Server 2016 Standard	2717	16	43 472
Microsoft Windows Server CAL 2016	943	30	28 290

Microsoft Office 2016	6015	30	180450
Microsoft SharePoint Server 2016	163 654,92	1	163 654,92
Microsoft SharePoint 2016 Standard CAL	3207,84	30	96 235,2
Microsoft Skype for Business Server 2015	88 541,6	1	88 541,6

Продовження табл. 3.1

Найменування програмного забезпечення	Ціна, грн	Кількість ліцензій, шт	Вартість, грн
Skype for Business Server 2015 CAL	1043,2	30	31296
Microsoft Exchange Server Enterprise 2016	106380,9	1	106380,9
Microsoft Exchange Server Standard CAL	2288,88	30	68666,4
Microsoft Exchange Server Enterprise 2016 CAL	1378,53	30	41355,9
		Разом:	848 342,92

Вартість закупівлі апаратного забезпечення та допоміжних матеріалів ($К_{аз}$), відображено у таблиці 3.2:

Таблиця 3.2 – Вартість апаратного забезпечення та допоміжних матеріалів

Найменування апаратного забезпечення	Ціна, грн	Кількість, шт	Вартість, грн
Сервер HPE ProLiant ML30 Gen9	26 899	2	53 798
		Разом:	53 798

Оскільки встановлюється вже розроблене програмне забезпечення, то вартість створення основного й додаткового програмного забезпечення ($К_{пз}$) складає 0 грн.

Витрати на навчання технічних фахівців і обслуговуючого персоналу ($К_{навч}$) та витрати на встановлення обладнання та налагодження локальної

інфраструктури ($К_н$) складатимуть 0 грн, оскільки підприємство має власний персонал.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта локальної інфраструктури за формулою 3.5 складають:

$$К = 848\ 342{,}92 + 0 + 53\ 798 + 0 + 0 + 0 = 902\ 140 \text{ грн.}$$

3.2.2 Поточні витрати.

Поточні витрати при використанні G Suite Enterprise

Річний фонд амортизаційних відрахувань ($С_а$) визначимо за прямолінійним методом:

$$С_а = В_{бал} : Т, \text{ грн}$$

де, $В_{бал}$ – балансова (первісна) вартість об'єкта основних фондів

Т – термін корисного використання об'єкта, років.

За формулою 3.6 річний фонд амортизаційних відрахувань, за умови експлуатації протягом 5 років, складає:

$$С_а = 902\ 140 : 5 = 180\ 428, \text{ грн}$$

За формулою 3.3 розрахуємо річний фонд мінімальної заробітної плати інженерно-технічного персоналу, що складається з 1 людини:

$$С_з = (3200 \cdot 12 + (3200 \cdot 12) \cdot 0{,}1) \cdot 1{,}22 = 51\ 532 \text{ грн.}$$

Вартість електроенергії, що споживається апаратним забезпеченням протягом року, визначаємо за формулою 3.4:

$$С_{ел} = 2 \cdot 0{,}5 \cdot 24 \cdot 365 \cdot 1{,}94 = 16\ 994{,}4 \text{ грн.}$$

Витрати на залучення сторонніх організацій ($С_о$) не передбачені.

Витрати на технічне й організаційне адміністрування та сервіс ($С_{тос}$) входять у заробітну плату інженерно-технічного персоналу.

Визначимо витрати на керування G Suite Enterprise:

$$С_к = 0 + 180428 + 51\ 532 + 16\ 994 + 0 + 0 = 248954 \text{ грн.}$$

3.3 Економічне обґрунтування

Розрахуємо вартість одного місяця обслуговування одного користувача при використанні G Suite Enterprise. Оскільки поточні (експлуатаційні) витрати на впровадження G Suite Enterprise, для підприємства з 30 працівниками склали 149 059,43 грн., то вартість одного місяця обслуговування одного користувача буде складати:

$$М_х = 149\ 059{,}43 : 30 : 12 = 414{,}05 \text{ грн/(кор·міс)}.$$

Витрати підприємства на організацію та налагодження локальної інфраструктури склали:

$$В_л = К + С_{ел} + С_з = 1\ 004\ 656{,}92 \text{ грн}.$$

А вартість одного місяця обслуговування одного користувача з використанням локальної інфраструктури для підприємства з 30 працівниками, за умови постійної експлуатації упродовж 3 років:

$$М_л = В_л : 3 : 30 : 12 = 930{,}24 \text{ грн/(кор·міс)}.$$

Побудуємо графік залежності місячної вартості обслуговування одного користувача при використанні G Suite Enterprisey порівнянні з використанням локальної інфраструктури (рисунок 3.1).

