© Martseniuk Y., Partyka A. Analysis of the Impact of Shadow IT on the Enterprise Cloud Infrastructure // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 2, pp. 270-280. ©

DOI: 10.18372/2225-5036.30.19239

АНАЛІЗ ВПЛИВУ ТІНЬОВИХ IT НА ІНФРАСТРУКТУРУ ХМАРНИХ СЕРЕДОВИЩ ПІДПРИЄМСТВА

Євгеній Марценюк, Андрій Партика

Національний Університет "Львівська Політехніка", Україна

МАРЦЕНЮК Євгеній Віталійович, асистент
Рік та місце народження: 1987 рік, м. Львів, Львівська обл., Україна.
Освіта: ЛДІНТУ ім. В. Чорновола 2010 рік.
Посада: асистент кафедри захисту інформації з 2023 року.
Наукові інтереси: розробка та впровадження безпечних хмарних рішень, оцінка та управління ризиками у хмарних середовищах, автоматизація бізнес процесів.
E-mail: yevhenii.v.martseniuk@lpnu.ua.
Orcid ID: 0009-0009-2289-0968.

ПАРТИКА Андрій Ігорович, к.т.н.
Рік та місце народження: 1984 рік, м. Львів, Україна.
Освіта: Національний університет «Львівська політехніка», 2006 рік.
Посада: доцент кафедри захисту інформації з 2024 року.
Наукові інтереси: безпека хмарних технологій та розподілених систем, методи і засоби захисту інформації в хмарах, бази даних та знань, безпека інфраструктури комп'ютерних мереж, етичний хакінг, AWS.
Публікації: більше 30 наукових публікацій, серед яких наукові статті, навчальний посібник, тези та матеріали доповідей на конференціях.
E-mail: andrijp14@gmail.com.
Orcid ID: 0000-0003-3037-8373.

Анотація. *Тіньові IT, які визначаються як використання IT-систем і послуг без офіційного схвалення IT-відділу, стали серйозним викликом для управління інфраструктурою хмарних середовищ у сучасних організаціях. Зростання тіньових IT напряму пов'язане зі збільшенням доступності та функціональних можливостей хмарних сервісів, що часто призводить до обходу встановлених IT-процедур і управлінських структур. Це загрожує порушенням цілісності організаційних даних і створює серйозні виклики для відповідності нормативним вимогам. У цій статті проаналізовано складну природу тіньових IT в публічних хмарних середовищах, зосереджено увагу на ризиках, які вони створюють, їхньому впливі на безпеку й операційну стабільність організацій, а також на стратегіях для їх ефективного контролю. Ризики, пов'язані з тіньовими IT, є багатогранними й включають значні загрози для захисту даних і кібербезпеки. Неконтрольоване використання хмарних сервісів може зробити організацію вразливою до зовнішніх атак та порушити дотримання нормативних стандартів, таких як GDPR чи PCI-DSS. Крім того, виникає проблема конфлікту політик, коли загальні корпоративні політики не враховують нюанси хмарних середовищ, що призводить до прогалин у безпеці. Юридичні та фінансові ризики також є значними, оскільки несанкціоноване використання хмарних послуг може призвести до штрафів і порушення регуляторних вимог.Важливою складовою контролю тіньових IT є впровадження автоматизації управління хмарними середовищами. Автоматизація дозволяє ефективно моніторити та контролювати використання хмарних ресурсів, швидко виявляти вразливості та забезпечувати дотримання стандартів безпеки. Крім того, переоцінка зручності використання офіційних IT-сервісів може знизити використання користувачами тіньових IT, роблячи офіційні рішення зручнішими та доступнішими для співробітників.*

Ключові слова: *тіньові IT, публічні хмарні середовища, AWS, ризики кібербезпеки, відповідність.*

Постановка проблеми

З розвитком хмарних технологій та їх широкою доступністю, все більше організацій використовують хмарні середовища для оптимізації своїх IT-процесів.

Однак, разом із перевагами зростає й кількість випадків використання тіньових IT, що створює нові виклики для управління інфраструктурою. Тіньові IT — це будь-яке використання інформаційних технологій, систем або послуг без офіційного схвалення IT-відділу. Їхнє поширення у хмарних середовищах сприяє обходу існуючих IT-політик, знижуючи рівень контролю над використанням ресурсів та забезпеченням безпеки.

Підприємства дедалі частіше стикаються з проблемами, спричиненими тіньовими IT у хмарних середовищах, таких як несанкціоноване використання хмарних сервісів, що може призвести до вразливостей в інфраструктурі. Наприклад, розробники або інші співробітники можуть самостійно реєструватися на хмарних платформах, таких як AWS, для швидкого тестування додатків, не інформуючи про це IT-відділ.

Аналіз останніх досліджень і публікацій

Такі дії підвищують ризик безконтрольного використання даних, створюють конфлікти між корпоративними політиками безпеки та налаштуваннями хмарних сервісів і призводять до порушення нормативної відповідності.

Основні форми тіньових IT в хмарних середовищах включають:

1. Сервіси хмарних обчислень, коли співробітники самостійно обирають хмарні платформи для своїх потреб без узгодження з IT-відділом.
2. Несанкціоноване програмне забезпечення, що використовується як альтернатива офіційним корпоративним рішенням.
3. Несанкціоноване обладнання, що не відповідає встановленим стандартам безпеки організації.
4. Несанкціонована розробка, що відбувається без належного контролю з боку IT-управління.
5. Несанкціоноване використання ресурсів, коли співробітники мають доступ до ресурсів або функцій, для яких вони не мають формального дозволу.

Тіньові IT можуть створити значні ризики для захисту даних, порушення нормативних вимог та операційної стабільності, що є серйозним викликом для підприємств, які покладаються на хмарні середовища.

Мета та постановка завдання

Метою цього дослідження є аналіз впливу тіньових IT на інфраструктуру хмарних середовищ підприємств і розробка ефективних стратегій управління для мінімізації ризиків, пов'язаних з несанкціонованим використанням IT-ресурсів. Важливо також виявити можливості автоматизації процесів та підвищення зручності використання офіційних IT-сервісів, що сприятиме зниженню випадків застосування тіньових IT.

Для досягнення мети було поставлено наступні завдання:

1. Проаналізувати природу тіньових IT у контексті хмарних середовищ;
2. Оцінити ризики, пов'язані з тіньовими IT, зокрема їх вплив на безпеку, відповідність нормативним вимогам, операційну стабільність та фінансові аспекти;
3. Дослідити можливості автоматизації управління хмарними сервісами для підвищення контролю за використанням IT-ресурсів;
4. Запропонувати стратегії підвищення зручності використання офіційних IT-сервісів, що зменшить мотивацію співробітників до використання тіньових IT;
5. Розробити рекомендації для ефективного впровадження політик і автоматизованих рішень для контролю та мінімізації ризиків, пов'язаних із тіньовими IT у хмарних середовищах.

Це дослідження дозволяє комплексно підійти до вирішення проблеми тіньових IT та забезпечити безпечне, контрольоване й ефективне використання хмарних середовищ в організаціях.

