УДК 004.5
DOI 10.18372/2786-5495.1.15757

Бут Володимир Анатолійович
кандидат наук з державного управління,
директор Інституту інноваційних освітніх технологій,
Національний авіаційний університет,
м. Київ, Україна
Гнатюк Віктор Олександрович
кандидат технічних наук, доцент,
заступник директора Інституту інноваційних освітніх технологій,
Національний авіаційний університет,
м. Київ, Україна

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ У НАЦІОНАЛЬНОМУ АВІАЦІЙНОМУ УНІВЕРСИТЕТІ

Анотація. *Сучасний ринок надання освітніх послуг підлаштовується під запити людей та обставин. Пандемія COVID-19 та карантин внесли корективи в освіту бакалаврів та магістрів майже в усіх університетах світу. Перехід до онлайн освіти з використанням сучасних Інтернет-технологій призвів до певних проблем у системі вищої освіти. Не винятком є і Національний авіаційний університет, який рік тому, згідно наказу ректора перейшов до дистанційного навчання на базі платформи Google Workspace. З огляду на це, метою роботи є дослідження особливостей організації освітнього процесу у Національному авіаційному університеті в період пандемії COVID-19. Також, у роботі здійснено проаналізовано рішення, що використовуються в Google Workspace для забезпечення кібербезпеки.*

Ключові слова: *освітній процес, дистанційне навчання, Google Workspace.*

Annotation. *The modern market for educational services adapts to the demands of people and circumstances. The COVID-19 pandemic and quarantine have made adjustments to the education of bachelors and masters in almost all universities around the world. The transition to online education using modern Internet technologies has led to certain problems in the higher education system. The National Aviation University switched to distance learning based on the Google Workspace platform a year ago. The aim of the work is to study the peculiarities of the organization of the educational process at the National Aviation University during the pandemic COVID-19. Also, the paper analyzes the solutions used in Google Workspace to ensure cybersecurity.*

Keywords: *educational process, distance learning, Google Workspace.*

Пандемія COVID-19 та карантин внесли корективи в освіту бакалаврів та магістрів майже в усіх університетах світу. Перехід до онлайн освіти з використанням сучасних Інтернет-технологій призвів до певних проблем у системі вищої освіти. Не винятком є і Національний авіаційний університет, який рік тому, згідно наказу ректора перейшов до дистанційного навчання на базі платформи Google Workspace.

Метою роботи є дослідження особливостей організації освітнього процесу у Національному авіаційному університеті в період пандемії COVID-19.

Сьогодні до структури Національного авіаційного університету входить: 10 факультетів; 1 навчально-науковий інститут; 90 кафедр; 4 науково-дослідних інститути; Державна льотна академія; кафедра військової підготовки; Інститут інноваційних освітніх технологій; Інститут новітніх технологій та лідерства; Інститут міжнародного співробітництва та освіти; Інститут ІКАО та 6 коледжів. Для належного забезпечення освітнього процесу в університеті використовується платформа Google Workspace [2] (попередні назви G Suite та Google Apps for Work або Google Apps for Your Domain) — це пакет спеціалізованого хмарного програмного забезпечення й інструментів для спільної

роботи від компанії Google, доступний за передплатою. Проект вперше було запущено 28 серпня 2006 року під назвою «Додатки Google для вашого домену». У пакет Google Workspace входять такі вебзастосунки від Google, як Gmail, Контакти, Календар, Meet та Chat для спілкування; Currents для залучення співробітників; Диск для зберігання; Пакет Google Документів для створення контенту. Ці продукти доступні широкому загалу безкоштовно, однак у версіях G Suite передбачені корпоративні функції: спеціальні адреси електронної пошти в домені компанії, від 30 ГБ хмарної пам'яті для збереження документів і електронних повідомлень, а також техпідтримка телефоном і електронною поштою цілодобово та без вихідних. На відміну від готового спеціалізованого програмного забезпечення для офісів, у хмарному пакеті G Suite дані користувачів зберігаються не на традиційних внутрішніх серверах компаній, а в мережі захищених центрів обробки даних Google. Також перевагою є те, що дані та інформація зберігаються миттєво, а потім синхронізуються з іншими центрами даних для резервного копіювання. На відміну від безкоштовних, споживчих послуг, користувачі G Suite не бачать реклами під час використання цих додатків, а інформація та дані в облікових записах G Suite не використовуються для цілей реклами. Крім того, адміністратори G Suite можуть самостійно налаштувати необхідні параметри безпеки та конфіденційності.

За даними Google, пакетами G Suite користуються понад 5 мільйонів організацій у всьому світі, зокрема 60 % компаній зі списку Fortune 500. Станом на січень 2017 року G Suite нараховував 3 мільйони підприємств, що сплачують абонплату за користування, та 70 мільйонів користувачів тарифу G Suite для освіти.

В Національному авіаційному університеті у період пандемії COVID-19 використовується в навчальних цілях також: навчальна платформа Moodle; Zoom (відеоконференції, онлайн-зустрічі, чат); вебінари Clarivate Analytics українською (Web of Science Core Collection); серія вебінарів GlobalLogic Education; онлайн курси компанії Cisco; платформа онлайн-освіти Coursera; 120 безкоштовних онлайн-курсів від українських навчальних платформ: Prometheus, Edera, ВУМonline, Wisecow.

