ЗАТВЕРДЖЕНО

Наказ Адміністрації
Державної служби
спеціального зв’язку та
захисту інформації України
__ _____ 2024 року № ___

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо забезпечення кіберзахисту при використанні технології хмарних обчислень

I. Загальні положення

1. Методичні рекомендації щодо забезпечення кіберзахисту при використанні технології хмарних обчислень (далі – Рекомендації) розроблено відповідно до пункту 1 частини другої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», абзаців другого та п’ятого частини першої статті 3, пунктів 85, 86 та 88 частини першої статті 14 Закону України «Про Державну службу спеціального зв’язку та захисту інформації України», пунктів 5 та 12 Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, та абзацу другого підпункту 1 пункту 3 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411.

2. Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання.

II. Терміни та визначення понять

У цих Рекомендаціях терміни вживаються в такому значенні:

аудит (Audit) – систематичний, незалежний, задокументований процес отримання та аналізу записів, заяв про факти або іншої інформації та їх об'єктивної оцінки для визначення ступеня виконання встановлених вимог;

безпека інформації в сфері хмарних послуг (Information Security in Cloud Computing) – стан захищеності хмари (забезпечення конфіденційності, цілісності та доступності та/або їхніх комбінацій) при наданні електронних

довірчих послуг (електронних послуг): електронної ідентифікації, електронної автентифікації, електронного підпису, електронного документа, електронної доставки, електронної автентифікації вебсайтів; електронної позначки часу;

дані користувача хмарних послуг (Cloud service customer data) – клас даних, що перебувають під контролем із законних чи інших причин користувача хмарної послуги, які були введені в хмару або виникли в результаті використання її можливостей від імені користувача хмарної послуги через опублікований інтерфейс хмару;

дані надавача хмарних послуг (Cloud service provider data) – клас даних, що виникає при функціонуванні хмари та знаходиться під контролем надавача хмарних послуг. Дані про надавача хмарних послуг включають, але не обмежуються інформацією про конфігурацію та використання ресурсів, конкретну віртуальну машину хмари, розподіл ресурсів сховища та мережі, загальну конфігурацію та використання центру обробки даних, рівень відмов фізичних та віртуальних ресурсів, експлуатаційні витрати тощо;

дані, отримані від хмари (Cloud service derived data), – клас даних, що перебувають під контролем надавача хмарних послуг, отримані в результаті взаємодії користувача хмарних послуг із хмарою;

життєвий цикл інформації – етапи, через які проходить інформація, наприклад: створення або збір, обробка, поширення, використання, зберігання і розпорядження, включно зі знищенням і видаленням;

запит – складається з пошуку відповідної інформації або опису кваліфікованих фахівців. Запити варіюються від офіційних письмових запитів до співбесід і неформальних усних запитів;

кіберзахист в сфері хмарних послуг – сукупність організаційних, правових, інженерно-технічних заходів та/або їхніх комбінацій при наданні електронних довірчих послуг у процесах виявлення, реагування та відновлення після настання кіберінциденту/кібератаки;

користувач хмарних послуг (Cloud service user) – фізична або юридична особа, яка використовує хмарні послуги для забезпечення власних потреб;

ланцюг довіри, ланцюг постачання – певний рівень довіри під час взаємодії в ланцюгу постачання такий, що кожен учасник відносин «користувач-надавач» забезпечує належний захист своїх компонентів продуктів, систем і послуг;

надавач хмарних послуг (Cloud service provider) – юридична особа або фізична особа – підприємець, яка надає одну або більше хмарні послуги самостійно або спільно з іншими надавачами хмарних послуг;

обґрунтована гарантія – порука, що забезпечує впевненість, при якій ризик може бути знижено до прийнятного рівня в обставинах, що визначені порукою.

обмежена гарантія – порука, що забезпечує впевненість, при якій ризик не може бути знижений до прийнятного рівня в обставинах, що визначені порукою.

постійний моніторинг безпеки – набір процедур, направлених на підтримку обізнаності (поінформованості) про поточний стан безпеки технології хмарних обчислень в організації, для прийняття рішень щодо управління ризиками безпеки;

профіль безпеки – набір заходів захисту, які застосовуються до інформації або технології хмарних обчислень для дотримання вимог чинних нормативно-правових актів, а також спрямовані на захист потреб з метою управління ризиками безпеки;

спостереження – полягає в нагляді та аналізі процесу або процедури, що виконуються усіма учасниками процесу (надавачі хмарних послуг, користувачі хмарних послуг та треті сторони) наприклад, наглядом за виконанням контрольних дій. Воно забезпечує докази результативності процесу або процедури, але обмежується моментом часу, коли відбувається спостереження, і тим фактом, що акт спостереження може вплинути на те, як виконується процес або процедура. Спостереження є належним способом отримання доказів, якщо немає документації про роботу заходу захисту. Спостереження також корисно для фізичного контролю;

тип можливостей «платформа» (Platform capabilities type) – тип хмарних можливостей, за допомогою яких користувач хмарних послуг може розгортати, керувати та запускати створені або придбані користувачем програми, використовуючи одну або кілька мов програмування та одне або кілька середовищ виконання, що підтримуються надавачем хмарних послуг;

тип можливостей «програма» (Application capabilities type) – тип хмарних можливостей, за допомогою яких користувач хмарних послуг може використовувати програми надавача хмарних послуг;

тип можливості «інфраструктура» (Infrastructure capabilities type) – тип хмарних можливостей, за допомогою яких користувач хмарних послуг може використовувати ресурси обробки, зберігання чи мережі;

тип хмарних можливостей (Cloud capabilities type) – перелік функціональних можливостей, що надаються технологією хмарних обчислень користувачу хмарних послуг на основі використаних ресурсів;

хмара (хмарна інфраструктура) (Cloud Infrastructure) – сукупність динамічно розподілюваних та налаштовуваних хмарних ресурсів, що можуть бути оперативно надані користувачу хмарних послуг і вивільнені через глобальну та локальні мережі передачі даних;

хмарна послуга (Cloud Service) – послуга з надання хмарних ресурсів за допомогою технології хмарних обчислень;

хмарний сервіс (Cloud Service) – одна або кілька можливостей, запропонованих за допомогою технології хмарних обчислень, які впроваджуються визначеним інтерфейсом;

хмарні обчислення (Cloud computing) – парадигма надання мережевого доступу до масштабованого та еластичного пулу спільних фізичних або віртуальних ресурсів із забезпеченням самообслуговування та

адмініструванням на вимогу;

хмарні ресурси (Cloud Resource) – будь-які технічні та програмні засоби або інші компоненти інформаційної (автоматизованої) системи, доступ до яких забезпечують технології хмарних обчислень, зокрема процесорний час (обчислювальна потужність), місце у сховищах даних, обчислювальні мережі, бази даних і комп'ютерні програми;

цільовий профіль безпеки (ЦПБ) – визначений набір заходів захисту, посилених заходів захисту та додаткових рекомендацій, отриманих на першому етапі налаштування базового (галузевого) профілю безпеки з урахуванням особливостей сфери хмарних послуг.

Інші терміни в цих Рекомендаціях вживаються у значенні, наведеному в нормативно-правових актах та нормативних документах України.

III. Скорочення

У цих Рекомендаціях наведено такі скорочення:

БІ – безпека інформації

ІС – інформаційна система

НД – нормативний документ

СБІ – система безпеки інформації

ЦПБ – цільовий профіль безпеки

CAB – Conformance Assessment Body (Орган з оцінки відповідності)

CCC – Complementary Customer Controls (додаткові засобі управління користувачами)

CERT – Computer Emergency Response Team (комп'ютерна група реагування на надзвичайні події)

CRM – Customer Relationship Management (система управління взаємодіями з користувачами)

CSC – Cloud service customer (користувач хмарних послуг)

CSOC – Complementary Subservice Organization Controls (додаткові елементи управління служб хмарних сервісів)

CSP – Cloud service provider (надавач хмарних послуг)

CSRC – Computer Security Resource Center (ресурсний центр комп'ютерної безпеки)

CVSS – Common Vulnerability Scoring System (загальна система оцінки вразливостей)

DDoS – Distributed Denial of Service (розподілені атаки відмови в

обслуговуванні)

DMZ – Demilitarized Zone (демілітаризована зона)

EOL – End of Life (закінчений термін служби)

EOS – End of Service (кінець підтримки)

IDT – Interdigitated (оцифрований стандарт)

IEC – International Electrotechnical Commission (Міжнародна електротехнічна комісія)

ISO – International Organization for Standardization (Міжнародна організація зі стандартизації)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій)

OWASP – Open Web Application Security Project (відкритий проєкт забезпечення безпеки вебзастосунків)

RPO – Recovery Point Objective (цілі точки відновлення)

RTO – Recovery Time Objective (цілі часу відновлення)

SBoM – Software Board of Materials (програмна дошка матеріалів)

SDN – Software-Defined Networking (програмно визначена мережа)

SIEM – Security Information and Event Management (інформація про безпеку та управління подіями)

SSDLC – Secure Software Development Life Cycle (життєвий цикл розробки програмного забезпечення)

VLAN – Virtual Local Area Network (віртуальна локальна комп'ютерна мережа)

IV. Вимоги (профілі) до кіберзахисту при використанні технології хмарних обчислень (послуг), порядок їх впровадження та підтвердження виконання

1. Передумови вибору рівня безпеки в сфері хмарних послуг

У сфері хмарних послуг загальна схема надання хмарних послуг виглядає так. На стороні надавача хмарних послуг (CSP) забезпечується належний рівень безпеки власної хмарної інфраструктури відповідно до національних та галузевих вимог безпеки. Це досягається за рахунок розгортання в складі надавача хмарних послуг відповідних служб, на які безпосередньо будуть впливати вимоги безпеки. Хмари входять до складу загальної хмарної інфраструктури надавача хмарних послуг та складаються з хмарних ресурсів. У цьому випадку вибір рівня безпеки для надавача хмарних послуг

ґрунтується на визначеній категорії критичності його хмарної інфраструктури.

Вибір рівня безпеки для надавача хмарної послуги є одним з етапів розгортання СБІ, який ґрунтується на моделі ПВПД (плануй – виконуй – перевіряй – дій), яка визначена в ISO/IEC 27001:2022 (рис.1).

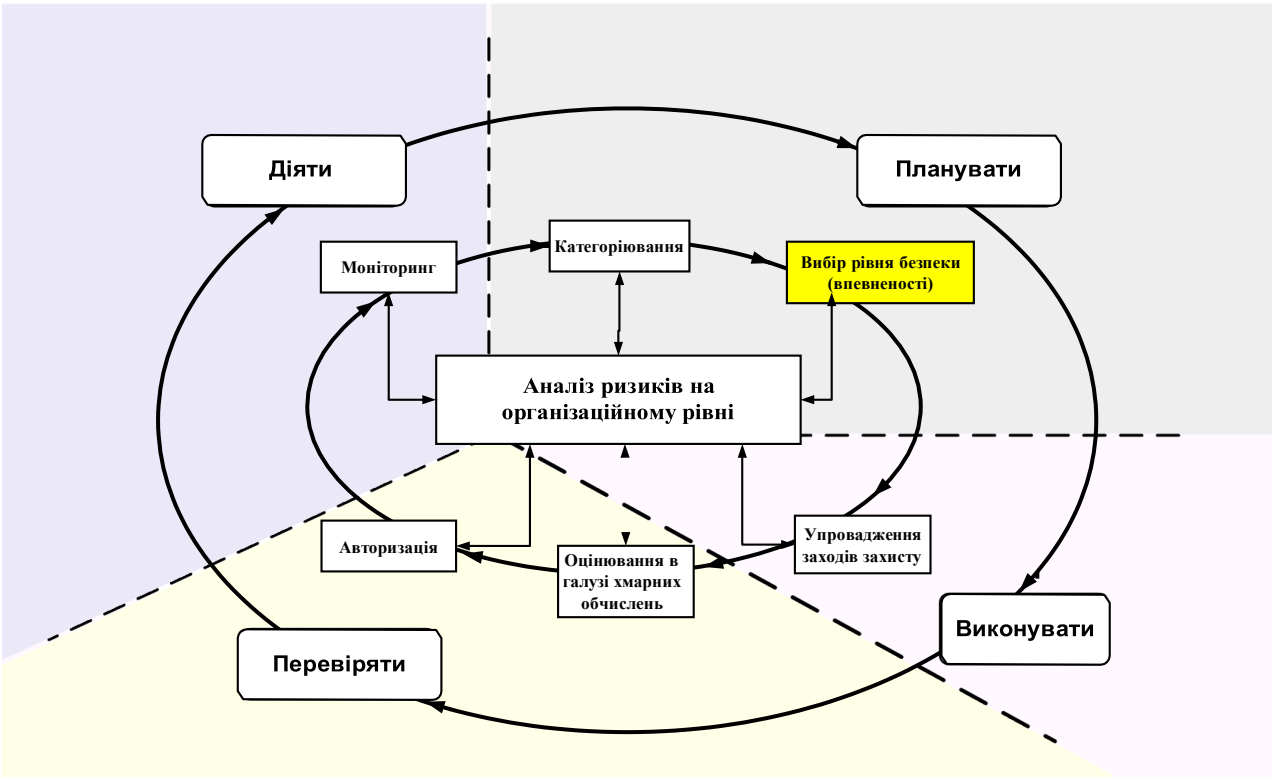

Рисунок 1 – Відповідність етапу вибору заходів захисту СБІ моделі ISO/IEC 27001:2022

Метою етапу є формулювання вимог рівня безпеки (впевненості) до хмарних послуг, а також вибір рівня галузевого профілю безпеки заходів захисту в сфері хмарних послуг.

У таблиці 1 наведено короткий опис завдань та очікуваних результатів етапу вибору рівня безпеки (впевненості) хмарних послуг.

Таблиця 1 – Завдання та результати етапу вибору рівня безпеки (впевненості) хмарних послуг

Завдання	Результати
Завдання В-1 Формулювання Програми безпекиінформації (БІ)	Програми БІ та приватності **розроблена** та **задокументована**
Завдання В-2 Вибір галузевого профілю безпеки заходів захисту в технології хмарних обчислень	**Обрано** та **задокументовано** рівень галузевогопрофілю безпеки заходів захисту в технології марних обчислень

Відповідальність за вибір заходів захисту для хмарних послуг покладається на надавача хмарних послуг (CSP). Безпосереднє виконання покладається на адміністратора безпеки або інших відповідальних осіб за БІ.

Для успішної реалізації завдань В-1 та В-2 з табл. 1 потрібно провести попередню процедуру категоріювання безпеки відповідно до НД ТЗІ 3.6-005-21, а також подальше впровадження обраних заходів захисту для хмарних послуг відповідно до НД ТЗІ 3.6-007-21.

2. Рівні безпеки (впевненості) хмарних послуг

Хмарна послуга користувачу хмарних послуг може надаватися на одному із трьох рівнів безпеки (впевненості): «Низький», «Середній» та «Високий». Вимоги до безпеки хмарних послуг зростають залежно від рівня, на якому надається хмарна послуга. Залежно від рівня відрізняються заходи захисту, які мають бути розгорнуті у хмарі. Заходи захисту, які є обов'язковими для «Низького» рівня безпеки, становлять базовий набір для забезпечення мінімально прийнятних вимог безпеки. Водночас цей перелік є широким та всеосяжним, оскільки охоплює всі основні аспекти безпеки хмарних послуг. Заходи захисту «Низького» рівня є також обов'язковими для виконання на «Середньому» та «Високому» рівнях. Заходи захисту «Середнього» рівня є також обов'язковими для виконання на «Високому» рівні. При цьому «Середній» та «Високий» рівні безпеки передбачають розширення переліку заходів захисту відповідно. При реалізації посиленого заходу захисту на будь-якому рівні безпеки (впевненості) обов'язковою вимогою є впровадження заходу захисту.

Рівень безпеки (впевненості) хмарних послуг «Низький» призначений мінімізувати ймовірність настання кіберінцидентів і кібератак і може бути визначений так:

рівень безпеки (впевненості) хмарних послуг «Низький» повинен забезпечувати обмежену гарантію того, що хмарний сервіс побудований та експлуатується з процедурами та механізмами для задоволення відповідних вимог безпеки на рівні, призначеному для мінімізації відомих основних ризиків інцидентів і кібератак;

рівень безпеки (впевненості) хмарних послуг «Низький» повинен бути придатним для хмар, які розроблені для задоволення типових вимог безпеки щодо служб для відкритих даних і систем з низькою категорію критичності;

типова модель порушника для рівня безпеки (впевненості) хмарних послуг «Низький» повинна бути визначена для суб'єктів з обмеженими навичками і повторювати відому атаку з обмеженими ресурсами, не включаючи здатність виконувати атаки соціальної інженерії.

Рівень безпеки (впевненості) хмарних послуг «Середній» призначений мінімізувати відомі ризики кіберзахисту та ризики інцидентів та кібератак, що

здійснюються суб’єктами, які мають обмежені навички та ресурси, і може бути визначений так:

рівень безпеки (впевненості) хмарних послуг «Середній» повинен забезпечити обґрунтовану гарантію шляхом оцінки Conformance Assessment Body (CAB), що хмарний сервіс побудований та експлуатується із процедурами та механізмами для мінімізації відомих ризиків кіберзахисту та ризиків інцидентів та кібератак, що здійснюються суб'єктами з обмеженими навичками та ресурсами. CAB повинен визначити, чи надавач хмарних послуг оцінив ці ризики та запровадив відповідні заходи захисту, які за ефективної роботи мінімізують ці ризики та відповідають відповідним вимогам безпеки протягом певного періоду;

рівень безпеки (впевненості) хмарних послуг «Середній» повинен підходити для хмар, які розроблені для задоволення типових вимог безпеки щодо служб для критично важливих бізнес-даних та систем із середньою категорією критичності;

типовою моделлю порушника для рівня безпеки (впевненості) хмарних послуг «Середній» має бути невелика група осіб із вмінням злому та отриманням доступу до широкого кола відомих методів злому, включаючи соціальну інженерію, але з обмеженими ресурсами, зокрема для здійснення широкого спектра атак або виявлення раніше невідомих вразливостей.

Рівень безпеки (впевненості) хмарних послуг «Високий» призначений мінімізувати ризик найсучасніших кібератак, що здійснюються суб’єктами, що володіють значними навичками та ресурсами, і може бути далі визначений так:

рівень безпеки (впевненості) хмарних послуг «Високий» повинен забезпечити обґрунтовану гарантію шляхом оцінки CAB, що хмарний сервіс побудований та експлуатується із процедурами та механізмами для мінімізації ризику найсучасніших кібератак, що здійснюються суб'єктами, які володіють значними навичками та ресурсами. CAB повинен визначити, що надавач хмарних послуг оцінив ці ризики та запровадив відповідні заходи захисту, які б ефективно діяли для мінімізації цих ризиків та відповідали вимогам безпеки протягом певного періоду;

у хмарі впроваджені заходи захисту відповідно до пункті 4 цього розділу для забезпечення автоматичного контролю за заходами захисту з метою гарантування безперервної роботи відповідно. «Високий» рівень безпеки також передбачає, що органи управління повинні регулярно перевірятися для підтвердження їх фактичної можливості запобігти порушення безпеки або виявити їх;

рівень їх з безпеки (впевненості) хмарних послуг «Високий» повинен підходити для хмарних сервісів, які розроблені для задоволення специфічних (вище рівня «Середній») вимог безпеки для критично важливих даних та систем із високою категорією критичності;

типовою моделлю порушника для рівня безпеки (впевненості) хмарних послуг «Високий» повинна бути команда висококваліфікованих працівників, які мають доступ до значних ресурсів для проєктування та виконання атак, отримання інсайдерського доступу, виявлення або придбання доступу до раніше невідомих вразливостей.

Усі рівні безпеки (впевненості) хмарних послуг, визначені у цих Рекомендаціях, можуть бути забезпечені відповідними заходами захисту (пункт 4 цього розділу), при цьому:

кожен рівень безпеки (впевненості) хмарних послуг відповідає рівню ризику, пов'язаного із передбачуваним використанням технології хмарних обчислень, як це продемонстровано у визначенні відповідних служб та типових профілів зловмисників;

кожен рівень безпеки (впевненості) хмарних послуг визначає вимоги та функціональні можливості, а також строгість та повноту, необхідні для оцінки;

кожен рівень безпеки (впевненості) хмарних послуг вимагає, щоб діяльність для оцінки передбачала перегляд технічної документації;

кожен рівень безпеки (впевненості) хмарних послуг вимагає перегляду основних процесів технології хмарних обчислень.

3. Вимоги до рівнів безпеки (впевненості) хмарних послуг

Каталог заходів захисту хмарних послуг (пункт 4 цього розділу), що визначені у цих Рекомендаціях, має чітко визначену організацію та структуру.

Характеристика заходів захисту в контексті надійності безпеки інформації та кіберзахисту хмарних послуг наведена в пункті 5 цього розділу.

Відображення каталогу заходів захисту для хмарних послуг та НД ТЗІ 3.6-006-21 наведено в пункті 6 розділу V.

На рисунку 2 проілюстровано структуру каталогу заходів захисту. У цьому каталозі визначаються технічні вимоги, які повинні виконувати Cloud Service Provider (CSP), щоб забезпечити потрібний рівень безпеки (впевненості).

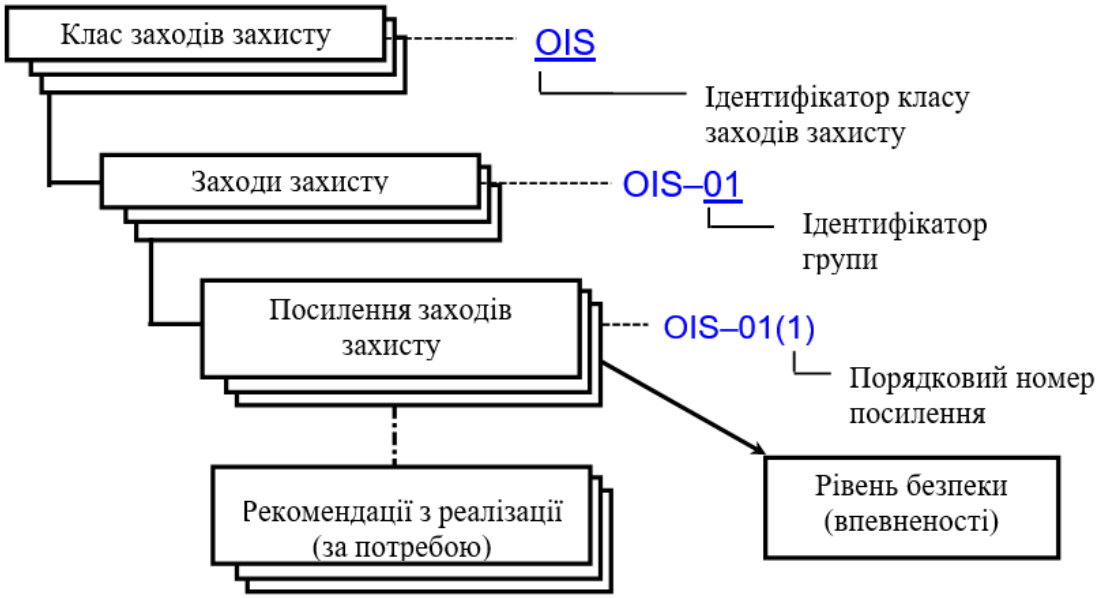

Рисунок 2 – Структура каталогу заходів захисту

Вимоги згруповані в 20 класів заходів захисту (таблиця 2), і кожен клас заходів захисту складається з певних заходів захисту. Далі наведено приклад опису вимог до хмарних послуг за класом заходів захисту (рисунок 3).

Клас заходів захисту → **Клас заходів захисту CCM – Управління змінами і конфігурацією**

Слід переконатися, що зміни та дії конфігурації інформаційних систем гарантують безпеку наданої хмарної служби.

Захід захисту → **CCM–04 Схвалення для забезпечення у виробничому середовищі**

Заходи захисту.

Зміни у хмарних службах повинні затверджуватися перед введенням у виробниче середовище.

Посилення заходів захисту → Посилення заходів:

1) затвердження змін. CSP затверджує будь-які зміни хмарної служби на основі визначених критеріїв, перш ніж вони стануть доступними CSC у виробничому середовищі.

Рекомендації з реалізації:

схвалення CSP може надавати уповноважений персонал CSP або автоматизована процедура, що забезпечує виконання визначених критеріїв;

2) залучення користувача до затвердження змін. CSP повинен залучати CSC до процесу затвердження відповідно до вимог контракту;

3) автоматичний контроль затвердження змін. CSP повинен автоматично контролювати затвердження змін, що застосовуються у виробничому середовищі, щоб гарантувати виконання CCM–04(1).

Пов'язані заходи: CCM–04(1).

Рисунок 3 – Приклад опису вимог до хмарних послуг за класом заходів захисту

Таблиця 2 – Класи заходів захисту до хмарних послуг

№ з/п	ID класу заходів захисту	Назва класу заходів захисту	Кількість груп заходів захисту	Кількість посилень заходів захистущодо рівня безпеки (впевненості) хмарних послуг		
				«Низький»	«Середній»	«Високий»
1	2	3	4	5	6	7
1	OIS	Організація безпеки інформації	4	7	11	14
2	ISP	Положення щодо безпеки інформації	3	11	15	19
3	RM	Управління ризиками	3	10	13	14
4	HR	Людські ресурси	6	14	27	33
5	AM	Управління активами	5	9	16	23
6	PHS	Фізична безпека	5	12	22	36
7	OPS	Операційна безпека	22	34	57	79
8	IAM	Управління ідентифікацією, автентифікацією і контролем доступу	9	19	51	67
9	CKM	Криптографія та управління ключами	4	4	10	13
10	CS	Безпека електронних комунікацій	9	16	27	34
11	PI	Портативність та взаємодійність	3	7	11	13
12	CCM	Управління змінами і конфігурацією	6	7	15	26
13	DEV	Розробка інформаційних систем	7	11	24	31
14	PM	Управління закупівлями	5	12	18	23
15	IM	Управління інцидентами	7	15	24	31

1	2	3	4	5	6	7
16	BC	Безперервність бізнесу	4	3	13	14
17	CO	Відповідність	4	6	11	16
18	DOC	Документація користувача хмарних послуг	6	13	23	26
19	INQ	Робота із запитами від державних органів щодо розслідувань	3	5	6	7
20	PSS	Безпека та захист виробу	5	5	14	16
		Усього:	120	220	408	535

Загальна кількість заходів захисту становить 120. Загальна кількість посилення заходів захисту (вимог до хмарних послуг) дорівнює 535, з яких до вимог «Низького» рівня безпеки (впевненості) хмарних послуг налічує 220, до «Середнього» рівня безпеки (впевненості) хмарних послуг – 188 та до «Високого» рівня безпеки (впевненості) хмарних послуг – 127.

Кожен клас заходів захисту складається із груп, які містять заходи, направлені на задоволення однотипних вимог безпеки. Група може містити один або більше відповідних заходів захисту, які структуровані так:

вимога, на яку спрямований захід захисту;

посилення заходів захисту (вимоги до хмарних послуг), яким повинен відповідати захід, спрямований на підтримку хмар, причому кожне посилення заходів захисту (вимога до хмарних послуг) пов'язано з рівнем безпеки (впевненості) хмарних послуг;

у деяких випадках вказуються додаткові рекомендації з реалізації відповідного (посиленого) заходу захисту.

3.1. Вимоги до хмарних послуг низького рівня безпеки (впевненості) хмарних послуг

Вимоги до хмарних послуг, які надаються на низькому рівні безпеки (впевненості), можуть бути повністю задоволені з упровадженням і розгортання заходів захисту, які віднесені до профілю безпеки «Низький».

У таблиці 3 розкриваються вимоги безпеки для «Низького» рівня. Вимоги безпеки задовольняються за допомогою впровадження набору заходів захисту – профілю безпеки «Низького» рівня. Метою є загальний опис рівня безпеки (впевненості) хмарних послуг.

Таблиця 3 – Вимоги безпеки для хмарних послуг «Низького» рівня

Вимоги безпеки	Рівень безпеки (впевненості) «Низький»
1	2
Гарантія безпеки	За результатами аудиту має бути зроблено висновок щодо можливості надання обмеженої гарантії того, що хмарний сервіс побудований та експлуатується з процедурами та механізмами для задоволення відповідних вимог безпеки на рівні, призначеному для мінімізації відомих основних ризиків інцидентів та кібератак.
Обґрунтування намірів	Сфера, глибина та суворість рівня безпеки (впевненості) хмарних послуг обмежуються процедурами та механізмами для тих вимог безпеки, які повинні мінімізувати лише добре відомі ризики.
Придатність	Низький рівень підходить для хмар, які розроблені для задоволення типових вимог безпеки щодо служб для некритичних даних та систем із низькою категорією критичності.
Обґрунтування придатності	«Низький» рівень забезпечує обмежену гарантію того, що існують базові процедури та механізми для запобігання ризикам та загрозам безпеці в інформаційно-комунікаційних системах з потенційно низьким впливом (наприклад: вебсайт, що містить публічну інформацію). Зазвичай він не підходить для можливостей платформи або інфраструктури, що використовуються великою кількістю служб. Низький рівень демонструє готовність системи вирішувати питання безпеки, у тому числі застосування вказівок щодо безпеки від надавачів хмарних послуг послуг.
Модель порушника	Одна людина з обмеженими навичками, що повторює відому атаку з обмеженими ресурсами, не включаючи здатність виконувати атаки соціальної інженерії.
Обґрунтування моделі порушника	«Низький» рівень передбачає мінімальні вимоги того, щоб хмарні сервіси, включаючи прості, розроблялися з урахуванням безпеки. Мета – усунути можливість стати жертвою тривіальних атак.
Опис сервісу та засобів відповідного рівня	Як визначено в описі хмарного сервісу та засобах його управління, що належать до «Низького» рівня, у тому числі процеси та програмне забезпечення, яке лежить в основі сервісу.

1	2
Обґрунтування опису сервісу та засобів відповідного рівня	При забезпеченні низько рівня безпеки для конкретного сервісу можуть додатково впроваджуватися заходи захисту більш високих рівнів. Це може бути необхідним для врахування особливостей певного хмарного сервісу.

3.2. Вимоги до хмарних послуг середнього рівня безпеки (впевненості) хмарних послуг

Рівень безпеки (впевненості) хмарних послуг «Середній» повинен відповідати додатковим вимогам:

на рівні безпеки (впевненості) хмарних послуг «Середній» заходи захисту передбачають діяльність з оцінки вразливостей, у процесі якої проводиться аналіз загальновідомих вразливостей;

заходи захисту мають передбачити функціональні тести можливостей безпеки хмари;

методологія оцінки рівня безпеки (впевненості) хмарних послуг «Середній» вимагає перегляду зіставлення документації функціональних можливостей безпеки та їх упровадження для забезпечення відповідності.

У таблиці 4 розкриваються вимоги безпеки для хмарних послуг «Середнього» рівня. Вимоги безпеки задовольняються за допомогою впровадження набору заходів захисту – профілю безпеки «Середнього» рівня. Метою є загальний опис рівня безпеки (впевненості) хмарних послуг.

Таблиця 4 – Вимоги безпеки для хмарних послуг «Середнього» рівня

Вимоги безпеки	Рівень безпеки (впевненості) «Середній»
1	2
Гарантія безпеки	За результатами аудиту має бути зроблено висновок щодо можливості надання обґрунтованої гарантії того, що хмарний сервіс побудований та експлуатується із процедурами та механізмами для задоволення відповідних вимог безпеки на рівні, призначеному для мінімізації відомих ризиків кібербезпеки, а також ризику інцидентів та кібератак, що здійснюються суб'єктами, які мають обмежені навички та ресурси. Мають бути розгорнуті та впроваджені відповідні заходи захисту, які відповідають висунутим вимогам безпеки для цього рівня та є ефективними протягом визначеного періоду часу.
Обґрунтування намірів	Обсяг, глибина та точність цього рівня безпеки (впевненості) хмарних послуг вимагають застосовування

1	2
	ризик-орієнтованого підходу для відповідної розробки та впровадження заходів захисту, що відповідають відповідним вимогам безпеки.
Придатність	Середній рівень підходить для хмарних сервісів, які розроблені для задоволення типових вимог безпеки служб, критично важливих для бізнесу даних та систем із середньою категорією критичності.
Обґрунтування придатності	«Середній» рівень забезпечує обґрунтовану гарантію того, що набір більш суворих (ніж на рівні «Низький») заходів захисту розроблений та діє для усунення ризиків та загроз безпеки в системах із середньою категорією критичності для захисту важливої для бізнесу інформації (наприклад: конфіденційні дані бізнесу, електронна пошта CRM - системи управління відносинами з користувачами хмарних послуг , особиста інформація).
Модель порушника	Невелика група людей зі здібностями злому та доступом до широкого кола відомих методів злому, включаючи соціальну інженерію, але з обмеженими ресурсами (зокрема для запуску широких атак або виявлення раніше невідомих вразливостей).
Обґрунтування моделі порушника	Стандартний зловмисник, який володіє навичками більшості відомих атак, що використовуються для розкриття інформації, викрадення ресурсів, відмови у наданні послуги або фальсифікації послуги. Їх основні характеристики походять від визначення рівня: «відомі атаки» та «обмежені ресурси». При цьому допускається вірогідність використання одразу декількох вразливостей.
Опис сервісу та засобів відповідного рівня	Як визначено в описі хмарного сервісу та засобів його управління, що належать до «Середнього» рівня, включаючи процеси та програмне забезпечення, яке лежить в основі сервісу, повинна бути продемонстрована оперативна ефективність заходів захисту.
Обґрунтування опису сервісу та засобів відповідного рівня	При забезпеченні середнього рівня безпеки для конкретного сервісу можуть додатково впроваджуватися заходи захисту низького та/або високого рівня. Це може бути необхідним для врахування особливостей певного хмарного сервісу

3.3. Вимоги до хмарних послуг високого рівня безпеки (впевненості) хмарних послуг

Рівень безпеки (впевненості) хмарних послуг «Високий» відповідає додатковим вимогам:

заходи захисту «Високого» рівня безпеки (впевненості) хмарних послуг мають передбачати діяльність з оцінки вразливості, яка реалізує огляд загальновідомих вразливостей;

заходи захисту «Високого» рівня безпеки (впевненості) хмарних послуг мають передбачати функціональні тести можливостей безпеки хмари, а також вимоги до автоматизованого моніторингу;

заходи захисту «Високого» рівня безпеки (впевненості) хмарних послуг мають вимагати використання найсучасніших функцій безпеки;

методологія оцінки рівня безпеки (впевненості) хмарних послуг «Високий» вимагає перегляду повної відповідності між документацією функціональних можливостей безпеки та їх впровадженням для забезпечення цієї відповідності;

методологія оцінки рівня безпеки (впевненості) хмарних послуг «Високий» передбачає забезпечення ефективності проєктування і експлуатаційної ефективності. Таке оцінювання передбачає тестування на проникнення для оцінки стійкості функціональних можливостей безпеки хмар.

У таблиці 5 розкриваються вимоги безпеки для хмарних послуг «Високого» рівня. Вимоги безпеки задовольняються за допомогою впровадження набору заходів захисту – профілю безпеки «Високого» рівня. Метою є загальний опис рівня безпеки (впевненості) хмарних послуг.

Таблиця 5 – Вимоги безпеки для хмарних послуг «Високого» рівня

Вимоги безпеки	Рівень безпеки (впевненості) «Високий»
1	2
Гарантія безпеки	За результатами аудиту має бути зроблено висновок щодо можливості надання обґрунтованої гарантії того, що хмарний сервіс побудований та експлуатується з процедурами та механізмами для задоволення відповідних вимог безпеки на рівні, призначеному для мінімізації ризиків кіберзахисту, а також ризику інцидентів та кібератак, що здійснюються суб'єктами, які мають значні навички та ресурси. Мають бути розгорнуті та впроваджені відповідні заходи захисту, які відповідають висунутим вимогам безпеки для цього рівня та є ефективними протягом визначеного періоду часу. Впроваджені заходи захисту мать піддаватися автоматичному контролю з метою перевірки їхньої фактичної здатності до забезпечення вимог безпеки.

Обґрунтування намірів	Обсяг, глибина та точність цього рівня безпеки (впевненості) хмарних послуг розширюють попередній рівень «Середній» за допомогою додаткових процедур, що виконуються для автоматизованого контролю. Автоматизований моніторинг запроваджується для виявлення винятків із застосуванням заходів захисту (наприклад, змін у конфігурації) та ініціюванням коригувальних дій.
Придатність	Високий рівень підходить для хмарних сервісів, які розроблені для задоволення конкретних вимог безпеки (вище за «Середній» рівень) для критично важливих даних та систем з високою категорією критичності.
Обґрунтування придатності	«Високий» рівень забезпечує обґрунтовану гарантію того, що набір ще більш суворих заходів захисту розроблено та експлуатується для вирішення ризиків та загроз безпеки в потенційно важливих інформаційних системах для захисту критично важливої інформації (наприклад, конфіденційні ділові дані, патенти).
Модель порушника	Команда висококваліфікованих працівників, які мають доступ до значних ресурсів для проєктування та реалізації атак, проводять інсайдерські атаки, виявляють або отримують доступ до раніше невідомих вразливостей.
Обґрунтування моделі порушника	Досвідчений зловмисник/група зловмисників, протидіяти якому на етапі реалізації атаки можна лише мінімізуючи негативні наслідки. Рекомендується розгортати превентивні методи боротьби із порушником такого рівня.
Опис сервісу та засобів відповідного рівня	Як визначено в описі хмарному сервісу та засобах його управління, що належать до «Високого» рівня, включаючи процеси та програмне забезпечення, яке лежить в основі сервісу, повинна бути продемонстрована оперативна ефективність заходів захисту (включаючи автоматизований моніторинг, якщо це вимагається).
Обґрунтування опису сервісу та засобів відповідного рівня	При забезпеченні високого рівня безпеки для конкретного сервісу можуть додатково впроваджуватися заходи захисту низького та/або середнього рівня. Це може бути необхідно для врахування особливостей певного хмарного сервісу

4. Каталог заходів захисту для хмарних послуг

Клас заходів захисту OIS – Організація безпеки інформації

Планувати, впроваджувати, підтримувати та постійно вдосконалювати систему захисту інформації.

4.1 OIS–01 Система захисту інформації

Заходи захисту.

CSP має розгортати систему захисту інформації, яка б містила в собі положення щодо управління ризиками безпеки протягом всього життєвого циклу хмарної системи.

Посилення заходів:

1) охоплення системи захисту інформації. Сфера застосування системи захисту інформації повинна охоплювати організаційний, процесний та системний рівні. CSP повинен визначати, впроваджувати, підтримувати та постійно вдосконалювати систему захисту інформації, яка має відповідати національним та/або міжнародним стандартам у галузі безпеки інформації та/або галузевим стандартам в сфері хмарних послуг;

2) відповідність стандартам безпеки інформації. CSP має розгортати систему захисту інформації відповідно до національних та/або міжнародних стандартів у галузі безпеки інформації та/або галузевих стандартів у сфері хмарних послуг;

3) сертифікація системи захисту інформації. Система захисту інформації має бути сертифікована відповідно до національних та/або міжнародних стандартів у галузі безпеки інформації та/або галузевих стандартів у сфері хмарних послуг;

4) документування моніторингу системи захисту інформації. CSP повинен задокументувати заходи щодо впровадження, підтримки та постійного вдосконалення системи захисту інформації;

5) ведення визначеної документації системи захисту інформації. Документація повинна містити щонайменше:

сферу застосування;

декларацію про придатність (або інший аналогічний документ);

результати останнього огляду керівництвом.

4.2 OIS–02 Розмежування обов'язків

Заходи захисту.

