Ляниця Я.

Науковий керівник – Луцик І.Б.

ХМАРНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ АВТОМАТИЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ

Постановка проблеми. Хмарні технології знаходять активне застосування у всіх розвинених країнах, забезпечуючи принципово нові, економічно ефективні можливості для бізнесу, управління, освіти і наукових досліджень.

Складні бізнес-процеси реалізуються в обчислювальних хмарах, які складаються з тисяч серверів, розміщених в дата-центрах, що забезпечують роботу десятків тисяч додатків, які одночасно використовують мільйони користувачів. Неодмінною умовою ефективного управління такою великомасштабною інфраструктурою є максимально повна автоматизація. Крім того, для забезпечення різних видів користувачів хмарним операторам, сервіс-провайдерам, IT-адміністраторам, користувачам додатків захищеного доступу до обчислювальних ресурсів хмарна інфраструктура повинна передбачати можливість самоврядування та делегування повноважень. Концепція хмарних обчислень значно змінила традиційний підхід до управління, доставки та інтеграції додатків. У порівнянні з традиційним підходом, хмарні обчислення дозволяють управляти більшими інфраструктурами, обслуговувати різні групи користувачів у межах однієї хмари, а також означають повну залежність від провайдера хмарних послуг [1]. Таким чином актуальним є дослідження, повязані із застосуванням корпоративних хмарних сервісів.

Метою статті є розробка плану заходів щодо автоматизації бізнес- процесів в організації засобами GSuite.

Основна частина. Керуючись даними дослідницької фірми Radicati [1], а також провівши власний аналіз корпоративних хмарних сервісів (WorkXpress, Dropbox, AppDynamics, Office 365, G Suite) нами визначено доцільність використання сервісу G Suite. Для роботи з пакетом бізнес-додатків необхідно створити акаунт G Suite, вказавши ім'я домену для сервісів Google (рис.1). Після підтвердження права власності на домен співробітники зможуть користуватися Gmail, Календарем, Диском та іншими основними продуктами G Suite. Доступними стануть додаткові сервіси, до яких відносяться Google+, Hangouts, Blogger та ін.

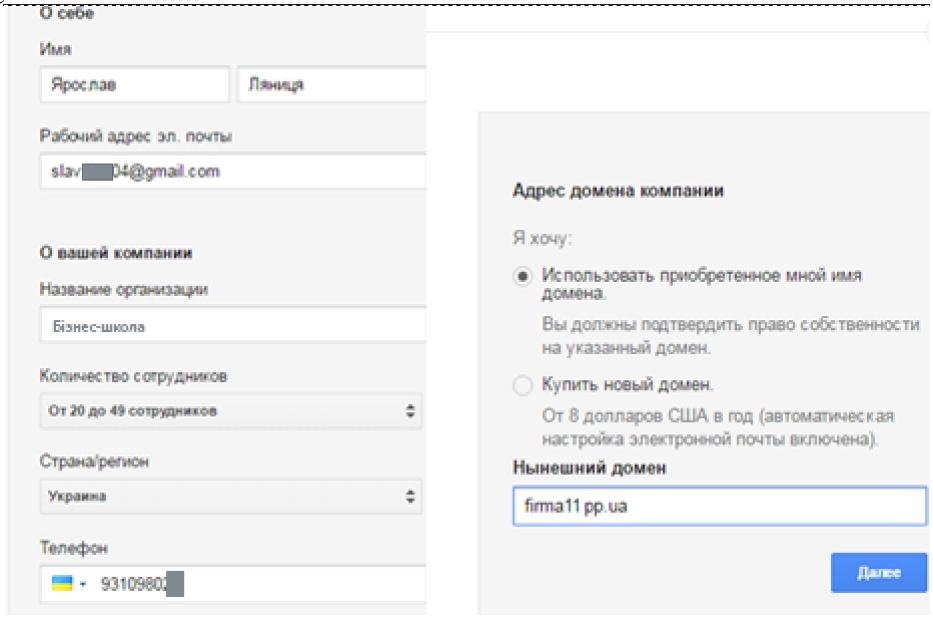

Рис. 1. Створення аккаунту в G Suite

Перед тим як працівники компанії зможуть увійти в систему і отримати доступ до послуг G Suite, вони потребують облікових записів користувачів, які будуть забезпечувати взаємодію співробітників на основі розмежованих прав доступу. Організаційно-функціональна структура організації (рис. 2) передбачає роботу 5 підрозділів: відділ маркетингу, відділ продажів, відділ продуктів, операційний відділ, інфраструктурний відділ.