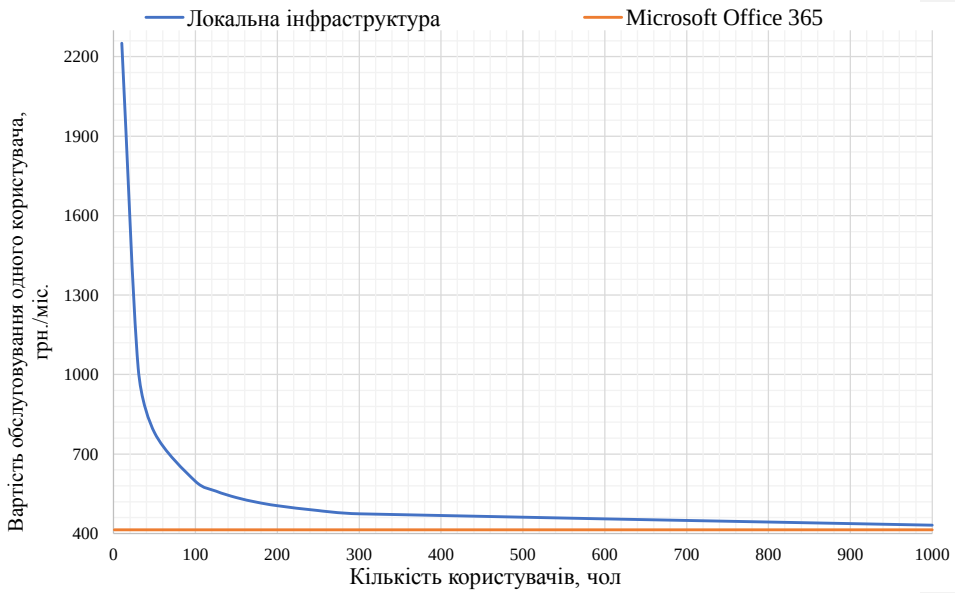

Рисунок 3.1 – Залежність місячної вартості обслуговування одного користувача при використанні G Suite Enterprise у порівнянні з використанням локальної інфраструктури

Економічнй ефект від впровадження G Suite Enterpris евизначається за формулою:

$$E = E_{л} – E_{хм} + K_{л} \quad (3.7)$$

де, $E_{л}$ – експлуатаційні витрати на локальну інфраструктуру, грн;

$E_{хм}$ – експлуатаційні витрати на хмарну інфраструктуру, грн;

$K_{л}$ – капітальні витрати на на локальну інфраструктуру, грн.

Відповідно до формули 3.7, економічний ефект становитиме:

$$E = 369\,240{,}84 – 149\,059{,}43 + 902\,140{,}92 = 1\,122\,322{,}33 \text{ грн.} > 0$$

Висновки до третього розділу

Незважаючи на те, що G Suite Enterprise дозволив компанія не створювати власні ЦОД, більшість компаній використовують сервери, розташовані на території самої компанії, і, відповідно, мають поточні витрати

на електроенергію, оренду приміщень та охолодження серверів. Однією з основних переваг G Suite Enterprise , як і будь-якої хмарної технології – це скорочення потреб в обслуговуванні і підтримці серверів, що призводить до зменшення системного персоналу, це дозволяє звернутися до послуг менш кваліфікованих системних адміністраторів, з чого випливають скорочення у витратах на заробітну плату.

Впровадження G Suite Enterprise надає можливості вивільнення обчислювальних ресурсів, що для нових компаній надає можливість відмовитись від початкових вкладень в сервера. Більш того, аналізоване хмарне рішення надає гнучкі тарифні плани для зберігання інформації.

Модель оплати за технологію G Suite Enterprise дуже прозора для кінцевого споживача. Залежно від кількості використовуваних сервісів розраховується вартість їх використання. Традиційний варіант використання технологій Google змушує користувачів купувати безліч ліцензій для кожного користувача і для кожного окремого продукту. Хмарна модель надає абсолютно іншу модель оплати ліцензій, більш того кінцевий споживач фактично не платить за ліцензію, а платить за використані ресурси, тобто вартість ліцензії включена у вартість користування послугою. Крім того, хмарне рішення G Suite Enterprise включає в свій склад програмне забезпечення, яке б довелося докуповувати окремо. До такого програмного забезпечення належать антивірусні і антиспам програми, програми архівування пошти тощо.

G Suite Enterprise надає різні механізми, які підвищують продуктивність процесів, що протікають в компаніях за рахунок уніфікації, централізації і відповідних додатків для роботи з поштою (Корпоративний Gmail) для здійснення комунікацій (Hangouts для бізнесу), для роботи з офісними додатками (Google Документи), а також, роботи з документами (Google Диск, Google Sites). Говорячи про продуктивність, необхідно виділити ще одну важливу характеристику, а саме мобільність користувачів і можливість роботи з мобільних пристроїв.

За результатом аналізу, вартість обслуговування одного користувача на місяць при використанні хмарної служби G Suite Enterprise на 45% дешевше ніж при розгортанні локальної інфраструктури, що є аналогом G Suite Enterprise, за умови експлуатації протягом 3 років.

ВИСНОВКИ

У першому розділі магістерської дипломної роботи було розглянуто основні властивості хмарних технологій, що визначені Національним інститутом стандартів і технологій США, а саме: самообслуговування за вимогою, універсальність доступу, об’єднання ресурсів, еластичність масштабування, облік споживання.

Самообслуговування за вимогою дає можливість споживачу самому виконувати всі дії, необхідні для модернізації наданих йому послуг, без необхідності звернення до постачальника послуг хмарних обчислень.

Універсальність доступу забезпечується широкою доступністю послуг і підтримкою безлічі термінальних пристроїв: персональних комп’ютерів, мобільних телефонів, смартфонів, інтернет-планшетів, з різними операційними системами та різної продуктивністю.

Об’єднання ресурсів призводить до збільшення коефіцієнта використання ресурсів, відповідно використовуючи віртуальну інфраструктуру та динамічний перерозподіл обчислювальних потужностей дозволяє заощадити певну частину коштів за рахунок збільшення кінцевих користувачів, але накладає відповідні обмеження на розробників програмного забезпечення, що мають передбачити можливість одночасного використання програмного продукту одночасно кількома користувачами.