1. Ризики і Вплив Тіньових IT

1.1 Ризики безпеки

Тіньові IT по самій своїй природі створюють значні виклики у сфері безпеки для організацій, оскільки включають в себе використання IT-ресурсів, які не були перевірені або схвалені офіційним IT-відділом. Ці нелегальні додатки та пристрої можуть бути вразливими з точки зору безпеки, потенційно містити шкідливе програмне забезпечення або мати експлуатаційні вразливості, які хакери можуть використати для отримання несанкціонованого доступу. Відсутність формального контролю означає, що такі пристрої та програмне забезпечення рідко оновлюються або патчаться вчасно, якщо взагалі оновлюються, залишаючи їх постійно вразливими до нових загроз. Більше того, неправильна конфігурація ресурсів тіньових IT може ненавмисно відкрити додаткові прогалини в безпеці. Стихійне управління конфіденційними даними в межах тіньових IT також викликає серйозні занепокоєння, оскільки такі дані можуть не бути належним чином резервовані або зберігатися з необхідними заходами безпеки, що підвищує ризик втрати або розголошення даних. Нарешті, неконтрольоване використання тіньових IT може призвести до немоніторованого доступу до критичної та конфіденційної інформації компанії, що значно підвищує ризик виникнення витоків даних та крадіжки інформації.

Захист Даних та Ризики Безпеки. Несанкціоноване впровадження хмарних сервісів, що є характерною рисою тіньових IT, значно ставить під загрозу захист даних та безпеку. У сфері хмарних обчислень, де дані часто зберігаються поза приміщенням, відсутність контролю над цими сервісами може призвести до витоків і несанкціонованого доступу. [2] наголошує на тому, як привабливість зручних хмарних рішень спонукає користувачів обходити встановлені IT-протоколи, тим самим піддаючи конфіденційні дані потенційним кіберзагрозам. Наприклад, нещодавно багатонаціональна корпорація зіткнулася з серйозним витоком даних, коли конфіденційна інформація про клієнтів була розкрита через несанкціонований хмарний сервіс зберігання даних. Цей інцидент підкреслює реальні ризики тіньових IT у порушенні цілісності та безпеки даних.

Затінення Політик у Хмарній Авторизації. Інший критичний ризик, асоційований з тіньовими IT у хмарних середовищах - це затінення політик. Як детально описано Захуром, Бібі та Перріном [3], політики вищого рівня в хмарних середовищах можуть випадково затушовувати або конфліктувати з політиками безпеки нижчого рівня, що призводить до непомічених вразливостей. Прикладом цього є організації, де загальні політики доступу до хмари не враховують детальні дозволи, необхідні для різних груп користувачів, що створює прогалини в безпеці, які можуть бути використані зловмисниками (рис. 1).

1.2 Ризики Відповідності

Присутність тіньових IT у організаціях, особливо в тих, що працюють у суворо регульованих сферах, становить значний ризик з точки зору дотримання нормативних вимог. Аудитори, завданням яких є перевірка дотримання організаціями конкретних нормативних стандартів, можуть негативно відреагувати на виявлення використання несанкціонованих IT-ресурсів. Ця негативна реакція зумовлена потенціалом таких ресурсів обійти встановлені протоколи захисту даних та безпеки, тим самим порушуючи вимоги дотримання нормативів.

Фінансові наслідки для організацій можуть бути значними, оскільки можуть накладатися великі

штрафи як покарання за відсутність адекватного контролю за даними. Ці штрафи є відчутним відображенням ризиків відповідності, пов'язаних з тіньовими IT, підкреслюючи необхідність для організацій встановити надійні управлінські рамки для зменшення ризиків, пов'язаних із несанкціонованими IT-активами, і забезпечення відповідності нормативним вимогам. [4]

1.2 Ризики Відповідності

Присутність тіньових IT у організаціях, особливо в тих, що працюють у суворо регульованих сферах, становить значний ризик з точки зору дотримання нормативних вимог.

Аудитори, завданням яких є перевірка дотримання організаціями конкретних нормативних стандартів, можуть негативно відреагувати на виявлення використання несанкціонованих IT-ресурсів.

Ця негативна реакція зумовлена потенціалом таких ресурсів обійти встановлені протоколи захисту даних та безпеки, тим самим порушуючи вимоги дотримання нормативів.

Рис. 1: Додатки з точки зору тіньових IT

Юридичні Наслідки Використання Несанкціонованих Хмарних Сервісів. Використання несанкціонованих хмарних сервісів у сценаріях тіньових IT може призвести до серйозних юридичних наслідків для організацій. Як обговорюють Уолтербуш, Фіц і Тойтеберг [5], багато співробітників, які займаються тіньовими IT-діяльностями, часто не усвідомлюють юридичних наслідків використання несанкціонованих хмарних сервісів.

Це може варіюватися від порушень законів про конфіденційність даних до порушень стандартів регуляторної відповідності. Наприклад, постачальник медичних послуг може ненавмисно порушити Закон про переносимість і підзвітність медичного страхування (HIPAA), якщо чутливі дані пацієнтів зберігаються або передаються через несанкціонований хмарний сервіс. Такі порушення можуть призвести до значних штрафів і шкоди репутації організації.

Ризики Відповідності в Тіньових IT. Ризики відповідності у тіньових IT переважно пов'язані з невиконанням галузевих регуляцій і стандартів. У таких секторах, як фінанси або охорона здоров'я, де безпека даних і конфіденційність мають велике значення, неконтрольоване використання хмарних сервісів може призвести до невідповідності таким стандартам, як Закон Сарбейнса-Оклей або GDPR. Ця невідповідність стосується не лише можливих штрафів, але й більш широкого аспекту довіри та надійності в очах клієнтів і зацікавлених сторін. Яскравим прикладом є фінансова установа, яка потрапила під регуляторний нагляд і отримала великі штрафи через невиконання моніторингу та контролю практик тіньових IT, що призвело до невідповідності стандартам фінансової звітності.

Вплив на управління IT. Підрив традиційних структур управління IT. Тіньові IT представляють собою значний виклик для традиційних структур управління IT. В середовищі, де рішення про IT-ресурси та послуги все частіше приймаються поза межами IT-відділу, централізований контроль та стратегічне планування IT-ресурсів підриваються. Ця децентралізація не тільки порушує встановлену структуру управління IT, але й призводить до несумісностей в IT-стандартах і політиках по всій організації. Наприклад, різні відділи можуть використовувати різні хмарні сервіси для подібних завдань, що призводить до неефективності та труднощів з інтеграцією і управлінням даними.

Балансування Гнучкості та Контролю. Зростання тіньових IT також підкреслює необхідність розвитку моделей управління IT, які повинні балансувати між потребою в контролі та вимогою гнучкості і швидкої інновації. Традиційні моделі управління, які часто сприймаються як жорсткі і повільні у відповіді на нові технологічні тенденції, можуть спонукати співробітників до тіньових IT як способу обійти ці обмеження. Отже, управління IT повинно адаптуватися, щоб надати рекомендації, які враховують швидке впровадження нових технологій, при цьому зберігаючи контроль над стандартами безпеки та відповідності. Наприклад, деякі організації зараз впроваджують гібридні моделі управління, які дозволяють контрольоване

використання певних хмарних сервісів, надаючи гнучкість, яку потребують співробітники, при цьому зберігаючи нагляд.[6]

Управління ІТ як Стратегічний Партнер. Щоб ефективно управляти тіньовими ІТ, управління ІТ повинно перейти від ролі контролера до стратегічного партнера. Це передбачає розуміння бізнес-потреб, які спонукають співробітників до тіньових ІТ, і надання рішень, які задовольняють ці потреби в межах управлінської структури. Приймаючи більш співпрацюючий підхід, ІТ-відділи можуть краще узгодити свої стратегії з бізнес-цілями, забезпечуючи, щоб впровадження технологій було як ефективним, так і безпечним. Успішні випадки показали, що коли управління ІТ тісно інтегроване з бізнес-стратегією, це може призвести до інноваційних рішень, які підвищують продуктивність без порушення безпеки та відповідності.

1.3 Фінансові ризики

Привабливість публічних хмарних платформ полягає в їх легкому доступі, масштабованості та сприйнятті як економічного рішення. Однак, коли співробітники чи відділи оминають офіційні канали, щоб використовувати ці сервіси без належного нагляду, організація стикається з багатогранними фінансовими ризиками.