Менеджмент суперечливих завдань та обов'язків необхідно розподіляти за результатами оцінки ризику RM–01 з метою зменшення ризиків

несанкціонованих або ненавмисних змін даних користувачів хмарних послуг, що обробляються, зберігаються або передаються в хмарі.

Пов’язані заходи: RM–01.

Посилення заходів:

1) оцінка ризику на організаційному рівні. CSP повинен проводити оцінку ризику відповідно до RM–01, в частині накопичення відповідальності ролей або осіб щодо надання хмарної послуги.

Пов’язані заходи: RM–01;

2) оцінка ризику на системному рівні. Оцінка ризику повинна охоплювати такі сфери:

права адміністрування профілів, затвердження та призначення доступу та авторизації доступу (див. IAM–01);

розробка, тестування та оновлення (див. DEV–01, CCM–01);

робота системних компонентів.

Пов’язані заходи: IAM–01, DEV–01, CCM–01;

3) застосування пом'якшувальних заходів. CSP повинен застосовувати пом'якшувальні заходи, які визначені в оцінці ризику, та передбачають привілейований розподіл обов'язків.

Рекомендації з реалізації:

Коли такий розподіл є неможливим з організаційних або технічних причин, то в цьому випадку заходи повинні містити моніторинг діяльності з метою виявлення несанкціонованих або ненавмисних змін, зловживання, подальші відповідні дії;

4) автоматичний контроль. CSP повинен запровадити засоби автоматичного контролю розподілу відповідальності та завдань для забезпечення виконання заходів, пов'язаних з розподілом обов'язків.

4.3 OIS–03 Взаємодія з органами державної влади і заінтересованими групами

Заходи захисту.

CSP залишається в курсі поточних загроз та вразливостей, підтримуючи співпрацю та координацію аспектів безпеки з відповідними органами державної влади та заінтересованими групами.

Рекомендації з реалізації:

Інформація попадає в процедури поводження з ризиками (див. RM–01) та вразливими місцями (див. OPS–17).

Пов’язані заходи: RM–01, OPS–17.

Посилення заходів:

1) відстеження змін. CSP повинен бути в курсі поточних загроз та вразливостей;

2) взаємообмін інформацією. CSP повинен підтримувати контакти з компетентними органами з точки зору безпеки інформації та відповідними технічними групами, щоб бути в курсі поточних загроз та вразливостей;

3) постійний контакт з CAB. CSP повинен підтримувати регулярні контакти зі своїм CAB, щоб бути в курсі поточних загроз та вразливостей.

4.4 OIS–04 Безпека інформації в управлінні проєктами

Заходи захисту.

Питання безпеки інформації враховується в управлінні проєктами, незалежно від характеру проєкту.

Посилення заходів:

1) внесення питань безпеки інформації всіх пов'язаних проєктів. CSP повинен включати питання безпеки інформації в процеси управління проєктами, які можуть мати вплив на хмару, що підтримує відповідний сервіс;

2) оцінка ризиків всіх пов'язаних проєктів. CSP повинен проводити оцінку ризиків відповідно до положень RM–01 для оцінки та усунення ризиків будь-якого проєкту, який може вплинути на надання хмарних послуг, незалежно від характеру проєкту.

Пов’язані заходи: RM–01.

Клас заходів захисту ISP – Положення щодо безпеки інформації

Задокументувати та поширити концепцію безпеки інформації, яка містить в явному або не явному вигляді наміри керівництва, основні положення щодо стратегії управління ризиками, що відповідають вимогам безпеки та для підтримки бізнесу.

4.5 ISP–01 Концепція безпеки інформації

Заходи захисту.

Найвище керівництво CSP затвердило концепцію безпеки інформації та поширило її серед внутрішніх та зовнішніх працівників, а також користувачів хмарних послуг.

Посилення заходів:

1) документування концепції безпеки інформації. CSP повинен задокументувати концепцію безпеки інформації, що охоплює щонайменше такі аспекти:

важливість безпеки інформації, яка заснована на вимогах користувачів хмарних послуг стосовно безпеки інформації, а також на необхідності забезпечення безпеки інформації, що обробляється та зберігається CSP, і активів, що підтримують надані послуги;

цілі безпеки та бажаний рівень безпеки, виходячи з бізнес-цілей та завдань CSP;

зобов’язання CSP виконувати заходи безпеки, необхідні для досягнення встановлених цілей безпеки;

найважливіші аспекти стратегії безпеки для досягнення поставлених цілей безпеки;

організаційну структуру службу, відповідальну за безпеку інформації;

2) затвердження концепції безпеки інформації. Найвище керівництво CSP затверджує концепцію безпеки інформації;

3) перегляд концепції безпеки інформації. CSP переглядає концепцію безпеки інформації принаймні після будь-яких істотних організаційних змін, які можуть вплинути на принципи, визначені в політиці, включаючи утвердження та схвалення вищим керівництвом;

4) щорічний перегляд концепції безпеки інформації. CSP повинен переглядати концепцію безпеки інформації щонайменше щороку;

5) поширення концепції безпеки інформації. CSP поширює концепцію безпеки інформації серед внутрішніх та зовнішніх працівників та користувачів хмарних послуг.

4.6 ISP–02 Правила і процедури безпеки

Заходи захисту.

Правила та процедури випливають із концепції безпеки інформації, документуються відповідно до єдиної структури, поширюються серед усіх внутрішніх та зовнішніх працівників.

Посилення заходів:

1) структуризація правил та процедур безпеки. CSP повинен доводити правила та процедури із концепції безпеки інформації до відома всіх заінтересованих сторін, задокументованих відповідно до єдиної структури, що містить принаймні такі аспекти:

цілі;

сфера дії;

ролі та обов'язки в організації;

ролі та залежності від інших організацій (особливо користувачів хмарних послуг та організацій, що надають послуги);

кроки для виконання стратегії безпеки;

відповідні законодавчі та нормативні вимоги;

2) кваліфікація персоналу. Правила та процедури повинні містити вимоги до кваліфікації персоналу та встановлення правил заміщення в їх описі ролей та відповідальності в організації;

3) поширення правил та процедур безпеки. CSP поширює правила та процедури серед усіх внутрішніх та зовнішніх працівників;

4) затвердження правил та процедур безпеки. Найвище керівництво CSP затверджує правила та процедури безпеки або делегує цю відповідальність уповноваженим органам;

5) звітування про впровадження правил та процедур безпеки. У разі делегування уповноважені органи щонайменше щороку звітують перед вищим керівництвом про політику безпеки та її впровадження;

6) оновлення правил та процедур безпеки. Експерти CSP повинні переглядати правила та процедури безпеки щонайменше щороку, коли концепція безпеки інформації оновлюється та коли серйозні зміни можуть вплинути на безпеку хмари.

Рекомендації з реалізації:

Огляд політики та процедур повинен враховувати принаймні такі аспекти:

організаційні та технічні зміни в процедурах надання хмарних послуг;

правові та нормативні зміни в середовищі CSP;

7) упровадження оновлень правил та процедур безпеки. Після оновлення процедур та політики вони повинні бути затверджені до набрання ними чинності, а потім поширюються серед внутрішніх та зовнішніх працівників.

4.7 ISP–03 Винятки

Заходи захисту.

Винятки з правил та процедур безпеки інформації, а також відповідних заходів захисту чітко перераховані.

Посилення заходів:

1) ведення переліку винятків. CSP повинен вести перелік винятків із правил та процедур безпеки, включаючи пов'язані заходи захисту;

2) часові обмеження винятків. Дія винятків повинна бути обмежена у часі;

3) управління ризиками винятків. Винятки підлягають процесу управління ризиками RM–01, включаючи затвердження цих винятків та прийняття пов'язаних з ними ризиків.

Пов’язані заходи: RM–01;

4) затвердження списку винятків. Винятки з правил та процедур безпеки повинні затверджуватися вищим керівництвом CSP або уповноваженим органом, який затвердив правила або процедури безпеки;

5) перегляд списку винятків. Список винятків переглядається щонайменше щороку;

6) схвалення списку винятків. Схвалення списку винятків повторюється щонайменше щороку, навіть якщо список не оновлювався;

7) контроль актуальності списку винятків. Перелік винятків повинен контролюватися автоматично, з метою забезпечення того, що термін дії затверджених винятків не минув і що всі огляди та схвалення є актуальними.

Клас заходів захисту RM – Управління ризиками

Переконатися, що ризики, пов’язані з безпекою інформації, належним чином ідентифіковані, оцінені та оброблені, а залишковий ризик є прийнятним для CSP.

4.8 RM–01 Політика управління ризиками

Заходи захисту.

Політика та процедури управління ризиками документуються та поширюються серед зацікавлених сторін.

Посилення заходів:

1) документування ризиків. CSP повинен документувати політику та процедури згідно з ISP–02 щодо таких аспектів:

визначення ризиків, пов’язаних із втратою конфіденційності, цілісності, доступності та достовірності інформації в рамках системи захисту інформації, та призначення власників ризиків;

аналіз ймовірності та наслідку виникнення та визначення рівня ризику;

оцінка аналізу ризиків на основі визначених критеріїв прийняття ризиків та визначення пріоритетів у роботі;

управління ризиками за допомогою заходів, включаючи затвердження дозволу та прийняття залишкових ризиків власниками ризиків;

документація проведених заходів для отримання послідовних, дійсних та порівнянних результатів.

Пов’язані заходи: ISP–02;

2) використання аналізу ризиків. CSP повинен використовувати задокументований метод аналізу ризику, який гарантує відтворюваність результатів та порівнянність підходу.

Рекомендації з реалізації:

Поняття «задокументований метод» близьке до «стандартизованого методу», але ідея полягає в тому, щоб застосовувати методи, що використовуються в національному, поточному або іншому конкретному контексті.

4.9 RM–02 Упровадження оцінки ризику

Заходи захисту.

Політика та процедури, пов’язані з оцінкою ризику, впроваджуються по всьому периметру хмари.

Посилення заходів:

1) сфера дії аналізу ризиків. CSP повинен упроваджувати політику та процедури, що охоплюють оцінку ризиків, по всьому периметру хмари.

Рекомендації з реалізації:

Сфера ідентифікації ризиків повинна містити наведені нижче аспекти, наскільки вони можуть бути застосовані до хмарних послуг, що надаються, і перебувають у зоні відповідальності CSP:

обробка, зберігання або передача даних користувачів хмарних послуг з різними потребами захисту;

поява слабких місць та несправності в технічних захисних заходах для розділення спільних ресурсів;

виникнення слабких місць та збоїв в інтеграції на системному рівні технічних захисних заходів;

атаки через точки доступу, у тому числі інтерфейси, доступні із загальнодоступних мереж (зокрема адміністративні інтерфейси);

суперечливі завдання та сфери відповідальності, які неможливо розділити з організаційних чи технічних причин;

залежності від організацій, що надають послуги.

Для вищих рівнів гарантії слід враховувати конкретні технічні ризики, у тому числі:

ризики виходу з ладу механізмів розподілу ресурсів технічної інфраструктури (пам’ять, обчислення, сховище, мережа), які розподіляються між користувачами хмарних послуг;

ризики, пов’язані з неповним або незахищеним стиранням даних, що зберігаються в областях пам'яті, або сховища, яке спільно використовується користувачами хмарних послуг, зокрема під час перерозподілу пам'яті та областей зберігання;

2) поширення результатів оцінки ризику. CSP поширює результати оцінки ризику серед відповідних заінтересованих сторін;

3) перегляд оцінки ризику. CSP повинен переглядати результати оцінки ризиків принаймні щороку та після кожної великої зміни, яка може вплинути на безпеку хмари;

4) контроль факторів ризику. CSP повинен контролювати розвиток факторів ризику та переглядати результати оцінки ризику.

4.10 RM–03 Упровадження усунення ризиків

Заходи захисту.

Пріоритетність ризиків визначається відповідно до їх критичності. Ризики обробляються відповідно до політики та процедур управління ризиками шляхом зменшення або уникання їх за допомогою основних або компенсаційних заходів захисту. Залишкові ризики приймаються власниками ризиків.

Посилення заходів:

1) визначення пріоритетів ризиків. CSP повинен визначити пріоритети ризиків відповідно до їх критичності;

2) реалізація плану усунення ризиків. CSP повинен визначити та реалізувати план усунення ризиків відповідно до рівня їх пріоритету шляхом зменшення або уникнення їх за допомогою основних або компенсаційних заходів захисту;

3) залишковий ризик. План управління ризиками повинен передбачати зниження рівня ризику до порогу, який надавач хмарних послуг вважають прийнятним (залишковий ризик);

4) затвердження плану управління ризиків. Власники ризиків повинні офіційно затвердити план управління ризиками та прийняти залишковий ризик;

5) поширення плану управління ризиками. CSP повинен поширювати план управління ризиками серед відповідних заінтересованих сторін;

6) спільні ризики. Спільні ризики повинні бути пов'язані з CCC та описані в документації користувача хмарних послуг. Рекомендації з реалізації:

Розподіл ризиків із користувачами хмарних послуг завжди має бути явним і пов'язаним з чіткими очікуваннями, як правило, вираженими як CCC, та внесеними до документації (див. DOC–01).

Пов’язані заходи: DOC–01;

7) перегляд плану управління ризиками. CSP повинен переглядати план управління ризиками щоразу, коли переглядається оцінка ризику;

8) адекватність аналізу ризиків. Адекватність аналізу ризиків, оцінка ризиків, включаючи затвердження дій щодо прийняття залишкових ризиків, мають перевірятися після кожного перегляду планів оцінки та управління ризиками.

Клас заходів захисту HR – Людські ресурси

Переконатися, що працівники розуміють свої обов’язки, усвідомлюють свої обов’язки щодо безпеки інформації та що активи організації захищаються у разі зміни відповідальності або припинення.

4.11 HR–01 Політика людських ресурсів

Заходи захисту.

Політика щодо управління внутрішніми та зовнішніми працівниками має містити положення, які охоплюють класифікацію ризиків на всіх посадах, етичний кодекс та відповідальність за порушення, скоєні працівниками, які беруть участь у наданні хмарних послуги.

Посилення заходів:

1) класифікація посад за рівнем ризику. CSP повинен класифікувати позиції, які стосуються питань безпеки інформації, відповідно до рівня їх

ризику, включаючи посади, пов'язані з адмініструванням IT та наданням хмарних послуг у виробничому середовищі, а також усі позиції, які передбачають доступ до хмарних даних користувачів хмарних послуг та системних компонентів;

2) етика персоналу. CSP повинен включати до своїх трудових договорів або етичного кодексу поведінки загальну угоду внутрішніх та зовнішніх працівників щодо етичного виконання своїх професійних обов'язків.

Рекомендації з реалізації:

угода повинна щонайменше передбачати, що з будь-якого питання, що стосується безпеки хмари:

професійні обов'язки виконуються з лояльністю, розсудливістю та неупередженістю;

внутрішні та зовнішні співробітники використовують лише ті методи, засоби та техніки, які були схвалені CSP.

Етичний кодекс також повинен враховувати такі положення, особливо на вищих рівнях:

працівники зобов'язуються не розголошувати інформацію третій стороні, навіть якщо вона конфіденційна, яка була отримана або створена як частина послуги, за винятком випадків, коли користувач хмарного сервісу дав офіційний письмовий дозвіл;

працівники зобов'язуються попередити надавача хмарних послуг про явно незаконний вміст, виявлений під час надання послуги;

працівники зобов'язуються дотримуватися чинного законодавства та нормативних актів та передового досвіду, пов'язаного з їх діяльністю;

3) дисциплінарні заходи щодо порушень. CSP повинен документувати, поширювати та впроваджувати політику, яка описує дії, які слід проводити у разі виявлення порушення, включаючи принаймні такі аспекти:

перевірка, чи мало місце порушення;

врахування характеру та тяжкості порушення та його наслідків;

4) запобігання та документування дисциплінарних заходів. Якщо дисциплінарні заходи визначені відповідно до HR–01(3), у такому випадку внутрішні та зовнішні працівники CSP повинні бути поінформовані про можливі дисциплінарні заходи, а використання цих дисциплінарних заходів має бути належним чином задокументоване.

Пов’язані заходи: HR–01(3).

4.12 HR–02 Перевірка кваліфікації і надійності

Заходи захисту.

Компетентність та доброчесність усіх внутрішніх та зовнішніх працівників, які займають посади, відповідно до HR–01, мають перевірятися до початку роботи згідно з національним законодавством та нормативними актами CSP.

Пов’язані заходи: HR–01.

Посилення заходів:

1) попередня перевірка персоналу. Компетентність та доброчесність усіх внутрішніх та зовнішніх співробітників CSP, які мають доступ до хмарних даних користувачів хмарних послуг або системних компонентів, що знаходяться під відповідальністю CSP, або відповідальні за надання хмарних послуг у виробничому середовищі, повинні бути перевірені перед початком роботи на посадах відповідно до HR–01. Обсяг перевірки повинен бути пропорційним діловому контексту, критичності інформації, до якої матиме доступ працівник, та пов'язаним із цим ризикам.

Пов’язані заходи: HR–01.

Рекомендації з реалізації:

угода повинна щонайменше передбачати, що з будь-якого питання, що стосується безпеки хмари:

професійні обов'язки виконуються з лояльністю, розсудливістю та неупередженістю;

внутрішні та зовнішні співробітники використовують лише ті методи, засоби та техніки, які були затверджені CSP.

2) перегляд компетентності та доброчесності. Компетентність та доброчесність внутрішніх та зовнішніх працівників CSP повинні бути переглянуті до початку роботи на посаді, яка передбачає більш високу кваліфікацію ніж їхня попередня;

3) циклічність перевірки персоналу. Компетентність та доброчесність внутрішніх та зовнішніх працівників CSP щорічно перевіряються для працівників на посадах з найвищим рівнем кваліфікації, починаючи з рівня, який визначається в кадровій політиці.

4.13 HR–03 Умови праці

Заходи захисту.

Внутрішні та зовнішні працівники CSP зобов’язані дотримуватися відповідної політики та інструкцій, що стосуються безпеки інформації, та етичного кодексу CSP. Ознайомлення з такими політиками та інструкціями має відбуватися перед наданням працівнику доступу до будь-яких хмарних даних або компонентів системи, що використовується для надання хмарних послуг, в тому числі у виробничому середовищі.

Посилення заходів:

1) забезпечення дотримання посадових обов'язків. CSP повинен забезпечити, щоб усі внутрішні та зовнішні працівники згідно з їхніми умовами працевлаштування дотримувалися всіх політик та процедур щодо захисту інформації;

2) умова про нерозголошення. CSP повинен забезпечити, щоб умови працевлаштування для всіх внутрішніх та зовнішніх працівників передбачали

положення (угоду) про нерозголошення, яке охоплює будь-яку інформацію, отриману та сформовану в рамках хмари, навіть якщо вона анонімна та деконтекстуалізована;

3) первинний інструктаж. CSP повинен поширити всі політики та процедури безпеки інформації серед внутрішніх та зовнішніх працівників, перш ніж надавати їм будь-який доступ до даних користувачів хмарних послуг, виробничого середовища та будь-якого їх компонента;

4) документування інструктажу. Усі внутрішні та зовнішні працівники повинні підтвердити в документованій формі факт ознайомлення із політиками та процедурами безпеки інформації перед наданням їм будь-якого доступу до даних користувачів хмарних послуг, виробничого середовища та будь-якого їх компонента;

5) контроль документування інструктажу. Перевірка підтвердження, визначеного в HR–03(4), повинна автоматично контролюватися автоматизованими системами, що використовуються для надання прав доступу працівникам.

Пов’язані заходи: HR–03(4).

4.14 HR–04 Обізнаність та навчання у сфері кіберзахисту

Заходи захисту.

У CSP має працювати програма навчання (тренінгів), орієнтована на цільові групи для підтримання обізнаності, яка регулярно викладається для усіх внутрішніх та зовнішніх працівників CSP.

Посилення заходів:

1) визначення програми обізнаності та навчання. CSP визначає програму підвищення обізнаності, яка охоплює такі аспекти:

обробка системних компонентів, що використовуються для надання хмарних послуг у виробничому середовищі, відповідно до політики та процедур;

обробка хмарних даних користувачів хмарних послуг відповідно до політики та інструкцій та чинних законодавчих та нормативних вимог;

інформація про поточну ситуацію із релевантними загрозами;

правильна поведінка у випадку інцидентів безпеки;

2) групова спрямованість. CSP визначає програму підвищення обізнаності для цільових груп, беручи до уваги класифікацію ризиків та технічні обов'язки на посаді;

3) перегляд програми обізнаності та навчання. CSP переглядає поточну програму підвищення обізнаності на основі змін у політиці та інструкціях, а також на основі результатів поточного аналізу ризиків;

4) періодичність оновлення програми обізнаності та навчання. CSP повинен оновлювати свою програму підвищення обізнаності щонайменше щороку;

5) обов'язковість проходження програм обізнаності та навчання. CSP повинен забезпечити, щоб усі працівники пройшли програму підвищення обізнаності та навчання, визначену для них;

6) умови проходження програм обізнаності та навчання. CSP повинен забезпечити проходження усіма працівниками програми підвищення обізнаності на регулярній основі, а також при зміні цільової групи;

7) контроль завершення програм обізнаності та навчання. CSP повинен автоматично контролювати завершення програми підвищення рівня обізнаності та підготовки кадрів;

8) оцінювання індивідуальних результатів навчання. CSP повинен оцінювати результати навчання, досягнуті завдяки програмі підвищення обізнаності та навчання;

9) оцінювання групових результатів навчання. CSP повинен оцінювати результати навчання для цільових груп, досягнуті за допомогою програми обізнаності та навчання. Оцінювання має містити кількісні та якісні аспекти, а результати використовуватимуться для покращення програми обізнаності та навчання;

10) перевірка програми обізнаності та навчання. CSP повинен перевіряти ефективність програми підвищення обізнаності та навчання шляхом використання практичних вправ з підготовки кадрів щодо безпеки, які імітують фактичні кібератаки.

4.15 HR–05 Припинення трудових відносин або зміна умов праці

Заходи захисту.

Внутрішні та зовнішні працівники повинні бути проінформовані про те, які обов'язки, що випливають із керівних принципів та інструкцій, які стосуються безпеки інформації, залишатимуться чинними після припинення трудових відносин або зміни умов праці та на який термін.

Після припинення трудових відносин або зміна умов праці всі права працівника скасовуються або змінюються, а всі облікові записи та активи обробляються належним чином.

Посилення заходів:

1) інформування про припинення трудових відносин або умов праці. CSP повідомляє внутрішнім та зовнішнім працівникам їхні постійні обов'язки, пов'язані з безпекою інформації, коли їхні трудові відносини припиняються або змінюються умови праці;

2) анулювання прав після звільнення. CSP застосовує спеціальну процедуру для анулювання прав доступу та відповідної обробки облікових записів та активів внутрішніх та зовнішніх працівників, коли їхні трудові відносини припиняються або змінюються умови праці;

3) контроль анулювання прав після звільнення. Процедура, згадана в HR–05(2), повинна визначати конкретні ролі та обов'язки та передбачати документований контрольний перелік усіх необхідних етапів.

Пов’язані заходи: HR–05(2);

4) автоматичний контроль анулювання прав після звільнення. CSP повинен автоматично контролювати застосування процедури, зазначеної в HR–05(2).

Пов’язані заходи: HR–05(2).

4.16 HR–06 Угоди про конфіденційність

Заходи захисту.

Угоди про нерозголошення та конфіденційність укладено з внутрішніми працівниками, зовнішніми надавачами хмарних послуг та CSP для захисту конфіденційності інформації, якою обмінюються між ними.

Посилення заходів:

1) узгодження угод. CSP повинен забезпечити узгодження угод про нерозголошення та конфіденційність із внутрішніми працівниками, зовнішніми надавачами хмарних послуг;

2) базові передумови угоди. Угоди про нерозголошення та конфіденційність базуються на вимогах, визначених CSP, щодо захисту конфіденційної інформації та деталей експлуатації;

3) прийняття угоди. Угоди приймаються зовнішніми надавачами хмарних послуг при узгодженні контракту;

4) умова черговості угоди. Угоди приймаються внутрішніми працівниками CSP до надання дозволу на доступ до даних користувачів хмарних послуг.

5) документування та перегляд угод. Вимоги, на яких базуються угоди, повинні документуватися та переглядатися регулярно, принаймні щороку. Якщо огляд свідчить, що вимоги потребують адаптації, угоди про нерозголошення та конфіденційність повинні бути відповідно оновлені;

6) інформування та підтвердження оновленої угоди. CSP інформує своїх внутрішніх та зовнішніх працівників, а також зовнішніх надавачів хмарних послуг та отримує підтвердження оновленої угоди про конфіденційність та/або нерозголошення;

7) автоматичний контроль підтвердження угоди. CSP повинен автоматично контролювати підтвердження угод про нерозголошення та конфіденційність внутрішніми та зовнішніми працівниками, а також зовнішніми надавачами хмарних послуг.

Клас заходів захисту AM – Управління активами

Слід визначити власні активи організації та забезпечити належний рівень захисту протягом їх життєвого циклу

4.17 AM–01 Опис активів

Заходи захисту.

CSP повинен встановити процедури інвентаризації активів, включаючи всі IT-активи, для забезпечення повної, точної, актуальної та послідовної інвентаризації протягом життєвого циклу активів.

Посилення заходів:

1) документування інвентаризації активів. CSP повинен документувати та впроваджувати політику і процедури ведення інвентаризації активів.

Рекомендації з реалізації:

активи містять фізичні та віртуальні об'єкти, необхідні для безпеки інформації хмари під час створення, обробки, зберігання, передачі, видалення або знищення інформації в зоні відповідальності CSP, наприклад, брандмауери, балансири навантаження, вебсервери, сервери додатків та сервери баз даних;

2) автоматизація та інвентаризація активів. Інвентаризація повинна виконуватися автоматично та/або працівниками або командами, відповідальними за активи, щоб забезпечити повну, точну, актуальну та послідовну інвентаризацію протягом життєвого циклу активу;

3) повнота інвентаризації активів. CSP повинен визначити для кожного активу інформацію, необхідну для застосування процедури управління ризиками, визначеної в PM–01.

Рекомендації з реалізації:

Записана інформація повинна містити:

інформацію для ідентифікації активу;

функцію активу;

модель та версію активу;

місцезнаходження активу.

CSP реєструє щонайменше всі зміни в інформації, що стосуються управління ризиками щодо кожного активу.

Пов’язані заходи: PM–01.

4) управління ризиками протягом життєвого циклу активу. Процедури, пов’язані з активами, повинні передбачати заходи, вжиті для управління ризиками, пов’язаними з активом, протягом його життєвого циклу;

5) моніторинг інвентаризації активів. Інформація про активи має аналізуватися програмами моніторингу для виявлення впливу на хмари та функції у випадку подій, які можуть призвести до порушення цілей захисту, а

також для надання інформації постраждалим користувачам хмарних послуг відповідно до договорів;

6) автоматичний контроль інвентаризації активів. CSP повинен автоматично контролювати інвентаризацію активів, щоб гарантувати її актуальність.

4.18 AM–02 Прийнятне використання та безпечна обробка політики активів

Заходи захисту.

Політика та процедури щодо прийнятого використання та безпечного поводження з активами мають документуватися та поширюватися відповідно до ISP–01.

Пов’язані заходи: ISP–01.

Посилення заходів:

1) документування політики використання активів. CSP повинен документувати, поширювати та впроваджувати політику та процедури щодо прийнятого використання та безпечного поводження з активами відповідно до ISP–01.

Рекомендації з реалізації:

Політика та процедури щодо прийнятного використання та безпечного поводження з активами повинні враховувати принаймні такі аспекти життєвого циклу активу, які застосовуються до активу:

процедури затвердження для придбання, введення в експлуатацію, технічного обслуговування, виведення з експлуатації та утилізації уповноваженим персоналом або компонентами системи;

інвентар;

класифікація та маркування на основі необхідності захисту інформації та визначених заходів щодо рівня захисту;

безпечна конфігурація механізмів обробки помилок, реєстрації, шифрування, автентифікації та авторизації;

вимоги до версій програмного забезпечення та зображень, а також застосування патчів;

обробка програмного забезпечення, для якого підтримка та виправлення безпеки більше не доступні;

обмеження встановлення програмного забезпечення або використання послуг;

захист від шкідливих програм;

віддалена деактивація, видалення або блокування;

фізична доставка та транспорт;

вирішення проблем та інцидентів;

повне і безповоротне видалення даних при виведенні з експлуатації.

Пов’язані заходи: ISP–01;

2) повнота політики та процедур використання активів. Політика та процедури щодо прийнятого використання та безпечного поводження з активами повинні враховувати щонайменше аспекти життєвого циклу активів, які зазначені в ISP–01.

Пов’язані заходи: ISP–01;

3) використання знімних носіїв. Коли знімний носій використовується в технічній інфраструктурі або для завдань IT-адміністрування, цей носій повинен бути призначений виключно для одного використання.

Рекомендації з реалізації:

Визначення з CSRC NIST: Портативний носій даних, який можна додати або вилучити з обчислювального пристрою або мережі. Приклади включають, але не обмежуються ними: оптичні диски (CD, DVD, Blu-ray); зовнішні/знімні жорсткі диски; зовнішні/знімні твердотільні дисководи (SSD); магнітні/оптичні стрічки; пристрої флеш-пам'яті (USB, eSATA, флеш-накопичувач); картки флеш-пам'яті (Secure Digital, CompactFlash, Memory Stick, MMC, xD); інші зовнішні/знімні диски (дискети, Zip, Jaz, Bernoulli, UMD).

4.19 AM–03 Введення в експлуатацію та виведення з експлуатації обладнання

Заходи захисту.

CSP повинен містити процедуру схвалення використання обладнання, що вводиться в експлуатацію або виводиться з експлуатації, яке використовується для надання хмарних послуг у виробничому середовищі, залежно від його цільового використання та на основі відповідної політики та процедур.

Посилення заходів:

1) документування процедур експлуатації обладнання. CSP повинен документувати, поширювати та впроваджувати процедуру введення в експлуатацію обладнання, яке використовується для надання хмарних послуг у виробничому середовищі, на основі політик та процедур, що застосовуються;

2) управління ризиками при експлуатації обладнання. Процедура, зазначена в AM–03(1), повинна забезпечувати виявлення, аналіз та пом'якшення ризиків, що виникають внаслідок введення в експлуатацію.

Пов’язані заходи: AM–03(1);

3) перевірка механізмів безпеки при експлуатації обладнання. Процедура, зазначена в AM–03(1), повинна передбачати перевірку безпечної конфігурації механізмів обробки помилок, реєстрації, шифрування, автентифікації та авторизації відповідно до передбачуваного використання та на основі відповідної політики, перш ніж може бути надано дозвіл на введення активу в експлуатацію.

Пов’язані заходи: AM–03(1);

4) особливості виведення обладнання з експлуатації. CSP повинен документувати, поширювати та впроваджувати процедуру виведення з експлуатації обладнання, що використовується для надання хмарних послуг у виробничому середовищі, спираючись на відповідні політики;

5) знищення обладнання після виведення з експлуатації. Процедура, зазначена в AM–03(4), повинна передбачати повне і остаточне видалення даних або належне знищення носія.

Пов'язані заходи: AM–03(4);

6) автоматичний контроль експлуатації обладнання. Схвалення введення в експлуатацію та виведення з експлуатації апаратного забезпечення має бути документально оформлене та автоматично контролюватися.

4.20 AM–04 Прийнятне використання, безпечна обробка та повернення активів

Заходи захисту.

Внутрішні та зовнішні працівники CSP мають доказово дотримуватися політики та інструкцій щодо використання та безпечного поводження з активами, якщо CSP визначив у оцінці ризику, що втрата або несанкціонований доступ може порушити безпеку інформації хмари.

Будь-які передані активи мають повертатися після припинення трудових відносин.

Посилення заходів:

1) документування поводження з активами. CSP повинен забезпечити та задокументувати, щоб усі внутрішні та зовнішні працівники дотримувалися політики та процедур для прийнятного використання та безпечного поводження з активами в ситуаціях, описаних у AM–03.

Пов'язані заходи: AM–03;

2) повернення активів після припинення трудових відносин. Процедура, зазначена в HR–06(2), повинна включати кроки для забезпечення повернення всіх активів, що надавалися працівнику, після припинення трудових відносин.

Пов'язані заходи: HR–06(2);

3) централізоване управління активами. CSP повинен централізовано управляти активами, які надаються внутрішнім та зовнішнім працівникам, у тому числі керування програмним забезпеченням, даними та політикою, а також управляти віддаленою деактивацією, видаленням або блокуванням, якщо це можливо;

4) автоматичний контроль документування поводження з активами. Перевірка зобов'язання, визначеного в AM–04(1), повинна контролюватися автоматично.

Пов'язані заходи: AM–04(1).

4.21 AM–05 Класифікація та маркування активів

Заходи захисту.

Активи мають класифікуватися та, якщо можливо, маркуватися. Класифікація та маркування активу разом відображають потреби у захисті інформації, яку він обробляє, зберігає та/або передає.

Посилення заходів:

1) документування схеми класифікації активів. CSP повинен визначити схему класифікації активів, яка відображає для кожного активу потреби у захисті інформації, яку він обробляє, зберігає та/або передає;

2) рівні захисту активів. Схема класифікації активів повинна забезпечувати рівні захисту для цілей захисту конфіденційності, цілісності, доступності та автентичності;

3) маркування активів. У відповідних випадках CSP повинен маркувати всі активи відповідно до їх класифікації.

Рекомендації з реалізації:

Визначення маркування: «Засіб, що використовується для асоціювання набору атрибутів захисту з активом». Слід зауважити, що маркування не обов’язково є фізичним;

4) відповідальність за маркування. Потреба в захисті визначається особами або групами, відповідальними за активи.

Клас заходів захисту PHS – Фізична безпека

Запобігайте несанкціонованому фізичному доступу та захищайте від крадіжок, пошкоджень, втрат та перебоїв у роботі.

4.22 PHS–01 Периметри фізичної безпеки

Заходи захисту.

Будівлі та приміщення, пов'язані з хмарною послугою, повинні бути розділені на зони за периметрами безпеки, залежно від рівня ризику, пов'язаного з діяльністю та активами, що зберігаються в цих будівлях та приміщеннях.

Посилення заходів:

1) визначення периметра безпеки. CSP повинен визначити периметри безпеки у будівлях та приміщеннях, що стосуються наданих хмарних послуг;

2) визначення зон безпеки. CSP повинен визначити щонайменше дві зони безпеки, одна з яких охоплює всі будівлі та приміщення, а інша охоплює будівлі та приміщення, в яких розміщена хмара для надання послуг;

3) визначення приватної території. CSP повинен визначити додаткову приватну територію, на якій можуть розміщуватися робочі станції з розвитку та управління, нагляду та експлуатації;

4) розмежування зон безпеки. CSP повинен забезпечити відсутність прямого доступу між публічною та критичною зонами;

5) контроль несанкціонованого проникнення. CSP повинен забезпечити, щоб усі зони доставки, завантаження та інші пункти, через які несанкціоновані особи можуть проникнути у приміщення без супроводу, були частиною публічної зони;

6) визначення вимог безпеки для зон безпеки. CSP повинен визначити та поширити набір заходів захисту для кожної зони безпеки в політиці згідно з ISP–02.

Пов’язані заходи: ISP–02;

7) обґрунтованість заходів захисту. Заходи захисту в PHS–01(5) повинні базуватися на вимогах безпеки хмари та оцінці ризиків для фізичної та екологічної безпеки.

Пов’язані заходи: PHS–01(5).

4.23 PHS–02 Контроль фізичного доступу

Заходи захисту.

Фізичний доступ через периметри безпеки має підлягати заходам контролю доступу, які відповідають вимогам безпеки кожної зони та підтримуються системою контролю доступу.

Посилення заходів:

1) документування фізичного доступу. CSP повинен документувати, поширювати та впроваджувати політику та процедури, пов'язані з фізичним контролем доступу до зон безпеки, що відповідають вимогам, визначеним у PHS–01, на основі принципів, визначених у IAM–01.

Пов’язані заходи: PHS–01, IAM–01;

2) автентифікація. Політика контролю доступу повинна вимагати принаймні однофакторної автентифікації для доступу до будь-якої критичної зони;

3) двофакторна автентифікація. Політика контролю доступу повинна вимагати щонайменше двофакторної автентифікації для доступу до критичних зон, на яких розміщуються компоненти системи, які обробляють хмарні дані користувачів хмарних послуг;

4) контроль за відвідувачами. Політика контролю доступу повинна містити заходи щодо індивідуального відстеження відвідувачів і сторонніх працівників під час їх роботи в приміщеннях та будівлях.

Рекомендації з реалізації:

До сторонніх працівників не належать зовнішні працівники, на яких поширюється політика управління персоналом, і вони не підлягають контролю;

5) винятки при надзвичайних ситуаціях. Політика контролю доступу повинна описувати винятки із політики фізичного контролю доступу у випадку надзвичайної ситуації;

6) часові інтервали доступу до зон безпеки. Політика контролю доступу повинна визначати часові інтервали та умови доступу до кожної зони відповідно до профілів користувачів хмарних послуг ;

7) попередження про обмеження. CSP повинен вивести на вході всіх публічних периметрів попередження про обмеження та умови доступу до цих периметрів;

8) запобігання несанкціонованому доступу. CSP повинен захищати периметри безпеки за допомогою заходів захисту для своєчасного виявлення та запобігання несанкціонованому доступу.

Рекомендації з реалізації:

Можлива сукупність заходів запобігання та виявлення і «своєчасність» будуть детально описані в документах для різних рівнів та сфер забезпечення;

9) повнота реєстрації доступу. Політика контролю доступу повинна містити процедури реєстрації всіх доступів до критичних зон, що дозволяє CSP перевірити, чи лише визначений персонал заходив у ці зони;

10) автоматичний контроль доступу. Запис протоколів доступу повинен контролюватися автоматично, щоб гарантувати виконання PHS–02(9).

Пов’язані заходи: PHS–02(9).

4.24 PHS–03 Робота в критичних зонах

Заходи захисту.

Мають бути визначені конкретні правила щодо роботи в критичних зонах, які застосовуються до всіх внутрішніх та зовнішніх працівників, які мають доступ до цих територій.

Посилення заходів:

1) документування правил та процедур роботи в критичних зонах. CSP повинен документувати, поширювати та впроваджувати політику та процедури щодо роботи в критичних зонах;

2) політика «чистого екрана» та документів і змінних носіїв інформації. Політика PHS–02(1) повинна передбачати чітку політику чистого екрана та чітку політику щодо документів та змінних носіїв інформації.

Пов’язані заходи: PHS–02(1);

3) документування розмежування діяльності та зон безпеки. CSP повинен задокументувати розмежування між діяльністю та зонами, яке вказує, які види діяльності можуть/не повинні/повинні виконуватися в кожній із зон безпеки;

4) документування розмежування між активами та зонами безпеки. CSP повинен задокументувати розмежування між активами та зонами, яке вказує,

які види діяльності можуть/не повинні/повинні використовуватися в кожній зоні безпеки.

4.25 PHS–04 Захист обладнання

Заходи захисту.

Обладнання, що використовується у приміщеннях та будівлях CSP, має бути фізично захищено від пошкодження та несанкціонованого доступу за допомогою певних заходів.

Посилення заходів:

1) документування процедур захисту обладнання. CSP повинен документувати, поширювати, впроваджувати політику та процедури щодо захисту обладнання, містити такі аспекти:

захист кабелів живлення та електронних комунікацій від перехоплення, перешкод або пошкодження;

захист обладнання під час операцій з технічного обслуговування;

захист обладнання, що зберігає дані користувачів хмарних послуг під час транспортування;

2) перевірка силових кабелів і кабелів електронних комунікаційних мереж. Процедури, визначені в PHS–04(1), повинні передбачати процедуру перевірки захисту силових кабелів та кабелів електронних комунікаційних мереж принаймні раз на два роки, а також у разі підозр.

Пов’язані заходи: PHS–04(1).