Наразі в Національному авіаційному університеті та його структурних підрозділах активно використовується близько 25000 акаунтів Google Workspace співробітників та студентів. З огляду на масштаби використання Google Workspace в Національному авіаційному університеті так і поза межами важливо враховувати загрози кібербезпеки, які можуть призвести до виникнення кіберінцидентів [1] та нанести матеріальні та іміджеві втрати. Зважаючи на сучасні загрози кібербезпеки компанія Google пропонує низку рішень для унеможливлення виникнення кіберінцидентів або мінімізації їх впливу. Історія Google почалась у «хмарі» та продовжується в ній, тому в компанії чудове розуміння ризиків, пов'язаних з безпекою робочих процесів у цьому середовищі. Корпоративні сервіси, які надаються, працюють на базі тієї самої інфраструктури (включно з механізмами захисту), що використовується для внутрішніх процесів Google. Відмовостійка глобальна інфраструктура, висококласні спеціалісти з безпеки та прагнення до інновацій – усе це дає змогу компанії Google бути лідером на ринку та пропонувати захищене й надійне середовище, яке відповідає всім нормативним вимогам. Створюючи центри обробки даних Google, в першу чергу дбають про безпеку й захист інформації. Серед засобів фізичного захисту, які використовуються, є спеціальні електронні картки доступу, огорожі по периметру та металодетектори. Щоб унеможливити проникнення зловмисників у центри обробки даних, застосовуються такі передові методи й інструменти, як ідентифікація за біометричними даними та лазери для виявлення вторгнення. У Google усі співробітники зобов'язані в першу чергу дбати про безпеку. Штат компанії налічує багато фахівців із гарантування захисту й конфіденційності даних і включає деяких провідних світових експертів у галузі безпеки інформації, додатків і мережі. Щоб захистити робочі процеси Google дбають про безпеку на всіх етапах розробки ПЗ. Це означає, що фахівці з безпеки аналізують запропоновані архітектури й перевіряють код, щоб виявити вразливі місця нового продукту чи функції та краще зрозуміти різні моделі можливих атак. У разі виникнення кіберінцидентів спеціальна команда Google Workspace [2] із

ліквідації аварій одразу реагує, аналізуючи та відновлюючи робочі процеси, щоб інцидент якнайменше вплинув на надання послуг клієнтам. Дослідницька й інформаційно-роз'яснювальна робота компанії Google сприяє захисту не лише безпосередньо клієнтів, а й набагато ширшої спільноти інтернет-користувачів. У штаті Google є команда Project Zero, яка працює над виявленням уразливих місць із високим рівнем впливу в популярних продуктах Google та інших постачальників. У разі виникнення помилок надсилається повідомлення безпосередньо постачальникам програмного забезпечення, не розголошуючи цю інформацію третім сторонам. Компанія Google – перший великий постачальник хмарних послуг, що застосовує повну пряму секретність для шифрування вмісту, коли він переміщується між серверами Google та серверами інших компаній. Оскільки для з'єднання використовуються короткотермінові приватні ключі, то ні зловмисники, ні навіть оператор сервера не зможуть потім дешифрувати сеанс HTTPS. Багато представників галузі вже перейняли даний приклад, а інші вирішили застосовувати цей підхід у майбутньому. Абсолютно всі вхідні й вихідні повідомлення електронної пошти шифруються під час переміщення між центрами обробки даних Google та між пристроями користувачів й серверами Gmail. За допомогою маркера TLS компанія Google першою почала повідомляти користувачам, коли їхні електронні листи надсилаються без захисту. Щоб захистити дані від криптоаналітичних атак, 2013 року компанія Google подвоїла довжину ключа шифрування RSA до 2048 бітів і почала змінювати це значення кожні кілька тижнів. Такі заходи стали прикладом для інших постачальників у галузі та стимулювали їх уживати заходів для посилення безпеки даних.

З пакетом Google Workspace [2] адміністратори отримують широкі можливості для керування конфігурацією системи та налаштуваннями додатків на рівні всієї компанії. Це все доступно на єдиній інформаційній панелі разом із функціями автентифікації, захисту ресурсів і оперативного контролю. Використовуються інтегровані функції Cloud Identity, щоб керувати користувачами й вимагати багатофакторну автентифікацію та введення ключів безпеки для кращого захисту. Користувачі можуть підібрати пакет Google Workspace [2], який найкраще відповідає потребам безпеки організації.

Інноваційні рішення Google Workspace [2] для безпеки продуктів мають такі складові: доступ і автентифікація (надійний метод автентифікації, відстеження підозрілого входу в систему, централізоване керування хмарним доступом, посилена безпека електронної пошти, доступ з урахуванням контексту, програма додаткового захисту), захист ресурсів (запобігання витокам даних, виявлення спаму, виявлення зловмисного програмного забезпечення, захист від фішингу, захист бренду від причетності до фішингу), оперативний контроль (інтегрована функція керування кінцевими точками, центр безпеки, контроль доступу до сторонніх додатків, керування правами доступу до інформації, центр сповіщень, регіони збереження даних), тощо.

Сервіси Google Workspace [2] утілюють передовий галузевий досвід, відповідають суворим стандартам безпеки та вимогам щодо конфіденційності даних.

Зважаючи на передовий галузевий досвід компанії Google, відповідність суворим стандартам безпеки та вимогам щодо конфіденційності даних можна зробити висновок, що сервіси Google Workspace є чудовим інструментом для побудови освітнього простору закладу освіти. Проте, в освітніх цілях, окрім Google Workspace може бути використано і навчальна платформа Moodle; Zoom (відеоконференції, онлайн-зустрічі, чат); платформа онлайн-освіти Coursera; Prometheus, Edera, BYMonline, Wisecow тощо.

Список використаних джерел

1. Гнатюк В. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі // Безпека інформації. – 2013. – №3. – С. 175-180.

2. Google Workspace [Електронний ресурс] – Режим доступу: https://workspace.google.com.ua/intl/uk/ (20.03.2021).