Економічна Надмірність при Використанні Публічних Хмарних Сервісів. Використання несанкціонованих публічних хмарних сервісів для функцій, які вже надаються санкціонованими організаційними ресурсами, є яскравим прикладом економічної надмірності. Організації опиняються в ситуації, коли оплачують дубльовані послуги, оскільки офіційні та тіньові публічні хмарні інстанції працюють паралельно для виконання одних і тих же операційних потреб. Ця надмірність не тільки необгрунтовано збільшує витрати на ІТ, але й ускладнює управління даними та процеси інтеграції, що призводить до неефективності і додаткового навантаження на ресурси організації.

Приховані Витрати та Наслідки для Безпеки. Навіть безкоштовні або на перший погляд дешеві публічні хмарні додатки можуть мати значні приховані витрати. Несанкціоноване використання публічних хмарних сервісів підвищує ризик витоків даних, оскільки ці платформи можуть не відповідати стандартам безпеки та відповідності організації. Наслідки таких витоків включають не лише прямі витрати на реагування на інцидент і відновлення даних, але й довгострокові фінансові зобов'язання, що виникають через регуляторні штрафи, юридичні дії та шкоду репутації. Непрямі витрати, пов’язані з втратою довіри клієнтів і можливими бізнес-перебоями, можуть значно перевищити будь-які уявні заощадження від використання несанкціонованих хмарних сервісів.

Дублювання Витрат і Операційні Ризики. Вибір несанкціонованих публічних хмарних рішень замість затверджених організаційних варіантів призводить до дублювання витрат на хмарні послуги. Ця практика не тільки є зайвими фінансовими витратами, але й впроваджує операційні ризики. Відсутність координації між тіньовими та санкціонованими ІТ-ресурсами може призвести до утворення інформаційних силосів, непослідовних практик управління даними та неефективного використання ресурсів. Додатково, неконтрольоване використання публічних хмарних сервісів може призвести до прогалин у дотриманні нормативних вимог, що піддає організацію регуляторному нагляду та можливим штрафам, витрати від яких є яскравим прикладом фінансових ризиків тіньових ІТ, що виходять за межі простого дублювання витрат. [7]

1.4 Інтероперабельність

Виклики Інтероперабельності в Публічній хмарній Інфраструктурі: Усунення Розриву між Тіньовими ІТ і Офіційними Діяльностями ІТ-відділу. Поява тіньових ІТ в організації, особливо коли це стосується публічних хмарних сервісів, суттєво ускладнює інтероперабельність між різними відділами та офіційним ІТ-відділом. Ця складність виникає через впровадження різних програм і хмарних сервісів без узгодженої стратегії, що призводить до фрагментованого ІТ-ландшафту, який перешкоджає когезії даних і операційній ефективності.

Виклики Гармонізації Даних. Використання різних програмних рішень у різних відділах вимагає додаткових процесів для забезпечення гармонізації даних. Це передбачає перетворення та форматування даних у загальноприйнятий формат, який можна безперешкодно інтегрувати і використовувати в усій організації. Такі зусилля потребують не лише технічних ресурсів, але й часу та фінансових витрат, часто вимагаючи використання спеціалізованих інструментів або платформ для інтеграції даних.

Фрагментація Хмарних Сервісів та Пов'язані Витрати. Коли відділи незалежно вибирають різні публічні хмарні сервіси, організація стикається з мультихмарним середовищем, де дані знаходяться в ізольованих екосистемах. Кожен постачальник хмарних послуг може мати свій набір протоколів, стандартів і сервісів, що ускладнює інтероперабельність даних. Більше того, передача даних між цими сервісами може спричинити додаткові витрати, особливо якщо йдеться про великі обсяги даних або частий обмін даними між платформами. Постачальники хмарних послуг часто стягують плату за вихідний трафік або виклики API, що може призвести до значних витрат, про які центральний ІТ-відділ може не знати.

1.5 Срібний Обрій Тіньових ІТ

Прийняття Інновацій та Рішень, Орієнтованих на Користувачів. Тіньові ІТ часто розглядаються через призму обережності через потенційні ризики для безпеки даних, відповідності нормативним вимогам та фінансового управління. Однак ця перспектива не враховує цінні інсайти та інноваційний потенціал, які діяльність тіньових ІТ може принести організації. Визнання та використання позитивних аспектів тіньових ІТ можуть перетворити сприйняті виклики на можливості для зростання та вдосконалення ІТ-стратегій.

Інсайт в Потреби та Вподобання Користувачів. Однією з найзначніших переваг тіньових ІТ є їх здатність виявляти справжні потреби та вподобання користувачів всередині організації. Коли співробітники звертаються до несанкціонованих інструментів і сервісів, це часто свідчить про те, що існуючі ІТ-рішення не повністю відповідають їхнім вимогам або що є прогалини у доступних технологічних пропозиціях. Цей прямий зворотний зв'язок від користувачів надає ІТ-відділу важливі інсайти щодо того, де необхідні покращення, що дозволяє більш орієнтоване на користувачів планування та розробку ІТ-рішень.

Ключова перевага 1: Тіньові ІТ діють як механізм зворотного зв'язку знизу вгору, висвітлюючи конкретні потреби та вподобання робочих процесів різних відділів. Аналізуючи типи рішень, які співробітники шукають самостійно, ІТ-відділ може краще зрозуміти змінювані технологічні потреби організації та відповідно адаптувати свою стратегію.

Коллективне Вирішення Проблем та Інновації. Тіньові ІТ представляють собою колективне вирішення проблем у дії. Співробітники, які займаються тіньовими ІТ, не просто обходять офіційні канали, а активно шукають рішення своїх проблем. Цей проактивний підхід до вирішення проблем може призвести до відкриття інноваційних інструментів і робочих процесів, які ІТ-відділ міг не врахувати. Багато успішних ІТ-програм та інструментів, що використовуються сьогодні, виникли з таких ініціатив знизу і пізніше були офіційно прийняті та інтегровані в ІТ-інфраструктуру організації.

Ключова перевага 2: Прийняття тіньових ІТ як форми колективної інновації сприяє культурі творчості та вирішення проблем в організації. Це визнає цінний внесок, який співробітники можуть зробити в ІТ-ландшафт, і використовує їхній практичний досвід для покращення та інновацій ІТ-послуг і рішень. [8]

1.6 Стратегічні Підходи до Використання Тіньових ІТ

Формалізуйте Процес Подання Інновацій: Створіть канали, через які співробітники можуть пропонувати інструменти та рішення, які вони вважають корисними, дозволяючи ІТ-відділу оцінювати та, можливо, офіційно впроваджувати ці інновації.

Проводьте Регулярні Оцінки Потреб: Спілкуйтеся з користувачами в усій організації, щоб зрозуміти їхні технологічні потреби та труднощі, прагнучи зменшити необхідність звернення до тіньових ІТ-рішень.

Сприяйте Культурі Співпраці в ІТ: Розвивайте етику ІТ-відділу, яка буде сприйматися як доступна та чутлива до потреб користувачів, заохочуючи відкритий діалог про нові інструменти та технології.

Змінивши наратив про тіньові ІТ з ризику, який потрібно пом'якшити, на можливість для інновацій, орієнтованих на користувачів, організації можуть скористатися творчістю та винахідливістю свого персоналу для вдосконалення своїх ІТ-стратегій і рішень. [9]

2. Стратегії Пом'якшення Ризиків та Зменшення Тіньових ІТ

Розуміння масштабу та впливу тіньових ІТ в організації, особливо в контексті публічних хмарних середовищ, є ключовим для розробки ефективних стратегій управління. Легкість доступу та широке впровадження публічних хмарних сервісів суттєво збільшили поширеність тіньових ІТ, оскільки відділи та окремі особи можуть легко придбати хмарні послуги без затвердження ІТ-відділу.