Рекомендації з реалізації:

Перевірки, які слід провести, повинні передбачати принаймні такі аспекти:

сліди насильницьких спроб відкрити закриті дистрибутиви;

актуальність документації у списку розсилки;

відповідність фактичної кабельної системи вимогам документації;

коротке замикання та заземлення непотрібних кабелів;

недопустимі встановлення та модифікації;

3) відповідність рівнів захисту під час утилізації. Політика та процедури, визначені в PHS–04(1), повинні передбачати процедуру передачі будь-якого обладнання, що містить дані користувача хмарних послуг, для утилізації, гарантуючи, що рівень захисту з точки зору конфіденційності та цілісності активів під час транспортування обладнання еквівалентний рівню, що був встановлений в процесі обробки.

Пов’язані заходи: PHS–04(1);

4) перевірка вищим керівництвом. Процедура, описана в PHS–04(3), має передбачати офіційну перевірку вищим керівництвом CSP або уповноваженим органом, який затвердив цю процедуру.

Пов’язані заходи: PHS–04(3);

5) угода підтримки. CSP повинен забезпечити наявність угод підтримки обладнання, яке використовується для надання хмарних послуг, з метою забезпечення оновлення обладнання;

6) управління оновленнями безпеки. CSP повинен забезпечити, щоб угоди про технічне обслуговування обладнання, що використовується для розміщення хмари, дозволяли своєчасно встановлювати оновлення безпеки на цьому обладнанні;

7) доступність хмарних сервісів при оновленні обладнання. Політика та процедури в PHS–04(1) повинні розглядати заходи для забезпечення того, щоб умови для встановлення та обслуговування відповідного технічного обладнання (наприклад, електроенергії, кондиціонування повітря, протипожежного захисту) були сумісними з вимогами щодо доступності та безпеки хмари.

Пов’язані заходи: PHS–04(1);

8) конфіденційність персональних даних користувачів хмарних послуг. CSP повинен забезпечити, щоб обладнання, що містить носій із даними користувача хмарних послуг, можна було повернути третій стороні, лише якщо дані про користувача хмарних послуг, що зберігаються на ньому, зашифровані відповідно до CKM–03 або були попередньо знищені за допомогою механізму безпечного видалення.

Пов’язані заходи: CKM–03;

9) шифрування змінних носіїв інформації. CSP повинен використовувати шифрування на знімному носії та резервному носії, призначеному для переміщення між зонами безпеки відповідно до чутливості даних, що зберігаються на носії.

4.26 PHS–05 Захист проти зовнішніх та екологічних загроз

Заходи захисту.

Приміщення, в яких працює хмара, зокрема її центри обробки даних, мають бути захищені від зовнішніх та екологічних загроз.

Посилення заходів:

1) документування ризиків зовнішніх та екологічних загроз. CSP повинен документувати та поширювати набір вимог безпеки, пов'язаних із зовнішніми та екологічними загрозами, у політиці згідно з ISP–02, розглядаючи такі ризики відповідно до чинних правових та договірних вимог:

недоліки в плануванні;

несанкціонований доступ;

недостатнє спостереження;

недостатня кількість кондиціонерів;

вогонь і дим;

вода;

збої живлення;

повітряна вентиляція та фільтрація.

Пов’язані заходи: ISP–02;

2) відповідність заходів захисту вимогам безпеки центру обробки даних. Вимоги до безпеки, визначені в PHS–05(1) для центрів обробки даних, повинні базуватися на критеріях, які відповідають встановленим технологічним правилам.

Рекомендації з реалізації:

«Встановлені правила технології» будуть уточнені у політиці.

Пов’язані заходи: PHS–05(1);

3) забезпечення безперервної роботи центру обробки даних. Вимоги безпеки, визначені в PHS–05(1) для центрів обробки даних, повинні містити обмеження часу для самодостатньої роботи у разі надзвичайних ситуацій та максимально допустимого простою.

Пов’язані заходи: PHS–05(1).

4) періодичні тестування засобів захисту. Вимоги до безпеки, визначені в PHS–05(1) для центрів обробки даних, повинні передбачати випробування засобів фізичного захисту, що проводяться принаймні щороку.

Пов’язані заходи: PHS–05(1);

5) забезпечення дублювання умов надання хмарного сервісу. CSP має забезпечувати хмарний сервіс принаймні з двох місць, які відокремлені на достатній відстані. Вони забезпечують одне одного оперативною надмірністю або стійкістю.

Рекомендації з реалізації:

Є CSP, які вже не вирішують питання надійності хмари на фізичному рівні через надмірність із двох незалежних місць, а вирішують його завдяки стійкості. Хмарна послуга надається одночасно з більш ніж двох місць. Основна архітектура розподіленого центру обробки даних гарантує, що відмова розташування або компонентів розташування не порушує визначені критерії доступності хмари;

6) забезпечення резервування умов надання хмарного сервісу. CSP повинен перевіряти ефективність резервування принаймні раз на рік за допомогою відповідних тестів та вправ (див. CCM–04).

Пов’язані заходи: CCM–04.

Клас заходів захисту OPS – Операційна безпека

Необхідно забезпечити належну та регулярну роботу, включаючи відповідні заходи для планування та моніторингу потужності, захисту від шкідливого програмного забезпечення, реєстрації та моніторингу подій, а також усунення вразливостей, несправностей та збоїв.

4.27 OPS–01 Управління можливостями – планування

Заходи захисту.

CSP має проводити планування розподілу та використання потенційно важливих ресурсів, таких як персонал та IT-ресурси з метою уникнення можливих вузьких місць.

Посилення заходів:

1) планування потужностей та ресурсів. CSP повинен задокументувати та впровадити процедури планування потужностей та ресурсів (персонал та IT-ресурси). Процедури планування мають містити прогнозування майбутніх потреб у потужності з метою виявлення тенденцій використання та управління;

2) планування безперервного надання послуг. CSP повинен відповідати вимогам, передбаченим умовами договору із користувачами хмарних послуг щодо надання хмарних послуг у разі виникнення недоступності персоналу та IT-ресурсів;

3) відповідність потужностей умовам договору. Прогнози потужності повинні розглядатися відповідно до угоди про рівень обслуговування для планування та підготовки забезпечення.

4.28 OPS–02 Управління можливостями – моніторинг

Заходи захисту.

Має бути забезпечено відстеження потужності таких важливих ресурсів, як персонал та IT-ресурси.

Посилення заходів:

1) гарантії моніторингу. CSP повинен визначити та впровадити технічні та організаційні гарантії для моніторингу надання та припинення надання хмарних послуг з метою забезпечення відповідності угоді про рівень обслуговування;

2) інформування користувача хмарних послуг щодо потужностей. CSP повинен надавати користувачу хмарних послуг відповідну інформацію щодо потужності та доступності на порталі самообслуговування;

3) автоматичний контроль. Надання та припинення надання хмарних послуг повинно контролюватися автоматично, щоб гарантувати виконання OPS–02(1).

Пов’язані заходи: OPS–02(1).

4.29 OPS–03 Управління можливостями – контроль ресурсів

Заходи захисту.

CSC мають мати можливість управляти виділеними їм IT-ресурсами, щоб уникнути переповнення ресурсів та досягти достатньої продуктивності.

Посилення заходів:

контроль системних ресурсів. CSP повинен дозволити CSC контролювати та моніторити розподіл призначених їм системних ресурсів, якщо відповідні хмарні можливості доступні CSC.

4.30 OPS–04 Антивірусний захист – політика

Заходи захисту.

Мають бути визначені правила, що забезпечують захист від зловмисного програмного забезпечення IT-обладнання, пов’язаного з хмарою.

Посилення заходів:

1) документування політики антивірусного захисту. CSP повинен задокументувати, поширити та впроваджувати політику та процедури згідно з ISP–02 для захисту своїх систем та своїх користувачів хмарних послуг від шкідливого програмного забезпечення, охоплюючи принаймні такі аспекти:

використання специфічних для системи механізмів захисту;

експлуатація програм захисту компонентів системи під відповідальністю CSP, які використовуються для надання хмарних послуг у виробничому середовищі;

функціонування програм захисту кінцевого (термінальне) обладнання працівників.

Пов’язані заходи: ISP–02;

2) звітування про проведення антивірусної перевірки. CSP має формувати регулярні звіти про проведені перевірки щодо шкідливого програмного забезпечення, які перевіряються та аналізуються уповноваженими органами під час перегляду політик, пов'язаних із шкідливим програмним забезпеченням;

3) технічне забезпечення антивірусного захисту. Політика та інструкції, пов’язані зі шкідливим програмним забезпеченням, повинні містити технічні заходи, спрямовані на безпечну конфігурацію, захист від шкідливого програмного забезпечення та моніторинг інтерфейсів адміністрування.

Рекомендації з реалізації:

Технічні заходи, спрямовані на безпечну конфігурацію, захист від шкідливого програмного забезпечення та моніторинг інтерфейсів адміністрування, мають стосуватися як самообслуговування користувача хмарних послуг, так і адміністрування CSP;

4) оновлення антивірусних продуктів. CSP повинен оновлювати антивірусні продукти з найвищою частотою, яку пропонують надавачі хмарних послуг.

4.31 OPS–05 Антивірусний захист– впровадження

Заходи захисту.

Захист від зловмисного програмного забезпечення має розгортатися і підтримуватися в системах, що надають хмарні послуги.

Посилення заходів:

1) обов'язковість розгортання засобів антивірусного захисту. CSP повинен застосовувати захист від шкідливого програмного забезпечення, якщо це технічно можливо, на всіх системах, що підтримують надання хмарних послуг у виробничому середовищі, відповідно до політики та процедур.

Рекомендації з реалізації:

Фраза «якщо це технічно можливо» стосується того, що деяке обладнання не може бути оснащене спеціальним захистом від шкідливих програм (як правило, вбудовані системи);

2) оновлення сигнатурних та евристичних баз. Засоби захисту від шкідливих програм на основі сигнатурного та евристичного аналізу повинні оновлюватися щонайменше щодня;

3) автоматичне сканування систем. CSP повинен проводити автоматичне сканування систем, на які поширюється захист від шкідливого програмного забезпечення, а також конфігурацій відповідних механізмів, щоб гарантувати виконання OPS–05(1).

Пов’язані заходи: OPS–05(1);

4) автоматичний контроль. CSP повинен автоматично контролювати сканування антивірусного програмного забезпечення для відстеження виявлених шкідливих програм або порушень.

4.32 OPS–06 Резервне копіювання та відновлення даних – політика

Заходи захисту.

Політика має визначати порядок створення резервних копій та порядок відновлення даних, які гарантують доступність даних, для захисту їх конфіденційності та цілісності.

Посилення заходів:

1) документування політики резервного копіювання. CSP повинен документувати, поширювати та впроваджувати політику та процедури згідно з ISP–02 щодо резервного копіювання та відновлення даних.

Пов’язані заходи: ISP–02;

2) склад політики резервного копіювання. Разом політика та процедури резервного копіювання та відновлення повинні охоплювати щонайменше такі аспекти:

обсяг та частота резервного копіювання даних та тривалість збереження даних узгоджуються за умовами договору із користувачем хмарних послуг;

резервне копіювання даних здійснюється у зашифрованому вигляді;

доступ до резервних копій та даних відновлення здійснюється лише уповноваженими особами;

випробування процедур відновлення (див. OPS–08).

Пов’язані заходи: OPS–08.

4.33 OPS–07 Резервне копіювання та відновлення даних – моніторинг

Заходи захисту.

Належне виконання резервних копій повинно відстежуватися. Посилення заходів:

1) документування процедур моніторингу. CSP повинен документувати та впроваджувати технічні та організаційні заходи для моніторингу виконання резервних копій відповідно до політики та процедур, визначених у OPS–06.

Пов’язані заходи: OPS–06;

2) портал самообслуговування. CSP має надати своїм користувачам портал самообслуговування для автоматичного контролю їх резервного копіювання даних, щоб гарантувати виконання OPS–07(1).

Пов’язані заходи: OPS–07(1);

3) автоматичне відстеження резервних копій. CSP повинен автоматично відстежувати їх резервні копії даних, щоб гарантувати виконання OPS–07(1).

Пов’язані заходи: OPS–07(1).

4.34 OPS–08 Резервне копіювання та відновлення даних – регулярні тестування

Заходи захисту.

Правильне відновлення резервних копій має регулярно перевірятися.

Посилення заходів:

1) періодичність тестування. CSP повинен перевіряти процедури відновлення щонайменше щороку;

2) узгодження тестування. Програми тестування мають бути узгоджені із користувачами хмарних послуг;

3) інформування про хід тестування. Про будь-які відхилення від специфікації під час випробування на відновлення слід повідомляти відповідальну особу CSP для оцінки та виправлення;

4) повідомлення користувача хмарних послуг про результати тестування. CSP має інформувати CSC (на їх прохання) про результати випробувань на відновлення;

5) внесення тестування до плану забезпечення безперервної роботи. Тести на відновлення повинні бути внесені до системи управління безперервною діяльності CSP.

4.35 OPS–09 Резервне копіювання та відновлення даних – зберігання

Заходи захисту.

Дані резервних копій мають зберігатися у відповідному віддаленому місці.

Посилення заходів:

1) передача резервних копій у віддалене місце. CSP має передавати дані резервного копіювання у віддалене місце або транспортувати їх на носії резервного копіювання у віддалене місце;

2) використання надійного каналу електронних комунікаційних мереж при транспортуванні резервних копій. Коли дані резервної копії передаються у віддалене місце через мережу, передача даних має відбуватися у зашифрованому вигляді, який відповідає найсучаснішому стану (див. CKM–02).

Пов’язані заходи: CKM–02;

3) визначення характеристик місця віддаленого копіювання. CSP повинен вибрати віддалене місце для зберігання своїх резервних копій, враховуючи відстань, час відновлення та можливі наслідки надзвичайних ситуацій, стихійного лиха тощо на обох ділянках;

4) фізична та екологічна безпека на місці віддаленого зберігання. Заходи фізичної та екологічної безпеки на віддаленій ділянці повинні мати той самий рівень, що і на головній;

5) автоматичний контроль за зберіганням резервних копій. Коли дані резервної копії передаються у віддалене місце через мережу, CSP повинен автоматично контролювати передачу, щоб гарантувати виконання OPS–09(1).

Пов’язані заходи: OPS–09(1).

4.36 OPS–10 Вхід і моніторинг – політика

Заходи захисту.

Політика визначена для управління реєстрацією подій і моніторингом подій системних компонентів.

Посилення заходів:

1) документування політики входу та моніторингу. CSP повинен документувати, поширювати та впроваджувати політику та процедури згідно з ISP–02, які регулюють реєстрацію та моніторинг подій на компонентах системи.

Пов’язані заходи: ISP–02;

2) склад політики входу та моніторингу. Разом політика та процедури повинні охоплювати такі аспекти:

визначення подій, які можуть призвести до порушення цілей захисту;

технічні умови для активації, зупинки та призупинення різних журналів;

інформація про призначення та термін зберігання журналів;

визначення ролей та обов'язків щодо моніторингу ведення журналів;

синхронізація часу системних компонентів;

дотримання вимог актів законодавства.

4.37 OPS–11 Вхід і моніторинг – управління похідними даними

Заходи захисту.

Політика визначена для управління керівництвом похідних даних CSP. Рекомендації з реалізації:

Похідні дані визначаються як «дані під контролем CSP, які отримуються в результаті взаємодії з хмарою CSC».

Це передбачає реєстрацію та дані моніторингу, але не тільки. Ідея цієї підкатегорії полягає у забезпеченні того, щоб декларації від CSP були повними.

Посилення заходів:

1) документування політики управління похідними даними. CSP повинен документувати, поширювати та впроваджувати політику та процедури згідно з ISP–02, які регулюють безпечну обробку похідних даних.

Пов’язані заходи: ISP–02;

2) склад політики управління похідними даними. Разом політика та процедури щодо похідних даних повинні охоплювати щонайменше такі аспекти:

мета збору та використання похідних даних за межами функціонування хмари, включаючи цілі, пов’язані зі здійсненням контролю безпеки;

анонімність даних, коли вони використовуються в контексті, який виходить за межі єдиного CSC;

строк зберігання, який обґрунтовано пов'язаний з цілями;

гарантії видалення, коли подальше зберігання більше не потрібно;

надання похідних даних CSC відповідно до договірних угод.

Рекомендації з реалізації:

Більшість похідних даних тимчасово використовуються в роботі хмари. Тут основна увага приділяється похідним даним, зібраним CSP;

3) умови договору між користувачем та надавачем хмарних послуг щодо похідних даних. CSP згідно з угодою з CSC повинен перерахувати всі цілі для збору та використання похідних даних, які не пов'язані з проведенням заходів безпеки;

4) відповідність похідних даних нормативно-правовим актам. Похідні дані, включаючи дані журналу, повинні враховуватися при оцінці відповідності нормативно-правовим актам.

4.38 OPS–12 Вхід і моніторинг – ідентифікація подій

Заходи захисту.

Журнали мають вестися для виявлення подій, які можуть призвести до інцидентів безпеки.

Посилення заходів:

1) аудит журналу моніторингу. CSP повинен контролювати дані журналу з метою виявлення подій, які можуть призвести до інцидентів безпеки, відповідно до вимог ведення журналу та моніторингу;

2) інформування відділів про події. Про виявлені події повідомляють відповідні відділи надавача хмарних послуг для своєчасної оцінки та усунення;

3) автоматизований моніторинг. Моніторинг подій, згаданих у OPS–12(1), повинен бути автоматизованим.

Пов’язані заходи: OPS–12(1);

4) автоматичний контроль ідентифікацій подій. CSP повинен автоматично контролювати, чи виявлення подій ефективним є відповідно до OPS–12(1).

Пов’язані заходи: OPS–12(1).

4.39 OPS–13 Вхід і моніторинг – доступ, зберігання та видалення

Заходи захисту.

Конфіденційність, цілісність та доступність даних реєстрації та моніторингу мають бути захищені заходами, адаптованими до їх конкретного використання.

Посилення заходів:

1) контроль цілісності журналу моніторингу. CSP повинен зберігати всі дані журналу у захищеній цілісній та агрегованій формі, що дозволяє проводити їх централізоване оцінювання;

2) видалення даних з журналу моніторингу. Дані журналу мають видалятися, якщо вони більше не потрібні для мети, для якої вони були зібрані;

3) автентифікація доступу. Зв'язок між ресурсами, що реєструються, та серверами реєстрації повинен бути автентифікованим та захищеним для забезпечення цілісності та конфіденційності;

4) шифрування доступу. Зв'язок між ресурсами, що реєструються, та серверами реєстрації повинен бути зашифрований із використанням найсучаснішого шифрування або повинен надаватися у спеціальній адміністративній мережі;

5) забезпечення авторизованого доступу. CSP повинен впроваджувати процедури для виконання вимог, що стосуються доступу, зберігання та видалення, що стосуються таких обмежень:

доступ лише для авторизованих користувачів хмарних послуг та систем;

зберігання протягом зазначеного періоду;

видалення, якщо подальше збереження більше не потрібно;

6) надання журналу моніторингу користувачу хмарних послуг. CSP повинен надавати CSC згідно з його запитом доступ до специфічного для користувача хмарних послуг журналу через API. Запис журналу повинен

відповідати вимогам захисту CSP, включаючи логічне або фізичне розділення журналу та даних користувача хмарних послуг.

Рекомендації з реалізації:

Реєстрація для конкретного користувача хмарних послуг може бути конкретною «з точки зору обсягу та тривалості періоду зберігання»;

7) автоматичний контроль агрегуванням та видаленням журналів. CSP повинен автоматично контролювати агрегування та видалення журналів та даних моніторингу для виконання OPS–13(2).

Пов’язані заходи: OPS–13(2).

4.40 OPS–14 Вхід і моніторинг – атрибути

Заходи захисту.

Дані журналу можна однозначно віднести до CSC. Посилення заходів:

1) ідентифікація користувача хмарних послуг. Згенеровані дані журналу мають дозволяти однозначно ідентифікувати доступ користувачів хмарних послуг на рівні CSC для підтримки аналізу в разі інциденту;

2) надання доступних інтерфейсів. CSP повинен надавати доступні інтерфейси для проведення криміналістичного аналізу та виконання резервних копій компонентів інфраструктури та їх мережевого зв'язку;

3) розслідування інцидентів. У контексті розслідування інциденту, що стосується CSC, CSP повинен мати можливість надавати CSC журнали, пов'язані з його хмарою.

Рекомендації з реалізації:

Повинні бути надані вказівки, що вказують на те, що внутрішні документи, що стосуються розслідувань, повинні керувати способом надання цих журналів.

4.41 OPS–15 Вхід і моніторинг – конфігурація

Заходи захисту.

Доступ до компонентів системи реєстрації та моніторингу та до їх конфігурації має бути суворо обмежений.

Посилення заходів:

1) права доступу. CSP обмежує лише уповноважених користувачів щодо доступу до системних компонентів, що використовуються для реєстрації та моніторингу під їх відповідальності;

2) узгодження конфігурації з політикою управління інформаційними системами. Зміни в конфігурації ведення журналу та моніторингу вносяться відповідно до відповідної політики (див. CCM–01).

Пов’язані заходи: CCM–01;

3) автентифікація доступу до системних компонентів. Процес доступу до системних компонентів для реєстрації та моніторингу повинен вимагати надійної автентифікації.

4.42 OPS–16 Вхід і моніторинг – доступність

Заходи захисту.

Системи реєстрації та моніторингу повинні бути спроможні до самоконтролю. Посилення заходів:

1) контроль компонентів системи. CSP повинен контролювати компоненти системи для ведення журналів та моніторингу, а також автоматично повідомляти про несправності відповідальним підрозділам для оцінки та виправлення;

2) системні компоненти для реєстрації. CSP повинен розробити системні компоненти для реєстрації та моніторингу таким чином, що загальна функціональність не буде обмежена, якщо окремі компоненти вийдуть з ладу.

4.43 OPS–17 Управління вразливостями, несправностями та помилками – політика

Заходи захисту.

Вразливості в системних компонентах, що використовуються для надання хмарної послуги, мають своєчасно виявлятися та усуватися.

Посилення заходів:

1) моніторинг вразливостей у системних компонентах. CSP повинен документувати, поширювати та впроваджувати політики та процедури відповідно до ISP–02 за допомогою технічних та організаційних заходів для забезпечення своєчасного виявлення та усунення вразливостей у системних компонентах, що використовуються для надання хмарних послуг.

Пов’язані заходи: ISP–02;

2) склад політик та процедур управління вразливостями. Разом політика та процедури повинні описувати заходи щонайменше щодо таких аспектів:

регулярне виявлення вразливих місць;

оцінка критичності виявлених вразливостей;

пріоритетність та реалізація дій для оперативного усунення або пом'якшення виявлених вразливостей на основі критичності та відповідно до визначених термінів;

обробка системних компонентів, до яких не вживаються заходи щодо своєчасного виправлення чи пом'якшення вразливостей;

3) система оцінювання вразливостей. CSP повинен використовувати систему оцінювання вразливостей, яка містить принаймні «критичні» та «високі» класи вразливостей.

Рекомендації з реалізації:

Вимога не потребує використання CVSS, хоча CSP рекомендується використовувати версію CVSS. Як правило:

критична вразливість відповідала б оцінкам CVSS між 9,0 і 10,0;

висока вразливість відповідала б оцінкам CVSS між 7,0 та 8,9;

4) усунення «критичних» вразливостей. У своїй політиці та процедурах CSP зобов'язує негайно обробляти «критичні» вразливості та обробляти «високі» вразливості протягом доби з подальшим відстеженням вразливості до її усунення.

Рекомендації з реалізації:

Очікується, що критична вразливість буде усунена протягом декількох годин. Вимога потребує, щоб CSP повідомила свій CAB про таку вразливість.

4.44 OPS–18 Управління вразливостями, несправностями та помилками- онлайн реєстр

Заходи захисту.

Онлайн-реєстри мають використовуватися для вивчення та публікації відомих вразливих місць.

Посилення заходів:

1) ведення онлайн-реєстру вразливостей. CSP повинен опублікувати та підтримувати загальнодоступний онлайн-реєстр відомих вразливостей, які впливають на хмарний сервіс та активи, що надаються CSP;

2) склад онлайн-реєстру вразливостей. Онлайн-реєстр повинен містити щонайменше таку інформацію щодо кожної вразливості:

презентація вразливості відповідно до загальновизнаної системи оцінювання;

опис варіантів усунення цієї вразливості;

інформація про доступність оновлень або виправлень для цієї вразливості;

інформація про виправлення або розгортання виправлень або оновлень CSP або CSC, включаючи детальні інструкції щодо операцій, які повинен виконувати CSC.

Рекомендації з реалізації:

Слід використовувати загальну систему оцінювання вразливостей (CVSS);

3) публікування посилань на онлайн-реєстри вразливостей. CSP повинен публікувати та оновлювати перелік посилань на онлайн-реєстри, його надавачів хмарних послуг, або регулярно інтегрувати вміст цих онлайн-реєстрів, що мають відношення до хмари, у власний онлайн-реєстр (див. OPS–18(1)).

Пов’язані заходи: OPS–18(1);

4) актуалізація онлайн-реєстрів вразливостей. CSP повинен регулярно проводити актуалізацію свого онлайн-реєстру вразливостей, а також онлайн-

реєстрів вразливостей своїх надавачів хмарних послуг, аналізувати потенційний вплив опублікованих вразливостей на хмару та обробляти їх відповідно до процесу обробки вразливостей (див. OPS–17).

Пов'язані заходи: OPS–17;

5) періодичність перевірки онлайн-реєстрів вразливостей. CSP повинен щонайменше щодня перевіряти онлайн-реєстри, опубліковані його надавачами хмарних послуг, та оновлювати власний онлайн-реєстр.

6) автоматичне оновлення активів. CSP повинен забезпечити механізмами автоматичне оновлення активів, що надані CSP, які CSC повинні встановити або експлуатувати під власну відповідальність, щоб полегшити розгортання виправлень та оновлень після первинного схвалення CSC.

4.45 OPS–19 Управління вразливостями, несправностями та помилками- ідентифікація вразливості

Заходи захисту.

Тести для виявлення вразливостей мають проводитися регулярно. Посилення заходів:

1) тестування виявлення вразливостей системних компонентів. CSP повинен регулярно проводити тести для виявлення загальновідомих вразливостей системних компонентів, що використовуються для надання хмарних послуг, відповідно до політики щодо обробки вразливостей (див. OPS–17).

Рекомендації з реалізації:

Ця вимога була додана для того, щоб відповідати рівню, який очікується для «Низького» рівня. Керівництво пояснює, що автоматичне тестування буде прийнятним на «Низькому» рівні.

Пов'язані заходи: OPS–17;

2) періодичність тестування. CSP повинен виконувати випробування, визначені в OPS–18(1), принаймні раз на місяць.

Рекомендації з реалізації:

Необхідна кваліфікація буде далі визначена у політиці, і вона повинна передбачати певний вид сертифікації особистого сервісу.

Пов'язані заходи: OPS–18(1);

3) тестування на проникнення. CSP повинен проводити тестування на проникнення кваліфікованим внутрішнім персоналом або зовнішніми надавачами хмарних послуг згідно із задокументованою методологією випробувань, включаючи системні компоненти, що мають відношення до надання хмарних послуг у зоні відповідальності CSP, як визначено в аналізі ризиків;

4) оцінка результатів тестування на проникнення. CSP повинен оцінити результати випробувань на проникнення та обробляти кожну виявлену вразливість відповідно до визначених політик і процедур (див. OPS–18).

Пов’язані заходи: OPS–18;

5) перегляд програми тестування. Тестування має проводитися за багаторічною робочою програмою, що переглядається щороку та охоплює компоненти системи та засоби захисту відповідно до розвитку хмари та простору загроз.

Рекомендації з реалізації:

Тут ідеться про те, щоб CAB переглянув план випробувань на проникнення та виявив невідповідності, що підлягають фіксації (тобто тести, яких немає, і, можливо, їх потрібно буде внести та виконати протягом наступних років), дотримуючись процедур, визначених у керівництві для аудиторів;

6) залучення зовнішніх надавачів хмарних послуг для тестування. Деякі тестування на проникнення, що проводяться щороку, повинні проводитися зовнішніми надавачами хмарних послуг.

Рекомендації з реалізації:

Ідея також полягає у використанні програми для забезпечення того, щоб, якщо існує внутрішня команда, вони використовували зовнішніх надавачів хмарних послуг, щоб переконатися, що їх компетенція залишається адекватною, та вивчати нові речі;

7) аналіз першопричини вразливостей. CSP повинен провести аналіз першопричини вразливостей, виявлених під час тестування на проникнення, щоб оцінити, наскільки подібні вразливості можуть бути наявні в хмарній системі.

Рекомендації з реалізації:

На цьому рівні CSP повинен поставити питання про можливу експлуатацію вразливості в минулому, визначивши потенційні ознаки експлуатації та шукаючи їх у журналах;

8) Співвіднесення виявлених вразливостей із попередніми інцидентами. CSP повинен зіставляти можливі випадки виявлених вразливостей із попередніми інцидентами, щоб визначити, чи вразливість могла бути використана до її виявлення.

4.46 OPS–20 Управління вразливостями, несправностями та помилками – вимірювання, аналіз і оцінка процедур

Заходи захисту.

Заходи щодо вразливості та врегулювання інцидентів мають регулярно оцінюватися та вдосконалюватися.

Посилення заходів:

1) аналіз інструментів обробки вразливостей та інцидентів. CSP повинен регулярно вимірювати, аналізувати та оцінювати процедури, за допомогою яких обробляються вразливості та інциденти, щоб перевірити їхню придатність, доцільність та ефективність;

2) перегляд результатів оцінки. CSP має організовувати щоквартальний перегляд результатів оцінки, визначений у OPS–20(1), підзвітними підрозділами.

Пов'язані заходи: OPS–20(1).

4.47 OPS–21 Управління вразливостями, несправностями та помилками- затвердження системи

Заходи захисту.

Компоненти системи мають бути затверджені для усунення потенційних векторів атаки.

Посилення заходів:

1) затвердження всіх системних компонентів. CSP повинен затвердити всі системні компоненти, що знаходяться під його відповідальністю, які використовуються для надання хмарних послуг, відповідно до прийнятих галузевих стандартів.

Рекомендації з реалізації:

Якщо CSP використовує зображення, що не піддаються модифікації, процес затвердження слід робити під час створення цих зображень. Слід зберігати файли конфігурації та журналів щодо постійної доступності зображень;

2) документування затвердження всіх системних компонентів. Затверджені вимоги для кожного компонента системи повинні бути задокументовані;

3) автоматичний контроль системних компонентів. CSP повинен автоматично контролювати компоненти сервісу на відповідність затвердженим специфікаціям.

4.48 OPS–22 Розподіл бази даних у хмарній інфраструктурі

Заходи захисту.

Компоненти системи мають бути затверджені для усунення потенційних векторів атак.

Посилення заходів:

1) відокремлення баз даних у хмарній інфраструктурі. CSP повинен відокремити дані CSC, що зберігаються та обробляються на спільних віртуальних та фізичних ресурсах, щоб забезпечити конфіденційність та цілісність цих даних відповідно до результатів аналізу ризиків (див. RM–01).

Пов'язані заходи: RM–01.

Клас заходів захисту IAM – Управління ідентифікацією, автентифікацією і контролем доступу

Обмежити доступ до інформації та засобів її обробки.

4.49 IAM–01 Політика контролю доступу до інформації

Заходи захисту.

З метою забезпечення лише авторизованого доступу до інформації, CSP має задокументувати та поширити серед зацікавлених осіб політику та процедури контролю доступу до інформаційних ресурсів.

Посилення заходів:

1) документування політики контролю доступу. CSP повинен документувати, поширювати та впроваджувати політику та процедури щодо ролей та прав контролю доступу до інформаційних ресурсів відповідно до положень, зазначених в ISP–02. Разом політика та процедури мають містить такі аспекти:

параметри, які слід враховувати для прийняття рішень щодо контролю доступу;

надання та зміна прав доступу на основі принципу «мінімізації привілеїв»;

використання механізму на основі ролей для надання прав доступу;

розподіл обов'язків між управлінням, затвердженням та передачею прав доступу;

окремі правила для користувачів хмарних послуг з привілейованим доступом;

вимоги до затвердження та документації управління правами доступу.

Пов’язані заходи: ISP–02;

2) кореляція політики контролю доступу з політикою фізичного доступу. З метою забезпечення контролю за доступом до приміщень, де знаходиться інформація, CSP повинен пов'язати політику контролю доступу, визначену в IAM–01(1), з політикою фізичного контролю доступу, визначену в PHS–02(1).

Пов’язані заходи: IAM–01(1), PHS–02(1);

3) використання рольового підходу. Політика контролю доступу CSP має базуватися на механізмі із використанням ролей.

4.50 IAM–02 Управління обліковими записами користувачів хмарних послуг

Заходи захисту.

З метою забезпечення лише санкціонованого доступу до інформаційних ресурсів, політики та процедури управління різними типами облікових записів

користувачів хмарних послуг, що мають бути затверджені та поширені серед заінтересованих осіб.

Посилення заходів:

1) документування політики управління обліковими записами. CSP повинен задокументувати політику управління обліковими записами згідно з ISP–02. Політика має містити принаймні такі аспекти:

присвоєння унікальних імен користувачів хмарних послуг;

визначення різних типів підтримуваних облікових записів та призначення параметрів та ролей контролю доступу, які слід враховувати для кожного типу;

події, що ведуть до блокування та скасування облікових записів.

Пов’язані заходи: ISP–02;

2) доступність політики управління обліковими записами CSP. CSP повинен затверджувати та поширювати серед заінтересованих сторін політику управління обліковими записами користувачів хмарних послуг, які відносяться до CAP, відповідно до ISP–02 та посилення, визначеного в IAM–02(1). Політика має містити принаймні такі аспекти:

обов'язки щодо управління, затвердження та призначення облікових записів користувачів хмарних послуг;

регулярність перегляду призначених облікових записів користувачів хмарних послуг та пов'язаних з ними прав доступу;

правила блокування та скасування облікових записів у разі бездіяльності або потенційної компрометації облікового запису;

вимоги щодо затвердження та документації управління обліковими записами користувачів хмарних послуг.

Пов’язані заходи: ISP–02, IAM–02(1);

3) доступність політики управління обліковими записами користувача хмарних послуг. CSP повинен затверджувати та поширювати серед заінтересованих сторін політику управління обліковими записами користувачів хмарних послуг, які відносяться до користувача хмарних послуг, відповідно до ISP–02 та посилення, визначеного в IAM–02(1). Політика має містити принаймні такі аспекти:

- механізми контролю доступу, які доступні CSC;
- параметри контролю доступу, які CSC дозволяє конфігурувати.

Пов’язані заходи: ISP–02, IAM–02(1);

4) документування політики управління обліковими записами працівників. CSP повинен затверджувати та поширювати процедури управління обліковими записами внутрішніх та зовнішніх працівників, а також правами доступу, які мають відповідати посадовим обов’язкаю та політиці управління обліковими записами;

5) документування політики управління груповими обліковими записами. CSP повинен затверджувати та поширювати процедури управління груповими обліковими записами та пов'язані з ними права доступу. Процедури управління мають базуватися на рольовому механізмі;

6) документування політики управління технічними обліковими записами. CSP повинен задокументувати та впровадити процедури управління технічними обліковими записами та відповідними правами доступу до системних компонентів, що беруть участь у роботі хмари. Процедури управління мають базуватися на рольовому механізмі;

7) самообслуговування облікових записів користувача хмарних послуг. CSP повинен запропонувати CSC самообслуговування, за допомогою якого вони можуть самостійно управляти обліковими записами своїх користувачів хмарних послуг;

8) надавання облікових записів нових користувачів хмарних послуг. CSP повинен мати можливість надавати для цього облікового запису користувача хмарних послуг інформацію, чи підпадає він під відповідальність CSP або CSC, а також перелік прав доступу, наданих цьому обліковому запису.

4.51 IAM–03 Блокування, розблокування та ануляція облікових записів користувача хмарних послуг

Заходи захисту.

Облікові записи, які тривалий час неактивні або зазнають впливу підозрілої діяльності, мають бути захищені належним чином, щоб зменшити можливості зловживань.

Посилення заходів:

1) автоматизований механізм блокування облікових записів. CSP повинен визначити та впровадити автоматизований механізм блокування облікових записів користувачів хмарних послуг через певний проміжок часу;

2) автоматизований механізм блокування облікових записів при бездіяльності. Автоматизований механізм у IAM–03(1) повинен блокувати особисті облікові записи користувачів хмарних послуг під відповідальністю CSP після двох місяців бездіяльності.

Пов’язані заходи: IAM–03(1);

3) автоматизований механізм блокування облікових записів при невдалій автентифікації. CSP повинен визначити та впровадити автоматизований механізм блокування облікових записів користувачів хмарних послуг після певної кількості невдалих спроб автентифікації;

4) обмеження спроб автентифікації. Обмеження спроб автентифікації, що використовуються в механізмі IAM–03(3) для облікових записів користувачів хмарних послуг під відповідальністю CSP, повинні базуватися на ризиках для облікових записів, відповідних правах доступу та механізмах автентифікації.

Пов’язані заходи: IAM–03(3);

5) моніторинг викрадених та скомпрометованих облікових записів. CSP документує процес моніторингу викрадених та скомпрометованих облікових

даних та блокує будь-які облікові записи, щодо яких виявлена проблема, до розгляду уповноваженою особою;

6) моніторинг облікових записів з привілейованими правами доступу. CSP повинен впровадити процес у IAM–03(5) на всіх облікових записах користувачів хмарних послуг, які знаходяться під його відповідальністю, яким надано привілейовані права доступу.

Пов'язані заходи: IAM–03(5);

7) моніторинг облікових записів. CSP повинен впровадити процес у IAM–03(5) на всіх облікових записах користувачів хмарних послуг, які знаходяться під його відповідальністю.

Пов'язані заходи: IAM–03(5);

8) підтвердження розблокування облікових записів. Для розблокування облікових записів, що були автоматично заблоковані, потрібно схвалення уповноваженого персоналу або компонентів системи;

9) автоматизований механізм скасування облікових записів. CSP повинен визначити та впровадити автоматизований механізм скасування облікових записів користувачів хмарних послуг, які були заблоковані іншим автоматичним механізмом через певний проміжок часу;

10) перегляд механізму скасування облікових записів. Автоматизований механізм у IAM–03(9) скасовує облікові записи користувачів хмарних послуг після їх блокування протягом шести місяців.

Пов'язані заходи: IAM–03(9);

11) автоматичний контроль механізму скасування облікових записів. CSP повинен автоматично контролювати впроваджені автоматизовані механізми, щоб гарантувати їх відповідність IAM–03.

Пов'язані заходи: IAM–03;

12) автоматизований контроль автентифікації. CSP повинен автоматично контролювати умови спроб автентифікації та повідомляти підозрілі події відповідному користувачеві хмарних послуг або уповноваженим особам.

4.52 IAM–04 Управління правами доступу

Заходи захисту.

Облікові записи, які тривалий час неактивні або зазнають впливу підозрілої діяльності, мають захищатися належним чином, щоб зменшити можливості зловживань.

Посилення заходів:

1) анулювання облікового запису користувача хмарних послуг. CSP повинен задокументувати та впровадити процедури надання, оновлення та анулювання облікового запису користувача хмарних послуг, а також права доступу до ресурсів інформаційної системи хмари;

2) документування процедури управління доступом. CSP повинен задокументувати та впровадити процедуру своєчасного оновлення або

скасування прав доступу внутрішнього або зовнішнього працівника, коли роль та обов'язки працівника змінюються;

3) терміновість оновлення або відкликання прав доступу. Процедура оновлення або відкликання прав доступу, визначена у IAM–04(2), виконується протягом 48 годин після зміни ролі для прав привілейованого доступу та протягом 14 днів для інших прав доступу.