Добавлено примечание ([V12]): https://remonsinnema.com/cloud-2/cloud-computing/resource-pooling/

Еластичність дозволяє хмарі швидко адаптуватися до поточного навантаження за допомогою масштабування вгору й вниз, тобто реалізує вертикальна та горизонтальна масштабованість. Вертикальна масштабованість передбачає збільшення або зменшення продуктивності одного вузла в системі, у той час як горизонтальна спрямована на зміну кількості вузлів у системі, що дозволяє обійти обмеження вертикальної масштабованості.

Для оперативного масштабування вгору чи вниз, потрібно постійно аналізувати поточний попит на обчислювальні ресурси хмари, тобто навантаження на центральний процесор, оперативну пам'ять та пропускну

Добавлено примечание ([V13]): https://remonsinnema.com/cloud-2/cloud-computing/measured-service/

здатність мережі, щоб переконатися, що споживачі не відчують вичерпності цих ресурсів, це реалізує така властивість як облік споживання.

Аналіз моделей обслуговування хмарних технологій призвів до виділення трьох основних моделей:

- інфраструктура як послуга;
- платформа як послуга;
- програмне забезпечення як послуга.

Інфраструктура як послуга надає споживачеві набір фізичних ресурсів, таких як сервери, мережеве обладнання та накопичувачі у оренду, що дозволяє переорієнтувати фінанси споживача на інші потреби, замість того щоб купувати власні сервери та обладнання. За концепцією IaaS споживач купує лише ті обчислювальні потужності, які необхідні йому для виконання конкретних завдань. При обслуговуванні за моделлю IaaS повнота відповідальності надається споживачеві, за виключенням захисту інфраструктури, що забезпечується постачальником хмарних послуг

Платформа як послуга дозволяє споживачу використовувати хмарну інфраструктуру для розміщення власного програмного забезпечення для подальшого його використання та модифікації, уникаючи витрат на обслуговування відповідної інфраструктури і сервісів для розробки, тестування, розгортання і розміщення додатків. Ця модель передбачає покладання відповідальності за забезпечення захисту додатку, що розробляється на споживача, захист платформ та інфраструктури забезпечує постачальник

Програмне забезпечення як послуга передбачає доступ до додатків як до сервісу, тобто додатки постачальника запускаються в хмарі і надаються користувачам на вимогу як послуга. Користувач отримує доступ до програмного забезпечення на віддалених серверах, за допомогою мережі Інтернет, а оновлення та керування ліцензіями виконується постачальником хмарних послуг. При використанні цієї моделі на споживача покладається

відповідальність лише за збереження конфіденційності автентифікаційних даних, а постачальник хмарних послуг забезпечує всі рівні захисту.

За моделями розгортання хмари поділяють на приватні, комунальні, публічні та гібридні.

Приватні хмари – модель розгортання хмарної інфраструктури, при якій обчислювальні ресурси хмари доступні тільки однієї організації, але споживачів у такої хмари може бути декілька.

Добавлено примечание ([V14]): http://www.treolancloud.ru/knowledge/articles/modeli_razvertyvaniya_oblaka_i_ih_osobennosti/

Громадською хмарою називають інфраструктуру яка слугує для використання конкретною множиною споживачів, що мають спільні задачі.

Публічні хмари – модель розгортання хмарної інфраструктури, при якій обчислювальні ресурси хмари доступні безлічі споживачів і організацій, але при цьому технологія віртуалізації забезпечує сегментацію віртуальних машин різних споживачів.

Гібридна хмара – модель розгортання хмарної інфраструктури, як комбінації приватної і публічної хмари. Поєднання цих двох моделей дозволить організації, яка вже побудувала свою приватну хмару, використовувати обчислювальні ресурси публічної хмари.

Впровадження хмарних технологій дозволяє відмовитися від застарілого локального інфраструктурного підходу до запуску сервісів у сфері інформаційно-комунікаційних технологій.

У другому розділі магістерської дипломної роботи були розглянуті послуги що надаються підписникам G Suite Enterprise та умови їх надання.

Перевагами використання хмарної служби G Suite Enterprise є:

– використання всієї потужності сучасних інформаційних технологій без необхідності вкладатися в створення власної мережевої інфраструктури, розгортати і супроводжувати складне програмне забезпечення;

– можливість перекласти рутинні роботи щодо створення резервної копії даних, встановлення оновлень безпеки на корпорацію Google і зосередити зусилля IT-підрозділів на стратегічних завданнях;

– оплата послуг за принципом оренди: перенесення витрат на програмне забезпечення з капітальних в операційні, прогнозованість платежів;

– знайомі користувачам інструменти роботи, швидке розгортання і використання співробітниками, низькі витрати на навчання кінцевих користувачів;

– краща в галузі система забезпечення безпеки і приватності даних: вбудовані антивірус і антиспам, відсутність перлюстрації пошти, відповідність стандарту ISO/IEC 27001, ISO/IEC 27017 та ISO/IEC 27018 і вимогам Європейського Союзу в галузі безпеки;

– прозора система оновлення ПЗ, інформування про нововведення, завжди актуальні версії програмного забезпечення;

– можливості збереження поточних інвестицій в IT за рахунок коштів інтеграції та реалізації гібридних моделей;

– фінансова відповідальність Google: гарантії доступності сервісу 99,9% часу.

На рівні служби G Suite Enterprise використовується підхід поглибленого захисту, у якому функції безпеки та передові робочі методики задіяно на кількох рівнях: фізичному, логічному і на рівні даних. Крім того, служба G Suite Enterprise містить засоби керування корпоративного класу для користувачів і адміністраторів, що додатково посилює захист середовища.