Як технологічні рішення, так і проактивна взаємодія є необхідними для отримання інсайтів щодо цих несанкціонованих ІТ-діяльностей. Зосередившись на публічних хмарних середовищах, організації можуть налаштувати свої стратегії управління для вирішення унікальних викликів та ризиків, пов'язаних з несанкціонованим використанням хмарних сервісів, забезпечуючи комплексний підхід до підтримки безпеки, відповідності вимогам і операційної ефективності.

2.1 Автоматизований підхід до стратегії пом'якшення ризиків

У вирішенні ризиків, пов'язаних з тіньовими ІТ, особливо в публічних хмарних середовищах, важливо визначити та пріоритизувати ключові зони ризику. Зосереджуючись на цих сферах, організації можуть розробити більш ефективну стратегію для пом'якшення потенційних загроз, які створюють тіньові ІТ. Основні зони ризику включають:

Впровадження Брокеру Безпеки Доступу до Хмари (CASB). Однією з основних стратегій пом'якшення ризиків тіньових ІТ є впровадження брокера безпеки доступу до хмари (CASB). CASB виступають як точка застосування політики безпеки, розташована між споживачами хмарних сервісів та постачальниками хмарних сервісів, для поєднання та впровадження політики безпеки підприємства під час доступу до хмарних ресурсів. CASB можуть забезпечити видимість несанкціонованих хмарних додатків, допомагаючи організаціям контролювати та моніторити хмарний трафік. Селвам [10] підкреслює ефективність CASB у вирішенні питань несанкціонованих SaaS-додатків та управлінні дозволами сторонніх додатків, тим самим зменшуючи ризики, які створюють тіньові ІТ.

Розробка Безпечних Моделей Обміну Інформацією в Публічних Хмарах. Створення безпечних моделей обміну інформацією в публічних хмарах є ще однією важливою стратегією.

Як зазначають Чжан, Патва та Сандху [11], ці моделі є важливими для пом'якшення ризиків, пов'язаних з тіньовими ІТ у публічних хмарах. Забезпечуючи безпечну та контрольовану співпрацю, ці моделі гарантують, що навіть коли співробітники використовують хмарні сервіси поза межами офіційної ІТ-інфраструктури, дані залишаються захищеними. Цей підхід сприяє балансу між гнучкістю хмарних послуг і вимогами безпеки організації.

Активне Управління та Контроль за Використанням Хмарних Сервісів. Проактивне управління та контроль за використанням хмарних сервісів в організації є ключем до запобігання поширенню тіньових ІТ. Це передбачає не лише впровадження технологічних рішень, але й сприяння культурі, в якій співробітники розуміють ризики, пов’язані з несанкціонованими хмарними сервісами. Уолтерс [12] пропонує, щоб ІТ-відділи тісно співпрацювали з іншими відділами для визначення та затвердження хмарних сервісів, які відповідають як бізнесовим, так і безпековим потребам організації. Цей колаборативний підхід може суттєво зменшити поширення тіньових ІТ та забезпечити безпечне та ефективне використання хмарних сервісів. [13]

2.2 Оптимізація ІТ-операцій для Стратегічного Узгодження з Бізнесом

У динамічному середовищі управління технологіями в організації балансування між задоволенням потреб користувачів і дотриманням вимог безпеки, відповідності та бюджетних обмежень є значним викликом. Вирішення цього виклику вимагає не лише управління ІТ-ресурсами, але й перетворення ІТ-відділу на стратегічного партнера, який тісно узгоджений з потребами та цілями бізнесу.

Оптимізація ІТ-процесів. Ефективність ІТ-операцій є критично важливою для задоволення швидко

змінюваних вимог сучасного бізнес-середовища. Оптимізація IT-процесів включає критичну оцінку існуючих процедур для виявлення вузьких місць і надлишків.

Цей процес включає:

- автоматизація: впровадження автоматизації для рутинних завдань, таких як оновлення програмного забезпечення, управління обліковими записами користувачів та резервне копіювання даних, може суттєво зменшити час і ресурси, необхідні для цих заходів, дозволяючи IT-персоналу зосередитися на більш стратегічних ініціативах;
- спрощення процесів затвердження: перегляд процесів затвердження для усунення непотрібних етапів без шкоди для безпеки або відповідності може прискорити надання IT-ресурсів і послуг, підвищуючи задоволеність користувачів та зменшуючи спокусу використовувати тіньові IT-рішення;
- частий перегляд і адаптація: безперервний моніторинг та адаптація IT-процесів для задоволення змінюваних потреб бізнесу забезпечує гнучкість і швидку реакцію IT-відділу. [14]

*Становлення Бізнес-Партнером***.** Перехід від традиційної орієнтованої на обслуговування ролі до ролі стратегічного бізнес-партнера передбачає проактивний підхід до розуміння та задоволення технологічних потреб організації:

- залучення та комунікація: регулярне залучення користувачів та зацікавлених сторін для обговорення їхніх викликів та вимог допомагає побудувати довіру і забезпечує, щоб IT-рішення були тісно узгоджені з бізнес-цілями;
- освіта та обізнаність: активне навчання користувачів про доступні IT-ресурси та рішення може розвіяти міфи про технології та надати користувачам можливість використовувати офіційні канали для задоволення своїх IT-потреб. Це включає проведення семінарів, розсилку інформаційних бюлетенів та індивідуальні консультації для обговорення можливих IT-рішень;
- колаборативна розробка рішень: залучення користувачів до процесу оцінки та вибору нових технологій сприяє формуванню відчуття відповідальності та партнерства. Колаборативне прийняття рішень забезпечує, щоб інвестиції в IT були безпосередньо пов'язані з підвищенням продуктивності та досягненням бізнес-цілей [15];
- розробка політик: співробітники повинні бути поінформовані про потенційні загрози безпеці та правові наслідки використання несанкціонованих хмарних послуг. Окрім освіти, організації повинні розробити IT-політики, які чітко визначають прийнятні та неприпустимі способи використання хмарних послуг, тим самим надаючи рамки, які спрямовують поведінку співробітників у безпечний та відповідний спосіб. [16]

Вплив Партнерства IT-бізнесу. Коли IT-відділ функціонує як інтегрований бізнес-партнер, він досягає глибшого розуміння потреб організації та краще позиціонує себе для розробки рішень, які є ефективними і стратегічно узгодженими. Це партнерство:

- зменшує поширеність тіньових IT, надаючи своєчасні та релевантні рішення, що задовольняють потреби користувачів;
- підвищує організаційну гнучкість, забезпечуючи швидшу адаптацію до змін на ринку та технологічних нововведень;
- покращує управління ризиками, забезпечуючи, щоб безпека та відповідність були невід'ємною частиною всіх IT-рішень та практик. [17]

Перетворення IT на стратегічного бізнес-партнера є процесом, що потребує зобов'язань, комунікації та безперервного вдосконалення. Зосереджуючи увагу на оптимізації процесів і сприянні колаборативним відносинам з рештою бізнесу, IT може суттєво сприяти успіху організації та її здатності до інновацій.

3. Автоматизація процесів надання послуг у публічних хмарах, яка допомагає виключити тіньові IT

Впровадження автоматизації для надання послуг у публічних хмарах відіграє ключову роль у зменшенні ризиків, пов'язаних з тіньовими IT, насамперед шляхом оптимізації розгортання хмарних ресурсів і забезпечення відповідності організаційним політикам. Автоматизація процесу надання послуг [18] може суттєво підвищити ефективність, безпеку та управління в публічних хмарних середовищах, безпосередньо вирішуючи фактори, які часто призводять до виникнення тіньових IT. Ось ключові аспекти, що ілюструють важливість автоматизації в цьому контексті.