Пов’язані заходи: IAM–04(2);

4) документування процедури надання прав доступу. CSP повинен задокументувати процедуру надання для ресурсу, який контролює доступ, списку всіх облікових записів користувачів хмарних послуг, які мають до нього доступ, незалежно від того, чи підпадають вони під відповідальність CSP або CSC, а для кожного такого облікового запису – список прав доступу, наданих йому в цей час;

5) документування несумісності прав доступу. CSP повинен задокументувати несумісність між правами доступу та застосовувати ці несумісності, коли права доступу надаються або оновлюються в обліковому записі користувача хмарних послуг;

6) динамічний підхід при управлінні правами доступу. Процедури управління правами доступу повинні відповідати динамічному підходу.

Рекомендації з реалізації:

«Динамічний підхід» передбачає, що зміна прав доступу набуває чинності негайно, не вимагаючи від користувача хмарних послуг виходу та повторного входу (якщо не надано нових прав доступу, які потребують більш жорсткого методу автентифікації);

7) самообслуговування користувачів хмарних послуг при управлінні правами доступу. CSP повинен запропонувати CSC самообслуговування, за допомогою якого вони можуть самостійно управляти правами доступу до всіх облікових записів користувачів хмарних послуг, які перебувають під їх відповідальністю.

4.53 IAM–05 Регулярний перегляд прав доступу

Заходи захисту.

Придатність для призначення облікових записів користувачів хмарних послуг усіх типів та пов'язаних з ними прав доступу регулярно перевіряється.

Посилення заходів:

1) періодичність перегляду прав доступу для визначеного рівня безпеки

CSP повинен переглядати права доступу до всіх облікових записів користувачів хмарних послуг, які перебувають під його відповідальністю, принаймні раз на рік, щоб переконатися, що вони все ще відповідають поточним потребам;

2) перегляд прав доступу уповноваженими особами. Перегляд, визначений у IAM–05(1), повинен проводитися уповноваженими особами, що

перебувають під відповідальністю уповноваженого органу, який затвердив політику щодо прав доступу.

Пов'язані заходи: IAM–05(1);

3) терміновість обробки відхилень. CSP обробляє виявлені відхилення своєчасно, але не пізніше 7 днів після їх виявлення шляхом належного скасування або оновлення прав доступу;

4) інструмент перегляду прав доступу. CSP надає CSC інструмент, що полегшує перегляд прав доступу до облікових записів користувачів хмарних послуг, що перебувають під їх відповідальністю;

5) періодичність перегляду прав доступу для високого рівня безпеки. CSP повинен проводити перевірку, визначену в IAM–05(1), кожні шість місяців.

Пов'язані заходи: IAM–05(1).

4.54 IAM–06 Привілейовані права доступу

Заходи захисту.

Привілейовані права доступу та облікові записи користувачів хмарних послуг усіх типів, яким вони надані, підлягають додатковому контролю.

Посилення заходів:

1) персоналізація привілейованих прав доступу. Привілейовані права доступу повинні бути обмеженими у часі відповідно до оцінки ризику і призначатися для виконання завдань (принцип «необхідності знати»);

2) реєстрація діяльності користувачів хмарних послуг з привілейованими правами доступу. Діяльність користувачів хмарних послуг із привілейованими правами доступу реєструється з метою виявлення будь-якого зловживання привілейованим доступом або функціонування у підозрілих випадках, а зареєстрована інформація автоматично контролюється на предмет визначених подій, які можуть свідчити про неправильне використання;

3) документування процедури недопущення зловживання правами доступу. CSP повинен задокументувати та впровадити процедуру, яка після виявлення потенційного зловживання моніторингом, визначеним у IAM–06(2), інформує відповідальний персонал, щоб він міг негайно оцінити, чи мало місце зловживання, та вжити відповідних заходів.

Пов'язані заходи: IAM–06(2);

4) призначення групових облікових записів. Групові облікові записи, за які відповідає CSP, призначаються лише внутрішніх або зовнішніх працівників.

Рекомендації з реалізації:

Груповий обліковий запис зазвичай є привілейованим; їх також слід розподілити більше ніж на одного працівника;

5) періодичність перегляду технічних облікових записів. CSP кожні три місяці повинен переглядати перелік працівників, які відповідають за технічний обліковий запис, у межах сфери його відповідальності;

6) інвентаризація привілейованих облікових записів. CSP повинен проводити сучасну інвентаризацію облікових записів користувачів хмарних послуг під свою відповідальність, які мають привілейовані права доступу;

7) автентифікація доступу до адміністративних інтерфейсів. CSP вимагає надійної автентифікації для доступу до адміністративних інтерфейсів, що використовуються;

8) автентифікація доступу до адміністративних інтерфейсів користувача хмарних послуг. CSP вимагає надійної автентифікації для доступу до адміністративних інтерфейсів, запропонованих CSC.

Рекомендації з реалізації:

Поняття «сильної автентифікації» потрібно буде описати в політиці.

4.55 IAM–07 Механізми автентифікації

Заходи захисту.

Адекватні механізми автентифікації використовуються для надання доступу до будь-якого середовища та у разі потреби у середовищі.

Посилення заходів:

1) документування механізмів автентифікації. CSP повинен задокументувати та впровадити в сукупності політику та процедури щодо механізмів автентифікації, що разом охоплюють принаймні такі аспекти:

підбір механізмів, придатних для кожного типу облікового запису та кожного рівня ризику;

захист облікових даних, що використовуються механізмом автентифікації;

створення та розподіл облікових даних для нових облікових записів;

правила поновлення повноважень, у тому числі періодичне поновлення, поновлення на випадок втрати або компрометації;

правила щодо необхідної сили повноважень, а також механізми передачі та забезпечення виконання правил;

2) автентифікація всіх середовищ. Доступ до всіх середовищ CSP повинен бути автентифікований, у тому числі невиробничі середовища;

3) автентифікація доступу до виробничого середовища. Доступ до виробничого середовища CSP повинен вимагати надійної автентифікації;

4) автентифікація доступу до даних користувача хмарних послуг. Доступ до всіх середовищ CSP, що містять дані CSC, повинен вимагати надійної автентифікації;

5) автентифікація користувача хмарних послуг. Автентифікація користувача хмарних послуг повинна виконуватися за допомогою паролів,

сертифікатів із електронними цифровими підписами або процедур, які забезпечують принаймні рівноцінний рівень безпеки;

6) автентифікація групових облікових записів. Для доступу до неперсональних групових облікових записів CSP повинен впровадити заходи, які вимагають автентифікації користувачів хмарних послуг за допомогою їхнього особистого облікового запису, перш ніж мати доступ до цих технічних облікових записів;

7) блокування облікового запису при невдалих спробах автентифікації. Усі механізми автентифікації повинні містити механізм блокування облікового запису після заздалегідь визначеної кількості невдалих спроб;

8) надання методів автентифікації користувачів хмарних послуг. CSP повинен запропонувати CSC надійні методи автентифікації для використання з обліковими записами під їх відповідальність.

4.56 IAM–08 Захист і повнота облікованих даних

Заходи захисту.

Протягом свого життєвого циклу облікові дані автентифікації захищаються, щоб гарантувати, що їх використання забезпечує достатній рівень гарантії в тому, що користувач хмарних послуг певного облікового запису пройшов аутентифікацію.

Посилення заходів:

1) документування рекомендацій щодо управління обліковими даними. CSP повинен документувати, поширювати та впроваджувати для всіх користувачів хмарних послуг правила щодо управління обліковими даними, у тому числі таке:

неповторне використання облікових даних;

компроміси між ентропією та здатністю запам’ятовувати;

рекомендації щодо оновлення паролів;

правила зберігання паролів;

2) особливі вимоги до управління обліковими даними. Разом правила та рекомендації CSP, визначені в IAM–08(1), повинні містити щонайменше такі аспекти:

рекомендації щодо менеджерів паролів;

рекомендації конкретно розглядати класичні атаки, у тому числі фішинг та соціальні атаки.

Пов’язані заходи: IAM–08(1);

3) декларація про конфіденційність. CSP вимагає від користувачів хмарних послуг, яким надаються облікові дані для автентифікації, підписати декларацію, в якій вони запевняють, що ставляться до особистої (або спільної) автентифікації конфіденційно;

4) використання криптографічно стійких геш-функцій. Паролі повинні зберігатися лише з використанням криптографічно стійких геш-функцій (див. CKM–01).

Пов’язані заходи: CKM–01;

5) механізми криптографічної автентифікації. Якщо використовуються механізми криптографічної автентифікації, вони повинні відповідати політиці та процедурам, передбаченим CKM–01.

Пов’язані заходи: CKM–01;

6) автоматичність створення облікових даних. При створенні облікових даних дотримання специфікацій забезпечується автоматично, наскільки це технічно можливо;

7) інформування при змінах облікових даних особистих облікових записів. Коли облікові дані, пов’язані з особистим обліковим записом, змінюються або поновлюються, особа, пов’язана з цим обліковим записом, отримує повідомлення;

8) обмеження на автоматичні паролі. Будь-який пароль, надісланий користувачеві хмарних послуг електронною поштою, повідомленням або подібним чином, повинен бути змінений користувачем хмарних послуг після його першого використання, і термін його дії не повинен перевищувати 14 днів після повідомлення користувачеві хмарних послуг.

9) інформаційна підтримка користувача хмарних послуг щодо управління обліковаными даними. CSP надає CSC сукупність правил і рекомендацій, що застосовуються або можуть застосовуватися до користувачів хмарних послуг, які перебувають під їх відповідальністю, та надає CSC інструменти для управління та забезпечення виконання цих правил.

4.57 IAM–09 Загальні обмеження доступу

Заходи захисту.

Керування активами в хмарі та навколо неї здійснюється так, щоб забезпечити дотримання обмежень доступу між різними категоріями активів.

Посилення заходів:

1) розмежування інформаційних систем. CSP повинен упровадити достатні заходи розподілу між інформаційною системою, що надає хмарну послугу, та іншими її інформаційними системами.

Рекомендації з реалізації:

Це не виключає зв’язку між наданням хмарної послуги та іншими інформаційними системами, наприклад, для виставлення рахунків або для резервного копіювання, але такі цілі повинні бути чітко визначені, а також повинні бути чітко визначені інтерфейси;

2) правила проєктування інформаційних систем та активів. CSP повинен спроєктувати, розробити, налаштувати та розгорнути інформаційну систему, що забезпечує хмарну послугу, у тому числі розподіл між технічною

інфраструктурою та обладнанням, необхідним для адміністрування хмари, і активами, які вона розміщує;

3) відокремлення адміністративних інтерфейсів. CSP повинен відокремлювати адміністративні інтерфейси, надані CSC, від інтерфейсів, доступних для його внутрішніх та зовнішніх працівників, зокрема:

управління обліковими записами, за яких відповідає CSP, керуватиметься за допомогою інструментів, які є окремими від тих, що використовуються для управління обліковими записами користувачів хмарних послуг, що знаходяться під відповідальністю CSC;

адміністративні інтерфейси, надані CSC, не дозволяють підключати облікові записи під відповідальністю CSP;

інтерфейси адміністрування, які використовує CSP, не повинні бути доступними із електронної комунікаційної мережі загального користування;

4) заходи розподілу користувачів хмарних послуг. CSP повинен упровадити відповідні заходи для розподілу між CSC;

5) інформування про відкритий канал електронних комунікаційних мереж. CSP повинен своєчасно інформувати CSC, коли внутрішні або зовнішні працівники CSP отримують доступ до даних CSC, які обробляються, зберігаються або передаються в хмарі без попередньої згоди CSC, включаючи при цьому:

причину, час, тривалість, тип та обсяг доступу;

достатньо деталей, щоб експерти з питань CSC могли оцінити ризики доступу;

6) погодження використання відкритого каналу електронних комунікаційних мереж. CSP потребує попередньої згоди CSC перед будь-яким доступом до даних CSC, що обробляються, зберігаються або передаються в хмарні, надаючи значущу інформацію, як визначено в IAM–09(5).

Пов’язані заходи: IAM–09(5);

7) розмежування інтерфейсів для адміністраторів та кінцевих користувачів хмарних послуг. Якщо CSP пропонує своїм CSC інтерфейси для адміністраторів та кінцевих користувачів хмарних послуг, ці інтерфейси повинні бути відокремлені.

Клас заходів захисту CKM – Криптографія та управління ключами

Забезпечити належне та ефективне використання криптографії для захисту конфіденційності, достовірності чи цілісності інформації.

4.58 CKM–01 Політика для використання механізмів шифрування та управління ключами

Заходи захисту.

Політика та процедури щодо механізмів шифрування та управління ключами, у тому числі технічні та організаційні гарантії, повинні визначитися, передаватися та впроваджуватися з метою забезпечення конфіденційності, достовірності та цілісності інформації.

Посилення заходів:

1) документування політики для шифрування та управління ключами. CSP повинен документувати, повідомляти, робити доступними та реалізовувати політику з технічними та організаційними гарантіями для шифрування та управління ключами згідно з ISP–02, в якій описані такі аспекти:

використання потужних процедур шифрування та захищених мережевих протоколів;

вимоги до безпечної генерації, зберігання, архівування, пошуку, розповсюдження, вилучення та видалення ключів;

розгляд відповідних вимог законодавства.

Пов’язані заходи: ISP–02.

2) криптографічна політика. Криптографічна політика та процедури повинні містити положення, що базуються на оцінці ризику, щодо використання шифрування, узгодженого зі схемами класифікації даних, та враховувати канал електронних комунікаційних мереж, тип, надійність та якість шифрування.

3) відповідність процедур шифрування сучасному стану. Потужні процедури шифрування та захищені мережеві протоколи, згадані в політиці та процедурах криптографії, повинні відповідати найсучаснішим технологіям.

Рекомендації з реалізації:

Надавачу хмарних послуг потрібно буде визначити поняття «найсучасніший», а також посилання на зовнішні посібники.

4.59 CKM–02 Шифрування даних при передачі

Заходи захисту.

Хмарні дані користувачів хмарних послуг, що передаються через електронні комунікаційні мережі загального користування, повинні бути захищені в конфіденційності, цілісності та автентичності.

Посилення заходів:

1) надійні механізми шифрування при передачі хмарних даних користувачів хмарних послуг. CSP повинен визначити та впровадити надійні механізми шифрування для передачі хмарних даних користувачів хмарних послуг через електронні комунікаційні мережі загального користування.

2) надійні механізми шифрування при передачі всіх даних. CSP повинен визначити та впровадити надійні механізми шифрування для передачі всіх даних через електронні комунікаційні мережі загального користування.

4.60 CKM–03 Шифрування даних при зберіганні

Заходи захисту.

CSP повинен встановити процедури та технічні запобіжні заходи, щоб запобігти розголошенню даних користувачів хмарних послуг під час зберігання.

Посилення заходів:

1) документування заходів шифрування під час зберігання. CSP повинен документувати та впроваджувати процедури та технічні запобіжні заходи для шифрування даних користувачів хмарних послуг під час зберігання;

2) персоналізація особистих та секретних ключів користувачів хмарних послуг. Особисті та секретні ключі, що використовуються для шифрування, повинні бути відомі лише користувачам хмарних послуг відповідно до вимог законодавства з можливістю винятків;

3) використання особистих та секретних ключів користувачів хмарних послуг. Процедури використання особистих та секретних ключів, включаючи конкретну процедуру для будь-яких винятків, узгоджуються за контрактом із користувачем хмарних послуг;

4) персоналізація особистих та секретних ключів користувачів хмарних послуг без винятків. Особисті та секретні ключі, що використовуються для шифрування, повинні бути відомі виключно користувачу хмарних послуг та без будь-яких винятків відповідно до вимог законодавства.

4.61 CKM–04 Безпечне управління ключами

Заходи захисту.

Мають бути встановлені відповідні механізми управління ключами для захисту конфіденційності, автентичності або цілісності криптографічних ключів.

Посилення заходів:

1) управління ключами. Процедури і технічні гарантії для безпечного управління ключами в зоні відповідальності CSP повинні містити такі аспекти:

генерацію ключів для різних криптографічних систем і додатків;

видачу та отримання сертифікатів відкритих ключів;

надання та активацію ключів;

безпечне зберігання ключів, включаючи опис того, як авторизовані користувачі хмарних послуг отримують доступ;

зміну або оновлення криптографічних ключів, у тому числі політики, що визначають, за яких умов та яким чином зміни та/або оновлення мають бути реалізовані;

обробку скомпрометованих ключів;

вилучення та видалення ключів;

2) зберігання ключів у відокремленому стані. Для безпечного зберігання ключів система управління ключами повинна бути відокремлена від програмного рівня та проміжного рівня програмного забезпечення;

3) зберігання ключів у безпечному місці. Для безпечного зберігання ключів та інших таємниць, що використовуються для адміністрування, CSP повинен використовувати відповідне безпечне місце зберігання, програмне чи апаратне забезпечення;

4) використання спільних ключів. Якщо використовуються попередньо спільні ключі, конкретні положення, що стосуються безпечного використання цієї процедури, повинні бути вказані окремо.

Клас заходів захисту CS – Безпека електронних комунікацій

Забезпечити захист інформації в електронних комунікаційних мережах та відповідних системах обробки інформації.

4.62 CS–01 Технічні заходи

Заходи захисту.

CSP повинен запровадити відповідні технічні захисні засоби для виявлення мережевих атак та реагування на них, а також для забезпечення захисту інформації та систем обробки інформації.

Посилення заходів:

1) документування систем виявлення та реагування на атаки. CSP повинен документувати, передавати та впроваджувати технічні засоби захисту, які є придатними для оперативного виявлення мережевих атак та реагування на них, а також для забезпечення захисту інформації та систем обробки інформації відповідно до ISP–02.

Рекомендації з реалізації:

На основі нерегулярних шаблонів вхідного або вихідного трафіка та/або розподілених атак відмови в обслуговуванні (DDoS).

Пов’язані заходи: ISP–02;

2) аналіз ризиків у системах виявлення та реагування на атаки. Технічні запобіжні заходи в CS–01(1) повинні базуватися на результатах аналізу ризиків, проведеного згідно з RM–01.

Пов’язані заходи: CS–01(1), RM–01;

3) інформування системи SIEM. CSP подає в систему SIEM (інформація про безпеку та управління подіями) всі дані з технічних гарантій, реалізованих так, щоб ініціювалися автоматичні контрзаходи щодо корелюючих подій;

4) гарантування відсутності несанкціонованого підключення пристроїв. CSP повинен впроваджувати технічні запобіжні заходи, щоб гарантувати, що жодні невідомі (фізичні чи віртуальні) пристрої не приєднуються до її (фізичної чи віртуальної) мережі;

5) унеможливлення одночасного прориву вразливістю декількох ліній захисту. CSP на своїх технічних запобіжних заходах повинен використовувати різні технології, щоб запобігти тому, що одна вразливість призводить до одночасного прориву декількох ліній захисту.

4.63 CS–02 Вимоги безпеки до підключення в мережі CSP

Заходи захисту.

Встановлення зв’язків у мережі CSP повинно регулюватися специфічними вимогами безпеки.

Посилення заходів:

1) документування заходів захисту всередині мережі CSP. CSP повинен документувати, передавати інформацію, робити доступними та реалізовувати конкретні вимоги безпеки для підключення всередині своєї мережі:

коли зони безпеки мають бути відокремлені та коли користувачі хмарних послуг мають бути логічно чи фізично відокремлені;

які взаємозв'язки та які мережеві та прикладні протоколи дозволені в кожному випадку;

як трафік даних для адміністрування та моніторингу відокремлений один від одного на рівні мережі;

яка внутрішня, міжлокаційна комунікація дозволена;

який зв’язок між мережами дозволений.

4.64 CS–03 Моніторинг підключень у мережі CSP

Заходи захисту.

Комунікаційні потоки в межах хмари, внутрішні та зовнішні, повинні контролюватися відповідно до норм, щоб належним чином реагувати на загрози.

Посилення заходів:

1) розрізняння довірених і ненадійних мереж. CSP повинен розрізняти довірені та ненадійні мережі на основі оцінки ризику;

2) розподіл областей з використанням демілітаризованих зон. CSP повинен розділити надійні та ненадійні мережі на різні зони безпеки для внутрішніх та зовнішніх областей мережі (та DMZ, якщо це можливо);

3) налаштування фізичного та віртуального середовища. CSP повинен розробити та налаштувати як фізичне, так і віртуалізоване мережеве середовище для обмеження та моніторингу підключення до надійних або ненадійних мереж відповідно до визначених вимог безпеки (див. CS–02).

Пов’язані заходи: CS–02;

4) сканування служб, протоколів та портів. CSP повинен перевіряти через визначені інтервали обґрунтування діяльності для використання всіх служб, протоколів та портів. Цей огляд також повинен передбачати

компенсаційні заходи, що застосовуються до протоколів, які вважаються небезпечними;

5) перегляд конфігурації моніторингу. CSP повинен щонайменше раз на рік переглядати розробку, впровадження та конфігурацію, що проводяться для моніторингу з'єднань, орієнтованих на ризик, з урахуванням визначених вимог безпеки;

6) оцінка ризиків. CSP повинен оцінити ризики виявлених вразливих місць відповідно до процедури управління ризиками (див. RM–01), а подальші заходи повинні бути визначені та відстежуватися (див. OPS–17).

Пов’язані заходи: RM–01, OPS–17;

7) захист журналів SIEM від фальсифікації. CSP повинен захищати всі журнали SIEM, щоб уникнути несанкціонованого доступу.

4.65 CS–04 Міжмережевий доступ

Заходи захисту.

Міжмережевий доступ повинен бути обмежений і дозволений лише на основі конкретних оцінок безпеки.

Посилення заходів:

1) контроль периметра шлюзами безпеки. Кожен периметр мережі повинен контролюватися шлюзами безпеки;

2) застосування матриці дозволених потоків. Шлюзи безпеки дозволяють лише законні підключення, визначені в матриці дозволених потоків;

3) доступ до системи для міжмережевого доступу. Авторизація доступу до системи для міжмережевого доступу повинна базуватися на оцінці безпеки на основі вимог користувачі хмарних послуг;

4) контроль периметра високодоступними шлюзами безпеки. Кожен периметр мережі повинен контролюватися надлишковими та високодоступними шлюзами безпеки;

5) автоматичний контроль периметра. CSP повинен автоматично моніторити контроль периметрів мережі, щоб гарантувати виконання CS–04(1).

Пов’язані заходи: CS–04(1).

4.66 CS–05 Мережі для адміністрування

Заходи захисту.

Адміністративні та оперативні управлінські обов'язки повинні виконуватися в мережах, відокремлених від інших мереж, для запобігання несанкціонованому трафіку та збереження розподілу обов'язків.

Посилення заходів:

1) відокремлення мережі адміністративного управління. CSP повинен визначити та впровадити окремі мережі для адміністративного управління інфраструктурою та функціонування консолей управління;

2) відокремлення мереж адміністрування від мереж користувачі хмарних послуг. CSP повинен логічно або фізично відокремити мережі для адміністрування від мереж CSC;

3) розподіл мереж віртуальних машин. CSP повинен фізично або логічно розділити мережі, що використовуються для переміщення або створення віртуальних машин;

4) шифрування каналів для невідокремлених мереж. Коли адміністративні мережі фізично не відокремлені від інших мереж, адміністративні потоки повинні передаватися в суворо зашифрованому каналі.

5) налаштування брандмауера. CSP повинен встановити та налаштувати програму брандмауера для захисту інтерфейсів адміністрування, призначених для CSC та доступних у електронній комунікаційній мережі загального користування.

4.67 CS–06 Розмежування трафіка у спільних мережевих середовищах

Заходи захисту.

Конфіденційність і цілісність даних користувачів хмарних послуг повинна захищатися заходом відокремлення при передачі через спільні мережі.

Посилення заходів:

1) розмежування механізмів трафіка. CSP повинен визначити, задокументувати та впровадити механізми розмежування на рівні мережі трафіка даних різних користувачів хмарних послуг;

2) безпечне відокремлення можливостей інфраструктури. При реалізації можливостей інфраструктури безпечне відокремлення повинно забезпечуватися фізично відокремленими мережами або суворо зашифрованими VLAN.

Рекомендації з реалізації:

Поняття надійного шифрування визначено у вказівках щодо класу CKM у пункти 4.58-4.61 розділу IV цих Рекомендацій.

4.68 CS–07 Мережева топологія документації

Заходи захисту.

Карти інформаційної системи слід вести і підтримувати, щоб уникнути адміністративних помилок під час роботи в режимі реального часу та забезпечити своєчасне відновлення у випадку несправностей.

Посилення заходів:

1) документування логічної структури мережі. CSP повинен підтримувати всю сучасну документацію щодо логічної структури мережі, яка використовується для надання або експлуатації хмарної послуги;

2) документування розподілу зон та географічного положення місць мережі. Документація повинна охоплювати принаймні те, як розподілено підмережі, як зоновано та сегментовано мережу, як вона з'єднується зі сторонніми та електронними комунікаційними мережами загального користування, а також географічні місця, в яких зберігаються дані користувачів хмарних послуг;

3) документування обладнання та серверів. У зв'язку з описом активів (див. AM–01) документація повинна охоплювати обладнання, що забезпечує функції безпеки, та сервери, що містять дані або забезпечують чутливі функції.

Пов’язані заходи: AM–01.

4) перегляд документації топології мережі. CSP повинен проводити повний огляд документації топології мережі щонайменше раз на рік.

4.69 CS–08 Програмно визначена мережа

Заходи захисту.

Програмно визначена мережа повинна використовуватися лише в тому випадку, якщо хмарні дані користувача хмарних послуг захищені відповідними заходами.

Посилення заходів:

1) забезпечення конфіденційності даних користувачів хмарних послуг. CSP повинен забезпечити конфіденційність даних користувачів хмарних послуг за допомогою відповідних процедур, пропонуючи функції програмно визначеної мережі (SDN);

2) функціональність функцій програмно визначеної мережі. CSP повинен перевірити функціональність функцій SDN перед наданням нових функцій SDN CSC або зміною існуючих функцій SDN;

3) відповідність конфігурації мереж політиці безпеки. CSP повинен забезпечити, щоб конфігурація мереж відповідала політиці безпеки мережі, незалежно від засобів, використаних для створення конфігурації.

4.70 CS–09 Політика передачі даних

Заходи захисту.

Політика повинна бути визначена для захисту передачі даних від несанкціонованого перехоплення, маніпуляцій, копіювання, модифікації, перенаправлення або знищення.

Посилення заходів:

1) документування заходів захисту передачі даних. CSP повинен документувати, повідомляти та впроваджувати політику та процедури з

технічними та організаційними гарантіями для захисту передачі даних від несанкціонованого перехоплення, маніпулювання, копіювання, модифікації, перенаправлення або знищення згідно з ISP–02.

Пов’язані заходи: ISP–02;

2) посилання на класифікацію активів. Політика та процедури повинні містити посилання на класифікацію активів (див. AM–05).

Пов’язані заходи: AM–05.

Клас заходів захисту PI – Портативність та взаємодійність

Увімкнути можливість доступу до хмари через інші хмари або IT-системи користувачів хмарних послуг, отримувати збережені дані перед закінченням строку дії договору і безпечно видаляти їх від CSP.

4.71 PI–01 Документація і безпека вхідних і вихідних інтерфейсів

Заходи захисту.

Мають бути задокументовані вхідний та вихідний інтерфейси до/із хмари для доступу з інших або IT-систем.

Посилення заходів:

1) доступність хмарних сервісів, задокументовані інтерфейси. Хмарний сервіс повинен бути доступний хмарним сервісам від інших CSP або IT-систем користувачів хмарних послуг через задокументовані вхідні та вихідні інтерфейси.

Рекомендації з реалізації:

Тип та обсяг документації щодо інтерфейсів пристосовані до потреб експертів користувачів хмарних послуг, щоб дозволити використання цих інтерфейсів;

2) чіткість документування інтерфейсів. Інтерфейси повинні бути чітко задокументовані, щоб експерти, які займаються питаннями, розуміли, як їх можна використовувати для отримання даних;

3) використання стандартизованих протоколів зв'язку. Зв'язок на цих інтерфейсах повинен використовувати стандартизовані протоколи зв'язку, які забезпечують конфіденційність та цілісність переданої інформації відповідно до вимог її захисту;

4) шифрування зв'язку через ненадійні мережі. Зв'язок через ненадійні мережі повинен шифруватися відповідно до CKM–02.

Пов’язані заходи: CKM–02;

5) забезпечення перевірки інтерфейсів користувачів хмарних послуг перед початком роботи. CSP повинен дозволити своїм користувачів хмарних послуг перевірити, що надані інтерфейси (та їх безпека) відповідають вимогам захисту перед початком використання хмари, і щоразу, коли інтерфейси змінюються.

4.72 PI−02 Договори про надання даних

Заходи захисту.

Договори повинні визначати відповідну інформацію щодо переміщення даних після припинення договірних відносин.

Посилення заходів:

1) з'ясування умов припинення договірних відносин. CSP вносить в договір про надання хмарних послуг про хмарні послуги щонайменше такі аспекти, що стосуються припинення договірних відносин:

тип, обсяг та формат даних, які CSP надає CSC;

методи доставки даних користувачу хмарних послуг;

визначення часових рамок, протягом яких CSP надає дані CSC;

визначення моменту часу, з якого CSP робить дані недоступними для CSC та видаляє їх;

обов'язки та зобов'язання CSC щодо співпраці у наданні даних;

2) експертна оцінка придатності хмари. Визначення в PI–02(1) повинні базуватися на потребах експертів з потенційних користувачів хмарних послуг, які оцінюють придатність хмари з урахуванням залежності від CSP, а також вимог законодавства.

Пов’язані заходи: в PI–02(1);

3) перегляд умов договорів. CSP повинен не рідше одного разу на рік визначати правові та нормативні вимоги, які можуть застосовуватися до цих аспектів, і відповідно коригує умови договору.

4.73 PI−03 Безпечне видалення даних

Заходи захисту.

Мають бути задокументовані вхідний та вихідний інтерфейси до/із хмари для доступу з інших хмар або IT-систем.

Посилення заходів:

1) упровадження процедур видалення даних після закінчення строку дії договору на надання хмарних послуг. CSP повинен впроваджувати процедури видалення даних своїх користувачів хмарних послуг після розірвання договору відповідно до умов договору;

2) видалення метаданих і даних у резервних копіях. Видалення даних CSC також міститиме метадані та дані, що зберігаються у резервних копіях даних;

3) запобігання відновленню криміналістичними засобами. Процедури видалення даних користувача хмарних послуг повинні запобігати відновленню криміналістичними засобами;

4) документування видалення даних користувача хмарних послуг. CSP повинен задокументувати видалення даних користувача хмарних послуг, у тому числі метаданих та даних, що зберігаються в резервних копіях даних,

таким чином, щоб користувач хмарних послуг у хмарі відстежував видалення своїх даних;

5) видалення технічних даних щодо користувача хмарних послуг. Після закінчення договору CSP видаляє технічні дані щодо користувача хмарних послуг.

Клас заходів захисту CCM – Управління змінами і конфігурацією

Слід переконатися, що зміни та дії конфігурації інформаційних систем гарантують безпеку наданої хмари.

4.74 CCM–01 Політика змін в інформаційних системах

Заходи захисту.

Політика та процедури повинні бути визначені для управління змінами в інформаційних системах.

Посилення заходів:

1) документування змін. CSP повинен документувати, впроваджувати та передавати політику та процедури управління змінами IT-систем, що підтримують хмарний сервіс, згідно з ISP–02.

Пов’язані заходи: ISP–02;

2) особливі аспекти управління змінами. Політика та процедури управління змінами повинні охоплювати щонайменше такі аспекти:

критерії оцінки ризику, категоризації та пріоритетності змін і пов'язаних вимог до типу та обсягу тестування, яке має бути проведено, та необхідних схвалень;

вимоги до виконання та документації випробувань;

вимоги до розподілу обов'язків під час планування, тестування та випуску змін;

вимоги до належної інформації користувачів хмарних послуг про тип та обсяг змін, а також зобов'язання щодо співпраці відповідно до умов договору;

вимоги до документації змін у системі, експлуатаційної документації та документації, призначеної для користувача хмарних послуг;

вимоги до впровадження та документування надзвичайних змін, які повинні відповідати тому самому рівню безпеки, що і звичайні зміни.

4.75 CCM–02 Оцінка ризиків, категоризація та пріоритетів змін

Заходи захисту.

Обов'язки мають бути розподілені всередині організації CSP так, щоб забезпечити достатню кількість ресурсів для визначення та виконання плану безперервності бізнесу та забезпечити підтримку діяльності, пов'язаної з безперервністю бізнесу.

Посилення заходів:

1) класифікація пріоритетів змін. CSP повинен класифікувати та визначити пріоритети змін, враховуючи потенційний вплив безпеки на відповідні компоненти системи;

2) ґрунтування класифікації пріоритетів змін. CSP базує рішення щодо класифікації та встановлення пріоритетів на оцінці ризику, проведеної згідно з RM–01, щодо потенційного впливу на відповідні компоненти системи;

Пов'язані заходи: RM–01;

3) вживання заходів пом'якшення наслідків при високому ризику. Якщо ризик, пов'язаний із запланованою зміною, високий, то перед розгортанням служби слід вжити відповідних заходів щодо пом'якшення наслідків;

4) проведення власної оцінки ризиків користувачами хмарних послуг. Відповідно до договірних домовленостей CSP подає уповноваженим органам CSC значущу інформацію про привід, час, тривалість, тип та обсяг змін, щоб вони могли провести власну оцінку ризику до того, як зміна стане доступною у виробничому середовищі;

5) інформування користувачів хмарних послуг про зміни з високою оцінкою ризику. Незалежно від умов договору CSP інформує CSC, як зазначено у CCM–02(3), про зміни, які мають найвищу категорію ризику на основі їх оцінки.

Пов'язані заходи: CCM–02(3).

4.76 CCM–03 Тестування змін

Заходи захисту.

Зміни щодо хмар повинні перевірятися перед розгортанням, щоб мінімізувати ризики збоїв при впровадженні.

Посилення заходів:

1) перевірка змін перед розгортанням. CSP перевіряє запропоновані зміни перед розгортанням;

2) відповідність тестувань оцінці ризиків. Тип та обсяг тестувань повинні відповідати оцінці ризику;

3) кваліфікація працівників для проведення випробувань. Тестування повинно проводитися кваліфікованими працівниками або автоматизованими процедурами тестувань, що відповідають найсучаснішим технологіям;

4) залучення користувачів хмарних послуг до тестувань. Відповідно до умов договору CSP залучає CSC до тестувань;

5) попередня анонімність користувачів хмарних послуг. CSP повинен спочатку отримати схвалення від CSC та зробити дані користувача хмарних послуг анонімними, перш ніж використовувати їх для тестів, і гарантувати конфіденційність даних протягом усього процесу;

6) визначення ступеня помилок та вразливостей при тестуванні. CSP визначає ступінь серйозності помилок та вразливостей, виявлених під час

тестів, які мають значення для рішення про розгортання, згідно з визначеними критеріями та ініціює дії щодо своєчасного виправлення або пом'якшення;

7) тестування змін служби. Тести, що виконуються для змін до їх розгортання, повинні включати тестування на сервісі, що виконується в попередньому виробничому середовищі;

8) документування процедур попередніх тестувань. CSP повинен задокументувати та впровадити процедуру, яка забезпечує цілісність даних тестувань, що використовуються у попередньому виробничому середовищі;

9) виконання регресійного тестування. Перед розгортанням змін на системному компоненті CSP повинен виконати регресійне тестування на інших компонентах хмари, які залежать від цього системного компонента, щоб перевірити відсутність небажаних ефектів;

10) автоматичний контроль тестування. CSP повинен автоматично контролювати визначення та виконання тестів щодо змін, а також виправлення або пом'якшення помилок.

4.77 CCM–04 Схвалення для забезпечення у виробничому середовищі

Заходи захисту.

Зміни у хмарах повинні затверджуватися перед введенням у виробниче середовище.

Посилення заходів:

1) затвердження змін. CSP затверджує будь-які зміни хмари на основі визначених критеріїв, перш ніж вони стануть доступними CSC у виробничому середовищі.

Рекомендації з реалізації:

схвалення CSP може надавати уповноважений персонал CSP або автоматизована процедура, що забезпечує виконання визначених критеріїв;

2) залучення користувача хмарних послуг до затвердження змін. CSP повинен залучати CSC до процесу затвердження відповідно до вимог контракту;

3) автоматичний контроль затвердження змін. CSP повинен автоматично контролювати затвердження змін, що застосовуються у виробничому середовищі, щоб гарантувати виконання CCM–04(1).

Пов’язані заходи: CCM–04(1).

4.78 CCM–05 Виконання та реєстрація змін

Заходи захисту.

Зміни в хмарах повинні виконуватися через авторизовані облікові записи та простежуватися до особи чи системного компонента, який їх ініціював.

Посилення заходів:

1) визначення ролей персоналу або компонентів системи для внесення змін. CSP визначає ролі та права відповідно до IAM–01 для уповноваженого персоналу або компонентів системи, яким дозволено вносити зміни до хмари у виробничому середовищі.

Пов'язані заходи: IAM–01;

2) реєстрація всіх змін. Усі зміни хмарного сервісу у виробничому середовищі повинні реєструватися та простежуватися до користувача хмарних послуг або системного компонента, який ініціював зміну;

3) автоматичний контроль. CSP повинен автоматично контролювати зміни у виробничому середовищі, щоб гарантувати виконання CCM–05(1).

Пов'язані заходи: CCM–05(1).

4.79 CCM–06 Контроль версій

Заходи захисту.

Необхідно використовувати контроль версій для відстеження окремих змін та увімкнення відновлення попередньої версії, якщо потрібно.

Посилення заходів:

1) упровадження контролю версій. CSP повинен впровадити процедури контролю версій для відстеження залежностей окремих змін та відновлення уражених компонентів системи до попереднього стану в результаті помилок або виявлених вразливостей;

2) запобіжні заходи контролю версій. Процедури контролю версій повинні забезпечувати відповідні запобіжні заходи для забезпечення того, щоб конфіденційність, цілісність та доступність хмарних даних користувачів хмарних послуг не були порушені, коли компоненти системи повертаються до попереднього стану.

Рекомендації з реалізації:

Доступність може бути повністю гарантована лише для даних, які були до зміни, оскільки дані, внесені зміною, можуть бути втрачені під час відновлення;

3) ведення історії версій. CSP повинен зберігати історію версій програмного забезпечення та систем, що впроваджуються, щоб мати можливість відновити, де це можливо у тестовому середовищі, повне середовище, яке було впроваджено на певну дату; час збереження для цієї історії повинен бути принаймні таким самим, як для резервних копій (див. OPS–06).

Пов'язані заходи: OPS–06.

Клас заходів захисту DEV – Розробка інформаційних систем

Забезпечити безпеку інформації в циклі розробки інформаційних систем.

4.80 DEV–01 Політика для розробки та закупівлі інформаційних систем

Заходи захисту.

Повинна бути визначена політика для технічних та організаційних заходів щодо розвитку хмари протягом її життєвого циклу.

Посилення заходів:

1) документування безпечного розвитку хмари. CSP повинен документувати, повідомляти та впроваджувати політику та процедури відповідно до ISP–02 з технічними та організаційними заходами для безпечного розвитку хмари.

Пов'язані заходи: ISP–02.

2) безпека інформації з перших етапів проєктування. Політика та процедури безпечного розвитку повинні враховувати безпеку інформації з найперших етапів проєктування;

3) базування політики розвитку. Політика та процедури безпечного розвитку повинні базуватися на визнаних стандартах та методах з урахуванням таких аспектів:

безпека при розробці програмного забезпечення (вимоги, проєктування, впровадження, тестування та перевірка);

безпека при розгортанні програмного забезпечення (включаючи постійне постачання);

безпека в роботі (реакція на виявлені несправності та уразливості);

безпечні стандарти кодування та практики (уникаючи введення вразливостей у коді).