Корпорація Google використовує регіональну стратегію розміщення центрів обробки даних. Вибір основного сховища для даних клієнта залежить від того, яку країну або регіон вказав адміністратор клієнта при початковій установці служб. Корпорація Google реплікує дані клієнтів принаймні в двох центрах обробки даних в будь-який момент часу, щоб запобігти збою або локальній аварійній ситуації.

Якщо з якої-небудь причини робота центру обробки даних припинена, втрата даних не відбувається, так як прикладна програма і пов'язані з нею дані клієнта також доступні в другому або третьому центрі обробки даних. Користувачі можуть не отримувати повідомлення при відпрацюванні відмови.

У деяких службах відпрацювання відмови може не призводити до порушення роботи служби. Клієнтам слід припускати, що в будь-який момент часу їх дані можуть оброблятися в одному або декількох центрах обробки даних в регіоні.

Фізичний доступ до центрів обробки даних G Suite Enterprise контролюється за допомогою дворівневої системи перевірки справжності, що включає в себе пристрій зчитування карт проксі-доступу, необхідний жетон доступу по карті, і біометричний зчитувач геометрії долоні.

Відповідальність співробітників центру обробки даних забезпечується цілим набором системних процедур, включаючи використання унікальних імен користувачів, засобів управління доступом до даних і аудиту.

Щокварталу співробітник служби безпеки Google відправляє звіт уповноваженим фахівцям, що мають право затверджувати доступ до центру обробки даних. Мережі в центрах обробки даних G Suite Enterprise розділені на сегменти, що забезпечує фізичну ізоляція критично важливих внутрішніх серверів і пристроїв зберігання даних від загальнодоступних інтерфейсів, а засоби безпеки прикордонних маршрутизаторів дозволяють виявляти спроби вторгнення і ознаки уразливості системи.

Підключення клієнтів до G Suite Enterprise відбувається по протоколу TLS, що забезпечує безпеку при доступі клієнті до веб-служб зі своїх комп'ютерів, підключених до Інтернету, а запити на доступ потрапляють до центру обробки даних компанії Google. Протокол TLS гарантують безпечне підключення клієнтів до сервера, конфіденційність і цілісність даних, що передаються між комп'ютером користувача і центром обробки даних.

Статичні дані, що не передаються у даний момент, безпосередньо зберігаються у зашифрованому вигляді у центрі обробки даних технологією BitLocker за допомогою алгоритму AES з можливою довжиною ключів 128 або 256 біт.

Коли клієнти видаляють дані або припиняють користуватися службою G Suite Enterprise , вони можуть зберегти дані локально і назавжди видалити їх з серверів Google.

Превентивний захист, як оборонна стратегія, спрямований на прогнозування і проактивний захист від вторгнень та вимагає постійного вдосконалення вбудованих засобів безпеки: сканування портів і усунення виявлених проблем, виявлення вразливостей периметра, оновлення операційних систем для інсталяції актуальних версій засобів забезпечення безпеки, виявлення і запобігання розподілених атак.

У G Suite Enterprise триває розвиток автоматизованих систем, які дозволяють виявляти аномальну і підозрілу поведінку і миттєво реагувати на неї з метою усунення ризику безпеки. Компанія Google постійно удосконалює високоефективні системи автоматичного розгортання виправлень, які вирішують проблеми, виявлені системами моніторингу, без втручання людини. Це значно підвищує рівень безпеки і гнучкість служби.

У G Suite Enterprise пропонує ряд функцій відповідності нормативним вимогам: запобігання втрати даних, виявлення електронних даних, а також інструменти проведення аудиту і звітності.

За допомогою технології DLP можна виявити конфіденційну інформацію в електронному повідомленні, наприклад номер соціального страхування або кредитної картки, і попередити користувача за допомогою повідомлення.

Метою пошуку технології DLP є всі результати, що відповідають запиту, а не частина найважливіших. Для захисту від поширених шкідливих атак, операції пошуку, що виконуються довше зазначеного часу, зупиняються. При обході контенту система пошуку створює пошуковий індекс. У цьому індексі зберігаються дані, використовувані при видачі результатів запиту. В індексі також зберігаються відомості про дозволи, необхідних для отримання доступу до елементів контенту. Система пошуку використовує пошуковий індекс для виявлення потрібних результатів.

Також були розглянуті можливі загрози та вразливості для інформації, що обробляється за допомогою хмарних технологій. Але через неможливість фізичної присутності споживача у центрі обробки даних, загрози, що

направлені безпосередньо на центр обробки даних мають знешкоджуватись безпосередньо корпорацією Google. Споживачу залишається дотримання відповідних організаційних заходів всередині підприємства.

Для кожного компоненту хмарної служби G Suite Enterprise було обрано відповідний функціональний профіль захищеності.

У третьому розділі магістерської дипломної роботи було визначено, що вартість обслуговування одного користувача на місяць при використанні хмарної служби G Suite Enterprisena 55,49% дешевше ніж при розгортанні локальної інфраструктури, що є аналогом G Suite Enterprise, за умови експлуатації локальної інфраструктури протягом 3 років.

На сьогодні користувачі з обережністю ставляться до хмарних обчислень, у зв'язку зі страхом втрати інформації. Відповідно, ця проблема має бути розглянута на законодавчому рівні.

В Україні використання систем хмарних обчислень регулюється загальними нормами законів про інформацію та нормативними документами у сфері технічного та криптографічного захисту інформації.