3.1 Підвищення Безпеки та Ефективності Хмари за Допомогою Самообслуговування та Автоматичного Сканування Конфігурацій

Автоматичне сканування конфігурацій стає ключовою стратегією для підтримки безпеки хмари та оперативної ефективності, використовуючи модель самообслуговування. Цей підхід використовує центральний оркестратор, а саме платформу Rundeck, доповнену надійним інструментарієм, включаючи Ansible для автоматизації IT та Python для написання скриптів. [19]

Ці інструменти є невід'ємною частиною процесу безперервної інтеграції (CI), який характеризується суворим контролем та тестуванням коду. Оркестратор і його сценарії ретельно розроблені, щоб уникнути зберігання будь-яких даних хмарного середовища безпосередньо, натомість покладаючись на REST API-комунікації з Rundeck для виконання завдань і оновлення статусу. Ця архітектура є ключовою для масштабованості, доступності системи та підвищеної безпеки. [20]

Для зміцнення системи безпеки оркестратора, особливо в контексті оцінок хмарного середовища, рекомендується інтеграція з HashiCorp Vault для безпечного зберігання інформації.

Суть сканування конфігурацій полягає в його здатності виявляти невідповідності в хмарних конфігураціях шляхом аналізу логів середовища (аудиторських логів, логів потоку). Цей аналіз порівнюється з усталеними стандартами кібербезпеки, такими як NIST 800-53, HIPAA, PCI-DSS, SOC та ISO, забезпечуючи дотримання конфігурацій найвищих протоколів безпеки.[21]

Впровадження безперервної інтеграції, що здійснюється за допомогою аудиторських та поточних логів між хмарними середовищами та платформами, такими як Prisma Cloud, забезпечує постійний моніторинг та відповідність вимогам. Ця конфігурація забезпечує миттєвий огляд хмарної інфраструктури, дозволяючи швидко виявляти та виправляти відхилення від

стандартів безпеки або операційних орієнтирів. Впровадження безперервної інтеграції не лише зміцнює заходи безпеки, але й підвищує надійність і ефективність операцій. [22]

Розширена аналітика відіграє ключову роль в інтерпретації даних логів, висвітлюючи тенденції використання та потенційні вразливості безпеки. Цей проактивний підхід до безпеки додатково посилюється застосуванням алгоритмів машинного навчання, які прогнозують можливі проблеми на основі історичних даних, що дозволяє розробляти стратегії запобігання ризикам. [23]

Операційна гнучкість і адаптивність також є центральними елементами дизайну цієї системи. Модульний характер архітектури сценаріїв забезпечує швидку адаптацію та налаштування, відповідаючи на динамічні потреби бізнесу та змінювані технологічні ландшафти.

Вибір Ansible і Python для автоматизації та сценаріїв розташовує систему на передовій технологій, підтримуваної широкою спільнотою та регулярними оновленнями. [24]

По суті, ця модель автоматизованого самостійного сканування конфігурацій досягає безперервного контролю над хмарними конфігураціями, зовнішніми периметрами безпеки, витратами та відповідністю стандартам безпеки, підкреслюючи відданість безпеці, операційній ефективності та адаптивності (рис. 2).

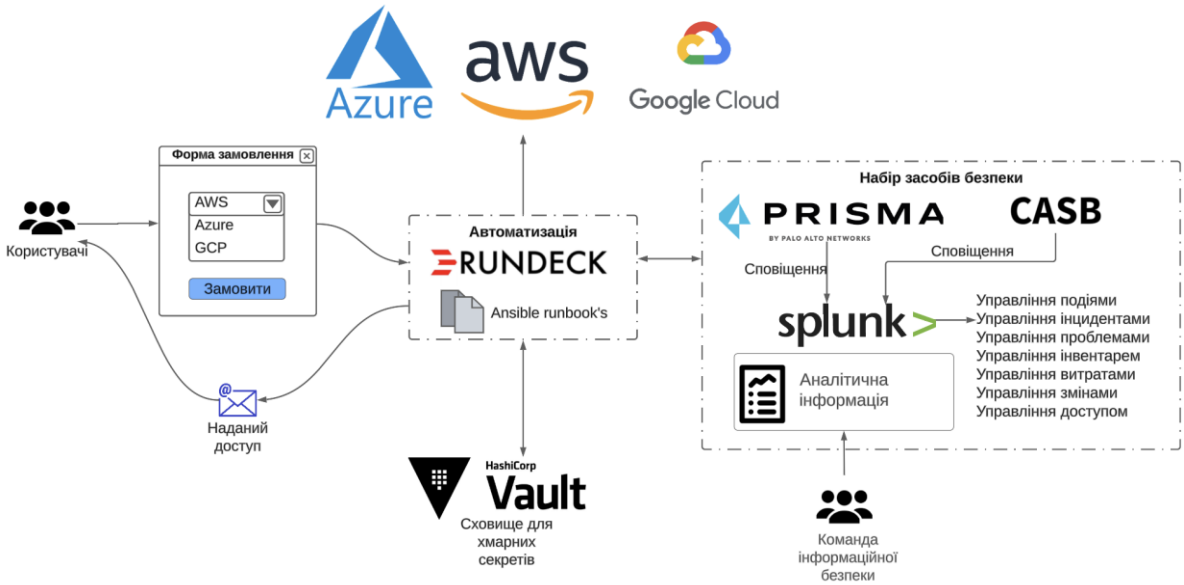

Рис. 2. Процес автоматизації забезпечення хмарних ресурсів

3.2. Фінансові Переваги Впровадження Автоматизованого Сканування Конфігурацій

Операційна Ефективність і Заощадження Витрат: Перехід на автоматизоване сканування конфігурацій значно знижує операційні витрати. Шляхом оптимізації рутинних перевірок і технічного обслуговування через автоматизацію, потреба в ручному контролі значно зменшується. Ця ефективність не лише зменшує трудозатрати та час, але й спрямовує зусилля персоналу на більш цінні завдання, що призводить до прямих фінансових вигод. [25]

Пом'якшення Фінансових Ризиків, Пов'язаних з Безпекою: Раннє виявлення вразливостей за допомогою автоматизованого сканування є критично важливим для запобігання витокам безпеки, які можуть бути фінансово виснажливими та шкодити репутації. Продовжуючи проактивно вирішувати ці вразливості, організації можуть уникнути значних витрат, пов'язаних з витоками даних, що робить автоматизоване сканування розумною інвестицією для захисту активів.

Оптимізація Хмарних Ресурсів: Автоматизоване сканування надає інформацію про використання хмарних ресурсів, виявляючи області витрат або недостатнього використання. Коригування цих ресурсів відповідно може призвести до значних заощаджень на витратах на хмари, а також підвищити ефективність і продуктивність хмарних операцій. [26]

Уникнення Штрафів, Пов'язаних із Дотриманням Вимог: Дотримання вимог комплаєнсу є важливим для уникнення фінансових штрафів та юридичних проблем. Автоматизоване сканування конфігурацій сприяє постійному дотриманню регуляторних стандартів, допомагаючи організаціям уникати фінансових проблем, пов'язаних з недотриманням вимог, і зміцнювати їх позиції в регульованих секторах.

Покращення Надійності Систем: Правильне управління конфігураціями за допомогою автоматизованого сканування сприяє надійності та безперебійній роботі систем. Фінансові наслідки простоїв—втрати доходів та витрати на відновлення—є значними, що робить стабільність, забезпечену регулярним скануванням, цінним активом для підтримки безперервної діяльності бізнесу.