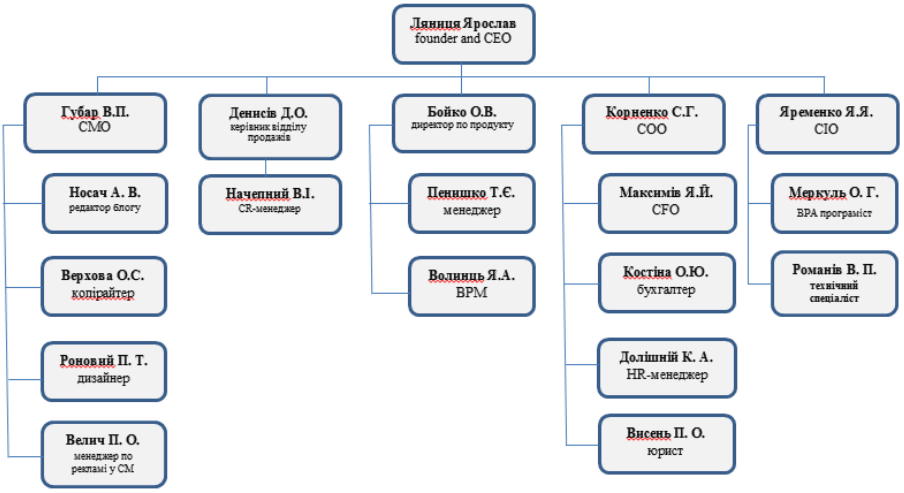

Рис. 2. Приклад організаційно-функціональної структури організації

Для розподілу функцій використовуємо інструмент «Групи», який дозволить розмежовувати права доступу відповідно до займаних посад. Додаємо 18 користувачів за допомогою консолі адміністратора (рис. 3), заповнивши необхідні поля: ім'я, прізвище, основна електронна адреса, номер телефону, адреса, ідентифікатор працівника, посада, відділ.

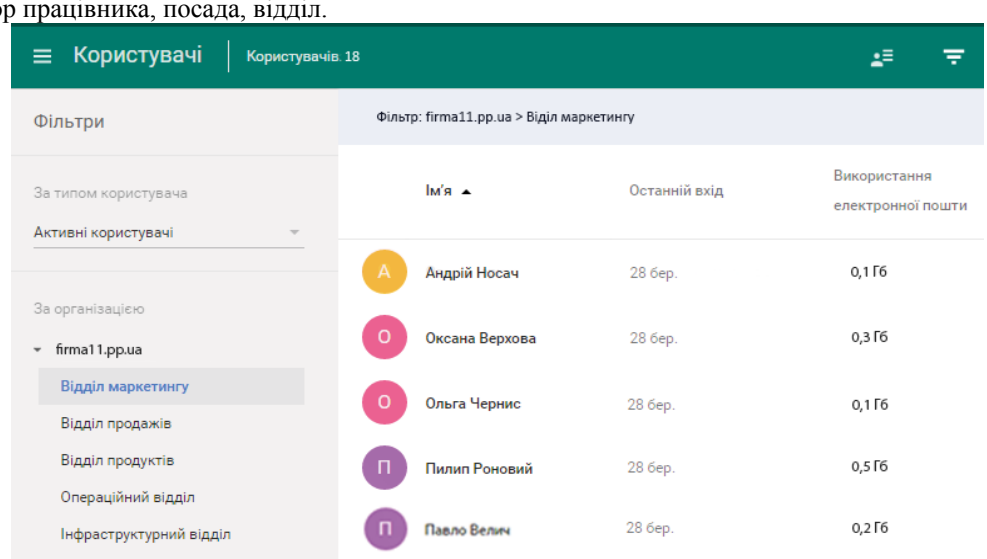

Рис. 3. Додавання облікових записів працівників маркетингового відділу

Варто відзначити, що багато сервісів, додатків та інструментів не будуть активними до того моменту, поки не відбудеться підтвердження доменного імені. Для виконання перевірки додаємо мета-тег, відредагувавши домашню сторінку firma11.pp.ua. Код не вплине на роботу веб-сайту або електронної пошти. Копіюємо та вставляємо мета-тег на домашнюю сторінку (в розділі <head> перед розділом <body> домашньої сторінки) за адресою http://firma11.pp.ua.

Мета-тег:

<meta name="google-site-verification"
content="<metaname="google-site-verification"
content="dI3oForp6bjurVR470EaahbnMTAgugsjo828dmbJmeM" />" />

Наступним кроком є створення нових записів MX для GSuite. Створюємо наведені нижче записи MX у вказаному порядку (табл. 1). Додаємо записи MX для GSuite із найвищим пріоритетом, тобто найменшим числовим значенням у стовпці пріоритету.