24 березня 2016 року у Верховній Раді України зареєстровано Проект Закону «Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень», який має роз'яснювати ситуацію із розпоряджанням інформацією, що оброблюється за допомогою хмарної технології. На жаль досі закон не прийнятий і знаходиться в стадії другого читання.

Із прийняттям вказаного проекту можна говорити про гарантії захисту інформації та забезпечення виконання належним чином обов'язку із її зберігання провайдером шляхом запропонованого у вказаному Проекті переліку чисельних умов, які мають міститись у договорі між надавачем хмарних послуг та володільцем інформації або власником системи. Головними із них є: порядок отримання володільцем інформації або власником системи інформації, яка оброблялась в системі хмарних обчислень, у випадку припинення надання хмарних послуг; порядок видалення інформації із

системи хмарних обчислень; відповідальність сторін договору, але станом на червень 2017 року, цей проект досі не прийнято . Суттєвою поправкою до цього закону є: «Забороняється обробка інформації, яка в установленому порядку віднесена до такої, що становить державну таємницю, службової інформації та інформації, що стосується систем керування об’єктів критичної інфраструктури в системі, де використовується технологія хмарних обчислень»

Суттєве нововведення стосується й сертифікації, прийняття цього Проекту робить можливим підтвердження належного рівня захисту інформації в системі хмарних обчислень іноземним органом чи організацією з оцінки відповідності та іноземним органом з акредитації, який є стороною угоди про визнання Міжнародного форуму з акредитації або Європейської кооперації з акредитації.

В майбутньому було б добре продовжити розвивати законодавство в напрямку популяризації хмарних систем, їх використання без остережень, а саме: посилити вимоги до тих з них, які використовуються державними органами, запровадити відповідальність державного органу за зберігання персональних даних і службової інформації в хмарі, визначити особливості надання адміністративних послуг за допомогою хмарних обчислень. Усе це створить правовий фундамент для розбудови якісно нової інформаційної інфраструктури країни.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology [Electronic resource] / Peter Mell, Timothy Grance – Special Publication 800-145 – 7 p. – Acess : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
2. Георгій Асєєв. Становлення й розвиток українського ринку систем управління підприємством / Асєєв Г. // Вісник Книжкової палати, 2014. – № 12
3. Що таке CRM система? [Електронний ресурс]. – Режим доступу : http://call-center.xrm.ua/uk/що-таке-crm-система
4. Максим Малаховский. С миру по нитке: Суперкомпьютер [Електронний ресурс] / М. Малаховський – Режим доступу : http://www.popmech.ru/techno-logies/9137-s-miru-po-nitke-superkompyuter/
5. On-Demand Self-Service [Electronic resource] – Acess : https://remonsinnema.com/cloud-2/cloud-computing/on-demand-self-service/
6. Broad Network Access [Electronic resource] – Acess : https://remonsin-nema.com/cloud-2/cloud-computing/broad-network-access/
7. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013.
8. Nilo Mitra. SOAP Version 1.2 Part 0: Primer [Електронний ресурс] – Режим доступу : https://www.w3.org/TR/2003/REC-soap12-part0-20030624/
9. Roy Thomas Fielding. Architectural Styles and the Design of Network-based Software Architectures. CHAPTER 5 Representational State Transfer (REST) [Електронний ресурс]. – Режим доступу : http://www.ics.uci.edu/~field-ing/pubs/dissertation/rest_arch_style.htm
10. Resource Pooling [Electronic resource] – Acess : https://remonsin-nema.com/cloud-2/cloud-computing/resource-pooling/
11. Rapid Elasticity. [Electronic resource] – Acess : https://remonsin-nema.com/cloud-2/cloud-computing/rapid-elasticity/

12. Measured Service. [Electronic resource] – Acess : https://remonsin-nema.com/cloud-2/cloud-computing/measured-service/

13. Gray, Jim. The Transaction Concept: Virtues and Limitations. Proceedings of the 7th International Conference on Very Large Databases [Electronic resource] – Acess : http://jimgray.azurewebsites.net/papers/thetransactionconcept.pdf

14. Pease, Marshall; Robert Shostak, Leslie Lamport. Reaching Agreement in the Presence of Faults. Journal of the Association for Computing Machinery – Vol 27 – No 2 – 1980 – [Electronic resource] – Acess : http://lamport.azurewebsites.net/pubs/reaching.pdf

15. А. Й. Наконечний, Р. Г. Пазан. Опрацювання сигналів з використанням сучасних хмарних технологій. / Наконечний А. Й., Пазан Р. Г. – 2015 Національний університет “Львівська політехніка” кафедра комп’ютеризованих систем автоматики

16. Монахов Д. Н. Облачные Технологии. Теория и практика / Д. Н. Монахов, Н. В. Монахов, Г. Б. Прончев, Д. А. Кузьменков. – М.: Видавництво МАКС Пресс. – МГУ, 2013

17. Введение в облачный хостинг. [Електронний ресурс] – Режим доступу : http://www.8host.com/blog/vvedenie-v-oblachnyj-xosting/

18. Edwin Schouten. Cloud computing defined: Characteristics & service levels [Electronic resource] / E. Schouten – 2014 – Acess : https://www.ibm.com/blogs/cloud-computing/2014/01/cloud-computing-defined-characteristics-service-levels/

19. Отримайте максимальну користь від Office завдяки Office 365. [Електронний ресурс] – Режим доступу : https://products.office.com/uk-ua/compare-all-microsoft-office-products?tab=2

20. Описание службы Gmail. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/gmail.html

21. Описание службы SharePoint Online. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/sharepoint-online-service-description.html

22. Описание службы OneDrive для бизнеса. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/onedrive-for-business-service-description.html