Стратегічний Організаційний Ріст: Окрім безпосередніх фінансових вигод, автоматизоване сканування конфігурацій відповідає більш широким стратегічним цілям, сприяючи формуванню організаційної культури ефективності, безпеки та відповідності регуляторним вимогам. Хоча ці переваги можуть бути не відразу вимірювальні, вони відіграють ключову роль у підтриманні довгострокової життєздатності та конкурентоспроможності бізнесу.

Фінансовий аналіз автоматизованого сканування конфігурацій підкреслює його значну цінність. Початкові витрати на технології автоматизації швидко ком-

пенсуються економією на операційних витратах, покращеними заходами безпеки, ефективним управлінням ресурсами, зниженими витратами на відповідність, покращенням часу безвідмовної роботи систем і стратегічними перевагами для організації. Цей аналіз підкреслює автоматизоване сканування конфігурацій як незамінний інструмент у сучасних рамках управління хмарами.

3.3 Залучення та Комунікація

Автоматизовані Системи Зворотного Зв'язку та Комунікації: Використання автоматизації для регулярного збору зворотного зв'язку, наприклад, через автоматизовані опитування та швидкі опитування, сприяє постійному діалогу між ІТ та користувачами. Автоматизовані системи зворотного зв'язку та комунікації:<x1/> Використання автоматизації для регулярного збору зворотного зв'язку, наприклад, через автоматизовані опитування та швидкі опитування, сприяє постійному діалогу між ІТ та користувачами.

Автоматизована Звітність: Дашборди та автоматизовані звіти про використання сервісів, вирішення інцидентів і статуси проектів можуть бути надані зацікавленим сторонам, підтримуючи всіх в курсі і узгодженими з організаційними цілями та ІТ можливостями. [28]

3.4 Освіта та Обізнаність

Платформи Електронного Навчання: Автоматизоване впровадження модулів електронного навчання, адаптованих до різних ролей в організації, допомагає систематично навчати співробітників безпечному та ефективному використанню ІТ-ресурсів, включаючи хмарні сервіси. Ці платформи можуть відстежувати прогрес і адаптувати навчальні маршрути на основі результатів та зворотного зв'язку від користувачів.

Автоматизовані Сповіщення: Регулярні автоматизовані комунікації, такі як інформаційні бюлетені, сповіщення про безпеку, оновлення щодо нових інструментів та найкращих практик, допомагають тримати всіх користувачів в курсі ресурсів, що є у їхньому розпорядженні, та важливості дотримання норм безпеки і відповідності.

3.5 Розробка Спільних Рішень

Портали Самообслуговування: Автоматизація може забезпечити функціонування порталів самообслуговування, де користувачі можуть запитувати нові інструменти, отримувати доступ до пробного програмного забезпечення та надавати відгуки про свої потреби та досвід. Такі платформи можуть збирати запити та відгуки користувачів, що сприяє прийняттю рішень на основі даних при виборі та впровадженні технологій.

Автоматизовані Інструменти Прототипування: Для команд розробників автоматизовані середовища для тестування та створення прототипів нових рішень можуть прискорити процес інновацій. Ці інструменти дозволяють швидко налаштовувати та знищувати тестові середовища, заохочуючи експериментування та ітеративну розробку з безпосередньою участю користувачів. [30]

3.6 Розробка Політик

Автоматизоване Забезпечення Політик: Інструменти автоматизації можуть моніторити ІТ-середовище для забезпечення відповідності встановленим політикам, автоматично виявляючи або обмежуючи використання несанкціонованих послуг. Це включає впровадження конфігурацій безпеки та стандартів відповідності в усіх хмарних сервісах.

Динамічні Оновлення Політик: Оскільки політики змінюються, автоматизовані системи можуть повідомляти користувачів про зміни та забезпечувати, щоб усі співробітники пройшли підтвердження або навчальні сесії, що стосуються нових політик. Це забезпечує постійну та актуальну обізнаність про політики. [31]

Використовуючи автоматизацію в цих ключових областях, організації можуть сприяти створенню більш залученої, поінформованої та співпраці культури щодо використання ІТ-ресурсів.

Це не тільки знижує залежність від тіньових ІТ, роблячи офіційні канали більш доступними та чутливими до потреб користувачів, але й зміцнює відповідність і позиції безпеки. Автоматизація процесів залучення, навчання, розробки рішень та управління політиками стає основною стратегією у впорядкуванні ІТ-практик з бізнес-цілями та вимогами користувачів. [32, 33]

4. Результати

Це комплексне дослідження демонструє стратегічний і структурований підхід до управління багатохмарною інфраструктурою (AWS, Azure та GCP), який розпочався наприкінці 2020 року і тривав впродовж 2023 року. Ось загальний огляд прогресу проєкту, досягнень та важливих віх.

Кінець 2020 року: Інфраструктура включала 230 відомих облікових записів, що стало базовим рівнем для подальших удосконалень.

Розклад 2021 року і стратегічні ініціативи:

1. Аудит і Моніторинг: розпочато активні аудиторські процеси та впроваджено системи моніторингу на всіх виявлених облікових записах для забезпечення повної видимості та контролю;
2. Покращення Відповідності: суворе виправлення проблем відповідності відповідно до стандартів NIST 800-53 рев.4, підвищуючи рівень безпеки та регуляторних стандартів у всіх напрямках. (рис. 3);
3. Виявлення та Управління: ідентифікація понад 120 раніше невідомих хмарних облікових записів, інтеграція їх у офіційну управлінську систему організації;
4. Оптимізація Облікових Записів: закриття більше 30 застарілих облікових записів, оптимізація операцій та усунення непотрібних ризиків безпеки.

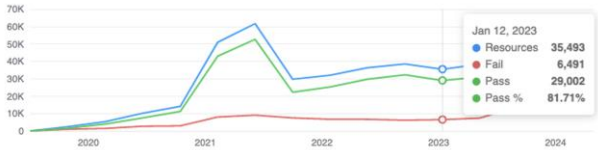

Рис. 3. Аналіз тенденцій відповідності з аналітичної панелі PaloAlto Prisma Cloud [34]

2022-2023 роки: Розширення та Стабілізація:

1. Зростання Інфраструктури: Систематичне збільшення кількості облікових записів у хмарі до 447, що відображає розширену та більш міцну інфраструктуру;

2. Безпека та Відповідність: Продовження вдосконалення заходів безпеки, що призвело до розвитку та стабілізації інфраструктури, здатної до аналізу ризиків та реагування на інциденти.

Кінець 2023 року. Основні Висновки та Досягнення:

1. Загальна кількість ресурсів: 35,493;
2. Рівень вразливостей: Нуль критичних та високих вразливостей; 954 середніх; 1,870 низьких; 3,667 неформальних. (Мал.4);
3. Рівень Відповідності: Збільшення з 67% до 82%, що свідчить про покращення управління та дотримання високих стандартів;
4. Покращення Безпеки: Усунення критичних та високих вразливостей до кінця 2023 року є свідченням ефективного управління безпекою та стратегій зменшення ризиків, що забезпечує високу безпеку хмарного середовища;
5. Зростання Відповідності: Значне підвищення рівня відповідності з 67% до 82% протягом трьох років підкреслює успішне вдосконалення управління та дотримання строгих стандартів безпеки;
6. Управління Обліковими Записами: Проактивне управління як відомими, так і раніше невідомими обліковими записами ілюструє рішучі дії проти практик тіньових IT, покращуючи контроль та видимість в хмарному середовищі;

Це дослідження випадку ілюструє важливість структурованого та проактивного підходу до управління хмарною інфраструктурою.