Рекомендації з реалізації:

Ці політики та процедури повинні зосереджуватися на безпечному життєвому циклі розробки програмного забезпечення (SSDLC). Очікується, що вони вплинуть на процедури, що перевищують поточну категорію, зокрема на класі CCM та OPS;

4) застосування автоматизованих засобів при розробці. Політика та процедури розробки повинні містити заходи щодо забезпечення встановлених стандартів та керівних принципів, включаючи автоматизовані засоби.

4.81 DEV–02 Розробка безпечного ланцюга постачання

Заходи захисту.

Ланцюг постачання системних компонентів повинен розглядатися в галузі безпеки розвитку.

Посилення заходів:

1) ведення переліку залежностей від апаратних та програмних продуктів. CSP повинен вести перелік залежностей від апаратних та програмних продуктів, що використовуються при розробці його хмари.

Рекомендації з реалізації:

Для програмних компонентів перелік залежностей часто називають SBoM.

Перелік потребує ідентифікації та документування відомих залежностей. Залежності повинні містити всі програмні модулі, що використовуються, бібліотеки або API, а також засоби розробки;

2) документування сторонніх програм і програм з відкритим кодом. CSP повинен задокументувати та впровадити політику щодо використання сторонніх програм та програм з відкритим кодом.

Рекомендації з реалізації:

політика повинна охоплювати такі аспекти:

обмеження віку компонентів;

обмеження застарілих компонентів та компонентів EOL/EOS;

обмеження на компоненти з відомими вразливими місцями;

обмеження використання відкритого сховища;

обмеження прийнятних ліцензій;

вимоги до оновлення компонентів;

заборона компонентів та версій, які входять до переліку заборонених;

прийнятні рекомендації щодо благодійних внесків.

Цей список обгрунтований вимогами OWASP щодо програмного забезпечення з відкритим кодом;

3) надання користувачам хмарних послуг списку залежностей. CSP надає користувачам хмарних послуг свій список залежностей за запитом;

4) оцінка ризику під час закупівель. Під час закупівель для розвитку хмари CSP повинен виконати оцінку ризику відповідно до RM–01 для кожного продукту.

Пов’язані заходи: RM–01.

Рекомендації з реалізації:

Використання сертифікованої продукції може значно спростити реалізацію цієї вимоги через гарантії безпеки, які може надати така сертифікація.

4.82 DEV–03 Безпечне середовище розробки

Заходи захисту.

Середовище розробки повинно враховувати безпеку інформації. Посилення заходів:

1) захист вихідного коду. CSP повинен забезпечити належний захист конфіденційності та цілісності вихідного коду на всіх стадіях розробки;

2) контроль версій. CSP повинен забезпечити використання контролю версій, щоб зберігати історію змін вихідного коду з віднесенням змін до індивідуальної розробки та цілісність вихідного коду, належним чином захищену на всіх стадіях розробки;

3) упровадження безпечного середовища розробки та тестування. CSP повинен впровадити безпечне середовище розробки та тестування, що дає можливість управляти всім циклом розробки інформаційної системи хмари;

4) урахування середовища розробки та тестування при оцінці ризиків. CSP повинен враховувати середовище розробки та тестування під час проведення оцінки ризику;

5) амортизаційні ресурси. CSP містить амортизаційні ресурси як частину політики резервного копіювання. Рекомендації з реалізації:

Ресурси розробки включають вихідний код, бази даних, засоби розробки та експлуатації та їх конфігурації.

4.83 DEV–04 Розподіл середовищ

Заходи захисту.

Середовище розробки має враховувати безпеку інформації. Посилення заходів:

1) розподіл виробничих середовищ. CSP повинен забезпечити, щоб виробничі середовища були фізично або логічно відокремлені від середовищ розробки, випробувань або попереднього виробництва;

2) невикористання даних виробничих середовищ. Дані, що містяться у виробничих середовищах, не повинні використовуватися в середовищах розробки, тестування або перед виробництвом, щоб не порушити їх конфіденційність.

Рекомендації з реалізації:

Існує ще одна вимога (CCM–03(5)), зокрема щодо передвиробничих середовищ, яка дозволяє CSP отримувати тестові дані з виробничих даних відповідно до конкретних вимог, але виробничі дані ніколи не повинні використовуватися безпосередньо для цілей тестування.

Пов’язані заходи: CCM–03(5);

3) еквівалентність вимог безпеки в електронних комунікаційних мережах загального користування. Коли невиробничі середовища діють через загальнодоступні мережі, вимоги до безпеки повинні бути еквівалентними тим, які визначені для виробничого середовища.

4.84 DEV–05 Розробка особливостей безпеки

Заходи захисту.

Середовище розробки повинно враховувати безпеку інформації. Посилення заходів:

1) документування підвищених вимог для тестування. CSP повинен документувати, повідомляти, надавати та впроваджувати конкретні процедури для розробки функцій, що реалізують технічні механізми або захисні заходи із підвищеними вимогами до тестування.

Рекомендації з реалізації:

Ця вимога застосовується на всіх рівнях. Для «Середнього» та «Високого» рівнів вона уточнюється поточним документом. Для «Низького» рівня вимоги слід розглядати як придатний спосіб задоволення підвищених вимог;

2) проєктна документація для функцій захисту. Проєктна документація для функцій захисту повинна містити специфікацію очікуваних вхідних, вихідних даних та можливих помилок, а також аналіз безпеки компетентності та запланованої ефективності функції;

3) всеохоплюваність тестами вхідних даних та результатів. Тести характеристик захисту повинні охоплювати всі зазначені вхідні дані та всі визначені результати, включаючи всі визначені умови помилок;

4) документування випробувань. Документація випробувань щодо засобів захисту повинна містити щонайменше опис випробування, початкові умови, очікуваний результат та інструкції щодо проведення випробування.

5) документування результатів випробувань. Документація випробувань повинна передбачати демонстрацію охоплення вихідного коду, у тому числі з критично важливим кодом.

4.85 DEV–06 Ідентифікація вразливостей хмари

Заходи захисту.

Повинні вживатися відповідні заходи для виявлення вразливих місць, що виникають у хмарі в процесі розробки.

Посилення заходів:

1) перевірка на наявність вразливостей. CSP застосовує відповідні заходи для перевірки хмари на наявність вразливостей, які могли бути інтегровані в хмару під час процесу розробки.

Рекомендації з реалізації:

Для «Низького» рівня заходи будуть простими та автоматизованими, але деякі заходи повинні бути реалізованими так, щоб відповідати вимогам.

2) інтеграція виявлення вразливостей. Процедури виявлення вразливостей повинні бути інтегровані в процес розробки.

Рекомендації з реалізації:

Для «Низького» рівня заходи будуть простими та автоматизованими, але деякі заходи повинні бути реалізованими так, щоб відповідати вимогам;

3) залежність процедур тестування оцінці ризиків. Процедури повинні містити такі види діяльності залежно від оцінки ризику:

статичне тестування безпеки додатків;

динамічне тестування безпеки додатків;

огляд коду експертами з предметних питань;

отримання інформації про підтверджені вразливості в бібліотеках програмного забезпечення, що надаються третіми сторонами та використовуються у власній хмарі.

Рекомендації з реалізації:

Через залежність від оцінки ризику передбачається, що багато заходів будуть застосовуватися на високому рівні.

Поняття огляду коду слід сприймати у широкому значенні, не лише обмежуючись вихідним кодом, але також застосовуючи до файлів конфігурації і загалом до всього вмісту, створеного розробниками, що може вплинути на безпеку хмари;

4) перевірка коду. Перевірка коду повинна регулярно проводитися кваліфікованим персоналом або підрядниками;

5) оцінка ступеня серйозності виявлених вразливостей. CSP повинен оцінити ступінь серйозності виявлених вразливостей згідно з критеріями, визначеними в OPS–17, та вжити заходів щодо їх негайного усунення або пом'якшення.

Пов’язані заходи: OPS–17;

6) перегляд коду і тестів на проникнення безпеки. Процедури для виявлення таких вразливих місць також міститимуть щорічні огляди коду та тести на проникнення експертами з предметних питань, як частину річної програми, визначеної в OPS–19.

Пов’язані заходи: OPS–19.

4.86 DEV–07 Аутсорсинг розробки

Заходи захисту.

Аутсорсингові розробки повинні забезпечувати такі гарантії безпеки, як і внутрішні розробки.

Посилення заходів:

1) взаємодія з підрядником розробки хмари. При передачі підряднику розробки хмари або її компонентів CSP та підрядник повинні домовитися про укладання договорів щодо специфікацій щодо таких аспектів:

безпека при розробці програмного забезпечення (вимоги, проєктування, впровадження, випробування та перевірки) відповідно до визнаних стандартів та методів;

приймальна перевірка якості послуг, що надаються відповідно до узгоджених функціональних та нефункціональних вимог;

надання доказів того, що було проведено достатньо перевірок, щоб виключити існування відомих вразливих місць;

2) попередня оцінка ризиків перед наданням субпідряду. Перед наданням субпідряду на розробку хмарного сервісу або його компонентів, CSP повинен провести оцінку ризику згідно з RM–01, яка враховує такі аспекти:

управління вихідним кодом субпідрядником;

кадрові процедури, реалізовані субпідрядником;

необхідний доступ до середовища розробки, тестування та попереднього виробництва CSP.

Пов’язані заходи: RM–01;

3) документування нагляду та контролю за сторонніми розробниками. CSP повинен задокументувати та впровадити процедуру, яка дає змогу здійснювати нагляд та контроль за заходами розробки сторонніми розробниками, щоб переконатися, що передана аутсорсингова діяльність розробника відповідає політиці безпечного розвитку CSP і дозволяє досягти рівня безпеки зовнішнього розвитку, що еквівалентна безпеці внутрішнього розвитку;

4) тестування розробленого підрядником проєкту. Внутрішні або зовнішні співробітники CSP повинні проводити тести, які релевантні для рішення про розгортання, коли зміни містять результат розробленого підрядником проєкту.

Клас заходів захисту PM – Управління закупівлями

Забезпечити захист інформації, до якої CSP можуть отримати доступ, та контролювати узгоджені вимоги щодо послуг та безпеки.

4.87 PM–01 Політика і процедури контролю та моніторинг третіх сторін

Заходи захисту.

Обов'язки повинні розподілятися всередині організації CSP, щоб забезпечити достатню кількість ресурсів для визначення та виконання плану безперервності бізнесу та підтримку діяльності, пов'язаної з безперервністю бізнесу.

Посилення заходів:

1) документування моніторингу третіх сторін. CSP повинен документувати, поширювати та впроваджувати політику та процедури згідно з ISP–02 для контролю та моніторингу третіх сторін, чиї продукти або послуги сприяють наданню хмарних послуг.

Пов’язані заходи: ISP–02;

2) взаємодія надавача хмарних послуг з третіми сторонами. Разом політика та процедури, визначені в PM–01(1), повинні охоплювати принаймні такі аспекти:

вимоги до оцінки ризиків, що виникають внаслідок закупівлі послуг третіх сторін;

вимоги до класифікації третіх сторін на основі оцінки ризиків CSP;

вимоги до безпеки інформації для обробки, зберігання або передачі інформації третіми сторонами на основі визнаних галузевих стандартів;

вимоги до обізнаності та підготовки персоналу щодо безпеки інформації;

відповідні вимоги законодавства;

вимоги щодо усунення вразливостей, інцидентів безпеки та несправностей;

специфікації укладання договору про надання хмарних послуг щодо цих вимог;

специфікації для моніторингу цих вимог;

специфікації щодо застосування цих вимог також до надавачів хмарних послуг, які використовуються третіми сторонами, оскільки послуги, що надаються цими надавачами хмарних послуг, також сприяють наданню хмарних послуг.

Пов’язані заходи: PM–01(1);

3) звітування незалежних аудиторів. CSP повинен за договором вимагати від своїх підпорядкованих організацій регулярних звітів незалежних аудиторів щодо придатності проєкту та ефективності роботи їхньої системи внутрішнього контролю, що стосується послуг.

Рекомендації з реалізації:

Захід PM–01(5) розглядається як прийнятний компенсуючий захід.

Пов’язані заходи: PM–01(5);

4) додатковий контроль третіх сторін. Звіти повинні містити додаткові заходи захисту служб хмарних сервісів, які необхідні разом із засобами захисту надавача хмарних послуг, що застосовуються з відповідною гарантією;

5) право додаткової перевірки надавачем хмарних послуг третіх сторін. Якщо треті сторони не можуть надати звіт про відповідність вимог, CSP залишає за собою право перевірити їх, щоб оцінити придатність та ефективність внутрішнього та додаткового контролю, пов'язаного з послугами, кваліфікованим персоналом.

4.88 PM–02 Оцінка ризиків надавачів хмарних послуг

Заходи захисту.

CSP повинні проходити оцінку ризиків, щоб визначити потреби в безпеці, пов'язані з товаром або послугою, яку вони надають.

Посилення заходів:

1) попередня оцінка ризиків надавачів хмарних послуг. CSP проводить оцінку ризиків своїх надавачів хмарних послуг відповідно до сукупності

політик та процедур контролю та моніторингу третіх сторін, перш ніж вони почнуть сприяти наданню хмарних послуг;

2) оцінка ризиків надавачів хмарних послуг. Оцінка ризиків повинна містити виявлення, аналіз, оцінку, обробку та документування, що стосуються таких аспектів:

потреби у захисті щодо конфіденційності, цілісності, доступності та достовірності інформації, що циркулює між надавачем хмарних послуг та третьою стороною;

вплив порушення захисту щодо надання хмарних послуг;

залежність CSP від надавача хмарних послуг від обсягу, складності та унікальності придбаної послуги, включаючи розгляд можливих альтернатив.

3) формування додаткових елементів управління службами хмарних сервісів. Після оцінки ризику надавачів хмарних послуг CSP визначає для кожної вимоги, що застосовується, перелік додаткових елементів управління службам хмарних сервісів , які повинні застосовуватися надавачем хмарних послуг;

4) надання послуг з охорони публічних послуг. CSP повинен забезпечити, щоб надавач хмарних послуг застосовував заходи з охорони публічних послуг, а також надав докази, що підтверджують оцінку їх ефективності відповідно до рівня цільової оцінки.

5) адекватність оцінки ризику. Компетентність оцінки ризику та визначення CSOC повинні регулярно перевірятися (бажано щорічно).

Рекомендації з реалізації:

Призначено для підготовки роботи щодо залежностей. Під час основного аудиту аудитор перевіряє наявність документації, що підтверджує достовірність, але перевірка цієї документації виконується в окремому завданні.

4.89 PM–03 Перелік надавачів хмарних послуг

Заходи захисту.

Для полегшення їх контролю та моніторингу має бути доступний централізований перелік надавачів хмарних послуг.

Посилення заходів:

1) ведення переліку надавачів хмарних послуг. CSP повинен вести перелік для контролю та моніторингу надавачів хмарних послуг, які сприяють наданню хмарних послуг;

2) вміст переліку надавачів хмарних послуг. Перелік повинен містити таку інформацію:

назва компанії;

адреса;

місця обробки та зберігання даних;

відповідальна контактна особа у надавача хмарних послуг;

опис послуги;

класифікація на основі оцінки ризику;

початок користування послугою;

доказ дотримання вимог, узгоджених із контрактом;

3) перегляд переліку надавачів хмарних послуг. CSP повинен щороку перевіряти перелік на повноту, точність та дійсність.

4.90 PM–04 Моніторинг відповідності вимогам

Заходи захисту.

Повинні бути встановлені механізми моніторингу для забезпечення дотримання третіми сторонами своїх регуляторних та договірних зобов'язань.

Посилення заходів:

1) контроль та моніторинг третіх сторін. CSP повинен контролювати відповідність своїх надавачів хмарних послуг вимогам щодо захисту інформації та вимогам законодавства, політик та процедур, що стосуються контролю та моніторингу третіх сторін;

2) огляд доказів. Діяльність з моніторингу повинна передбачати щонайменше регулярний огляд таких доказів, наданих надавачами хмарних послуг згідно з умовами договору:

звіти про якість наданої послуги;

сертифікати відповідності систем управління міжнародним стандартам;

незалежні звіти третіх сторін про придатність та операційну ефективність їх систем внутрішнього контролю, пов'язаних з обслуговуванням;

записи третіх сторін про обробку вразливостей, інцидентів безпеки та несправностей;

3) частота моніторингу третіх сторін. Частота моніторингу повинна відповідати класифікації третьої сторони на основі оцінки ризику, проведеної надавачем хмарних послуг (див. PM–02), а результати моніторингу слід вносити в огляд оцінки ризику третьої сторони.

Пов’язані заходи: PM–02;

4) виявлені порушення та відхилення. Виявлення порушення та відхилення повинні бути проаналізовані, оцінені та розглянуті відповідно до процедури управління ризиками (див. PM–01).

Пов’язані заходи: PM–01;

5) інформування користувача хмарних послуг про зміну третьої сторони. Коли відбувається зміна третьої сторони, яка сприяє наданню хмарної послуги та впливає на рівень її безпеки, CSP повідомляє всі свої CSC без затримки;

6) перегляд вимог щодо нерозголошення інформації. CSP повинен задокументувати та впровадити процедуру перегляду та оновлення (раз на рік), вимог щодо нерозголошення інформації або конфіденційності щодо надавачів, що сприяють наданню послуги;

7) автоматичний моніторинг. CSP повинен доповнити процедури контролю за дотриманням автоматичного моніторингу, використовуючи автоматичні процедури, що стосуються таких аспектів:

конфігурація системних компонентів;

продуктивність та доступність системних компонентів;

час реакції на несправності та інциденти безпеки;

час відновлення (час до завершення обробки помилок).

Рекомендації з реалізації:

Цей автоматизований моніторинг може також призвести до виявлення невідповідностей, про що, можливо, доведеться повідомляти CAB як частину зобов'язань щодо постійного моніторингу CSP;

8) автоматичний контроль виявлених порушень та розбіжностей. CSP повинен автоматично контролювати виявлені порушення та розбіжності, і про них автоматично повідомляти відповідальний персонал або системні компоненти надавача хмарних послуг для оперативної оцінки та дій.

Рекомендації з реалізації:

Цей автоматизований моніторинг може також призвести до виявлення невідповідностей, про що, можливо, доведеться повідомляти CAB як частину зобов'язань щодо постійного моніторингу CSP.

4.91 PM–05 Стратегія виходу

Заходи захисту.

Повинні бути задокументовані стратегії, що забезпечують мінімальну зупинку бізнесу, якщо відносини з надавачем хмарних послуг припиняються.

Посилення заходів:

1) визначення стратегії виходу із закупівлі послуг. CSP повинен визначити стратегію виходу із закупівлі послуг, коли рівень ризику надавача хмарних послуг виявився високим;

2) узгодження стратегії виходу планами роботи. Стратегії виходу повинні узгоджуватися з планами безперервної роботи та містити такі аспекти:

аналіз потенційних витрат, наслідків, ресурсів та термінів переходу придбаної послуги до альтернативного надавача хмарних послуг;

визначення та розподіл ролей, відповідальності та достатніх ресурсів для виконання заходів щодо переходу;

визначення критеріїв успіху для переходу;

визначення показників для моніторингу ефективності послуги, які повинні ініціювати відмову від послуги, якщо результати є неприйнятними.

Клас заходів захисту IM – Управління інцидентами

Забезпечити послідовний та комплексний підхід до захоплення, оцінки, зв'язку та посилення інцидентів безпеки.

4.92 IM–01 Політика управління інцидентами безпеки

Заходи захисту.

Повинна бути визначена політика для реагування на інциденти безпеки швидко, ефективно та впорядковано.

Посилення заходів:

1) документування реагування на інциденти безпеки. CSP повинен документувати, поширювати та впроваджувати сукупність політик та процедур згідно з ISP–02, що містять технічні та організаційні гарантії для забезпечення швидкого, ефективного та належного реагування на всі відомі інциденти безпеки.

Пов’язані заходи: ISP–02;

2) встановлення пріоритетів та ескалації інцидентів безпеки. Разом політика та процедури повинні містити вказівки щодо класифікації, встановлення пріоритетів та ескалації інцидентів безпеки та створювати інтерфейси для управління інцидентами та управління безперервністю бізнесу;

3) створення комп'ютерної групи реагування на надзвичайні ситуації. CSP повинен створити комп'ютерну групу реагування на надзвичайні ситуації (CERT), яка сприяє скоординованому вирішенню інцидентів у галузі безпеки.

Рекомендації з реалізації:

На рівні «Низький» CERT може бути спрощеною групою, яка здійснює нагляд за реагуванням на інциденти.

4) інформування постраждалих від інцидентів безпеки користувачів хмарних послуг. CSP повинен своєчасно та належним чином інформувати користувачів хмарних послуг, котрі постраждали від інцидентів безпеки;

5) внесення процедури збору даних при інциденті безпеки. Політика управління інцидентами повинна містити процедури щодо того, як можна збирати дані підозрілої системи у випадку інциденту безпеки;

6) внесення планів аналізу типових випадків безпеки. Політика управління інцидентами повинна містити плани аналізу типових випадків безпеки;

7) методологія оцінки. Політика управління інцидентами повинна містити методологію оцінки, щоб зібрана інформація не втрачала своєї доказової цінності в будь-якій наступній правовій оцінці;

8) регулярне тестування можливостей реагування на інциденти. Політика управління інцидентами повинна містити положення щодо регулярного тестування можливостей реагування на інциденти для визначення загальної ефективності можливостей та виявлення потенційних недоліків.

4.93 IM–02 Обробка інцидентів безпеки

Заходи захисту.

Повинна бути визначена та застосована методологія для швидкої, ефективної та впорядкованої обробки випадків безпеки.

Посилення заходів:

1) аналіз першопричин для подій загрози безпеки. CSP класифікує, визначає пріоритети та проводить аналіз першопричин для подій, які можуть становити загрозу для безпеки, використовуючи у разі потреби своїх експертів та зовнішніх надавачів безпеки хмарних послуг;

2) ведення каталогу інцидентів безпеки. CSP повинен вести каталог, який чітко ідентифікує інциденти безпеки, що впливають на дані користувачів хмарних послуг, і використовувати цей каталог для класифікації інцидентів;

3) кореляція подій. Механізм класифікації інцидентів повинен передбачати положення щодо кореляції подій. Крім того, ці корельовані події повинні самі оцінюватися та класифікуватися відповідно до їх критичності;

4) перегляд моделювання, аналізу та захисту від інцидентів та атак. CSP повинен моделювати виявлення, аналіз та захист від інцидентів безпеки та атак щонайменше один раз на рік за допомогою відповідних тестів та навчань.

Рекомендації з реалізації:

Наприклад, тренування «Червоної команди» CERT;

5) контроль обробки інцидентів. CSP повинен контролювати обробку інцидентів, щоб перевірити застосування політики та процедур управління інцидентами.

Рекомендації з реалізації:

Типовий моніторинг може відбуватися шляхом аналізу системи управління бізнес-процесами.

4.94 IM–03 Документація та звітність про інциденти безпеки

Заходи захисту.

Інциденти, що стосуються безпеки, мають бути задокументовані та повідомляються користувачам хмарних послуг вчасно.

Посилення заходів:

1) документування заходів за результатами обробки інцидентів безпеки. CSP повинен задокументувати реалізовані заходи після обробки інциденту з безпекою і відповідно до умов договорів надіслати документ постраждалим користувачам хмарних послуг для підтвердження;

2) надання інформації про інциденти. CSP надає інформацію про інциденти безпеки або підтверджені порушення безпеки усім заінтересованим користувачам хмарних послуг;

3) повідомлення про інциденти безпеки. CSP повинен постійно повідомляти про інциденти безпеки постраждалим користувачам хмарних

послуг, доки інцидент безпеки не буде закритий, а рішення застосовано та задокументовано відповідно до визначеного SLA та умов договору.

4) затвердження рішень щодо обробки інцидентів. CSP повинен дозволити користувачам хмарних послуг самостійно затверджувати рішення, перш ніж автоматично затверджувати його через певний період.

4.95 IM–04 Обов'язок користувача хмарних послуг звітувати щодо інцидентів безпеки

Заходи захисту.

Інциденти, що стосуються безпеки, повинні бути задокументовані та повідомлятися користувачам хмарних послуг вчасно.

Посилення заходів:

1) інформування працівників про зобов'язання. CSP інформує працівників та користувачів хмарних послуг про їхні договірні зобов'язання повідомляти про всі події безпеки, які їм стають відомими і безпосередньо пов'язані з хмарою;

2) звільнення від відповідальності користувачів хмарних послуг за «неправдиві повідомлення» про події. CSP не повинен вживати жодних негативних заходів щодо тих, хто надає «неправдиві повідомлення» про події, які згодом не виявляються інцидентами, і повинен повідомляти цю політику працівникам та користувачам хмарних послуг;

3) визначення контактної особи для повідомлення про події безпеки. CSP повинен визначити, поширити та затвердити єдину контактну особу для повідомлення про події безпеки та вразливості.

4.96 IM–05 Участь користувачів хмарних послуг у подіях інцидентів

Заходи захисту.

Користувачі хмарних послуг повинні регулярно отримувати інформацію про статус інцидентів, які їх стосуються.

Посилення заходів:

1) інформування користувачів хмарних послуг про стан інцидентів. CSP періодично інформує своїх користувачів хмарних послуг про стан інцидентів, що стосуються CSC, або у разі потреби залучає їх до вирішення, згідно з умовами договору;

2) інформування користувачів хмарних послуг про вжиті дії щодо інциденту. Як тільки інцидент буде вирішено, CSP повідомляє своїм користувачам хмарних послуг про вжиті заходи відповідно до умов договору.

4.97 IM–06 Процес оцінки та навчання

Заходи захисту.

Повинно бути вжито заходів для постійного вдосконалення послуги на основі досвіду, отриманого в результаті інцидентів.

Посилення заходів:

1) аналіз інцидентів безпеки. CSP повинен проводити аналіз інцидентів безпеки для виявлення повторних або значних інцидентів та виявлення потреби в подальшому захисті, якщо це необхідно, за підтримки зовнішніх органів;

2) залучення кваліфікованих підрядників. CSP укладає договори на підтримку зовнішніх органів, які є кваліфікованими надавачів хмарних послуг з реагування на аварії або є державними установами;

3) сховище інформації про інциденти безпеки. CSP повинен визначити, впровадити та підтримувати сховище інформації про інциденти безпеки та заходи, вжиті для їх вирішення, а також інформацію, що стосується активів, на які вплинули ці інциденти, і використовувати цю інформацію для розширення класифікаційного каталогу;

4) моніторинг сховища інформації про інциденти безпеки. Інформація, отримана внаслідок управління інцидентами та зібрана у сховищі, повинна використовуватися для виявлення повторюваних інцидентів або потенційних суттєвих інцидентів та для визначення потреби в удосконалених гарантіях та їх реалізації.

4.98 IM–07 Збереження доказів інцидентів

Заходи захисту.

Повинно бути вжито заходів щодо збереження інформації, пов’язаної з інцидентами в галузі безпеки.

Посилення заходів:

1) документування процедури архівування доказів про інциденти. CSP повинен задокументувати та впровадити процедуру архівування всіх документів та доказів, що містять деталі щодо інцидентів безпеки;

2) особливі вимоги щодо доказів про інциденти. Документи та докази повинні бути заархівовані таким чином, щоб вони могли бути використані як докази в суді;

3) додаткова експертиза інцидентів. Якщо CSP вимагає додаткової експертизи з метою збереження доказів та забезпечення безпеки ланцюга зберігання, CSP має укласти контракт лише з кваліфікованим надавачем хмарних послуг щодо реагування на інциденти;

4) захист інформації про інциденти. CSP повинен впроваджувати механізми та процедури захисту для захисту всієї інформації, що стосується інцидентів безпеки, відповідно до рівнів критичності та вимог законодавства;

5) група реагування на інциденти. Надавач хмарних послуг повинен створити інтегровану групу персоналу судового реагування або реагування на

інциденти, спеціально навченого з питань збереження доказів та управління ланцюгом зберігання.

Клас заходів захисту BC – Безперервність бізнесу

Слід планувати, впроваджувати, підтримувати та перевіряти процедури та заходи для безперервності бізнесу та управління надзвичайними ситуаціями

4.99 BC–01 Політика безперервності бізнесу і відповідальність керування

Заходи захисту.

Обов'язки повинні розподілятися всередині CSP, щоб забезпечити достатню кількість ресурсів для визначення та виконання плану безперервності бізнесу, а також забезпечити підтримку діяльності, пов'язаної з безперервністю бізнесу.

Посилення заходів:

1) стратегія забезпечення безперервності бізнесу. CSP повинен документувати, поширювати та впроваджувати політику та процедури, що встановлюють стратегію та керівні принципи для забезпечення безперервності бізнесу та управління надзвичайними ситуаціями;

2) призначення керівника та відповідальних осіб за забезпечення безперервності бізнесу. CSP повинен призначити відповідальну особу із членів вищого керівництва власником процесу безперервності бізнесу та управління надзвичайними ситуаціями, а також відповідальним за налагодження процесу в компанії, дотримуючись стратегії, а також забезпечення дотримання вказівок, та достатніх ресурсів, доступних для ефективного процесу;

3) відповідальність керівника за забезпечення безперервності бізнесу. Власник процесу безперервності бізнесу та управління непередбачуваними ситуаціями повинен забезпечити достатньо ресурсів для ефективного процесу.

4.100 BC–02 Процедури аналізу впливу на бізнес

Заходи захисту.

Разом політика та процедури безперервності бізнесу охоплюють визначення наслідків будь-якої несправності або переривання роботи хмари чи CSP.

Посилення заходів:

1) аналіз впливу на бізнес. Разом політика та процедури щодо безперервності бізнесу та управління непередбачуваними ситуаціями повинні передбачати необхідність проведення аналізу впливу на бізнес для визначення впливу будь-якої несправності на хмару або CSP;

2) склад політики та процедур аналізу впливу на бізнес. Разом політика та процедури аналізу впливу на бізнес повинні враховувати принаймні такі аспекти:

можливі сценарії, засновані на аналізі ризиків;

визначення критично важливих товарів та послуг;

визначення залежностей (у тому числі процесів і необхідних ресурсів), програми, ділових партнерів та третіх сторін;

виявлення загроз критично важливим продуктам та послугам;

виявлення наслідків запланованих і незапланованих несправностей та змін із часом;

визначення максимально допустимої тривалості несправностей;

визначення пріоритетів відновлення;

визначення часових цілей для відновлення критично «важливих» продуктів та послуг протягом максимально прийнятного періоду часу (RTO);

визначення часових цілей для максимально «розумного» періоду, протягом якого дані можуть бути втрачені та не відновлені (RPO);

оцінка ресурсів, необхідних для відновлення;

3) перегляд політики та процедур аналізу впливу на бізнес. Аналіз впливу на бізнес, що випливає з цієї політики та процедур, повинен перевірятися через регулярні проміжки часу, принаймні раз на рік, або після значних організаційних змін чи змін, пов'язаних із довкіллям.

4.101 BC–03 Безперервність бізнесу та план дій у непередбачених ситуаціях

Заходи захисту.

Повинна бути доступна система безперервності бізнесу, що містить план безперервності бізнесу та відповідні плани на випадок непередбачених ситуацій.

Посилення заходів:

1) документування планів забезпечення безперервності бізнесу. CSP повинен задокументувати та впровадити план безперервності бізнесу та плани на випадок непередбачуваних ситуацій, щоб забезпечити безперервність послуг, беручи до уваги обмеження безпеки інформації та результати аналізу впливу на бізнес;

2) відповідність планів безперервності бізнесу чинному законодавству. План безперервності бізнесу та плани на випадок непередбачених ситуацій повинні базуватися на прийнятих у галузі стандартах.

3) склад планів безперервності бізнесу. Разом план безперервності бізнесу та плани на випадок непередбачених ситуацій повинні охоплювати такі аспекти:

визначена мета та сфера застосування, у тому числі відповідні бізнес-процеси та залежності;

доступність та зрозумілість планів для осіб, які повинні діяти відповідно;

право власності принаймні однієї призначеної особи, відповідальної за перегляд, оновлення та затвердження;

визначені канали ктронних комунікаційних мереж, ролі та обов'язки, у тому числі повідомлення користувача хмарних послуг;

процедури відновлення, проміжні рішення та довідкова інформація (з урахуванням пріоритетності відновлення компонентів та послуг хмарної інфраструктури та узгодження з користувачами хмарних послуг);

методи реалізації планів;

постійне вдосконалення процесу;

інтерфейси для управління інцидентами безпеки.

4) перегляд планів безперервності бізнесу. План безперервності бізнесу повинен переглядатися через регулярні проміжки часу, принаймні раз на рік, або після значних організаційних змін чи змін, пов'язаних з навколишнім середовищем (зовнішніми факторами).

4.102 BC–04 Тестування та навчання щодо безперервності бізнесу

Заходи захисту.

Система безперервності бізнесу повинна регулярно перевірятися. Посилення заходів:

1) перегляд планів забезпечення безперервності бізнесу. Аналіз впливу на бізнес, план безперервності бізнесу та плани на випадок непередбачених ситуацій повинні перевірятися через регулярні проміжки часу (принаймні раз на рік) або після оновлення;

2) документування тестів. Тести повинні бути задокументовані, а результати розглянуті для оновлення плану безперервності бізнесу та визначення майбутніх заходів щодо безперервності роботи;

3) участь третьої сторони у тестах. У тестах повинні брати участь CSC та відповідні треті сторони, такі як зовнішні надавачі хмарних послуг;

4) обов'язковість додаткового навчання. Додатково до тестів також повинні проводитися навчання, які базуються на сценаріях, що виникли внаслідок інцидентів безпеки, які вже мали місце в минулому.

Клас заходів захисту CO – Відповідність

Слід уникати невиконання правових, нормативних, самовстановлених або договірних вимог безпеки інформації та відповідності.

4.103 CO–01 Ідентифікація вимог на відповідність, що застосовуються

Заходи захисту.

Повинно бути визначено та задокументовано правові, нормативні, самовстановлені та договірні вимоги, що стосуються безпеки інформації хмари.

Посилення заходів:

1) документування вимог безпеки інформації хмари. CSP повинен задокументувати правові, нормативні, самовстановлені та договірні

вимоги, що стосуються безпеки інформації хмари.

Рекомендації з реалізації:

Як правило, такі вимоги можуть містити:

вимоги щодо захисту персональних даних;

вимоги дотримання, засновані на договірних зобов'язаннях із користувачами хмарних послуг (наприклад, ISO/IEC 27001);

загальновизнані принципи звітності;

національне законодавство;

2) дотримання вимог безпеки інформації хмари. CSP повинен задокументувати та впровадити процедури для дотримання вимог безпеки інформації;

3) надання процедур користувачу хмарних послуг. CSP повинен надавати ці процедури на запит CSC;

4) документування та моніторинг безпеки інформації хмари. CSP повинен документувати та проводити активний моніторинг правових, нормативних та договірних вимог, що впливають на послугу.

4.104 CO–02 Політика щодо планування та проведення аудитів

Заходи захисту.

Слід визначити умови, які дозволяють проводити аудит таким чином, що полегшує збір доказів, мінімізуючи втручання у надання хмарних послуг.

Посилення заходів:

1) документування політики планування та проведення аудитів. CSP повинен документувати, поширювати та впроваджувати політику і процедури планування та проведення аудитів, які в сукупності складені відповідно до ISP–02 та враховують такі аспекти:

обмеження доступу «лише читання» до компонентів системи відповідно до узгодженого плану аудиту;

діяльність, яка може призвести до несправностей хмари або порушень контрактних вимог, виконується під час планового технічного обслуговування або поза піковими періодами;

протоколювання та моніторинг діяльності.

Пов’язані заходи: ISP–02;

2) обсяг і частота аудитів. CSP повинен визначати обсяг та частоту аудитів відповідно до правил управління змінами, політики та результатів оцінки ризику.

Рекомендації з реалізації:

Програма аудиту повинна надавати високоякісний опис аудитів, які будуть надані протягом наступних трьох років;

3) програма аудиту. CSP повинен задокументувати та впровадити програму аудиту протягом трьох років, яка надає CSC інформацію, гарантовану контрактом, та визначає їх права аудиту.

4.105 CO–03 Внутрішній аудит системи внутрішнього контролю

Заходи захисту.

Експерти повинні регулярно перевіряти відповідність системи захисту інформації відповідним правовим, самонакладеним або договірним вимогам.

Посилення заходів:

1) періодичність внутрішнього аудиту. CSP має проводити принаймні щорічно внутрішні аудити, щоб перевірити відповідність їх системи внутрішнього контролю безпеки вимогам, визначеним у CO–01.

Пов’язані заходи: CO–01;

2) актуалізація аудиту. Внутрішній аудит повинен перевіряти відповідність вимогам на цільовому рівні гарантій;

3) виявлення вразливостей. Виявлені вразливості та відхилення підлягають оцінці ризиків відповідно до процедури управління ризиками (див. RM–01), а подальші заходи визначаються та відстежуються (див. OPS–17).

Пов’язані заходи: RM–01, OPS–17;

4) автоматичний контроль за вимогами аудиту. Внутрішній аудит повинен доповнюватися процедурами автоматичного контролю за дотриманням застосовних вимог політики;

5) автоматизований моніторинг виявлення вразливостей. CSP повинен впровадити автоматизований моніторинг для виявлення вразливостей та відхилень, про що автоматично повідомляється відповідним експертам CSP для негайної оцінки та дій;

6) документування відхилень. CSP повинен задокументувати конкретні відхилення, у тому числі оцінку їх серйозності, та відстежувати їх усунення.

Рекомендації з реалізації:

Зокрема, схема вимагає, щоб CSP повідомляла свій CAB про основні невідповідності;

7) інформування користувачів хмарних послуг щодо невідповідності вимог. CSP має інформувати CSC, які працюють із сертифікованою хмарою, щодо невідповідності вимог.

Рекомендації з реалізації:

Це вимога до складу, щоб забезпечити належну передачу невідповідностей по ланцюгу електронних комунікацій.

4.106 CO–04 Інформація про оцінювання системи внутрішнього контролю

Заходи захисту.

Найвище керівництво CSP повинно постійно інформуватися про ефективність роботи системи внутрішнього контролю з метою забезпечення її адекватності та ефективності.

Посилення заходів:

1) інформування про ефективність безпеки інформації. CSP має регулярно інформувати керівництво про ефективність безпеки інформації в межах системи внутрішнього контролю;

2) перегляд системи оцінювання внутрішнього контролю. Ця інформація повинна бути внесена до огляду керівництвом системи внутрішнього контролю, який проводиться раз на рік.

Клас заходів захисту DOC – Документація користувача хмарних послуг

Документація надає актуальну інформацію про безпечну конфігурацію та відомі вразливості хмари для користувачів хмарних послуг.

4.107 DOC–01 Вказівки і рекомендації для користувачів хмарних послуг

Заходи захисту.

Необхідно надавати інформацію, яка допоможе користувачам хмарних послуг у безпечній конфігурації, інсталяції та використанні хмари.

Посилення заходів:

1) публікація рекомендацій щодо конфігурацій. CSP повинен зробити загальнодоступними настанови та рекомендації, щоб допомогти CSC у безпечній конфігурації, інсталяції, розгортанні, експлуатації та обслуговуванні хмарної послуги, що надається;

2) склад рекомендацій для користувачів хмарних послуг. Настанови та рекомендації щодо безпечного використання хмари повинні охоплювати такі аспекти, якщо це стосується хмари:

інструкції щодо безпечної конфігурації;

джерела інформації про відомі вразливості та механізми оновлення;

механізми обробки та реєстрації помилок;

механізми автентифікації;

концепція ролей та прав, включаючи комбінації, що призводять до підвищеного ризику;

послуги та функції для адміністрування хмари привілейованими користувачами хмарних послуг;

додатковий заходи контролю користувачів хмарних послуг (CCC);

3) застосування рекомендацій. CSP повинен підтримувати настанови та рекомендації, що застосовуються до хмари, у версії, призначеній для продуктивного використання;

4) взаємообмін інформацією про ризики. CSP спільно із користувачем хмарної послуги повинен описати в документації, призначеній користувачеві хмарних послуг, всі ризики.