23. Описание службы Skype для бизнеса online. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/skype-for-business-online-service-description.html

24. Описание службы Office Online. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/office-online-service-description.html

25. Описание службы приложений Office. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/office-applications-service-description.html

26. Описание службы Power BI. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/mt282164.html

27. Описание службы Yammer. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/yammer-service-description.html

28. Где находятся мои данные? [Електронний ресурс] – Режим доступу : https://www.google.com/online/legal/v2/?docid=25&langid=ru-RU

29. Административный доступ. [Електронний ресурс] – Режим доступу : https://www.google.com/online/legal/v2/?docid=24&langid=ru-RU

30. Использование ваших данных корпорацией Microsoft. [Електронний ресурс] – Режим доступу : https://www.google.com/online/legal/v2/?docid=23&langid=ru-RU

31. Шифрование в G Suite Enterprise . [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/dn569286.html

32. Средства безопасности G Suite Enterprise . [Електронний ресурс] – Режим доступу : https://www.google.com/ru-RU/download/details.html?id=26552

33. Шифрування повідомлень G Suite Enterprise . [Електронний ресурс] – Режим доступу : https://products.google.com/ru-RU/message-encryption.html

34. Overview of data loss prevention policies. [Electronic resource] – Acess : https://support.office.com/en-us/article/Overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e?ui=en-US&rs=en-US&ad=US.

35. Защита от потери данных. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/jj150527(v=exchg.150).html

36. Включение аудита почтовых ящиков в G Suite Enterprise . [Електронний ресурс] – Режим доступу : https://google.com/library/dn879651.html

37. Перегляд звітів журналу аудиту. [Електронний ресурс] – Режим доступу : https://support.office.com/uk-ua/article/Перегляд-звітів-журналу-аудиту-b37c5869-1b47-4a82-a30d-ea20070fe527?ui=uk-UA&rs=uk-UA&ad=UA

38. Мониторинг, составление отчетов и трассировка сообщений в Exchange Online. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/jj200725(v=exchg.150).html

39. Планирование eDiscovery. [Електронний ресурс] – Режим доступу : https://technet.google.com/ru-ru/library/ff453933(v=office.14).html

40. Защита от спама в G Suite Enterprise . [Електронний ресурс] – Режим доступу : https://support.office.com/ru-ru/article/Защита-от-спама-в-Office-365-6a601501-a6a8-4559-b2e7-56b59c96a586

41. Security and Compliance: Customer Controls for Information Protection in G Suite Enterprise . [Електронний ресурс] – Режим доступу : http://download.google.com/download/F/2/B/F2B9D8BB-30C3-427C-8FBE-E687D986BD91/Whitepaper%20-20Customer%20controls%20for%20Information%20protection%20in%20Office%20365.docx

42. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

43. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі

ДОДАТОК А. ПЕРЕЛІК МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

1 Титульна сторінка.
2 РЕФЕРАТ.
3 СПИСОК СКОРОЧЕНЬ.
4 ЗМІСТ.
5 ВСТУП.
6 СТАН ПИТАННЯ.
7 СПЕЦІАЛЬНАЯ ЧАСТИНА.
8 ЕКОНОМІЧНА ЧАСТИНА.
9 ВИСНОВКИ.
10 ПЕРЕЛІК ПОСИЛАНЬ.
11 Додаток А.
12 Додаток Б.
13 Додаток В.
14 Додаток Г.
15 Презентація дипломної роботи.
16 Оптичний носій.

ДОДАТОК Б. КОПІЯ НАУКОВОЇ СТАТТІ

ТАКТИКА ВПРОВАДЖЕННЯ G SUITE ENTERPRISE НА ПІДПРИЄМСТВІ

Автор: Журавель Владислав Костянтинович
Науковий керівник: Флоров Сергій Володимирович
Державний ВНЗ «Національний гірничий університет», http://www.nmu.org.ua/ua/,
E-mail: Zhuravel.V.K@nmu.one

У статті розглянуто варіанти впровадження G Suite Enterprisena підприємстві, його переваги та внутрішні та клієнтські засоби забезпечення безпеки G Suite Enterprise.

Ключові слова – Microsoft Office, G Suite Enterprise, хмарні обчислення, AES, SSL, TLS, Active Directory.

ВСТУП

Багатьом користувачам, що використовують офісний пакет Microsoft Office, важко уявити чим саме є G Suite Enterprise. Вони вважають, що отримують Word, Excel, PowerPoint і інші додатки у «хмарі» для використання у веб-браузері стаціонарного ПК або смартфону.

Так, G Suite Enterprise передбачає використання аналогів оффлайн версій офісного пакету у вигляді веб-застосунків, але це лише частина пропонованих компонентів, що створюють комплексні і стратегічні напрями в рамках підприємства. Крім таких функцій, як Gmail, Google Site, Google Drive або Hangouts, G Suite Enterprise передбачає функції безпеки, аналіз даних, роботу над проектами, онлайн-комунікацію, соціальні мережі та багато іншого.

ВАРІАНТИ ВПРОВАДЖЕННЯ G SUITE ENTERPRISE

G Suite Enterprise постачається у вигляді підписки на пакети, що направленні на різні цілі та сегменти ринку та слугують для забезпечення різних потреб з різними варіаціями цін.

Серед пропонованих пакетів можна виділити різні варіанти відписок для дому та для бізнесу.