Завдяки регулярним аудитам, безперервному моніторингу та сильному акценту на відповідність і безпеку організація не лише покращила свою операційну безпеку, але й краще узгодила свої хмарні ресурси з організаційними цілями.

Стратегічне управління хмарними обліковими записами, включаючи ідентифікацію та усунення непотрібних або зайвих облікових записів, зіграло вирішальну роль у підвищенні ефективності витрат і управлінні ресурсами. Загалом, цей шлях відображає модель ефективного управління хмарами, яка може служити орієнтиром для подібних підприємств, що прагнуть забезпечити безпеку та оптимізувати свої хмарні середовища (рис. 4).

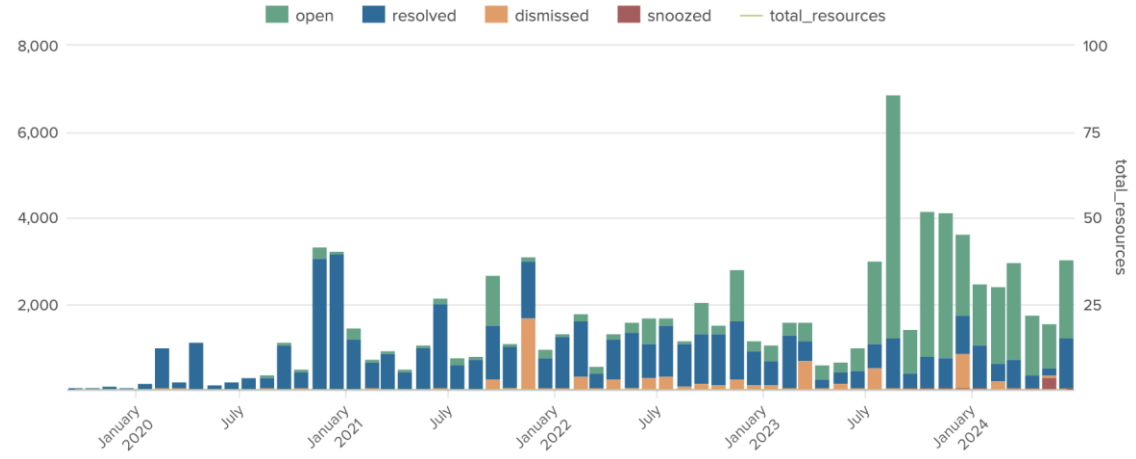

Рис. 4. Аналіз тенденцій відповідності за пріоритетами сповіщень з аналітичної панелі Splunk

Висновки. На основі проведеного дослідження було виявлено, що тіньові IT у публічних хмарних середовищах становлять значний ризик для організацій, особливо в контексті захисту даних, відповідності та безпеки. Використання несанкціонованих хмарних сервісів підвищує ймовірність витоку конфіденційної інформації, що може мати серйозні юридичні та фінансові наслідки для компаній. Окрім цього, тіньові IT ускладнюють управління ресурсами, що може призвести до додаткових витрат та втрат операційної ефективності.

Однак, разом із загрозами, тіньові IT можуть стати джерелом інновацій, якщо вони будуть належним чином інтегровані в організаційні процеси. Прийняття більш гнучкого підходу до управління IT, з акцентом на автоматизацію та співпрацю між IT-відділами та іншими структурними підрозділами, може значно зменшити ризики, пов'язані з несанкціонованим використанням хмарних сервісів.

У цьому контексті ключову роль відіграє впровадження моделі автоматизації управління конфігураціями та ресурсами хмарних сервісів. Автоматизована система, яка базується на використанні центрального оркестратора (наприклад, Rundeck) разом із такими інструментами, як Ansible та Python для автоматизації й написання скриптів, забезпечує постійний контроль над хмарними ресурсами. Важливою складовою є автоматичне сканування конфігурацій, яке дозволяє виявляти невідповідності з безпековими стандартами (NIST, HIPAA, PCI-DSS) та своєчасно їх виправляти. Це сприяє підвищенню безпеки та відповідності, знижуючи ризики тіньових IT.

Завдяки впровадженню такої автоматизованої моделі, організації можуть не лише покращити безпеку й операційну ефективність, але й оптимізувати витрати на управління хмарними ресурсами, усуваючи дублювання облікових записів і несанкціоноване використання хмарних сервісів. Впровадження таких підходів сприяє створенню культури прозорості, ефективності та безпеки в управлінні IT-інфраструктурою. Таким чином, запропоновані стратегії, зокрема впровадження брокера безпеки доступу до хмари (CASB) разом з моделями автоматизації управління хмарними ресурсами, дозволяють ефективно контролювати та

керувати використанням хмарних сервісів, що підвищує рівень захисту інформації та сприяє оптимізації витрат на IT-інфраструктуру.

Список літератури

[1]. Taylor, R. (2022, June 22). Everything you need to know about shadow IT. BlueCat Networks. https://bluecatnetworks.com/blog/everything-you-need-to-know-about-shadow-it/.

[2]. Kirin, Ivana, Shadow IT: Data Protection and Cloud Security (August 17, 2017). Available at SSRN: https://ssrn.com/abstract=3020880 or http://dx.doi.org/10.2139/ssrn.3020880.

[3]. Khan, H., Zahoor, E., Akhtar, S., & Perrin, O. (2022). A Blockchain-Based approach for secure data migration from the cloud to the decentralized storage systems. International Journal of Web Services Research, 19(1), 1-20. https://doi.org/10.4018/ijwsr.296688.

[4]. Šedivcová, Lada & Potančok, Martin. (2019). Shadow IT Management Concept for Public Sector. 65-73. 10.1007/978-3-030-37632-1_6.

[5]. Walterbusch, Marc & Fietz, Adrian & Teuteberg, Frank. (2017). Missing Cloud Security Awareness: Investigating Risk Exposure in Shadow IT. Journal of Enterprise Information Management. 30. 10.1108/JEIM-07-2015-0066.

[6]. Silic, M., & Back, A. (2014). Shadow it – A View from Behind the Curtain. Information Systems & Economics eJournal.

[7]. Edwards, Kasper. (2004). Expected and Realized Costs and Benefits when Implementing Product Configuration Systems. Mass Customization for Personalized Communication Environments: Integrating Human Factors. 10.4018/978-1-60566-260-2.ch012.

[8]. Ren, K., Wang, C., & Wang, Q. (2012). Security Challenges for the Public Cloud. IEEE Internet Computing.

[9]. Akello, P. (2021). Volitional Non-Malicious Insider Threats: At the Intersection of COVID-19, WFH and Cloud-Facilitated Shadow-Apps. 27th Annual Americas Conference on Information Systems, AMCIS 2021.

[10]. Selvam, P. (2022). Secure Cloud Services by Integrating CASB Based Approach. International Journal of Scientific Research in Engineering and Management.

[11]. Zhang, Y., Patwa, F., & Sandhu, R. (2015). Community-Based Secure Information and Resource Sharing in AWS Public Cloud. 2015 IEEE Conference on Collaboration and Internet Computing (CIC).

[12]. Walters, R. (2013). Bringing IT out of the shadows. Netw. Secur.

[13]. Zeng, X., Chen, X., Shao, G., He, T., Han, Z., Wen, Y., & Wang, Q. (2019). Flow Context and Host Behavior Based Shadowsocks's Traffic Identification. IEEE Access.

[14]. Jouini, Mouna & Aissa, Anis & Ben Arfa Rabai, Latifa. (2012). Towards quantitative measures of Information Security: A Cloud Computing case study. International Journal of Cyber-Security and Digital Forensics (IJCSDF).

[15]. Pandita, U., Katy, H., Kalpana, & Sonawane, D. (2017). Effective Management Of Proofs Of Log. International Journal of Advance Research and Innovative Ideas in Education.