Рекомендації з реалізації:

Ця вимога пов'язана з прийняттям ризику власниками ризику в процедурах управління ризиками (див. RM–03).

Пов’язані заходи: RM–03;

5) перегляд рекомендацій для користувачів хмарних послуг. CSP повинен регулярно аналізувати, як CSC застосовують рекомендації щодо безпеки та додаткові заходи захисту користувачів хмарних послуг, та вживати заходів для заохочення дотримання рекомендацій, спираючись на визначену модель спільної відповідальності.

4.108 DOC–02 Онлайн-реєстр відомих вразливостей

Заходи захисту.

Слід надати інформацію, яка допоможе користувачам хмарних послуг у безпечній конфігурації, інсталяції та використанні хмари.

Посилення заходів:

1) посилання на онлайн-реєстр відомих вразливостей. CSP повинен щоденно оновлюваний онлайн-реєстр відомих вразливостей, які впливають на надану хмарну послугу;

2) всеосяжність онлайн-реєстру вразливостей. Онлайн-реєстр вразливостей також повинен містити відомі вразливості, які впливають на активи, надані CSP, які користувачі хмарних послуг повинні встановлювати, надавати або експлуатувати самостійно;

3) аналіз вразливостей. Представлення вразливостей повинно відповідати загальновизнаній системі оцінки для опису вразливостей;

4) повнота онлайн-реєстру вразливостей. Інформація, що міститься в онлайн-реєстрі, повинна містити достатньо інформації для формування належної основи для оцінки ризику та можливих подальших заходів користувачів хмарних послуг.

Рекомендації з реалізації:

Слід використовувати систему загальної оцінки вразливості (CVSS);

5) актуалізація онлайн-реєстру вразливостей. Для кожної вразливості в онлайн-реєстрі вказується, чи доступні оновлення програмного забезпечення, коли вони будуть розгорнуті та чи будуть вони розгорнуті CSP, CSC або обома;

6) автоматичний контроль оновлення активів. CSP повинен забезпечити механізмами автоматичного оновлення активів, які він надає, що повинні встановлюватися, надаватися або експлуатуватися CSC в межах їх зони відповідальності.

4.109 DOC–03 Місця обробки і зберігання даних

Заходи захисту.

Необхідно надавати прозору інформацію про місцезнаходження даних та їх обробку. Посилення заходів:

1) склад інформації про місце зберігання даних. CSP надає зрозумілу та прозору інформацію про:

його юрисдикцію;

розташування системних компонентів, включаючи її субпідрядників, де дані користувачів хмарних послуг обробляються, зберігаються та створюються резервні копії;

2) доступність інформації для юридичної оцінки. CSP повинен надати достатню інформацію для предметних експертів CSC, щоб визначити, як оцінити відповідність юрисдикції та розташування хмари з юридичної та нормативної точок зору.

Рекомендації з реалізації:

Зокрема, якщо CSP використовує сертифікованих надавачів хмарних послуг, CSP вносить у свій власний опис усіх відповідних надавачів хмарних послуг;

3) склад інформації, що надається користувачу хмарних послуг. CSP повинен надати інформацію про:

місцезнаходження з питань адміністрування та нагляду, які можуть здійснюватися в хмарі;

місця, куди можна передавати, обробляти або зберігати будь-які хмарні дані користувачів хмарних послуг, метадані або похідні дані.

4) документування місця технічної підтримки користувачів хмарних послуг. CSP повинен задокументувати місця, з яких він проводить операції з підтримки користувачів хмарних послуг, а також документувати перелік операцій, які може виконувати служба підтримки користувачів хмарних послуг у кожному місці.

4.110 DOC–04 Обґрунтування цільового рівня безпеки (гарантій)

Заходи захисту.

Повинно бути надано обґрунтування цільового рівня безпеки (гарантій) хмарою.

Посилення заходів:

1) обґрунтування рівня безпеки (гарантій). CSP повинен надати обґрунтування рівня безпеки (гарантій), націленого на сертифікацію, на основі ризиків, пов'язаних із цільовими користувачами хмарних послуг та випадками використання;

2) відповідність рівню профілю безпеки. Якщо CSP заявляє про відповідність профілям безпеки для своєї хмари, обґрунтування повинно охоплювати профілі безпеки;

3) викладення обґрунтування в пакеті сертифікації. Коротке викладення обґрунтування повинно бути загальнодоступним як частина пакета сертифікації, що дозволяє CSC проводити аналіз високого рівня щодо власних випадків використання;

4) урахування результатів аналізу ризиків. Обґрунтування має ґрунтуватися на аналізі ризиків згідно з RM–01.

Пов’язані заходи: RM–01.

4.111 DOC–05 Настанови та рекомендації для структури послуги

Заходи захисту.

Потрібно надати інформацію, необхідну користувачам хмарних послуг, які хочуть використовувати хмарну послугу як базову послугу для власної сертифікованої хмари.

Посилення заходів:

1) надання користувачам хмарних послуг документації хмарного сервісу. Якщо CSP очікує, що CSC сертифікують власні послуги на основі її хмарного сервісу із використанням композиції, вона надає для них конкретну документацію на основі додаткового контролю користувачам хмарних послуг (CCC), який вони визначили.

Рекомендації з реалізації:

Очікування CSP повинні бути задекларовані в документі заявки, оскільки CAB повинен знати, що ця документація повинна бути доступною, а також повинна бути внесена в аудит;

2) додатковий контроль користувачів хмарних послуг. CSP повинен включати в опис, наданий для кожного CCC, перелік чинних вимог до CSC, і він пов'язує кожен CCC з відповідною вимогою;

3) опис для додаткового контролю користувачів хмарних послуг. CSP має видати документацію, визначену в DOC–05(1), що є доступною для користувачів хмарних послуг, за запитом.

Пов’язані заходи: в DOC–05(1);

4) мінімальний рівень надійності. CSP повинен позначити кожну вимогу, пов'язану з CCC, найнижчим рівнем гарантії, для якого вона потрібна.

4.112 DOC–06 Внесок до виконання вимог для композиції

Заходи захисту.

Повинна бути надана інформація, необхідна користувачам хмарних послуг, які хочуть використовувати CSP як організацію надання послуг хмарі.

Посилення заходів:

1) сертифікація користувачем своїх хмарних послуг. Якщо CSP очікує, що CSC сертифікують свої власні послуги на основі своєї хмари, використовуючи композицію, CSP повинен документувати для кожного заходу захисту, як його хмара буде сприяти (якщо необхідно) виконанню заходів захисту хмарною службою, розробленою CSC та яка використовує CSP як організацію з надання послуг хмарні.

2) доступність документації. CSP повинен розробити документацію, визначену в DOC–06(1) та доступну для користувачів хмарних послуг за запитом.

Пов'язані заходи: DOC–06(1);

3) супровідний документ. CSP повинен обґрунтувати внески у супровідному документі.

Клас заходів захисту INQ – Робота із запитами від державних органів щодо розслідувань

Забезпечити належну обробку запитів державних органів з розслідувань задля юридичного перегляду інформації для користувачів хмарних послуг та обмеження доступу до даних або їх розкриття.

4.113 INQ–01 Юридична оцінка запитів правоохоронних органів

Заходи захисту.

запити правоохоронних органів повинні оцінюватися перед визначенням подальших кроків, які слід вжити.

Посилення заходів:

1) правова оцінка запитів. CSP повинен надати запиту правоохоронних органів правову оцінку за допомогу експертів у зазначеній сфері;

2) визначення правової оцінки. Правова оцінка визначає, чи має правоохоронний орган відповідну та юридично обґрунтовану основу для таких запитів та яких подальших кроків необхідно вжити.

4.114 INQ–02 Інформування користувачів хмарних послуг про запити правоохоронних органів

Заходи захисту.

Користувачі хмарних послуг мають бути поінформовані про поточні розслідування, якщо це дозволено законом.

Посилення заходів:

інформування користувачів хмарних послуг про розкриття даних. CSP інформує користувача хмарних послуг, щодо якого було отримано запит, без зайвої затримки, якщо тільки відповідна правова основа, на якій базується запит правоохоронного органу, не забороняє цього або якщо немає чітких ознак незаконних дій у зв'язку з використанням хмари.

4.115 INQ–03 Умови доступу та розкриття даних при запитах правоохоронних органів

Заходи захисту.

Слідчі повинні допускатися до даних, необхідних для їх розслідування, лише після підтвердження законності їх запиту.

Посилення заходів:

1) доступ до даних користувачів хмарних послуг при проведенні розслідуванні. CSP надаватиме доступ або розкриватиме дані користувачів хмарних послуг лише на підставі запитів правоохоронних органів після того, як правова оцінка CSP (див. INQ–01) засвідчить, що існує застосовна та чинна правова основа та що запит на розслідування відповідає цій основі.

Пов’язані заходи: INQ–01;

2) гарантування відсутності всеосяжного доступу до даних правоохоронним органам. CSP повинен задокументувати та впровадити процедури, які гарантують, що правоохоронні органи мають доступ лише до даних, необхідних для розслідування;

3) анонімність даних. Коли чіткий витяг даних неможливий, CSP анонімізує або псевдонімізує дані, щоб правоохоронні органи могли призначити їх лише тим користувачам хмарних послуг, які є предметом запиту;

4) автоматичний контроль доступу. CSP повинен автоматично контролювати доступ, який здійснюється слідчими або від їх імені, щоб переконатися, що вони відповідають вимогам законодавства.

Клас заходів захисту PSS – Безпека та захист виробу

Забезпечити відповідні механізми для користувачів хмарних послуг.

Під словом "виріб" розуміється набір апаратних та програмних засобів CSP та їх конфігурація.

4.116 PSS–01 Механізми обробки помилок і входу

Заходи захисту.

Користувачі хмарних послуг повинні мати доступ до достатньої інформації про хмари за допомогою механізмів обробки помилок та механізмів входу.

Посилення заходів:

1) упровадження механізмів помилок і входу. CSP повинен запропонувати своїм користувачам хмарних послуг механізми обробки помилок та входу, які дозволяють отримувати інформацію, пов'язану з безпекою, про стан безпеки хмарни і про дані, послуги або функції, які вона надає;

2) достатність інформації щодо помилок і входу. Надана інформація повинна бути достатньо детальною, щоб користувачі хмарних послуг могли перевірити такі аспекти, наскільки вони застосовні до хмарни:

інформація про те, хто отримував доступ та коли і до яких даних, послуг чи функцій, доступних користувачеві хмарних послуг в хмарні (журнали аудиту);

несправності під час обробки автоматичних або ручних дій;

зміни параметрів конфігурації, що стосуються безпеки, механізмів обробки помилок та входу, автентифікації користувачів хмарних послуг, авторизації дій, криптографії та безпеки зв'язку;

3) захист інформації від несанкціонованого доступу. Інформація про вхід повинна бути захищена від несанкціонованого доступу та модифікації та може бути видалена користувачем хмарних послуг;

4) ведення журналу активацій або типу і обсягу реєстрації. Коли користувач хмарних послуг відповідає за активацію або тип і обсяг даних про вхід, CSP повинен забезпечити відповідні можливості ведення журналу;

5) інформування користувачів хмарних послуг через задокументовані інтерфейси. CSP надає інформацію користувачу хмарних послуг через задокументовані інтерфейси, придатні для подальшої обробки цієї інформації, як частину SIEM.

4.117 PSS–02 Управління сесіями

Заходи захисту.

Відповідне управління сесією повинно бути використано для захисту конфіденційності, доступності, цілісності та автентичності під час взаємодії з хмарою.

Посилення заходів:

1) система управління сесіями. Повинна бути використана відповідна система управління сесіями, яка відповідає найсучаснішому рівню техніки та захищена від відомих атак.

Рекомендації з реалізації:

Керівництво CSP роз'яснить поняття «найсучасніший рівень техніки»;

2) деактивація сеансів. Система управління сесіями повинна містити механізми, які роблять сеанс недійсним після того, як його було визнано неактивним;

3) визначення періоду бездіяльності. Якщо бездіяльність виявляється за допомогою вимірювання часу, інтервал часу повинен бути налаштований CSP або, якщо це технічно можливо, CSC.

Рекомендації з реалізації:

CSP повинен визначити прийнятний діапазон і значення за замовчуванням для часового інтервалу, а CSC повинен мати можливість вибору значення в межах прийнятного діапазону. У разі технічної неможливості це слід чітко продемонструвати.

4.118 PSS–03 Програмно-конфігурована мережа

Заходи захисту.

Програмно-конфігурована мережа має використовуватися лише в тому випадку, якщо хмарні дані користувача хмарних послуг захищені відповідними заходами.

Посилення заходів:

1) конфіденційність даних користувачів хмарних послуг. CSP повинен забезпечити конфіденційність даних користувачів хмарних послуг за допомогою відповідних процедур, пропонуючи функції програмно-конфігурованої мережі (SDN);

2) перевірка функціональності SDN. CSP повинен перевірити функціональність функцій програмно-конфігурованої мережі перед наданням нових функцій SDN користувачу хмарних послуг або зміною існуючих функцій SDN;

3) перевірка конфігурації мережі. CSP повинен забезпечити, щоб конфігурація мереж відповідала політиці безпеки мережі, незалежно від засобів, використаних для створення конфігурації.

4.119 PSS–04 Зображення для віртуальних машин і контейнерів

Заходи захисту.

Послуги з надання та управління віртуальними машинами та контейнерами повинні містити відповідні заходи захисту.

Посилення заходів:

1) особливості експлуатації віртуальних машин. CSP повинен забезпечити такі аспекти, якщо користувачі хмарних послуг експлуатують віртуальні машини або контейнери з хмарною:

користувач хмарних послуг може обмежити вибір зображень віртуальних машин або контейнерів відповідно до його специфікацій, так що користувачі хмарних послуг цього CSC можуть запускати лише зображення або контейнери, визначені відповідно до цих обмежень;

крім того, ці зображення, надані CSP, зміцнюються відповідно до загальновизнаних галузевих стандартів;

2) інформування користувача хмарних послуг про використання віртуальних машин. CSP повинен забезпечити такий аспект, якщо CSC експлуатують віртуальні машини або контейнери з хмарою:

якщо CSP надає CSC зображення віртуальних машин або контейнерів, CSP належним чином інформує CSC про зміни, внесені до попередньої версії;

3) автоматичний контроль перевірки цілісності. Перевірка цілісності повинна виконуватися і автоматично контролюватися для виявлення маніпуляцій із зображеннями. Результати повідомляються CSC під час запуску та виконання зображень віртуальної машини або контейнера.

4.120 PSS–05 Місця обробки і зберігання даних

Заходи захисту.

Користувачам хмарних послуг повинно бути надано можливість вибору місця розташування даних та їх обробки.

Посилення заходів:

1) визначення місця обробки і зберігання даних. CSP повинен дозволити CSC визначати місця обробки та зберігання даних (місце/країну), включаючи резервне копіювання даних, відповідно до наявних у договорі варіантів;

2) контроль за місцем обробки і зберігання даних. Усі зобов’язання CSP щодо місць обробки та зберігання даних повинні бути забезпечені архітектурою хмари.

Рекомендації з реалізації:

Згадані тут зобов'язання також передбачають зобов'язання, пов'язані з інформацією, розкритою в DOC–03.

Пов’язані заходи: DOC–03.

5. Характеристика заходів захисту в контексті надійності безпеки інформації та кіберзахисту хмарних послуг

У таблиці 6 наведено характеристику заходів захисту інформації для технології хмарних обчислень. Таблиця надає характеристику класів заходів захисту в контексті надійності безпеки інформації та кіберзахисту хмарних послуг. У таблиці використовуються такі позначення:

«X» — заходи захисту, які внесені до галузевого профілю безпеки;

«T» — заходи захисту, що можуть бути реалізовані технічними засобами в хмарі;

«O» — заходи захисту, що впроваджуються людиною за допомогою нетехнічних засобів (організаційні заходи захисту);

«O/T» — заходи захисту, що можуть бути реалізовані як технічними, так і організаційними засобами або їх комбінацією.