Для домашнього використання доступні варіанти:

- G Suite Home;
- G Suite Personal;

У той же час, для корпоративного сегменту варіанти підписки більш різноманітні:

- G Suite Business;
- G Suite Business Essentials;
- G Suite Business Premium;
- G Suite ProPlus;
- G Suite Enterprise.

Розглянемо програмні продукти, що включені у різні варіанти.

G Suite Personal включає доступ до всіх хмарних додатків Google Документы, Google Таблицы, Google Презентации, Gmail, Google Диск для домашнього/некомерційного використання (PC чи Mac), а також передбачає інсталяцію на одному планшеті (Android, iOS чи Windows RT) або телефоні. Додатково до цього є можливість використовувати 1 TB сховища на Google Drive і 120 хвилин міжнародних дзвінків у Hangouts.

G Suite Home є аналогічним G Suite Personal, за винятком того, що Home-версія передбачає використання пакету на п’яти стаціонарних ПК, планшетах і смартфонах, замість одного у Personal.

Версії G Suite Home та G Suite Personal передбачає підписку строком на один рік чи місяць, у той час як Office Home & Student доступний для одноразового придбання.

G Suite Business Essentials надає доступ до бізнес-пошти, Gmail, Google Site, Hangouts, Google Диск сервісів.

G Suite Business Premium є комбінацією планів G Suite Business та G Suite Business Essentials.

G Suite ProPlus дублює функціонал G Suite Business, але додатково включає Hangouts for Business.

G Suite Enterprise надає доступ до всіх програм Office, Gmail, Google Site, Google Drive, Hangouts, а також особливі сервіси та підтримку для бізнесу.

Всі версії G Suite Enterprise для бізнесу є річною підпискою з оплатою за кожного користувача [1].

ПЕРЕВАГИ ПІДПИСКИ НА G SUITE ENTERPRISE ДЛЯ ПІДПРИЄМСТВА

Існує ряд переваг для підприємства при підписці на G Suite Enterprise, наприклад:

1. Економія. При використанні G Suite компанії не потрібно купувати власні сервера та комплектуючі. З’являється можливість заощадити на техніці, електроживленні і оренді приміщень. Є можливість платити лише за ті ліцензії, які фактично використовуються.
2. Спрощення IT-інфраструктури. Перехід на роботу з G Suite дозволяє відмовитися від самостійного розгортання серверів Exchange, Skype for Business і SharePoint, скоротити навантаження на сервер SQL.
3. Гнучкість. Якщо компанія швидко росте або, навпаки, скорочує штат, стає простіше адаптувати структуру IT-сервісів до роботи, підключати або відключати нових співробітників.
4. Мобільність. G Suite дозволяє отримати доступ до корпоративних ресурсів практично з будь-якої точки – з власного офісу, з офісів партнерів і клієнтів, з дому та інших місць, з мобільного пристрою або звичного комп’ютера.
5. Актуальність. Використання G Suite забезпечує роботу з останніми і перевіреними версіями програмного забезпечення.
6. Розподіленість. Інформація зберігається у розподілених дата-центрах по світі. Технологія

геореплікації забезпечує постійну доступність даних.

ЗАСОБИ БЕЗПЕКИ G SUITE ENTERPRISE

G Suite – це служба з підвищеним рівнем безпеки, створена відповідно до принципів життєвого циклу розробки захищених додатків Microsoft.

Для забезпечення безпеки на фізичному і логічному рівнях, а також на рівні даних в службі G Suite використовуються комплексні заходи захисту на основі рекомендацій, вироблених в процесі експлуатації подібних систем.

До вбудованих засобів безпеки належать:

Цілодобовий нагляд за обладнанням. Дані G Suite зберігаються в мережі центрів обробки даних (ЦОД), які розміщені в стратегічних точках і знаходяться під управлінням служби Google Global Services. Це гарантує надання послуг і захист інформації від стихійних лих або несанкціонованого доступу. Контроль фізичного доступу здійснюється за допомогою процедур аутентифікації і використання бейджів і смарт-карт, біометричних сканерів, двофакторної автентифікації, в будівлі присутні співробітники локальної служби безпеки, ведеться постійне відеоспостереження. Центри обробки даних обладнані датчиками руху, системами відеоспостереження та сигналізації.

Ізольовані дані клієнтів. Зберігання та обробка даних кожного клієнта здійснюється окремо за допомогою Active Directory і інших засобів, спеціально розроблених для контролю і забезпечення безпеки багатокористувацьких середовищ. Active Directory ізолює клієнтів, використовуючи зони безпеки. Такий підхід не дозволяє одним клієнтам отримати доступ до даних інших клієнтів або поставити під загрозу безпеку цієї інформації.

Захищена мережа. Мережі центрів обробки даних G Suite сегментовані і забезпечують фізичний поділ критично важливих внутрішніх серверів і пристроїв зберігання від загальнодоступних інтерфейсів. Засоби безпеки прикордонних маршрутизаторів виявляють спроби вторгнення і ознаки уразливості системи. Підключення клієнтів до G Suite відбувається по протоколу SSL, що забезпечує безпеку Gmail, Outlook, Outlook Web App, Exchange ActiveSync, POP3 і IMAP. Підключення шифруються з використанням стандартних протоколів безпеки Transport Layer Security (TLS) і Secure Sockets Layer (SSL). Протоколи TLS/SSL гарантують безпечне підключення клієнтів до сервера, конфіденційність і цілісність даних, що передаються між ПК і ЦОД.