[16]. Shevchuk, D., Harasymchuk, O., Partyka, A., Korshun N. Designing Secured Services for Authentication, Authorization, and Accounting of Users, Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, (2023), pp. 217-225.

[17]. Silic, Mario & Silic, Dario & Oblakovic, Goran. (2016). Influence of Shadow IT on Innovation in Organizations. Complex Systems Informatics and Modeling Quarterly. pp. 68-80. 10.7250/csimq.2016-8.06.

[18]. Vakhula, O., Opirskyy, I., Mykhaylova, O. Research on Security Challenges in Cloud Environments and Solutions based on the security-as-Code Approach, Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, (2023), pp. 55-69.

[19]. Fujinoki, Hiroshi & Mahmoudiandehkordi, Siamak. (2012). Split clouds: New security architecture for protecting user information from cloud insiders - Designs, implementation, and performance evaluations. 824-829.

[20]. Rajavaram, Harika & Rajula, Vineet & Balasubramanian, Thangaraju. (2019). Automation of Microservices Application Deployment Made Easy By Rundeck and Kubernetes. pp. 1-3. 10.1109 / CONECCT47791. 2019. 9012811.

[21]. Kenaza, Tayeb & Messai, Sami & Debicha, Islam & Sehaki, Mehdi. (2023). A Secure and Interoperable Architecture for Blockchain/IPFS Assisted Electronic Health Record Access Control and Sharing. 10.21203/rs.3.rs-3209163/v1.

[22]. Murakami, Koki & Yamada, Tsuyoshi & Yamaguchi, Rie & Goshima, Masahiro & Sakai, Shuichi. (2014). A cloud architecture for protecting guest's information from malicious operators with memory management. 155-158. 10.1145/2557547.2557585.

[23]. Wang, Huaqun. (2013). Proxy Provable Data Possession in Public Clouds. Services Computing, IEEE Transactions on. 6. 551-559. 10.1109/TSC.2012.35.

[24]. Deineka, O., Harasymchuk, O., Partyka, A., Obshta, A., Korshun N. Designing Data Classification and Secure Store Policy According to SOC 2 Type II, Workshop on Cybersecurity Providing in Information and Telecommunication Systems 2024, vol. 3654, (2024) pp. 398-409.

[25]. Rajaraman, Vaidy. (2014). Cloud computing. Resonance. 19. 242-258. 10.1007/s12045-014-0030-1.

[26]. Technology, Panel & Programs, Committee & Board, Laboratory & Sciences, Division & Medicine, National. (2016). An Assessment of the National Institute of Standards and Technology Center for Neutron Research. 10.17226/21878.

[27]. Buyya, Rajkumar & Yeo, Chee Shin & Venugopal, Srikumar & Broberg, James & Brandic, Ivona. (2009). Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems. 25. 599-616. 10.1016/j.future.2008.12.001.

[28]. Çevik, Sezi & Ustundag, Alp. (2018). Smart and Connected Product Business Models. 10.1007/978-3-319-57870-5_2.

[29]. Clark, Ruth & Mayer, Richard & Thalheimer, Will. (2003). E-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning. Performance Improvement. 42. 10.1002/pfi.4930420510.

[30]. Nordby, Anders & Vibeto, Håvard & Mobbs, Sophie & Sverdrup, Harald. (2024). System Thinking in Gamification. SN Computer Science. 5. 10.1007/s42979-023-02579-2.

[31]. Yaseen, Fenik. (2024). Chapter 2 2. Literature review 2.1. Information Security Policy availability and compliance literature.

[32]. Martseniuk, Y., Partyka, A., Harasymchuk, O., Korshun N. Automated Conformity Verification Concept for Cloud Security, Workshop on Cybersecurity Providing in Information and Telecommunication Systems 2024, vol. 3654, (2024) 25–37.

[33]. Vakhula, O., Kurii, Y., Opirskyy, I., Susukailo V. Security as Code Concept for Fulfilling ISO/IEC 27001: 2022 Requirements, Workshop on Cybersecurity Providing in Information and Telecommunication Systems 2024, vol. 3654, (2024) 59-72.

[34]. Prisma Cloud | Comprehensive Cloud Security. (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/prisma/cloud.

[35]. Splunk Enterprise | Splunk. (n.d.). Splunk. https://www.splunk.com/en_us/products/splunk-enterprise.html.

УДК 004.056.5

Martseniuk Y., Partyka A. Analysis of the Impact of Shadow IT on the Enterprise Cloud Infrastructure

Abstract. *Shadow IT, defined as the use of IT systems and services without official approval from the IT department, has become a significant challenge for managing cloud infrastructure in modern organizations. With the expansion of cloud technologies, particularly their availability and scalability, an increasing number of employees are independently implementing technological solutions, bypassing official channels. These actions are often driven by a desire for faster results, improved productivity, or convenience. However, by circumventing formal IT governance procedures, these decisions can pose serious threats to data integrity and create significant challenges for regulatory compliance.*

The growth of Shadow IT is directly linked to the increasing functionality and accessibility of cloud services, such as AWS, Microsoft Azure, or Google Cloud. These services allow quick and minimal-effort access to computing power, data storage, and additional features without the need for interaction with the IT department. This can lead to bypassing established IT procedures and governance structures, jeopardizing data confidentiality, losing control over information, and creating substantial financial and legal risks for the company. One of the key problems arising from Shadow IT is data protection and cybersecurity. Uncontrolled use of cloud services can leave an organization vulnerable to external attacks, as such services may not meet internal security standards or provide the necessary level of protection. This can lead to unauthorized access to sensitive information, data breaches, or violations of requirements such as GDPR or PCI-DSS. Additionally, conflicts between corporate policies and the specific configurations of cloud services can create security gaps. Shadow IT also increases the risk of legal and financial liability. The use of unauthorized cloud services can result in fines for regulatory violations, reputational damage, and increased costs for restoring security. The lack of proper management and control also complicates audit compliance and creates serious challenges for the organization, especially under growing regulatory pressure. One of the most effective ways to mitigate the impact of Shadow IT is to implement automation for managing cloud environments. Automation significantly improves control over cloud resource usage, allowing IT departments to quickly respond to changes, identify vulnerabilities, and ensure compliance with security standards. Additionally, automated monitoring systems provide real-time visibility into the use of cloud services, reducing the likelihood of unauthorized usage. Another important strategy for combating Shadow IT is reevaluating the usability of official IT solutions used within the organization. Shadow IT often arises as a response to the inadequacy or complexity of existing corporate solutions. If official services are more user-friendly and better tailored to the needs of users, employee motivation to use unauthorized tools will decrease. Providing access to more intuitive and functional official cloud services can significantly reduce the number of Shadow IT incidents and increase security. Thus, combining automation with a constant reevaluation of the convenience and efficiency of official IT solutions is a key strategy for minimizing the risks associated with Shadow IT. These approaches not only enhance control and security but also make IT services more attractive to users, encouraging active use within established rules and procedures.

Keywords: *Shadow IT, public cloud environments, AWS, cybersecurity risks, compliance.*

Партика Андрій Ігорович, к.т.н., старший викладач кафедри захисту інформації Національного університету «Львівська політехніка».

Andrii Partyka, Ph.D., assistant professor of the Information Protection Department of Information Security, Lviv Polytechnic National University.

Марценюк Євгеній Віталійович, аспірант, спеціальності 125 Кібербезпека Національного університету «Львівська політехніка».

Yevhenii Martseniuk, PhD sudent the Department of Information Security, Lviv Polytechnic National University.

Отримано *2 червня 2024 року*, затверджено редколегією *26 червня 2024 року*