Таблиця 6 – Характеристика заходів захисту

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ОРГАНІЗАЦІЯ БЕЗПЕКИ ІНФОРМАЦІЇ (OIS)					
OIS–01	**Система захисту інформації**	O	X	X	X
OIS–01(1)	Охоплення системи захисту інформації	O	X	X	X
OIS–01(2)	Відповідність стандартам безпеки інформації	O		X	X
OIS–01(3)	Сертифікація системи захисту інформації	O/T			X
OIS–01(4)	Документування моніторингу системи захисту інформації	T	X	X	X
OIS–01(5)	Ведення визначеної документації системи захисту інформації	O/T		X	X
OIS–02	**Розмежування обов'язків**	O/T	X	X	X
OIS–02(1)	Оцінка ризику на організаційному рівні	O	X	X	X
OIS–02(2)	Оцінка ризику на системному рівні	O/T	X	X	X
OIS–02(3)	Застосування пом'якшувальних заходів	O/T	X	X	X
OIS–02(4)	Автоматичний контроль	T			X
OIS–03	**Взаємодія з органами державної влади і заінтересованими групами**	O/T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
OIS–03(1)	Відстеження змін	О/Т	X	X	X
OIS–03(2)	Взаємообмін інформацією	О/Т		X	X
OIS–03(3)	Постійний контакт з CAB	О/Т			X
OIS–04	**Безпека інформації в управлінні проєктами**	О/Т	X	X	X
OIS–04(1)	Внесення питань безпеки інформації всіх пов'язаних проєктів	О/Т	X	X	X
OIS–04(2)	Оцінка ризиків всіх пов'язаних проєктів	О/Т		X	X
ПОЛОЖЕННЯ ЩОДО БЕЗПЕКИ ІНФОРМАЦІЇ (ISP)					
ISP–01	**Концепція безпеки інформації**	О	X	X	X
ISP–01(1)	Документування концепції безпеки інформації	О	X	X	X
ISP–01(2)	Затвердження концепції безпеки інформації	О	X	X	X
ISP–01(3)	Перегляд концепції безпеки інформації	О		X	X
ISP–01(4)	Щорічний перегляд концепції безпеки інформації	О			X
ISP–01(5)	Поширення концепції безпеки інформації	О	X	X	X
ISP–02	**Правила і процедури безпеки**	О/Т	X	X	X
ISP–02(1)	Структуризація правил та процедур безпеки	О	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ISP–02(2)	Кваліфікація персоналу	O		X	X
ISP–02(3)	Поширення правил та процедур безпеки	O/T	X	X	X
ISP–02(4)	Затвердження правил та процедур безпеки	O	X	X	X
ISP–02(5)	Звітування про впровадження правил та процедур безпеки	O			X
ISP–02(6)	Оновлення правил та процедур безпеки	O/T	X	X	X
ISP–02(7)	Упровадження оновлень правил та процедур безпеки	O/T	X	X	X
ISP–03	**Винятки**	O	X	X	X
ISP–03(1)	Ведення переліку винятків	O	X	X	X
ISP–03(2)	Часові обмеження винятків	O	X	X	X
ISP–03(3)	Управління ризиками винятків	O/T		X	X
ISP–03(4)	Затвердження списку винятків	O			X
ISP–03(5)	Перегляд списку винятків	O	X	X	X
ISP–03(6)	Схвалення списку винятків	O		X	X
ISP–03(7)	Контроль актуальності списку винятків	T			X
УПРАВЛІННЯ РИЗИКАМИ (RM)					
RM–01	**Політика управління ризиками**	O	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
RM–01(1)	Документування ризиків	O	X	X	X
RM–01(2)	Використання аналізу ризиків	O		X	X
RM–02	**Упровадження оцінки ризику**	O	X	X	X
RM–02(1)	Сфера дії аналізу ризиків	O	X	X	X
RM–02(2)	Поширення результатів оцінки ризику	O	X	X	X
RM–02(3)	Перегляд оцінки ризику	O	X	X	X
RM–02(4)	Контроль факторів ризику	O			X
RM–03	**Упровадження усунення ризиків**	O	X	X	X
RM–03(1)	Визначення пріоритетів ризиків	O	X	X	X
RM–03(2)	Реалізація плану усунення ризиків	O	X	X	X
RM–03(3)	Залишковий ризик	O	X	X	X
RM–03(4)	Затвердження плану управління ризиків	O		X	X
RM–03(5)	Поширення плану управління ризиків	O	X	X	X
RM–03(6)	Спільні ризики	O	X	X	X
RM–03(7)	Перегляд плану управління ризиками	O	X	X	X
RM–03(8)	Адекватність аналізу ризиків	O		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ЛЮДСЬКІ РЕСУРСИ (HR)					
HR–01	**Політика людських ресурсів**	O	X	X	X
HR–01(1)	Класифікація посад за рівнем ризику	O	X	X	X
HR–01(2)	Етика персоналу	O	X	X	X
HR–01(3)	Дисциплінарні заходи щодо порушень	O	X	X	X
HR–01(4)	Запобігання та документування дисциплінарних заходів	O	X	X	X
HR–02	**Перевірка кваліфікації і надійності**	O	X	X	X
HR–02(1)	Попередня перевірка персоналу	O	X	X	X
HR–02(2)	Перегляд компетентності та доброчесності	O		X	X
HR–02(3)	Циклічність перевірки персоналу	O			X
HR–03	**Умови праці**	O	X	X	X
HR–03(1)	Забезпечення дотримання посадових обов'язків	O	X	X	X
HR–03(2)	Умова нерозголошення	O	X	X	X
HR–03(3)	Первинний інструктаж	O	X	X	X
HR–03(4)	Документування інструктажу	O		X	X
HR–03(5)	Контроль документування інструктажу	O			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
HR–04	**Обізнаність та навчання безпеки**	O	X	X	X
HR–04(1)	Визначення програми обізнаності та навчання	O	X	X	X
HR–04(2)	Групова спрямованість	O		X	X
HR–04(3)	Перегляд програми обізнаності та навчання	O	X	X	X
HR–04(4)	Періодичність оновлення програми обізнаності та навчання	O		X	X
HR–04(5)	Обов'язковість проходження програм обізнаності та навчання	O	X	X	X
HR–04(6)	Умови проходження програм обізнаності та навчання	O		X	X
HR–04(7)	Контроль завершення програм обізнаності та навчання	O			X
HR–04(8)	Оцінювання індивідуальних результатів навчання	O		X	X
HR–04(9)	Оцінювання групових результатів навчання	O			X
HR–04(10)	Перевірка програми обізнаності та навчання	O		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
HR–05	**Припинення трудових відносин або зміна умов праці**	O	X	X	X
HR–05(1)	Інформування про припинення або зміну трудових відносин або умов праці	O	X	X	X
HR–05(2)	Анулювання прав після звільнення	O	X	X	X
HR–05(3)	Контроль анулювання прав після звільнення	O		X	X
HR–05(4)	Автоматичний контроль анулювання прав після звільнення	O			X
HR–06	**Угоди про конфіденційність**	O	X	X	X
HR–06(1)	Узгодження угод	O	X	X	X
HR–06(2)	Базові передумови угоди	O		X	X
HR–06(3)	Прийняття угоди	O		X	X
HR–06(4)	Умова черговості угоди	O		X	X
HR–06(5)	Документування та перегляд угод	O		X	X
HR–06(6)	Інформування та підтвердження оновленої угоди	O		X	X
HR–06(7)	Автоматичний контроль підтвердження угоди	T			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
УПРАВЛІННЯ АКТИВАМИ (АМ)					
АМ–01	**Опис активів**	О	Х	Х	Х
АМ–01(1)	Документування інвентаризації активів	О	Х	Х	Х
АМ–01(2)	Автоматизація та інвентаризація активів	О		Х	Х
АМ–01(3)	Повнота інвентаризації активів	О	Х	Х	Х
АМ–01(4)	Управління ризиками протягом життєвого циклу активу	О		Х	Х
АМ–01(5)	Моніторинг інвентаризації активів	О/Т			Х
АМ–01(6)	Автоматичний контроль інвентаризації активів	Т			Х
АМ–02	**Прийнятне використання та безпечна обробка політики активів**	О	Х	Х	Х
АМ–02(1)	Документування політики використання активів	О	Х	Х	Х
АМ–02(2)	Повнота політики та процедур використання активів	О		Х	Х
АМ–02(3)	Використання змінних носіїв	О/Т			Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
АМ–03	**Введення в експлуатацію та виведення з експлуатації обладнання**	О	Х	Х	Х
АМ–03(1)	Документування процедур експлуатації обладнання	О	Х	Х	Х
АМ–03(2)	Управління ризиками при експлуатації обладнання	О/Т		Х	Х
АМ–03(3)	Перевірка механізмів безпеки при експлуатації обладнання	О/Т		Х	Х
АМ–03(4)	Особливості виведення обладнання з експлуатації	О/Т	Х	Х	Х
АМ–03(5)	Знищення обладнання після виведення з експлуатації	О/Т	Х	Х	Х
АМ–03(6)	Автоматичний контроль експлуатації обладнання	Т			Х
АМ–04	**Прийнятне використання, безпечна обробка та повернення активів**	О	Х	Х	Х
АМ–04(1)	Документування поводження з активами	О	Х	Х	Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
AM–04(2)	Повернення активів після припинення трудових відносин	O	X	X	X
AM–04(3)	Централізоване управління активами	O			X
AM–04(4)	Автоматичний контроль документування поводження з активами	T			X
AM–05	**Класифікація та маркування активів**	O	X	X	X
AM–05(1)	Документування схеми класифікації активів	O	X	X	X
AM–05(2)	Рівні захисту активів	O		X	X
AM–05(3)	Маркування активів	O			X
AM–05(4)	Відповідальність за маркування	O		X	X
ФІЗИЧНА БЕЗПЕКА (PHS)					
PHS–01	**Периметри фізичної безпеки**	O	X	X	X
PHS–01(1)	Визначення периметра безпеки	O	X	X	X
PHS–01(2)	Визначення зон безпеки	O	X	X	X
PHS–01(3)	Визначення приватної території	O			X
PHS–01(4)	Розмежування зон безпеки	O/T			X
PHS–01(5)	Контроль несанкціонованого проникнення	O/T			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
PHS–01(6)	Визначення вимог безпеки для зон безпеки	O	X	X	X
PHS–01(7)	Обґрунтованість заходів захисту	O		X	X
PHS–02	**Контроль фізичного доступу**	O/T	X	X	X
PHS–02(1)	Документування фізичного доступу	O/T	X	X	X
PHS–02(2)	Автентифікація	O/T	X	X	X
PHS–02(3)	Двофакторна автентифікація	O/T		X	X
PHS–02(4)	Контроль за відвідувачами	O/T		X	X
PHS–02(5)	Винятки при надзвичайних ситуаціях	O/T	X	X	X
PHS–02(6)	Часові інтервали доступу до зон безпеки	O/T			X
PHS–02(7)	Попередження про обмеження	O/T	X	X	X
PHS–02(8)	Запобігання несанкціонованому доступу	O/T	X	X	X
PHS–02(9)	Повнота реєстрації доступу	O/T		X	X
PHS–02(10)	Автоматичний контроль доступу	T			X
PHS–03	**Робота в критичних зонах**	O	X	X	X
PHS–03(1)	Документування правил та процедур роботи в критичних зонах	O	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
PHS–03(2)	Політика «чистого екрана» та документів і змінних носіїв інформації	O/T		X	X
PHS–03(3)	Документування розмежування діяльності та зон безпеки	O			X
PHS–03(4)	Документування розмежування між активами та зонами безпеки	O			X
PHS–04	**Захист обладнання**	O/T	X	X	X
PHS–04(1)	Документування процедур захисту обладнання	O	X	X	X
PHS–04(2)	Перевірка силових і кабелів електронних комунікаційних мереж	T		X	X
PHS–04(3)	Відповідність рівнів захисту під час утилізації	O/T		X	X
PHS–04(4)	Перевірка вищим керівництвом	O			X
PHS–04(5)	Угода підтримки	O			X
PHS–04(6)	Управління оновленнями безпеки	O/T			X
PHS–04(7)	Доступність хмарних сервісів при оновленні обладнання	T			X
PHS–04(8)	Конфіденційність персональних даних	T			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	користувачів хмарних послуг				
PHS–04(9)	Шифрування змінних носіїв інформації	T	X	X	X
PHS–05	**Захист проти зовнішніх та екологічних загроз**	O/T	X	X	X
PHS–05(1)	Документування ризиків зовнішніх та екологічних загроз	O	X	X	X
PHS–05(2)	Відповідність заходів захисту вимогам безпеки центру обробки даних	O		X	X
PHS–05(3)	Забезпечення безперервної роботи центру обробки даних	T			X
PHS–05(4)	Періодичні тестування засобів захисту	O/T			X
PHS–05(5)	Забезпечення дублювання умов надання хмарного сервісу	T		X	X
PHS–05(6)	Забезпечення резервування умов надання хмарного сервісу	T		X	X
ОПЕРАЦІЙНА БЕЗПЕКА (OPS)					
OPS–01	**Управління можливостями – планування**	O	X	X	X
OPS–01(1)	Планування потужностей та ресурсів	O	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
OPS–01(2)	Планування безперервного надання послуг	O	X	X	X
OPS–01(3)	Відповідність потужностей умовами договору	O			X
OPS–02	**Управління можливостями – моніторинг**	O/T	X	X	X
OPS–02(1)	Гарантії моніторингу	O	X	X	X
OPS–02(2)	Інформування користувача хмарних послуг щодо потужностей	O	X	X	X
OPS–02(3)	Автоматичний контроль	T			X
OPS–03	**Управління можливостями – контроль ресурсів**	O/T	X	X	X
OPS–03(1)	Контроль системних ресурсів	O/T	X	X	X
OPS–04	**Антивірусний захист – політика**	O/T	X	X	X
OPS–04(1)	Документування політики антивірусного захисту	O	X	X	X
OPS–04(2)	Звітування про проведення антивірусної перевірки	O		X	X
OPS–04(3)	Технічне забезпечення антивірусного захисту	T			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
OPS–04(4)	Оновлення антивірусних продуктів	О/Т			X
OPS–05	**Антивірусний захист – впровадження**	О/Т	X	X	X
OPS–05(1)	Обов'язковість розгортання засобів антивірусного захисту	О	X	X	X
OPS–05(2)	Оновлення сигнатурних та евристичних баз	О/Т		X	X
OPS–05(3)	Автоматичне сканування систем	Т			X
OPS–05(4)	Автоматичний контроль	Т			X
OPS–06	**Резервне копіювання та відновлення даних – політика**	О/Т	X	X	X
OPS–06(1)	Документування політики резервного копіювання	О	X	X	X
OPS–06(2)	Склад політики резервного копіювання	О/Т		X	X
OPS–07	**Резервне копіювання та відновлення даних – моніторинг**	О/Т	X	X	X
OPS–07(1)	Документування процедур моніторингу	О	X	X	X
OPS–07(2)	Портал самообслуговування	Т			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
OPS–07(3)	Автоматичне відстеження резервних копій	T			X
OPS–08	**Резервне копіювання та відновлення даних – регулярні тестування**	O	X	X	X
OPS–08(1)	Періодичність тестування	O	X	X	X
OPS–08(2)	Узгодження тестування	O		X	X
OPS–08(3)	Інформування про хід тестування	O		X	X
OPS–08(4)	Повідомлення користувача хмарних послуг про результати тестування	O			X
OPS–08(5)	Включення тестування до плану забезпечення безперервної роботи	O			X
OPS–09	**Резервне копіювання та відновлення даних – зберігання**	O/T	X	X	X
OPS–09(1)	Передача резервних копій у віддалене місце	O/T	X	X	X
OPS–09(2)	Використання надійного каналу електронних комунікаційних мереж при транспортуванні резервних копій	T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
OPS–09(3)	Визначення характеристик місця віддаленого копіювання	О		Х	Х
OPS–09(4)	Фізична та екологічна безпека на місці віддаленого копіювання	О/Т		Х	Х
OPS–09(5)	Автоматичний контроль за зберіганням резервних копій	Т			Х
OPS–10	**Вхід і моніторинг – політика**	О	Х	Х	Х
OPS–10(1)	Документування політики входу та моніторингу	О	Х	Х	Х
OPS–10(2)	Склад політики входу та моніторингу	О		Х	Х
OPS–11	**Вхід і моніторинг – управління похідними даними**	О	Х	Х	Х
OPS–11(1)	Документування політики управління похідними даними	О	Х	Х	Х
OPS–11(2)	Склад політики управління похідними даними	О		Х	Х
OPS–11(3)	Умови договору між користувачем хмарних послуг та надавачем хмарних послуг щодо похідних даних	О		Х	Х
OPS–11(4)	Відповідність похідних даних	О			Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	нормативно-правовим актам				
OPS–12	**Вхід і моніторинг - ідентифікація подій**	O/T	X	X	X
OPS–12(1)	Аудит журналу моніторингу	T	X	X	X
OPS–12(2)	Інформування відділів про події	O/T	X	X	X
OPS–12(3)	Автоматизований моніторинг	T		X	X
OPS–12(4)	Автоматичний контроль ідентифікацій подій	T			X
OPS–13	**Вхід і моніторинг - доступ, зберігання та видалення**	T	X	X	X
OPS–13(1)	Контроль цілісності журналу моніторингу	T	X	X	X
OPS–13(2)	Видалення даних з журналу моніторингу	T	X	X	X
OPS–13(3)	Автентифікація доступу	T	X	X	X
OPS–13(4)	Шифрування доступу	T		X	X
OPS–13(5)	Забезпечення авторизованого доступу	T		X	X
OPS–13(6)	Надання журналу моніторингу користувачу хмарних послуг	T			X
OPS–13(7)	Автоматичний контроль агрегуванням та	T			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	видаленням журналів				
OPS–14	**Вхід і моніторинг – атрибути**	O/T	X	X	X
OPS–14(1)	Ідентифікація користувачів хмарних послуг	O/T	X	X	X
OPS–14(2)	Надання доступних інтерфейсів	T		X	X
OPS–14(3)	Розслідування інцидентів	O/T			X
OPS–15	**Вхід і моніторинг – конфігурація**	O/T	X	X	X
OPS–15(1)	Права доступу	O/T	X	X	X
OPS–15(2)	Узгодження конфігурації з політикою управління інформаційними системами	O	X	X	X
OPS–15(3)	Автентифікація доступу до системних компонентів	T		X	X
OPS–16	**Вхід і моніторинг – доступність**	T	X	X	X
OPS–16(1)	Контроль компонентів системи	T	X	X	X
OPS–16(2)	Системні компоненти для реєстрації	T			X
OPS–17	**Управління вразливостями, несправностями та помилками – політика**	T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
OPS–17(1)	Моніторинг вразливостей у системних компонентах	T	X	X	X
OPS–17(2)	Склад політик та процедур управління вразливостями	T		X	X
OPS–17(3)	Система оцінювання вразливостей	T	X	X	X
OPS–17(4)	Усунення «критичних» вразливостей	T		X	X
OPS–18	**Управління вразливостями, несправностями та помилками-онлайн реєстр**	O/T	X	X	X
OPS–18(1)	Ведення онлайн-реєстру вразливостей	O/T	X	X	X
OPS–18(2)	Склад онлайн-реєстру вразливостей	O	X	X	X
OPS–18(3)	Публікування посилань на онлайн-реєстри вразливостей	O/T	X	X	X
OPS–18(4)	Актуалізація онлайн-реєстрів вразливостей	O/T	X	X	X
OPS–18(5)	Періодичність перевірки онлайн-реєстрів вразливостей	O/T		X	X
OPS–18(6)	Автоматичне оновлення активів	T			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
OPS–19	**Управління вразливостями, несправностями та помилками - ідентифікація вразливості**	О/Т	X	X	X
OPS–19(1)	Тестування виявлення вразливостей системних компонентів	Т	X	X	X
OPS–19(2)	Періодичність тестування	О		X	X
OPS–19(3)	Тестування на проникнення	Т		X	X
OPS–19(4)	Оцінка результатів тестування на проникнення	Т		X	X
OPS–19(5)	Перегляд програми тестування	О		X	X
OPS–19(6)	Залучення зовнішніх надавачів хмарних послуг для тестування	О			X
OPS–19(7)	Аналіз першопричини вразливостей	Т			X
OPS–19(8)	Співвіднесення виявлених вразливостей із попередніми інцидентами	О/Т			X
OPS–20	**Управління вразливостями, несправностями та помилками - вимірювання,**	О	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	аналіз і оцінка процедур				
OPS–20(1)	Аналіз інструментів обробки вразливостей та інцидентів	O	X	X	X
OPS–20(2)	Перегляд результатів оцінки	O		X	X
OPS–21	**Управління вразливостями, несправностями та помилками - затвердження системи**	O/T	X	X	X
OPS–21(1)	Затвердження всіх системних компонентів	O	X	X	X
OPS–21(2)	Документування затвердження всіх системних компонентів	O	X	X	X
OPS–21(3)	Автоматичний контроль системних компонентів	T			X
OPS–22	**Розподіл бази даних у хмарній інфраструктурі**	T	X	X	X
OPS–22(1)	Відокремлення баз даних у хмарній інфраструктурі	T	X	X	X
УПРАВЛІННЯ ІДЕНТИЧНІСТЮ, АВТЕНТИФІКАЦІЄЮ І КОНТРОЛЕМ ДОСТУПУ (IAM)					
IAM–01	**Політика контролю доступу до інформації**	O	X	X	X
IAM–01(1)	Документування політики контролю доступу	O	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
IAM–01(2)	Кореляція політики контролю доступу з політикою фізичного доступу	O	X	X	X
IAM–01(3)	Використання рольового підходу	O		X	X
IAM–02	**Управління обліковими записами користувачів** хмарних послуг	O/T	X	X	X
IAM–02(1)	Документування політики управління обліковими записами	O/T	X	X	X
IAM–02(2)	Доступність політики управління обліковими записами CSP	O/T		X	X
IAM–02(3)	Доступність політики управління обліковими записами користувача хмарних послуг	O/T		X	X
IAM–02(4)	Документування політики управління обліковими записами працівників	O/T	X	X	X
IAM–02(5)	Документування політики управління груповими обліковими записами	O/T	X	X	X
IAM–02(6)	Документування політики управління технічними	O/T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	обліковими записами				
IAM–02(7)	Самообслуговування облікових записів користувача хмарних послуг	О/Т		Х	Х
IAM–02(8)	Надавання облікових записів нових користувачів хмарних послуг	О/Т			Х
IAM–03	**Блокування, розблокування та ануляція облікових записів користувача хмарних послуг**	О/Т	Х	Х	Х
IAM–03(1)	Автоматизований механізм блокування облікових записів	Т	Х	Х	Х
IAM–03(2)	Автоматизований механізм блокування облікових записів при бездіяльності	О		Х	Х
IAM–03(3)	Автоматизований механізм блокування облікових записів при невдалій автентифікації	Т	Х	Х	Х
IAM–03(4)	Обмеження спроб автентифікації	Т		Х	Х
IAM–03(5)	Моніторинг викрадених та скомпрометованих облікових записів	О/Т		Х	Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
IAM–03(6)	Моніторинг облікових записів з привілейованими правами доступу	О/Т		X	X
IAM–03(7)	Моніторинг облікових записів	О/Т			X
IAM–03(8)	Підтвердження розблокування облікових записів	О		X	X
IAM–03(9)	Автоматизований механізм скасування облікових записів	Т		X	X
IAM–03(10)	Перегляд механізму скасування облікових записів	Т		X	X
IAM–03(11)	Автоматичний контроль механізму скасування облікових записів	Т			X
IAM–03(12)	Автоматизований контроль автентифікації	Т			X
IAM–04	**Управління правами доступу**	О/Т	X	X	X
IAM–04(1)	Анулювання облікового запису користувача хмарних послуг	Т	X	X	X
IAM–04(2)	Документування процедури управління доступом	О	X	X	X
IAM–04(3)	Терміновість оновлення або відкликання прав доступу	О		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
IAM–04(4)	Документування процедури надання прав доступу	O			X
IAM–04(5)	Документування несумісності прав доступу	O			X
IAM–04(6)	Динамічний підхід при управлінні правами доступу	T			X
IAM–04(7)	Самообслуговування користувачів хмарних послуг при управлінні правами доступу	T		X	X
IAM–05	**Регулярний перегляд прав доступу**	O/T	X	X	X
IAM–05(1)	Періодичність перегляду прав доступу для низького рівня безпеки	O	X	X	X
IAM–05(2)	Перегляд прав доступу уповноваженими особами	O		X	X
IAM–05(3)	Терміновість обробки відхилень	O		X	X
IAM–05(4)	Інструмент перегляду прав доступу	T		X	X
IAM–05(5)	Періодичність перегляду прав доступу для високого рівня безпеки	O			X
IAM–06	**Привілейовані права доступу**	O/T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
IAM–06(1)	Персоналізація привілейованих прав доступу	T		X	X
IAM–06(2)	Реєстрація діяльності користувачів хмарних послуг з привілейованими правами доступу	T		X	X
IAM–06(3)	Документування процедури недопущення зловживання правами доступу	O		X	X
IAM–06(4)	Призначення групових облікових записів	T	X	X	X
IAM–06(5)	Періодичність перегляду технічних облікових записів	O			X
IAM–06(6)	Інвентаризація привілейованих облікових записів	T			X
IAM–06(7)	Автентифікації для доступу до адміністративних інтерфейсів	T		X	X
IAM–06(8)	Автентифікації для доступу до адміністративних інтерфейсів користувача хмарних послуг	T			X
IAM–07	**Механізми автентифікації**	T	X	X	X
IAM–07(1)	Документування механізмів автентифікації	T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
IAM–07(2)	Автентифікація всіх середовищ	T		X	X
IAM–07(3)	Автентифікація доступу до виробничого середовища	T			X
IAM–07(4)	Автентифікація доступу до даних користувача хмарних послуг	T			X
IAM–07(5)	Автентифікація користувача хмарних послуг	T		X	X
IAM–07(6)	Автентифікація групових облікових записів	T		X	X
IAM–07(7)	Блокування облікового запису при невдалих спробах автентифікації	T	X	X	X
IAM–07(8)	Надання методів автентифікації користувачам хмарних послуг	T		X	X
IAM–08	**Захист і повнота облікованих даних**	O/T	X	X	X
IAM–08(1)	Документування рекомендацій щодо управління обліковими даними	O/T	X	X	X
IAM–08(2)	Особливі вимоги до управління обліковими даними	T		X	X
IAM–08(3)	Декларація про конфіденційність	T			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
IAM–08(4)	Використання криптографічно стійких геш-функцій	T	X	X	X
IAM–08(5)	Механізми криптографічної автентифікації	T	X	X	X
IAM–08(6)	Автоматичність створення облікових даних	T		X	X
IAM–08(7)	Інформування при змінах облікових даних особистих облікових записів	O/T		X	X
IAM–08(8)	Обмеження на автоматичні паролі	T		X	X
IAM–08(9)	Інформаційна підтримка користувача хмарних послуг щодо управління облікованими даними	O/T		X	X
IAM–09	**Загальні обмеження доступу**	O/T	X	X	X
IAM–09(1)	Розмежування інформаційних систем	T	X	X	X
IAM–09(2)	Правила проєктування інформаційних систем та активів	T		X	X
IAM–09(3)	Відокремлення адміністративних інтерфейсів	T			X
IAM–09(4)	Заходи розподілу користувачів хмарних послуг	T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ІАМ–09(5)	Інформування про відкритий канал електронних комунікаційних мереж	О		Х	Х
ІАМ–09(6)	Погодження використання відкритого каналу електронних комунікаційних мереж	О/Т			Х
ІАМ–09(7)	Розмежування інтерфейсів для адміністраторів та користувачів хмарних послуг	Т		Х	Х
КРИПТОГРАФІЯ ТА УПРАВЛІННЯ КЛЮЧАМИ (СКМ)					
СКМ–01	**Політика для використання механізмів шифрування та управління ключами**	О/Т	Х	Х	Х
СКМ–01(1)	Документування політики для шифрування та управління ключами	О	Х	Х	Х
СКМ–01(2)	Криптографічна політика	Т		Х	Х
СКМ–01(3)	Відповідність процедур шифрування сучасному стану	Т		Х	Х
СКМ–02	**Шифрування даних при передачі**	Т	Х	Х	Х
СКМ–02(1)	Надійні механізми шифрування при передачі хмарних	Т	Х	Х	Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	даних користувачів хмарних послуг				
СКМ–02(2)	Надійні механізми шифрування при передачі всіх даних	Т			Х
СКМ–03	**Шифрування даних при зберіганні**	О/Т	Х	Х	Х
СКМ–03(1)	Документування заходів шифрування під час зберігання	О/Т	Х	Х	Х
СКМ–03(2)	Персоналізація особистих та секретних ключів користувачів хмарних послуг	О/Т		Х	Х
СКМ–03(3)	Використання особистих та секретних ключів користувачів хмарних послуг	О/Т		Х	Х
СКМ–03(4)	Персоналізація особистих та секретних ключів користувачів хмарних послуг без винятків	О/Т			Х
СКМ–04	**Безпечне управління ключами**	Т	Х	Х	Х
СКМ–04(1)	Управління ключами	Т	Х	Х	Х
СКМ–04(2)	Зберігання ключів у відокремленому стані	Т		Х	Х
СКМ–04(3)	Зберігання ключів у безпечному місці	Т			Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
CKM–04(4)	Використання спільних ключів	T		X	X
БЕЗПЕКА ЕЛЕКТРОННИХ КОМУНІКАЦІЙ (CS)					
CS–01	**Технічні заходи**	T	X	X	X
CS–01(1)	Документування систем виявлення та реагування на атаки	T	X	X	X
CS–01(2)	Аналіз ризиків у системах виявлення та реагування на атаки	T		X	X
CS–01(3)	Інформування системи SIEM	T		X	X
CS–01(4)	Гарантування відсутності несанкціонованого підключення пристроїв	T			X
CS–01(5)	Унеможливлення одночасного прориву вразливістю декількох ліній захисту	T			X
CS–02	**Вимоги безпеки до підключення в мережі CSP**	O	X	X	X
CS–02(1)	Документування заходів захисту всередині мережі CSP	O	X	X	X
CS–03	**Моніторинг підключень у мережі CSP**	T	X	X	X
CS–03(1)	Позрізняння довірених і ненадійних мереж	T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
CS–03(2)	Розподіл областей з використанням демілітаризованих зон	T	X	X	X
CS–03(3)	Налаштування фізичного та віртуального середовища	T	X	X	X
CS–03(4)	Сканування служб, протоколів та портів	T	X	X	X
CS–03(5)	Перегляд конфігурації моніторингу	T		X	X
CS–03(6)	Оцінка ризиків	T		X	X
CS–03(7)	Захист журналів SIEM від фальсифікації	T		X	X
CS–04	**Міжмережевий доступ**	T	X	X	X
CS–04(1)	Контроль периметра шлюзами безпеки	T	X	X	X
CS–04(2)	Застосування матриці дозволених потоків	T		X	X
CS–04(3)	Доступ до системи для міжмережевого доступу	T		X	X
CS–04(4)	Контроль периметра високодоступними шлюзами безпеки	T			X
CS–04(5)	Автоматичний контроль периметра	T			X
CS–05	**Мережі для адміністрування**	T	X	X	X
CS–05(1)	Відокремлення мережі	T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	адміністративного управління				
CS–05(2)	Відокремлення мереж адміністрування від мереж користувачів хмарних послуг	T	X	X	X
CS–05(3)	Розподіл мереж віртуальних машин	T	X	X	X
CS–05(4)	Шифрування каналів для невідокремлених мереж	T			X
CS–05(5)	Налаштування брандмауера	T			X
CS–06	**Розмежування трафіка у спільних мережевих середовищах**	T	X	X	X
CS–06(1)	Розмежування механізмів трафіка	T	X	X	X
CS–06(2)	Безпечне відокремлення можливостей інфраструктури	T			X
CS–07	**Мережева топологія документації**	O/T	X	X	X
CS–07(1)	Документування логічної структури мережі	O/T	X	X	X
CS–07(2)	Документування розподілу зон та географічного положення місць мережі	O/T	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
CS–07(3)	Документування обладнання та серверів	О/Т		X	X
CS–07(4)	Перегляд документації топології мережі	О		X	X
CS–08	**Програмно визначена мережа**	Т	X	X	X
CS–08(1)	Забезпечення конфіденційності даних хмарних користувачів хмарних послуг	Т	X	X	X
CS–08(2)	Функціональність функцій програмно визначеної мережі	Т	X	X	X
CS–08(3)	Відповідність конфігурації мереж політиці безпеки	Т		X	X
CS–09	**Політика передачі даних**	О/Т	X	X	X
CS–09(1)	Документування заходів захисту передачі даних	О/Т	X	X	X
CS–09(2)	Посилання на класифікацію активів	Т		X	X
ПОРТАТИВНІСТЬ ТА ВЗАЄМОДІЙНІСТЬ (PI)					
PI–01	**Документація і безпека вхідних і вихідних інтерфейсів**	О/Т	X	X	X
PI–01(1)	Доступність хмарних сервісів, задокументовані інтерфейси	О	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
PI–01(2)	Чіткість документування інтерфейсів	О	X	X	X
PI–01(3)	Використання стандартизованих протоколів зв'язку	Т	X	X	X
PI–01(4)	Шифрування зв'язку через ненадійні мережі	Т	X	X	X
PI–01(5)	Забезпечення перевірки інтерфейсів користувачам хмарних послуг перед початком роботи	О/Т			X
PI–02	**Договори про надання даних**	О	X	X	X
PI–02(1)	З'ясування умов припинення договірних відносин	О	X	X	X
PI–02(2)	Експертна оцінка придатності хмарни	О		X	X
PI–02(3)	Перегляд умов договору	О			X
PI–03	**Безпечне видалення даних**	О/Т	X	X	X
PI–03(1)	Упровадження процедур видалення даних після закінчення договору	Т	X	X	X
PI–03(2)	Видалення метаданих і даних у резервних копіях	Т	X	X	X
PI–03(3)	Запобігання відновленню	О		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	криміналістичними засобами				
PI–03(4)	Документування видалення даних користувача користувачами хмарних послуг	O		X	X
PI–03(5)	Видалення технічних даних щодо користувача хмарних послуг	T		X	X
УПРАВЛІННЯ ЗМІНАМИ І КОНФІГУРАЦІЄЮ (CCM)					
CCM–01	**Політика зміни в інформаційних системах**	O	X	X	X
CCM–01(1)	Документування змін	O	X	X	X
CCM–01(2)	Особливі аспекти управління змінами	O		X	X
CCM–02	**Оцінка ризиків, категоризація та пріоритетів змін**	O	X	X	X
CCM–02(1)	Класифікація пріоритетів змін	O	X	X	X
CCM–02(2)	Ґрунтування класифікації пріоритетів змін	O		X	X
CCM–02(3)	Вживання заходів пом’якшення наслідків при високому ризику	O			X
CCM–02(4)	Проведення власної оцінки ризиків користувачами хмарних послуг	O			X
CCM–02(5)	Інформування користувачів	O			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	хмарних послуг про зміни з високою оцінкою ризику				
CCM–03	**Тестування змін**	O/T	X	X	X
CCM–03(1)	Перевірка змін перед розгортанням	T	X	X	X
CCM–03(2)	Відповідність тестувань оцінці ризиків	T		X	X
CCM–03(3)	Кваліфікація працівників проведення випробувань	O		X	X
CCM–03(4)	Залучення користувачів хмарних послуг до тестувань	O		X	X
CCM–03(5)	Попередня анонімність користувача хмарних послуг	O		X	X
CCM–03(6)	Визначення ступеня помилок та вразливостей при тестуванні	T		X	X
CCM–03(7)	Тестування змін служби	T			X
CCM–03(8)	Документування процедур попередніх тестувань	O/T			X
CCM–03(9)	Виконання регресійного тестування	T			X
CCM–03(10)	Автоматичний контроль тестування	T			X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
CCM–04	**Схвалення для забезпечення у виробничому середовищі**	O/T	X	X	X
CCM–04(1)	Затвердження змін	O	X	X	X
CCM–04(2)	Залучення користувача хмарних послуг до затвердження змін	O		X	X
CCM–04(3)	Автоматичний контроль затвердження змін	T			X
CCM–05	**Виконання та реєстрація змін**	O/T	X	X	X
CCM–05(1)	Визначення ролей персоналу або компонентів системи для внесення змін	O	X	X	X
CCM–05(2)	Реєстрація всіх змін	O/T	X	X	X
CCM–05(3)	Автоматичний контроль	O			X
CCM–06	**Контроль версій**	O	X	X	X
CCM–06(1)	Упровадження контролю версій	O	X	X	X
CCM–06(2)	Запобіжні заходи контролю версій	O			X
CCM–06(3)	Ведення історії версій	O			X
РОЗРОБКА ІНФОРМАЦІЙНИХ СИСТЕМ (DEV)					
DEV–01	**Політика для розробки та закупівлі**	O	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	інформаційних систем				
DEV–01(1)	Документування безпечного розвитку хмари	О	X	X	X
DEV–01(2)	Безпека інформації з перших етапів проєктування	О	X	X	X
DEV–01(3)	Базування політики розвитку	О		X	X
DEV–01(4)	Застосування автоматизованих засобів при розробці	О		X	X
DEV–02	**Розробка безпечного ланцюга постачання**	О/Т	X	X	X
DEV–02(1)	Ведення переліку залежностей від апаратних та програмних продуктів	О/Т	X	X	X
DEV–02(2)	Документування сторонніх програм та програм з відкритим кодом	О		X	X
DEV–02(3)	Надання користувачам хмарних послуг списку залежностей	О		X	X
DEV–02(4)	Оцінка ризику під час закупівель	О			X
DEV–03	**Безпечне середовище розробки**	О/Т	X	X	X
DEV–03(1)	Захист вихідного коду	О/Т	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
DEV–03(2)	Контроль версій	О	X	X	X
DEV–03(3)	Упровадження безпечного середовища розробки та тестування	Т		X	X
DEV–03(4)	Врахування середовища розробки та тестування при оцінці ризиків	Т		X	X
DEV–03(5)	Включення амортизаційних ресурсів	Т		X	X
DEV–04	**Розподіл середовищ**	Т	X	X	X
DEV–04(1)	Розподіл виробничих середовищ	Т	X	X	X
DEV–04(2)	Не використання даних виробничих середовищ	Т	X	X	X
DEV–04(3)	Еквівалентність вимог безпеки в загальнодоступних мережах	Т			X
DEV–05	**Розробка особливостей безпеки**	О/Т	X	X	X
DEV–05(1)	Документування підвищених вимог для тестування	О	X	X	X
DEV–05(2)	Проєктна документація для функцій захисту	О/Т		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
DEV–05(3)	Всеохоплюваність тестами вхідних даних та результатів	T		X	X
DEV–05(4)	Документування випробувань	O		X	X
DEV–05(5)	Документування результатів випробувань	O			X
DEV–06	**Ідентифікація вразливостей хмари**	T	X	X	X
DEV–06(1)	Перевірка на наявність вразливостей	T	X	X	X
DEV–06(2)	Інтеграція виявлення вразливостей	T	X	X	X
DEV–06(3)	Залежність процедур тестування оцінці ризиків	T		X	X
DEV–06(4)	Перевірка коду	T			X
DEV–06(5)	Оцінка ступеня серйозності виявлених вразливостей	T		X	X
DEV–06(6)	Перегляд коду і тестів на проникнення безпеки	T			X
DEV–07	**Аутсорсинг розробки**	O/T	X	X	X
DEV–07(1)	Взаємодія з підрядником розробки хмари	O	X	X	X
DEV–07(2)	Попередня оцінка ризиків перед	O		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	наданням субпідряду				
DEV–07(3)	Документування нагляду та контролю за сторонніми розробниками	О			X
DEV–07(4)	Тестування розробленого підрядником проєкту	Т			X
УПРАВЛІННЯ ЗАКУПІВЛЯМИ (PM)					
PM–01	**Політика і процедури контролю та моніторинг третіх сторін**	О	X	X	X
PM–01(1)	Документування моніторингу третіх сторін	О	X	X	X
PM–01(2)	Взаємодія надавача з третіми сторонами	О		X	X
PM–01(3)	Звітування незалежних аудиторів	О			X
PM–01(4)	Додатковий контроль третіх сторін	О			X
PM–01(5)	Право додаткової перевірки надавачем третіх сторін	О			X
PM–02	**Оцінка ризиків надавачів**	О	X	X	X
PM–02(1)	Попередня оцінка ризиків надавачів	О	X	X	X
PM–02(2)	Оцінка ризиків, категоризація та пріоритетів змін	О		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
РМ–02(3)	Формування додаткових елементів управління службами хмарних сервісів	О	X	X	X
РМ–02(4)	Надання послуг з охорони публічних послуг	О	X	X	X
РМ–02(5)	Адекватність оцінки ризику	О	X	X	X
РМ–03	**Перелік надавачів хмарних послуг**	О/Т	X	X	X
РМ–03(1)	Ведення каталогу надавачів хмарних послуг	О	X	X	X
РМ–03(2)	Вміст каталогу надавачів хмарних послуг	О/Т		X	X
РМ–03(3)	Перегляд каталогу надавачів хмарних послуг	О	X	X	X
РМ–04	**Моніторинг відповідності вимогам**	О/Т	X	X	X
РМ–04(1)	Контроль та моніторинг третіх сторін	О	X	X	X
РМ–04(2)	Огляд доказів	О/Т		X	X
РМ–04(3)	Частота моніторингу третіх сторін	О	X	X	X
РМ–04(4)	Виявлення порушення та відхилення	Т	X	X	X
РМ–04(5)	Інформування користувача	О	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	хмарних послуг про зміну третьої сторони				
РМ–04(6)	Перегляд вимог щодо нерозголошення інформації	О		Х	Х
РМ–04(7)	Автоматичний моніторинг	Т			Х
РМ–04(8)	Автоматичний контроль виявлених порушень та розбіжностей	Т			Х
РМ–05	**Стратегія виходу**	О	Х	Х	Х
РМ–05(1)	Визначення стратегії виходу із закупівлі послуг	О	Х	Х	Х
РМ–05(2)	Узгодження стратегії виходу планами роботи	О		Х	Х
УПРАВЛІННЯ ІНЦИДЕНТАМИ (ІМ)					
ІМ–01	**Політика управління інцидентами безпеки**	О	Х	Х	Х
ІМ–01(1)	Документування реагування на інциденти безпеки	О	Х	Х	Х
ІМ–01(2)	Встановлення пріоритетів та ескалації інцидентів безпеки	О	Х	Х	Х
ІМ–01(3)	Створення комп'ютерної групи реагування на надзвичайні ситуації	О	Х	Х	Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ІМ–01(4)	Інформування постраждалих від інцидентів безпеки користувачів хмарних послуг	О		Х	Х
ІМ–01(5)	Внесення процедур збору даних при інциденті безпеки	О		Х	Х
ІМ–01(6)	Внесення планів аналізу типових випадків безпеки	О			Х
ІМ–01(7)	Методологія оцінки	О			Х
ІМ–01(8)	Включення регулярного тестування можливостей реагування на інциденти	О			Х
ІМ–02	**Обробка інцидентів безпеки**	О/Т	Х	Х	Х
ІМ–02(1)	Аналіз першопричин для подій загрози безпеки	О	Х	Х	Х
ІМ–02(2)	Ведення каталогу інцидентів безпеки	О		Х	Х
ІМ–02(3)	Кореляція подій	О/Т		Х	Х
ІМ–02(4)	Перегляд моделювання, аналізу та захисту від інцидентів та атак	Т			Х
ІМ–02(5)	Контроль обробки інцидентів	О			Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ІМ–03	**Документація та звітність про інциденти безпеки**	О	Х	Х	Х
ІМ–03(1)	Документування заходів за результатами обробки інцидентів безпеки	О	Х	Х	Х
ІМ–03(2)	Надання інформації про інциденти	О	Х	Х	Х
ІМ–03(3)	Повідомлення про інциденти безпеки	О		Х	Х
ІМ–03(4)	Затвердження рішень щодо обробки інцидентів	О			Х
ІМ–04	**Обов'язок користувача хмарних послуг звітувати щодо інцидентів безпеки**	О	Х	Х	Х
ІМ–04(1)	Інформування працівників про зобов'язання	О	Х	Х	Х
ІМ–04(2)	Звільнення від відповідальності користувачів хмарних послуг за «неправдиві повідомлення» про події	О	Х	Х	Х
ІМ–04(3)	Визначення контактної особи для повідомлення про події безпеки	О	Х	Х	Х
ІМ–05	**Участь користувачів хмарних послуг у подіях інцидентів**	О	Х	Х	Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ІМ–05(1)	Інформування користувачів хмарних послуг про стан інцидентів	О	Х	Х	Х
ІМ–05(2)	Інформування користувачів хмарних послуг про вжиті дії щодо інциденту	О	Х	Х	Х
ІМ–06	**Процес оцінки та навчання**	О/Т	Х	Х	Х
ІМ–06(1)	Аналіз інцидентів безпеки	Т	Х	Х	Х
ІМ–06(2)	Залучення кваліфікованих підрядників	О	Х	Х	Х
ІМ–06(3)	Сховище інформації про інциденти безпеки	О		Х	Х
ІМ–06(4)	Моніторинг сховища інформації про інциденти безпеки	О		Х	Х
ІМ–07	**Збереження доказів інцидентів**	О/Т	Х	Х	Х
ІМ–07(1)	Документування процедури архівування доказів про інциденти	О	Х	Х	Х
ІМ–07(2)	Особливі вимоги щодо доказів про інциденти	О		Х	Х
ІМ–07(3)	Додаткова експертиза інцидентів	О		Х	Х
ІМ–07(4)	Захист інформації про інциденти	О/Т	Х	Х	Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ІМ–07(5)	Група реагування на інциденти	О			Х
БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ (ВС)					
ВС–01	**Політика безперервності бізнесу і відповідальність керування**	О	Х	Х	Х
ВС–01(1)	Стратегі забезпечення безперервності бізнесу	О	Х	Х	Х
ВС–01(2)	Призначення керівника та відповідальних осіб за забезпечення безперервності бізнесу	О		Х	Х
ВС–01(3)	Відповідальність керівника за забезпечення безперервності бізнесу	О		Х	Х
ВС–02	**Процедури аналізу впливу на бізнес**	О	Х	Х	Х
ВС–02(1)	Аналіз впливу на бізнес	О	Х	Х	Х
ВС–02(2)	Склад політики та процедур аналізу впливу на бізнес	О		Х	Х
ВС–02(3)	Перегляд політики та процедур аналізу впливу на бізнес	О		Х	Х
ВС–03	**Безперервність бізнесу та план дій у непередбачених ситуаціях**	О	Х	Х	Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
ВС–03(1)	Документування планів забезпечення безперервності бізнесу	О	Х	Х	Х
ВС–03(2)	Відповідність планів безперервності бізнесу чинному законодавству	О		Х	Х
ВС–03(3)	Склад планів безперервності бізнесу	О		Х	Х
ВС–03(4)	Перегляд планів безперервності бізнесу	О		Х	Х
ВС–04	**Тестування та навчання щодо безперервності бізнесу**	О		Х	Х
ВС–04(1)	Перегляд планів забезпечення безперервності бізнесу	О		Х	Х
ВС–04(2)	Документування тестів	О		Х	Х
ВС–04(3)	Участь третьої сторони у тестах	О		Х	Х
ВС–04(4)	Обов'язковість додаткового навчання	О			Х
ВІДПОВІДНІСТЬ (СО)					
СО–01	**Ідентифікація вимог на відповідність, що застосовуються**	О	Х	Х	Х
СО–01(1)	Документування вимог безпеки інформації хмари	О	Х	Х	Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
СО–01(2)	Дотримання вимог безпеки інформації хмари	О		Х	Х
СО–01(3)	Надання процедур користувачу хмарних послуг	О			Х
СО–01(4)	Документування та моніторинг безпеки інформації хмари	О			Х
СО–02	**Політика щодо планування та проведення аудитів**	О	Х	Х	Х
СО–02(1)	Документування політики планування та проведення аудитів	О	Х	Х	Х
СО–02(2)	Обсяг та частоту аудитів	О		Х	Х
СО–02(3)	Програма аудиту	О			Х
СО–03	**Внутрішній аудит системи внутрішнього контролю**	О	Х	Х	Х
СО–03(1)	Періодичність внутрішнього аудиту	О	Х	Х	Х
СО–03(2)	Актуалізація аудиту	О	Х	Х	Х
СО–03(3)	Виявлення вразливостей	О		Х	Х
СО–03(4)	Автоматичний контроль за вимогами аудиту	О			Х
СО–03(5)	Автоматизований моніторинг	О			Х

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
	виявлення вразливостей				
CO–03(6)	Документування відхилень	O	X	X	X
CO–03(7)	Інформування користувачів хмарних послуг щодо невідповідності вимог	O		X	X
CO–04	**Інформація про оцінювання системи внутрішнього контролю**	O	X	X	X
CO–04(1)	Інформування про ефективність безпеки інформації	O	X	X	X
CO–04(2)	Перегляд системи оцінювання внутрішнього контролю	O		X	X
ДОКУМЕНТАЦІЯ КОРИСТУВАЧА ХМАРНИХ ПОСЛУГ (DOC)					
DOC–01	**Вказівки і рекомендації для користувачів хмарних послуг**	O/T	X	X	X
DOC–01(1)	Публікація рекомендацій щодо конфігурацій	O	X	X	X
DOC–01(2)	Склад рекомендацій для користувачів хмарних послуг	O		X	
DOC–01(3)	Застосування рекомендацій	O	X	X	X
DOC–01(4)	Взаємообмін інформацією про ризики	O/T		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
DOC–01(5)	Перегляд рекомендацій для користувачів хмарних послуг	О			X
DOC–02	**Онлайн-реєстр відомих вразливостей**	О/Т	X	X	X
DOC–02(1)	Посилання на онлайн-реєстр відомих вразливостей	О/Т	X	X	X
DOC–02(2)	Всеосяжність онлайн-реєстру вразливостей	О		X	X
DOC–02(3)	Аналіз вразливостей	О		X	X
DOC–02(4)	Повнота онлайн-реєстру вразливостей	О/Т		X	X
DOC–02(5)	Актуалізація онлайн-реєстру вразливостей	О/Т		X	X
DOC–02(6)	Автоматичний контроль оновлення активів	Т			X
DOC–03	**Місця обробки і зберігання даних**	О	X	X	X
DOC–03(1)	Склад інформації про місце зберігання даних	О	X	X	X
DOC–03(2)	Доступність інформації для юридичної оцінки	О	X	X	X
DOC–03(3)	Склад інформації, що надається користувачу хмарних послуг	О		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
DOC–03(4)	Документування місця технічної підтримки користувачів хмарних послуг	O			X
DOC–04	**Обґрунтування цільового рівня безпеки (гарантій)**	O	X	X	X
DOC–04(1)	Обґрунтування рівня безпеки (гарантій)	O	X	X	X
DOC–04(2)	Відповідність рівню профілю безпеки	O	X	X	X
DOC–04(3)	Викладення обґрунтування в пакеті сертифікації	O	X	X	X
DOC–04(4)	Врахування результатів аналізу ризиків	O		X	X
DOC–05	**Настанови та рекомендації для структури послуги**	O	X	X	X
DOC–05(1)	Надання користувачу хмарних послуг документації хмарного сервісу	O	X	X	X
DOC–05(2)	Додатковий контроль користувачів хмарних послуг	O	X	X	X
DOC–05(3)	Опис для додаткового контролю користувачів хмарних послуг	O	X	X	X
DOC–05(4)	Мінімальний рівень надійності	O		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
DOC–06	**Внесок до виконання вимог для композиції**	O	X	X	X
DOC–06(1)	Сертифікація користувачем своїх хмарних послуг	O	X	X	X
DOC–06(2)	Доступність документації	O	X	X	X
DOC–06(3)	Супровідний документ	O		X	X
РОБОТА ІЗ ЗАПИТАМИ ВІД ДЕРЖАВНИХ ОРГАНІВ ЩОДО РОЗСЛІДУВАНЬ (INQ)					
INQ–01	**Правова оцінка запитів правоохоронних органів**	O	X	X	X
INQ–01(1)	Правова оцінка запитів	O	X	X	X
INQ–01(2)	Визначення правової оцінки	O	X	X	X
INQ–02	**Інформування користувачів хмарних послуг про запити правоохоронних органів**	O	X	X	X
INQ–02(1)	Інформування користувачів хмарних послуг про розкриття даних	O	X	X	X
INQ–03	**Умови доступу та розкриття даних при запитах правоохоронних органів**	O/T	X	X	X
INQ–03(1)	Доступ для даних користувача хмарних послуг	O	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
INQ–03(2)	Гарантування відсутності всеосяжного доступу до даних правоохоронним органам	О	X	X	X
INQ–03(3)	Анонімність даних	О/Т		X	X
INQ–03(4)	Автоматичний контроль доступу	Т			X
БЕЗПЕКА ТА ЗАХИСТ ВИРОБУ (PSS)					
PSS–01	**Механізми обробки помилок і входу**	О/Т	X	X	X
PSS–01(1)	Впровадження механізмів помилок і входу	О/Т	X	X	X
PSS–01(2)	Достатність інформації щодо помилок і входу	О		X	X
PSS–01(3)	Захист інформації від несанкціонованого доступу	О/Т		X	X
PSS–01(4)	Ведення журналу активацій або типу і обсягу реєстрації	О/Т		X	X
PSS–01(5)	Інформування користувача хмарних послуг через задокументовані інтерфейси	О			X
PSS–02	**Управління сесіями**	О/Т	X	X	X
PSS–02(1)	Система управління сесіями	О/Т	X	X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
PSS–02(2)	Деактивація сеансів	О/Т		X	X
PSS–02(3)	Визначення періоду бездіяльності	О/Т		X	X
PSS–03	**Програмно-конфігурована мережа**	О/Т	X	X	X
PSS–03(1)	Конфіденційність даних користувачів хмарних послуг	О/Т	X	X	X
PSS–03(2)	Перевірка функціональності SDN	Т	X	X	X
PSS–03(3)	Перевірка конфігурації мережі	Т		X	X
PSS–04	**Зображення для віртуальних машин і контейнерів**	О/Т	X	X	X
PSS–04(1)	Особливості експлуатації віртуальних машин	О	X	X	X
PSS–04(2)	Інформування користувача хмарних послуг про використання віртуальних машин	О/Т		X	
PSS–04(3)	Автоматичний контроль перевірки цілісності	Т			X
PSS–05	**Місця обробки і зберігання даних**	О/Т		X	X
PSS–05(1)	Визначення місця обробки і зберігання даних	О		X	X

Шифр	Назва заходу захисту	Упровадження	Профіль безпеки		
			«Низький»	«Середній»	«Високий»
PSS–05(2)	Контроль над місцем обробки і зберігання даних	О/Т		X	X

6. Відображення каталогу заходів захисту для хмарних послуг та НД ТЗІ 3.6-006-21

Таблиця 7 – Відображення каталог заходів захисту для хмарних послуг та НД ТЗІ 3.6-006-21

№ з/п	Каталог заходів захисту для хмарних послуг	НД ТЗІ 3.6-006-21
1.	OIS–01	PM–9
2.	OIS–02	PM–32
3.	OIS–03	PM–15
4.	OIS–04	PM–31
5.	ISP–01	PM–1, PM–18
6.	ISP–02	PM–4
7.	ISP–03	–
8.	RM–01	RA–1
9.	RM–02	RA–3
10.	RM–03	PM–32
11.	HR–01	AT–1, PS–1, PS–2
12.	HR–02	–
13.	HR–03	AT–2
14.	HR–04	AT–3, AT–4
15.	HR–05	PS–4, PS–5
16.	HR–06	PS–6
17.	AM–01	CM–8, PM–5, PM–29
18.	AM–02	–
19.	AM–03	–
20.	AM–04	MP–7
21.	AM–05	MP–3, PE–20, PE–22
22.	PHS–01	PE–1
23.	PHS–02	PE–2, PE–3, PE–6, PE–7, PE–8
24.	PHS–03	–
25.	PHS–04	PE–9, PE–10
26.	PHS–05	PE–9, PE–10, PE–11, PE–12, PE–13

№ з/п	Каталог заходів захисту для хмарних послуг	НД ТЗІ 3.6-006-21
27.	OPS–01	CP–1, CP–2
28.	OPS–02	CP–10, SI–4
29.	OPS–03	CP–2, CP–4
30.	OPS–04	SI–4
31.	OPS–05	AC–19, SC–3
32.	OPS–06	CP–9
33.	OPS–07	CP–9, SI–4
34.	OPS–08	CP–9, PM–14
35.	OPS–09	CP–6, CP–9, AC–20
36.	OPS–10	AC–7, AC–9
37.	OPS–11	AC–9, CM–11
38.	OPS–12	AC–9, AU–3, AU–14
39.	OPS–13	AC–9, AU–9, AU–12
40.	OPS–14	IA–2, IA–3, AU–6
41.	OPS–15	AC–9, CM–1, CM–5
42.	OPS–16	AC–9, SC–7, SC–32
43.	OPS–17	RA–5, CA–2
44.	OPS–18	RA–5, PE–8, AU–14
45.	OPS–19	RA–5, CA–8
46.	OPS–20	RA–5, CA–7, IR–4
47.	OPS–21	RA–5, CA–9, SC–32
48.	OPS–22	AC–3, AC–23, IA–9
49.	IAM–01	AC–1
50.	IAM–02	AC–2
51.	IAM–03	AC–7, AC–11
52.	IAM–04	AC–2
53.	IAM–05	AC–2
54.	IAM–06	AC–6
55.	IAM–07	IA–10
56.	IAM–08	IP–5, IA–12
57.	IAM–09	AC–5, CM–4(1), SC–2
58.	CKM–01	SA–9(6), SC–17
59.	CKM–02	SC–8, AC–17(2)
60.	CKM–03	AC–19(5)
61.	CKM–04	SC–12
62.	CS–01	IR–4, IR–7
63.	CS–02	CA–9, CM–2(6)
64.	CS–03	AC–17

№ з/п	Каталог заходів захисту для хмарних послуг	НД ТЗІ 3.6-006-21
65.	CS–04	CA–3
66.	CS–05	–
67.	CS–06	–
68.	CS–07	PM–7
69.	CS–08	–
70.	CS–09	SC–8
71.	PI–01	AC–17
72.	PI–02	SI–12
73.	PI–03	SI–18
74.	CCM–01	CM–1, CM–3
75.	CCM–02	CM–4
76.	CCM–03	CM–3(2)
77.	CCM–04	CM–3(1)
78.	CCM–05	CM–3(5)
79.	CCM–06	CM–2(3)
80.	DEV–01	SA–15,SA–4
81.	DEV–02	SA–17(3), SA–12
82.	DEV–03	SA–17(1),(2)
83.	DEV–04	SA–3(1), SA–8
84.	DEV–05	SA–11
85.	DEV–06	SA–15(3), SA–15(7)
86.	DEV–07	SA–9
87.	PM–01	AU–13, AU–16
88.	PM–02	RA–03, SA–12
89.	PM–03	SA–9, MA–2
90.	PM–04	SA–12
91.	PM–05	AT–1
92.	IM–01	AU–6, IR–1, IR–8
93.	IM–02	IR–4
94.	IM–03	IR–7
95.	IM–04	IR–6
96.	IM–05	IR–6
97.	IM–06	IR–2, IR–5
98.	IM–07	IR–3, IR–10
99.	BC–01	CP–2, IR–4
100.	BC–02	CP–1
101.	BC–03	CP–2, PM–4
102.	BC–04	PM–14, CP–3, CP–4

№ з/п	Каталог заходів захисту для хмарних послуг	НД ТЗІ 3.6-006-21
103.	CO–01	CA–1
104.	CO–02	AU–1, AU–12
105.	CO–03	–
106.	CO–04	CA–2
107.	DOC–01	CM–6
108.	DOC–02	IR–4, RA–5
109.	DOC–03	AC–20, AC–23, MP–7
110.	DOC–04	PL–2, RA–7
111.	DOC–05	SA–5
112.	DOC–06	CM–3
113.	INQ–01	–
114.	INQ–02	PM–16, PM–21
115.	INQ–03	AC–3, PM–27
116.	PSS–01	AC–7
117.	PSS–02	AC–12
118.	PSS–03	SC–8
119.	PSS–04	AC–6, SC–29
120.	PSS–05	AC–20

V. Вимоги до (профілів) кіберзахисту при використанні технології хмарних обчислень в інтересах об'єктів критичної інфраструктури та сектору безпеки і оборони

1. Вимоги до формування цільових профілів безпеки при використанні технології хмарних обчислень в інтересах об'єктів критичної інфраструктури та сектору безпеки і оборони

Формування цільового профілю безпеки при використанні технології хмарних обчислень в інтересах об'єктів критичної інфраструктури та сектору безпеки і оборони має відбуватися відповідно до положень НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» з урахуванням особливостей галузі та можливого обмеження доступу.

Впровадження заходів захисту для технології хмарних обчислень є одним з етапів розгортання системи безпеки інформації (СБІ) для надавача хмарних послуг, що ґрунтується на моделі ПВПД (планувати – виконувати – перевіряти – діяти), яка визначена в ISO/IEC 27001:2022 (рис. 4).

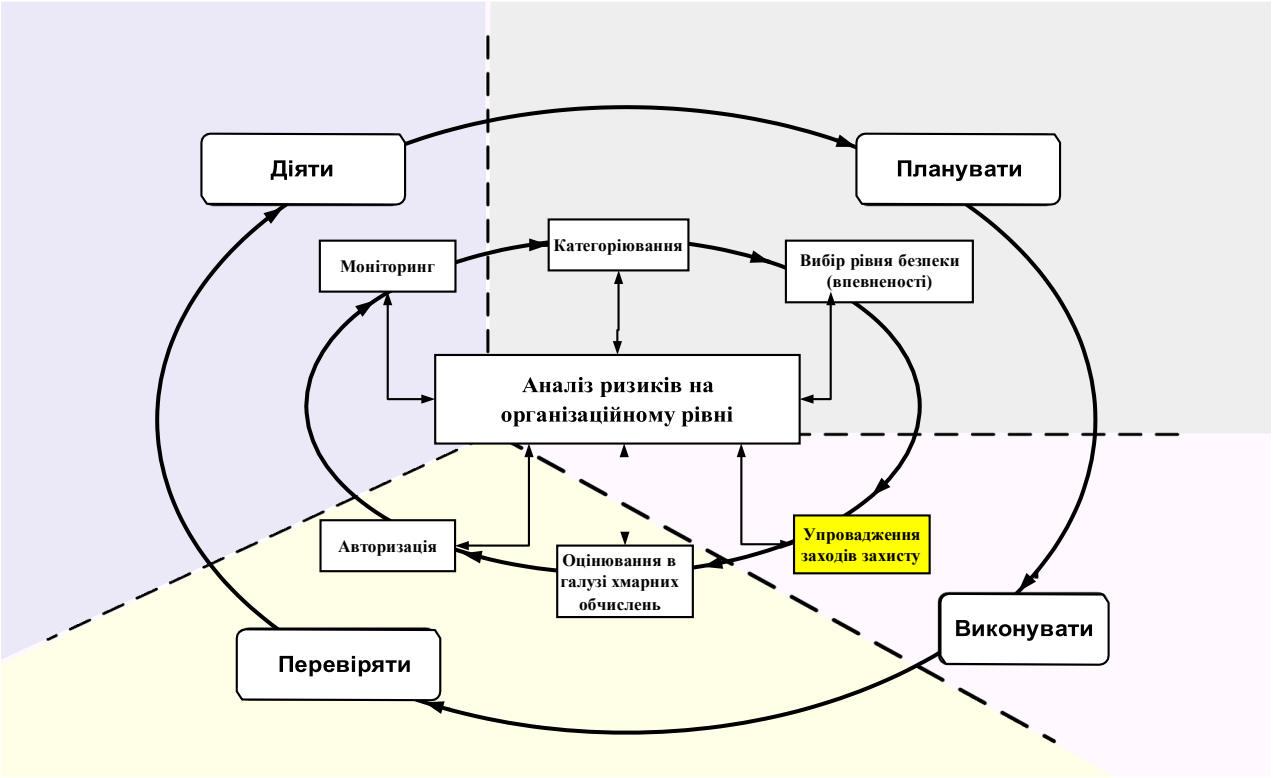

Рисунок 4 – Відповідність етапу вибору заходів захисту СБІ моделі ISO/IEC 27001

Упровадження заходів захисту здійснюється відповідно до розробленої CSP Концепції безпеки інформації (БІ) та приватності із застосуванням методології проєктування систем безпеки інформації.