Таблиця 1

Записи MX

Пріоритет	Ім'я | Хост | Псевдонім	Значення | Призначення
1	@	ASPMX.L.GOOGLE.COM
5	@	ALT1.ASPMX.L.GOOGLE.COM
5	@	ALT2.ASPMX.L.GOOGLE.COM
10	@	ALT3.ASPMX.L.GOOGLE.COM
10	@	ALT4.ASPMX.L.GOOGLE.COM

Видаляємо існуючі та зберігаємо нові записи MX. Після цього натискаємо кнопку «Підтвердити домен і налаштувати пошту» і отримуємо повідомлення про успішне підтвердження домену. (рис. 2.7)

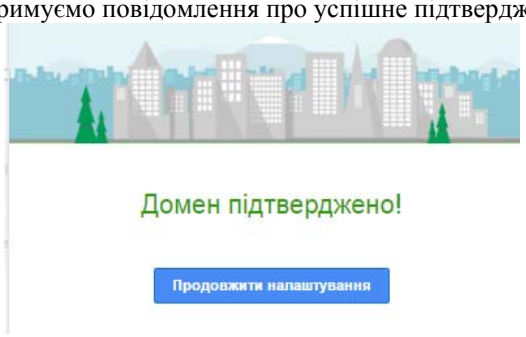

Рис. 4. Вікно підтвердження домену

Оптимальна робота організації залежитиме від безпеки електронної пошти, тому ми налаштовуємо аутентифікацію електронної пошти за допомогою DKIM. Один із способів захиститися від спуфінгу – додати цифровий підпис в заголовки вихідних повідомлень відповідно до стандарту DKIM. Цей спосіб передбачає шифрування заголовків вихідних повідомлень за допомогою закритого ключа домену, а також додавання відкритої версії ключа в запис DNS домену. Сервери-одержувачі можуть завантажити відкритий ключ, щоб розшифрувати заголовки вхідних повідомлень і перевірити, чи дійсно повідомлення виходить від заявленого відправника.

Для додавання підпису у вихідні повідомлення створюємо ключ домену, на основі якого G Suite буде формувати підписані поштові заголовки, унікальні для нашого домену. Також потрібно додати відкритий ключ до записів DNS домену. Щоб перевірити джерело повідомлення, одержувач може завантажити відкритий ключ і з його допомогою переконатися в справжності підпису.

Тепер генеруємо 2048-розрядний ключ в консолі адміністратора, перейшовши в Додатки>Gmail>Аутентифікація електронної пошти. Вибираємо домен firma11.pp.ua>Створити новий запис> 2048-бітний ключ>Створити. Текстове поле містить інформацію, необхідну для створення запису DNS. Одержувачам потрібен цей запис для завантаження відкритого ключа домену(рис. 5).

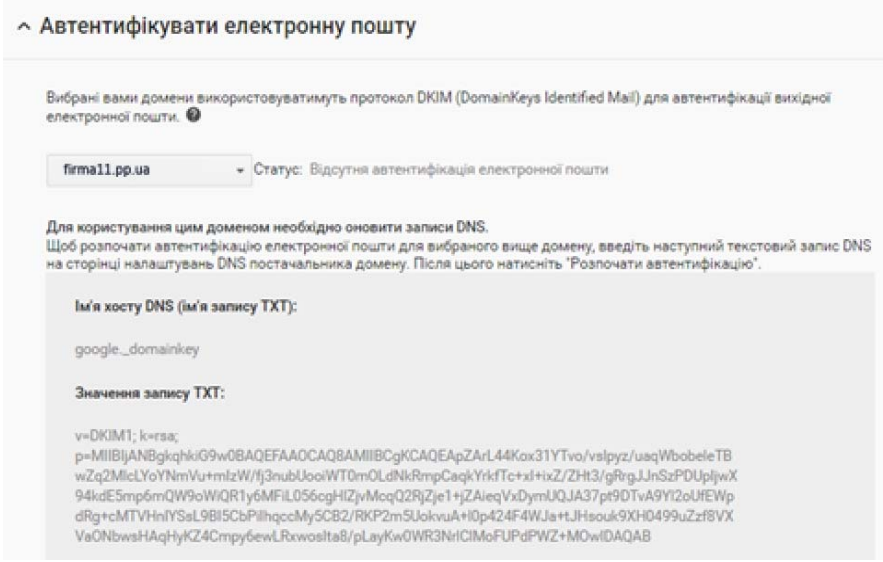

Рис. 5. Аутентифікація електронної пошти

Вмикаємо підпис повідомлень електронної пошти. Тепер заголовки DKIM додаватимуться у вихідні повідомлення. Це дозволить відслідковувати потік кореспонденції та переконатися, що джерела вихідних повідомлень належним чином проходять аутентифікацію.

Висновки. Для автоматизації бізнес-процесів доцільно використовувати хмарний сервіс GSuite, оскільки співробітники можуть користуватися Gmail, Календарем, Диском,Google+, Hangouts, Blogger та іншими основними продуктами G Suite. Як наслідок – збільшення ефективності функціонування організації, за рахунок підвищення продуктивності праці працівників. Налаштування аутентифікації електронної пошти за допомогою DKIM дозволило захиститись від спуфінгу та загалом підвищити безпеку використання електронної пошти.

ЛІТЕРАТУРА

1. Thomas Erl. Cloud Computing: Concepts, Technology &Architecture / Thomas Erl – O. : Prentice Hall, 2014 – 506 p.
2. Матеріали центру навчання GSuite: [Електронний ресурс]. Режим доступу: https://gsuite.google.ru/learning-center.