Шифрування даних. Вміст електронного повідомлення зашифровано на диску за допомогою алгоритму AES з ключем 128 або 256 біт. Під захистом знаходяться всі диски поштових серверів. Крім того, G Suite здійснює транспортування і збереження повідомлень типу S/MIME, а також повідомлень, зашифрованих за допомогою інструментів шифрування від сторонніх розробників (наприклад, PGP).

Керування функціями безпеки передбачає:

Використання функцій шифрування. Увімкнувши служби шифрування G Suite, з'являється можливість шифрувати переписку з сторонніми користувачами. Адміністратори можуть задавати алгоритми шифрування і підписування документів.

Надання доступу користувачам. Послуги G Suite захищаються на наступних рівнях: ЦОД, мережевий, логічний, рівень зберігання та передачі. G Suite інтегрується з локальної службою каталогів Active Directory і іншими системами зберігання і ідентифікації каталогів.

Двофакторна перевірка автентичності. Двофакторна перевірка автентичності підвищує рівень безпеки в середовищі з безліччю пристроїв, орієнтованої на хмарні технології. Компанія Microsoft пропонує рішення для двофакторної перевірки автентичності з можливістю аутентифікації за телефоном, а також підтримує рішення сторонніх розробників. При двофакторній перевірці автентичності з використанням телефону користувач отримує СМС повідомлення з кодом і вводить його в якості другого пароля при вході в службу [2].

ВИСНОВОК

Щороку з'являються нові версії програмного забезпечення, що розширюють вже існуючий функціонал. У разі ігнорування IT-відділом цих оновлень, залишаються помилки у встановлених програмних продуктах та недоступні функції нових версій продукту. Використання G Suite дозволяє компаніям використовувати останні версії програмного забезпечення Microsoft.

Впровадження G Suite забезпечує стійке шифрування як для даних, що передаються між клієнтом і ЦОД, так і при зберіганні у ЦОД. Розподіленість ЦОД та реплікація гарантує доступність даних в незалежності від стихійних лих чи інших факторів, а гнучкі налаштування доступу для користувачів, забезпечують необхідний захист від інсайдерів та несанкціонованого доступу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Get the most from with G Suite [Електронний ресурс]. – Режим доступу: https://products.gmail.com/en-us/compare-all-microsoft-office-products (дата звернення 05.04.2017), вільний.
2. Средства безопасности G Suite [Електронний ресурс]. – Режим доступу: https://www.google.com/ru-RU/download/confirmation.html?id=26552 (дата звернення 05.04.2016), вільний.

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

ДОДАТОК Г. ВІДГУК НА МАГІСТЕРСЬКУ ДИПЛОМНУ РОБОТУ

на тему:

«Дослідження методів захисту інформаційних ресурсів підприємства при використанні хмарних технологій»

студента групи 125м-16-1 Журавель Владислава Костянтиновича

Дипломна робота за спеціальністю 125 «Кібербезпека» Журавель В.А. представлена пояснювальною запискою на _ стор., містить _ рис., _ табл., _ додатка, 43 джерела.

Мета дипломної роботи – підвищення ефективності забезпечення інформаційної безпеки підприємств, що обробляють інформацію за допомогою служби G Suite Enterprise.

Очікувані результати роботи повністю відповідає вимогам які пред'являються до магістерських робіт

У пояснювальній записці сформульована постановка завдання та ідея роботи, проаналізовані моделі розгортання та обслуговування хмарних технологій.

У спеціальній частині досліджено методів забезпечення інформаційної безпеки при використанні хмарної служби G Suite Enterprise, визначено загрози при використанні хмарних технологій для обробки інформації, для кожного компоненту хмарної служби G Suite Enterprise було обрано відповідний функціональний профіль захищеності.

В якості недоліків слід відзначити наступне: недотримання графіка проведення розробки, нечіткість окремих висновків і визначень.

В цілому дипломна робота виконано у відповідності до вимог, які пред’являються до дипломних робіт магістра і заслуговує оцінки "добре", а Журавель Владислав Костянтинович присвоєння йому кваліфікації професіонала із організації інформаційної безпеки.

Керівник спеціальної частини к.т.н., доц. Флоров С.В.

РЕЦЕНЗІЯ НА МАГІСТЕРСЬКУ ДИПЛОМНУ РОБОТУ

на тему:

«Дослідження методів захисту інформаційних ресурсів підприємства при використанні хмарних технологій»

студента групи 125м-16-1Журавель Владислава Костянтиновича

Дипломна робота за спеціальністю 125 «Кібербезпека» Журавель В.А. представлена пояснювальною запискою на _ стор., містить _ рис., _ табл., _ додатка, 43 джерела.

Мета дипломної роботи – підвищення ефективності забезпечення інформаційної безпеки підприємств, що обробляють інформацію за допомогою служби G Suite Enterprise.

Очікувані результати роботи повністю відповідає вимогам які пред'являються до магістерських робіт

У пояснювальній записці сформульована постановка завдання та ідея роботи, проаналізовані моделі розгортання та обслуговування хмарних технологій.

У спеціальній частині досліджено методів забезпечення інформаційної безпеки при використанні хмарної служби G Suite Enterprise, визначено загрози при використанні хмарних технологій для обробки інформації, для кожного компоненту хмарної служби G Suite Enterprise було обрано відповідний функціональний профіль захищеності.

В якості недоліків слід відзначити наступне: недотримання графіка проведення розробки, нечіткість окремих висновків і визначень.

В цілому дипломна робота виконано у відповідності до вимог, які пред’являються до дипломних робіт магістра і заслуговує оцінки "добре", а Журавель Владислав Костянтинович присвоєння йому кваліфікації професіонала із організації інформаційної безпеки.

Рецензент