Метою етапу є впровадження заходів захисту, а також документування результатів впровадження заходів захисту у їх базовій конфігурації. При цьому, виконання завдання Р-1, що визначено в НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем», слід проводити у два кроки, а виконання решти завдань Р-2 – Р-6 слід залишити без змін (таблиця 8).

Таблиця 8 – Завдання та результати етапу впровадження (реалізації) заходів захисту

Завдання	Результати
Завдання Р-1 Крок 1. Часткове налаштування базового (галузевого) профілю безпеки	Базовий (галузевий) профілю безпеки частково налаштований
Крок 2. Встановлення значень параметрів заходів захисту	Параметри заходів захисту встановлено

На першому кроці проводиться часткове налаштування базового (галузевого) профілю безпеки шляхом додавання або виключення заходів захисту для актуалізації профілю безпеки відповідно до технології хмарних обчислень. Перелік класів заходів захисту обирається на основі визначеного рівня безпеки (впевненості) до хмарних послуг. Залежно від особливостей функціонування надавача хмарних послуг цільовий профіль безпеки може бути доповненим новими класами та/або заходами захисту з інших джерел.

Прикладом взаємозв'язку заходів захисту, визначених в НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці», каталогу заходів захисту для хмарних послуг є Методичні рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури, затверджені наказом Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601.

Обов'язковою умовою використання сторонніх заходів захисту є наявність стандартизованої методики їхнього оцінювання відповідно до НД ТЗІ 2.3-025-21 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

Частково налаштований цільовий профіль безпеки при використанні технології хмарних обчислень в інтересах об'єктів критичної інфраструктури та сектору безпеки і оборони (наводиться в пункті 5.3). Процес налаштування профілю передбачає перелік заходів захисту високого рівня безпеки (впевненості) до хмарних послуг, а також специфічні заходи захисту, які визначаються відповідно до НД ТЗІ 3.6-006-21.

На другому кроці проводиться встановлення значень параметрів заходів захисту з урахуванням організаційних та структурних особливостей надавача хмарних послуг.

2. Відповідність вимог НД ТЗІ 3.6-006-21, каталогу заходів захисту для хмарних послуг та Методичним рекомендаціям щодо підвищення рівня кіберзахисту критичної інформаційної структури, що затвердженим наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601.

НД ТЗІ 3.6-006-21	Каталог заходів захисту для хмарних послуг	Заходи кіберзахисту, наведені у Методичних рекомендаціях щодо підвищення рівня кіберзахисту критичної інформаційної структури, що затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 (зі змінами)

1	2	3
AC-1	IAM-01	ID.GV-1, ID.GV-3, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6
AC-2	IAM–02, IAM–04, IAM–05	PR.AC-1, PR.AC-4, PR.AC-6, DE.CM-1, DE.CM-3
AC-3	OPS–22, INQ–03	PR.AC-4, PR.AC-6, PR.PT-3
AC-4	–	ID.AM-3, PR.AC-5, PR.DS-5, PR.PT-4, DE.AE-1
AC-5	IAM–09	PR.AC-4, PR.DS-5
AC-6	IAM–06, PSS–04	PR.AC-4, PR.DS-5
AC-7	OPS–10, IAM–03, PSS–01	PR.AC-7
AC-8	–	PR.AC-7
AC-9	OPS–10, OPS–11, OPS–12, OPS–13, OPS–15, OPS–16	PR.AC-7
AC-10	–	PR.AC-5
AC-11	OPS–11, IAM–03	PR.AC-7
AC-12	PSS–02	PR.AC-7
AC-13	–	–
AC-14	–	PR.AC-4, PR.AC-7
AC-15	–	–
AC-16	–	PR.AC-4, PR.AC-6
AC-17	CKM–02, CS–03, PI–01	PR.AC-3, PR.PT-4
AC-18	–	PR.PT-4
AC-19	OPS–05, CKM–03	PR.AC-3, PR.AC-6
AC-20	OPS–09, DOC–03, PSS–05	ID.AM-4, PR.AC-3
AC-21	–	PR.IP-8
AC-22	–	–
AC-23	OPS–22, DOC–03	–
AC-24	–	PR.AC-4, PR.AC-6
AC-25	–	–
AT-1	HR-01, PM–05	ID.GV-1, ID.GV-3
AT-2	HR–03	PR.AT-1
AT-3	HR–04	PR.AT-2, PR.AT-4, PR.AT-5
AT-4	HR–04	–
AT-5	–	–
AU-1	CO–02	ID.GV-1, ID.GV-3, PR.PT-1
AU-2	–	ID.SC-4, PR.PT-1
AU-3	OPS–12	PR.PT-1

1	2	3
AU-4	–	PR.DS-4, PR.PT-1
AU-5	–	PR.PT-1
AU-6	OPS–14, IM–01	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1
AU-7	–	PR.PT-1, RS.AN-3
AU-8	–	PR.PT-1
AU-9	OPS–13	PR.PT-1
AU-10	–	PR.PT-1
AU-11	–	PR.PT-1
AU-12	OPS–13, CO–02	PR.PT-1, DE.CM-1, DE.CM-3, DE.CM-7
AU-13	PM-01	PR.PT-1, DE.CM-3
AU-14	OPS–12, OPS–18	PR.PT-1
AU-15		PR.PT-1
AU-16	PM-01	ID.SC-4, PR.PT-1
CA-1	CO–01	ID.GV-1, ID.GV-3
CA-2	OPS-17, CO–04	ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.CO-3
CA-3	CS–04	ID.AM-3, DE.AE-1
CA-4	–	–
CA-5	–	–
CA-6	–	–
CA-7	OPS–20	ID.RA-1, PR.IP-7,PR.IP-8,DE.AE-2,DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, DE.DP-5, RS.CO-3, RS.AN-1, RS.MI-3
CA-8	OPS-19	ID.RA-1
CA-9	OPS–21, CS–02	ID.AM-3
CM-1	OPS–15, CCM-01	ID.GV-1, ID.GV-3
CM-2	CS–02, CCM–06	PR.DS-7, PR.IP-1, DE.AE-1
CM-3	CCM-01, CCM–03, CCM–04, CCM–05, DOC–06	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7
CM-4	IAM–09, CCM–02	PR.IP-1, PR.IP-3
CM-5	OPS–15	PR.IP-1
CM-6	DOC–01	PR.IP-1
CM-7	–	PR.IP-1, PR.PT-3
CM-8	AM–01	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7
CM-9	–	PR.IP-1

1	2	3
CM-10	–	DE.CM-3
CM-11	–	DE.CM-3
CM-12	–	–
CP-1	OPS–01, BC–02	ID.GV-1, ID.GV-3
CP-2	OPS–01, OPS–03, BC–01, BC–03	ID.AM-5, ID.AM-6, ID.BE-1, ID.BE-5, ID.SC-5, PR.DS-4, PR.IP-7, PR.IP-9, DE.AE-4, RS.RP-1, RS.CO-1, RS.CO-3, RS.CO-4, RS.AN-2, RS.AN-4, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2, RC.CO-3
CP-3	BC–04	RS.CO-1
CP-4	OPS–03, BC–04	ID.SC-5, PR.IP-4, PR.IP-10
CP-5	–	–
CP-6	OPS–09	PR.IP-4
CP-7	–	PR.PT-5
CP-8	–	ID.BE-4, PR.PT-4, PR.PT-5
CP-9	OPS–06, OPS–07, OPS–08, OPS–09	PR.IP-4
CP-10	OPS–02	RS.RP-1, RC.RP-1
CP-11	–	ID.BE-5, PR.PT-5
CP-12	–	–
CP-13	–	PR.PT-5
IA-1	–	ID.GV-1, ID.GV-3, PR.AC-1, PR.AC-6, PR.AC-7
IA-2	OPS–14	PR.AC-1, PR.AC-6, PR.AC-7
IA-3	OPS–14	PR.AC-1, PR.AC-7
IA-4	–	PR.AC-1, PR.AC-6, PR.AC-7
IA-5	–	PR.AC-1, PR.AC-6, PR.AC-7
IA-6	–	PR.AC-1
IA-7	–	PR.AC-1
IA-8	–	PR.AC-1, PR.AC-6, PR.AC-7
IA-9	OPS–22	PR.AC-1, PR.AC-7
IA-10	IAM–07	PR.AC-1, PR.AC-7
IA-11	–	PR.AC-1, PR.AC-7
IA-12	IAM–08	PR.AC-1
IP-1	–	ID.GV-1, ID.GV-3
IP-2	–	–
IP-3	–	–
IP-4	–	–
IP-5	IAM–08	–

1	2	3
IP-6	–	–
IR-1	IM–01	ID.GV-1, ID.GV-3
IR-2	IM–06	PR.AT-5
IR-3	IM–07	ID.SC-5, PR.IP-10, RS.CO-1
IR-4	OPS–20, CS–01, IM–02, BC–01, DOC–02	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-3
IR-5	IM–06	DE.AE-3, DE.AE-5, RS.AN-1, RS.AN-4
IR-6	IM–04, IM–05	ID.SC-5, RS.CO-2
IR-7	CS–01, IM–03	–
IR-8	IM–01	ID.SC-5, PR.IP-7, PR.IP-9, DE.AE-3, DE.AE-5, RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-4, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2
IR-9	–	ID.SC-5
IR-10	IM–07	–
MA-1	–	ID.GV-1, ID.GV-3
MA-2	PM–03	PR.MA-1
MA-3	–	PR.MA-1
MA-4	–	PR.MA-2
MA-5	–	PR.MA-1
MA-6	–	–
MP-1	–	ID.GV-1, ID.GV-3
MP-2	–	PR.PT-2
MP-3	AM–05	–
MP-4	–	PR.PT-2
MP-5	–	PR.PT-2
MP-6	–	PR.DS-3, PR.IP-6
MP-7	AM–04, DOC–03	PR.PT-2
MP-8	–	–
PA-1	–	ID.GV-1, ID.GV-3
PA-2	–	–
PA-3	–	–
PA-4	–	–
PE-1	PHS–01	ID.GV-1, ID.GV-3

1	2	3
PE-2	PHS–02	PR.AC-2, PR.AC-6
PE-3	PHS–02	PR.AC-2, DE.CM-2, DE.CM-7, DE.DP-3
PE-4	–	PR.AC-2
PE-5	–	PR.AC-2
PE-6	PHS–02	PR.AC-2, DE.CM-2, DE.CM-7, RS.CO-3, RS.AN-1
PE-7	PHS–02	–
PE-8	PHS–02, OPS–18	–
PE-9	PHS–04, PHS–05	ID.BE-4, ID.GV-3, PR.AC-2
PE-10	PHS–04, PHS–05	PR.IP-5
PE-11	PHS–05	ID.BE-4, ID.GV-3
PE-12	PHS–05	PR.IP-5
PE-13	PHS–05	PR.IP-5
PE-14	–	PR.IP-5
PE-15	–	PR.IP-5
PE-16	–	PR.DS-3
PE-17	–	–
PE-18	–	PR.IP-5
PE-19	–	PR.DS-5
PE-20	AM–05	DE.CM-2, DE.CM-7
PE-21	–	–
PE-22	AM–05	–
PL-1	–	ID.GV-1, ID.GV-3, ID.GV-3
PL-2	DOC–04	PR.IP-7, DE.DP-5
PL-3	–	–
PL-4	–	–
PL-5	–	–
PL-6	–	–
PL-7	–	–
PL-8	–	ID.AM-3, PR.IP-2, PR.PT-5
PL-9	–	–
PL-10	–	–
PL-11	–	–
PM-1	ISP-01	ID.GV-1, ID.GV-2
PM-2	–	–
PM-3	–	–
PM-4	ISP-02, BC–03	ID.RA-6
PM-5	AM–01	–
PM-6	–	PR.IP-7
PM-7	CS–07	–

1	2	3
PM-8	–	ID.BE-2, ID.BE-4, ID.RM-3
PM-9	OIS-01	ID.GV-4, ID.RA-4, ID.RA-6 ID.RA-6, ID.RM-1, ID.RM-2, ID.RM-3, ID.SC-1, ID.SC-2, ID.SC-3
PM-10	–	–
PM-11	–	ID.AM-6, ID.BE-3, ID.GV-4, ID.RA-4, ID.RM-3
PM-12	–	ID.RA-3
PM-13	–	PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5
PM-14	OPS–08, BC–04	PR.IP-10, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-5
PM-15	OIS–03	ID.RA-2, RS.CO-5, RS.AN-5
PM-16	INQ–02	ID.RA-2, ID.RA-3, ID.RA-5
PM-17	–	–
PM-18	ISP-01	–
PM-19	–	–
PM-20	–	–
PM-21	INQ–02	–
PM-22	–	–
PM-23	–	–
PM-24	–	–
PM-25	–	–
PM-26	–	–
PM-27	INQ–03	–
PM-28	–	–
PM-29	AM–01	–
PM-30	–	–
PM-31	OIS–04	–
PM-32	OIS–02, RM–03	–
PS-1	HR-01	ID.GV-1, ID.GV-3, PR.IP-11
PS-2	HR-01	PR.IP-11
PS-3	–	PR.AC-6, PR.DS-5, PR.IP-11
PS-4	HR–05	PR.IP-11
PS-5	HR–05, OPS–20	PR.IP-11
PS-6	HR–06	PR.DS-5, PR.IP-11
PS-7	–	ID.AM-6, ID.GV-2, ID.SC-4, PR.AT-3, PR.IP-11, DE.CM-6
PS-8	–	PR.IP-11
RA-1	RM-01	ID.GV-1, ID.GV-3
RA-2		ID.AM-5, ID.RA-4, ID.RA-5, ID.SC-2
RA-3	RM–02, PM–02	ID.RA-1, ID.RA-3, ID.RA-4,

1	2	3
		ID.RA-5, ID.SC-2, PR.IP-12, DE.AE-4, RS.MI-3
RA-4	–	–
RA-5	OPS-17, OPS–18, OPS-19, DOC–02	ID.RA-1, PR.IP-12, DE.CM-8, DE.DP-4, DE.DP-5, RS.CO-3, RS.MI-3
RA-6	–	–
RA-7	DOC–04	–
RA-8	–	–
RA-9	–	–
SA-1	–	ID.GV-1, ID.GV-3
SA-2	–	–
SA-3	DEV–04	PR.IP-2
SA-4	DEV-01	PR.IP-2, DE.CM-6
SA-5	DOC–05	ID.RA-1
SA-6	–	–
SA-7	–	–
SA-8	DEV–04	PR.IP-2
SA-9	CKM–01, DEV–07, PM–03	ID.AM-4, ID.SC-1, ID.SC-3, ID.SC-4, PR.AT-3, DE.CM-6
SA-10	–	PR.IP-1, PR.IP-2, PR.IP-3
SA-11	DEV–05	ID.RA-1, ID.SC-3, PR.IP-2
SA-12	DEV–02, PM–02, PM–04	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, PR.IP- 2
SA-13	–	–
SA-14	–	ID.AM-5, ID.BE-3, ID.BE-4, ID.BE-5, ID.RA-4, ID.RM-3, ID.SC-2, PR.PT-5
SA-15	DEV-01, DEV–06	ID.SC-2, PR.IP-2
SA-16	–	–
SA-17	DEV–02, DEV–03	PR.IP-2
SA-18	–	–
SA-19	–	–
SA-20	–	–
SA-21	–	–
SA-22	–	–
SC-1	–	ID.GV-1, ID.GV-3
SC-2	IAM–09	–
SC-3	OPS–05	–
SC-4	–	–
SC-5	–	PR.DS-4, DE.CM-1
SC-6	–	PR.PT-5

1	2	3
SC-7	OPS–16	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1
SC-8	CKM–02, CS–09, PSS–03	PR.DS-2, PR.DS-5
SC-9	–	–
SC-10	–	–
SC-11	–	–
SC-12	CKM–04	–
SC-13	–	PR.DS-5
SC-14	–	–
SC-15	–	PR.AC-3
SC-16	–	–
SC-17	CKM–01	–
SC-18	–	DE.CM-5
SC-19	–	–
SC-20	–	–
SC-21	–	–
SC-22	–	–
SC-23	–	–
SC-24	–	–
SC-25	–	–
SC-26	–	–
SC-27	–	–
SC-28	–	PR.DS-1
SC-29	PSS–04	–
SC-30	–	–
SC-31	–	PR.DS-5
SC-32	OPS–16, OPS–21	–
SC-33	–	–
SC-34	–	–
SC-35	–	–
SC-36	–	–
SC-37	–	–
SC-38	–	–
SC-39	–	–
SC-40	–	–
SC-41	–	–
SC-42	–	–
SC-43	–	–
SC-44	–	DE.CM-5
SI-1	–	ID.GV-1, ID.GV-3

1	2	3
SI-2	–	ID.RA-1, PR.IP-12
SI-3	–	DE.CM-4, DE.DP-3
SI-4	OPS–02, OPS–04, OPS–07	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.CO-3, RS.AN-1
SI-5	–	ID.RA-1, ID.RA-3, RS.CO-5, RS.AN-5
SI-6	–	ID.RA-2
SI-7	–	PR.DS-6
SI-8	–	–
SI-9	–	–
SI-10	–	–
SI-11	–	–
SI-12	PI–02	–
SI-13	–	–
SI-14	–	–
SI-15	–	–
SI-16	–	–
SI-17	–	–
SI-18	PI–03	–
SI-19	–	–
SI-20	–	–

3. Частково налаштований цільовий профіль безпеки при використанні технології хмарних обчислень в інтересах об'єктів критичної інфраструктури та сектору безпеки і оборони

ЦПБ високого рівня впевненості (гарантій) безпеки		
Захід захисту	Посилення заходу захисту	Специфічні заходи захисту*
1	2	3
OIS-01	OIS-01(1), OIS-01(2), OIS-01(3), OIS-01(4), OIS-01(5)	
OIS-02	OIS-02(1), OIS-02(2), OIS-02(3), OIS-02(4)	
OIS-03	OIS-03(1), OIS-03(2), OIS-03(3)	
OIS-04	OIS-04(1), OIS-04(2)	
ISP-01	ISP-01(1), ISP-01(2), ISP-01(3), ISP-01(4), ISP-01(5)	CA-6
ISP-02	ISP-02(1), ISP-02(2), ISP-02(3), ISP-02(4), ISP-02(5), ISP-02(6), ISP-02(7)	

1	2	3
ISP-03	ISP-03(1), ISP-03(2), ISP-03(3), ISP-03(4), ISP-03(5), ISP-03(6), ISP-03(7)	
RM-01	RM-01(1), RM-01(2)	
RM-02	RM-02(1), RM-02(2), RM-02(3), RM-02(4)	SI-16
RM-03	RM-03(1), RM-03(2), RM-03(3), RM-03(4), RM-03(5), RM-03(6), RM-03(7), RM-03(8)	CA-5, RA-9
HR-01	HR-01(1), HR-01(2), HR-01(3), HR-01(4)	
HR-02	HR-02(1), HR-02(2), HR-02(3)	PS-3, PS-8
HR-03	HR-03(1), HR-03(2), HR-03(3), HR-03(4), HR-03(5)	PE-18
HR-04	HR-04(1), HR-04(2), HR-04(3), HR-04(4), HR-04(5), HR-04(6), HR-04(7), HR-04(8), HR-04(9), HR-04(10)	SA-16
HR-05	HR-05(1), HR-05(2), HR-05(3), HR-05(4)	
HR-06	HR-06(1), HR-06(2), HR-06(3), HR-06(4), HR-06(5), HR-06(6), HR-06(7)	
AM-01	AM-01(1), AM-01(2), AM-01(3), AM-01(4), AM-01(5), AM-01(6)	
AM-02	AM-02(1), AM-02(2), AM-02(3)	MA-1, CM-11
AM-03	AM-03(1), AM-03(2), AM-03(3), AM-03(4), AM-03(5), AM-03(6)	MP-6(1), PE-16, SI- 6
AM-04	AM-04(1), AM-04(2), AM-04(3), AM-04(4)	
AM-05	AM-05(1), AM-05(2), AM-05(3), AM-05(4)	
PHS-01	PHS-01(1), PHS-01(2), PHS-01(3), PHS-01(4), PHS-01(5), PHS-01(6), PHS-01(7)	
PHS-02	PHS-02(1), PHS-02(2), PHS-02(3), PHS-02(4), PHS-02(5), PHS-02(6), PHS-02(7), PHS-02(8), PHS-02(9), PHS-02(10)	AC-8, MP-2, PE-4, SI-5(1)
PHS-03	PHS-03(1), PHS-03(2), PHS-03(3), PHS-03(4)	MA-3(2), MP-1
PHS-04	PHS-04(1), PHS-04(2), PHS-04(3), PHS-04(4), PHS-04(5), PHS-04(6), PHS-04(7), PHS-04(8), PHS-04(9)	PA-2, PA-4, IP-2, MA-4(3), MP-5
PHS-05	PHS-05(1), PHS-05(2), PHS-05(3), PHS-05(4), PHS-05(5), PHS-05(6)	PE-15(1)
OPS-01	OPS-01(1), OPS-01(2), OPS-01(3)	PL-1, PS-7
OPS-02	OPS-02(1), OPS-02(2), OPS-02(3)	CP-7(2)
OPS-03	OPS-03(1)	
OPS-04	OPS-04(1), OPS-04(2), OPS-04(3), OPS-04(4)	SI-3(1)
OPS-05	OPS-05(1), OPS-05(2), OPS-05(3), OPS-05(4)	
OPS-06	OPS-06(1), OPS-06(2)	
OPS-07	OPS-07(1), OPS-07(2), OPS-07(3)OPS-08	
OPS-08	OPS-08(1), OPS-08(2), OPS-08(3), OPS-08(4), OPS-08(5)	

1	2	3
OPS-09	OPS-09(1), OPS-09(2), OPS-09(3), OPS-09(4), OPS-09(5)	MP-4
OPS-10	OPS-10(1), OPS-10(2)	
OPS-11	OPS-11(1), OPS-11(2), OPS-11(3), OPS-11(4)	
OPS-12	OPS-12(1), OPS-12(2), OPS-12(3), OPS-12(4)	
OPS-13	OPS-13(1), OPS-13(2), OPS-13(3), OPS-13(4), OPS-13(5), OPS-13(6), OPS-13(7)	AC-18(1), SI-7(1)
OPS-14	OPS-14(1), OPS-14(2), OPS-14(3)	IA-4(4), IA-8(4)
OPS-15	OPS-15(1), OPS-15(2), OPS-15(3)	
OPS-16	OPS-16(1), OPS-16(2)	
OPS-17	OPS-17(1), OPS-17(2), OPS-17(3), OPS-17(4)	
OPS-18	OPS-18(1), OPS-18(2), OPS-18(3), OPS-18(4), OPS-18(5), OPS-18(6)	
OPS-19	OPS-19(1), OPS-19(2), OPS-19(3), OPS-19(4), OPS-19(5), OPS-19(6), OPS-19(7), OPS-19(8)	
OPS-20	OPS-20(1), OPS-20(2)	
OPS-21	OPS-21(1), OPS-21(2), OPS-21(3)	
OPS-22	OPS-22(1)	
IAM-01	IAM-01(1), IAM-01(2), IAM-01(3)	
IAM-02	IAM-02(1), IAM-02(2), IAM-02(3), IAM-02(4), IAM-02(5), IAM-02(6), IAM-02(7), IAM-02(8)	IA-1
IAM-03	IAM-03(1), IAM-03(2), IAM-03(3), IAM-03(4), IAM-03(5), IAM-03(6), IAM-03(7), IAM-03(8), IAM-03(9), IAM-03(10), IAM-03(11), IAM-03(12)	AC-14, AU-11
IAM-04	IAM-04(1), IAM-04(2), IAM-04(3), IAM-04(4), IAM-04(5), IAM-04(6), IAM-04(7)	IA-11
IAM-05	IAM-05(1), IAM-05(2), IAM-05(3), IAM-05(4), IAM-05(5)	
IAM-06	IAM-06(1), IAM-06(2), IAM-06(3), IAM-06(4), IAM-06(5), IAM-06(6), IAM-06(7), IAM-06(8)	
IAM-07	IAM-07(1), IAM-07(2), IAM-07(3), IAM-07(4), IAM-07(5), IAM-07(6), IAM-07(7), IAM-07(8)	
IAM-08	IAM-08(1), IAM-08(2), IAM-08(3), IAM-08(4), IAM-08(5), IAM-08(6), IAM-08(7), IAM-08(8), IAM-08(9)	IA-5 (1), IA-7, IA-8(1)
IAM-09	IAM-09(1), IAM-09(2), IAM-09(3), IAM-09(4), IAM-09(5), IAM-09(6), IAM-09(7)	AC-18(4)
CKM-01	CKM-01(1), CKM-01(2), CKM-01(3)	SC-13, SI-1
CKM-02	CKM-02(1), CKM-02(2)	
CKM-03	CKM-03(1), CKM-03(2), CKM-03(3), CKM-03(4)	
CKM-04	CKM-04(1), CKM-04(2), CKM-04(3), CKM-04(4)	IA-5 (2)

1	2	3
CS-01	CS-01(1), CS-01(2), CS-01(3), CS-01(4), CS-01(5)	SC-5
CS-02	CS-02(1)	CP-7(1)
CS-03	CS-03(1), CS-03(2), CS-03(3), CS-03(4), CS-03(5), CS-03(6), CS-03(7)	SC-1
CS-04	CS-04(1), CS-04(2), CS-04(3), CS-04(4), CS-04(5)	
CS-05	CS-05(1), CS-05(2), CS-05(3), CS-05(4), CS-05(5)	AC-4(4)
CS-06	CS-06(1), CS-06(2)	SC-15
CS-07	CS-07(1), CS-07(2), CS-07(3), CS-07(4)	
CS-08	CS-08(1), CS-08(2), CS-08(3)	CM-7(1)
CS-09	CS-09(1), CS-09(2)	
PI-01	PI-01(1), PI-01(2), PI-01(3), PI-01(4), PI-01(5)	
PI-02	PI-02(1), PI-02(2), PI-02(3)	MA-3(3)
PI-03	PI-03(1), PI-03(2), PI-03(3), PI-03(4), PI-03(5)	
CCM-01	CCM-01(1), CCM-01(2)	AC-21
CCM-02	CCM-02(1), CCM-02(2), CCM-02(3), CCM-02(4), CCM-02(5)	
CCM-03	CCM-03(1), CCM-03(2), CCM-03(3), CCM-03(4), CCM-03(5), CCM-03(6), CCM-03(7), CCM-03(8), CCM-03(9), CCM-03(10)	CM-9
CCM-04	CCM-04(1), CCM-04(2), CCM-04(3)	
CCM-05	CCM-05(1), CCM-05(2), CCM-05(3)	
CCM-06	CCM-06(1), CCM-06(2), CCM-06(3)	
DEV-01	DEV-01(1), DEV-01(2), DEV-01(3), DEV-01(4)	
DEV-02	DEV-02(1), DEV-02(2), DEV-02(3), DEV-02(4)	CM-9, CM-10
DEV-03	DEV-03(1), DEV-03(2), DEV-03(3), DEV-03(4), DEV-03(5)	
DEV-04	DEV-04(1), DEV-04(2), DEV-04(3)	SC-4
DEV-05	DEV-05(1), DEV-05(2), DEV-05(3), DEV-05(4), DEV-05(5)	
DEV-06	DEV-06(1), DEV-06(2), DEV-06(3), DEV-06(4), DEV-06(5), DEV-06(6)	
DEV-07	DEV-07(1), DEV-07(2), DEV-07(3), DEV-07(4)	
PM-01	PM-01(1), PM-01(2), PM-01(3), PM-01(4), PM-01(5)	
PM-02	PM-02(1), PM-02(2), PM-02(3), PM-02(4), PM-02(5)	AC-22, SA-1, SA-2, SA-10
PM-03	PM-03(1), PM-03(2), PM-03(3)	
PM-04	PM-04(1), PM-04(2), PM-04(3), PM-04(4), PM-04(5), PM-04(6), PM-04(7), PM-04(8)	
PM-05	PM-05(1), PM-05(2)	CP-8(2)
IM-01	IM-01(1), IM-01(2), IM-01(3), IM-01(4), IM-01(5), IM-01(6), IM-01(7), IM-01(8)	

1	2	3
IM-02	IM-02(1), IM-02(2), IM-02(3), IM-02(4), IM-02(5)	
IM-03	IM-03(1), IM-03(2), IM-03(3), IM-03(4)	
IM-04	IM-04(1), IM-04(2), IM-04(3)	
IM-05	IM-05(1), IM-05(2)	IP-1
IM-06	IM-06(1), IM-06(2), IM-06(3), IM-06(4)	AU-4
IM-07	IM-07(1), IM-07(2), IM-07(3), IM-07(4), IM-07(5)	AU-10(3)
BC-01	BC-01(1), BC-01(2), BC-01(3)	CP-8(4)
BC-02	BC-02(1), BC-02(2), BC-02(3)	
BC-03	BC-03(1), BC-03(2), BC-03(3), BC-03(4)	CP-8(1)
BC-04	BC-04(1), BC-04(2), BC-04(3), BC-04(4)	
CO-01	CO-01(1), CO-01(2), CO-01(3), CO-01(4)	IP-6
CO-02	CO-02(1), CO-02(2), CO-02(3)	AU-2, MA-6
CO-03	CO-03(1), CO-03(2), CO-03(3), CO-03(4), CO-03(5), CO-03(6), CO-03(7)	AU-7
CO-04	CO-04(1), CO-04(2)	
DOC-01	DOC-01(1), DOC-01(2), DOC-01(3), DOC-01(4), DOC-01(5)	
DOC-02	DOC-02(1), DOC-02(2), DOC-02(3), DOC-02(4), DOC-02(5), DOC-02(6)	
DOC-03	DOC-03(1), DOC-03(2), DOC-03(3), DOC-03(4)	CM-12(1)
DOC-04	DOC-04(1), DOC-04(2), DOC-04(3), DOC-04(4)	PL-10, PL-11
DOC-05	DOC-05(1), DOC-05(2), DOC-05(3), DOC-05(4)	
DOC-06	DOC-06(1), DOC-06(2), DOC-06(3)	
INQ-01	INQ-01(1), INQ-01(2)	
INQ-02	INQ-02(1)	
INQ-03	INQ-03(1), INQ-03(2), INQ-03(3), INQ-03(4)	SC-20
PSS-01	PSS-01(1), PSS-01(2), PSS-01(3), PSS-01(4), PSS-01(5)	
PSS-02	PSS-02(1), PSS-02(2), PSS-02(3)	AC-10, SC-23
PSS-03	PSS-03(1), PSS-03(2), PSS-03(3)	
PSS-04	PSS-04(1), PSS-04(2), PSS-04(3)	
PSS-05	PSS-05(1), PSS-05(2)	

* відповідно до НД ТЗІ 3.6-006-21.

VI. Вимоги безпеки (та приватності) до об'єктів критичної інфраструктури

1. Вимоги щодо розгортання та обслуговування систем безпеки інформації у сфері хмарних послуг:

1) необхідно забезпечити планування, впровадження та постійне вдосконалення системи безпеки інформації, яка містить такі положення щодо

управління ризиками безпеки протягом всього життєвого циклу хмари;

2) забезпечити впровадження механізмів оцінки ризиків на організаційному та системному рівнях;

3) забезпечити підтримку актуального стану поінформованості всіх заінтересованих сторін про актуальні поточні загрози;

4) забезпечити впровадження заходів безпеки інформації та питань щодо оцінки ризиків у всіх поточні та/або потенційні проєкти;

5) упровадити процедури затвердження, документування та поширення, а також перегляду концепції безпеки інформації;

6) встановити єдину структуру правил та процедур безпеки;

7) сформулювати та затвердити винятки із правил та процедур безпеки;

8) визначити правові, нормативні, самовстановлені та договірні вимоги, що стосуються безпеки інформації хмари;

9) запровадити проведення аудитів з мінімізацією втручання у наданні хмарних послуг;

10) проводити внутрішній аудит системи внутрішнього контролю;

11) оцінювати систему внутрішнього контролю на предмет ефективності безпеки інформації;

12) має бути забезпечена доступність хмарного сервісу іншим хмарним сервісам від інших CSP або IT-систем користувачів хмарних послуг через чітко задокументовані вхідні та вихідні інтерфейси, зв’язок на яких використовує стандартизовані протоколи зв'язку, а через ненадійні мережі зв'язок повинен шифруватися;

13) базуючись на потребах експертів з потенційних користувачів хмарних послуг, CSP вносить в договори про надання хмарних послуг хмарні послуги аспекти, що стосуються припинення договірних відносин. При цьому CSP повинен не рідше одного разу на рік визначати правові та нормативні вимоги, які можуть застосовуватися до цих аспектів і коригує умови договору;

14) процедури видалення даних повинні бути застосовані до цих користувачів хмарних послуг CSP після розірвання їхнього договору відповідно до умов договору між ними (включно з метаданими та даними, що зберігаються у резервних копіях даних), унеможливлювати відновлення криміналістичними засобами; видалення даних користувача хмарних послуг повинно бути задокументовано задля надання можливості користувачу хмарних послуг перевірити дотримання умов договору;

15) проводити та здійснювати документування моніторингу третіх сторін, їх додатковий контроль та незалежне аудит;

16) проходити оцінку ризиків, щоб визначити потреби в безпеці, пов'язані з товаром або послугою, яку вони надають;

17) запровадити ведення централізованого каталогу надавачів;

18) встановити механізми моніторингу для забезпечення дотримання третіми сторонами своїх регуляторних та договірних зобов'язань;

19) визначити стратегії виходу, якщо відносини з надавачами хмарних

послуг припиняються.

2. Управління ризиками у сфері хмарних послуг або технології хмарних обчислень:

1) затвердити аспекти щодо аналізу та документування результатів оцінки ризиків;

2) провести аналіз оцінки ризиків відповідно до встановлених процедур, а також забезпечити поширення результатів аналізу серед усіх заінтересованих сторін;

3) встановити пріоритетність ризиків та провести оцінку залишкових та спільних ризиків.

3. Організація управління ІТ-активами в технології хмарних обчислень та їх документування:

1) встановити політику щодо управління людськими ресурсами, яка класифікує ризики на всіх посадах, етичний кодекс та відповідальність за порушення;

2) забезпечити процедури перевірки кваліфікації та компетентностей працівників до моменту початку їхньої роботи;

3) встановити порядок дотримання умов праці, який передбачає угоду про нерозголошення, первинний інструктаж, а також інші аспекти у разі потреби;

4) упровадити та постійно оновлювати програми навчання (тренінгів), орієнтованої на цільові групи для підтримання обізнаності працівників;

5) запровадити механізм інформування працівників про те, які обов'язки, що випливають із керівних принципів та інструкцій, що стосуються безпеки інформації, залишатимуться чинними після припинення або зміни їх трудових відносин та на який термін;

6) встановити порядок погодження та підписання угод про нерозголошення та конфіденційність;

7) встановити процедури щодо інвентаризації ІТ-активів;

8) встановити політику та процедури прийнятого використання та безпечного поводження з активами;

9) процедури введення та виведення з експлуатації обладнання мають враховувати положення щодо управління ризиками при цих процесах;

10) забезпечити доказове дотримання працівниками політики та інструкцій щодо використання та безпечного поводження з активами;

11) ввести схему маркування активів;

12) публікувати та переглядати рекомендації для користувачів хмарних послуг;

13) вести онлайн-реєстр відомих вразливостей, який допоможе користувачу хмарних послуг у безпечній конфігурації, інсталяції та використанні хмари;

14) інформувати користувачів хмарних послуг про місцезнаходження даних та їх обробку;

15) обгрунтувати цільовий рівень безпеки (гарантій) хмарою;

16) запроваджувати надання документації, яка необхідна користувачам хмарних послуг, на основі додаткового контролю користувачів хмарних послуг;

17) використовувати внески до виконання вимог у випадках сертифікації користувачем хмарних послуг своїх власних послуг на основі своєї хмари.

4. Визначення умов середовищ функціонування в технології хмарних обчислень:

1) визначити периметри та зони безпеки;

2) встановити відповідні заходи захисту щодо фізичної безпеки для кожної із визначеної зон;

3) встановити особливі правила для роботи в критичних зонах, у тому числі політику чистого екрана та змінних носіїв;

4) застосовувати заходи фізичного захисту для запобігання пошкодженням на несанкціонованому доступу до обладнання та комунікацій;

5) впровадити заходи захисту, направлені на запобігання зовнішнім та екологічним загрозам, заснованим на результатах оцінки відповідних ризиків;

6) забезпечити належну та регулярну роботу з безперервного надання хмарних послуг за рахунок планування розподілу та використання потенційно важливих ресурсів, таких як персонал та ІТ-ресурси;

7) забезпечити належну та регулярну роботу з безперервного надання хмарних послуг за рахунок постійного моніторингу та відстеження потужності таких важливих ресурсів, як персонал та ІТ-ресурси;

8) надавати можливість користувачам хмарних послуг здійснювати контроль та моніторинг призначених їм системних ресурсів;

9) визначити політику антивірусного захисту від зловмисного програмного забезпечення ІТ-обладнання, пов’язаного з хмарою;

10) впровадити політику антивірусного захисту від зловмисного програмного забезпечення з обов'язковим оновленням сигнатур та евристичних баз та автоматичним скануванням систем;

11) визначати порядок створення резервних копій та порядок відновлення даних, які гарантують доступність даних, для захисту їх конфіденційності та цілісності;

12) відстежувати виконання резервних копій;

13) проводити регулярне тестування засобів відновлення резервних копій;

14) забезпечити зберігання резервних копій у відповідному віддаленому місці;

15) реалізовувати політику та процедури, які регулюють реєстрацію та моніторинг подій на компонентах системи;

16) запровадити політику управління керівництвом похідних даних

надавача хмарних послуг в результаті взаємодії з хмарою користувача хмарних послуг;

17) вести та контролювати журнали подій, які можуть призвести до інцидентів безпеки;

18) забезпечити конфіденційність, цілісність та доступність даних реєстрації та журналу моніторингу;

19) забезпечити однозначну ідентифікацію доступу користувачів хмарних послуг на рівні користувачів хмарних послуг;

20) обмежити доступ до компонентів системи реєстрації та моніторингу;

21) здійснювати самоконтроль для систем реєстрації та моніторингу;

22) встановити політику та процедури управління вразливостями у системних компонентах, що використовуються для надання хмарних послуг;

23) вести онлайн-реєстр вразливостей, які впливають на хмарний сервіс;

24) проводити ідентифікацію вразливостей за рахунок регулярного тестування системних компонентів, що використовуються для надання хмарних послуг;

25) вдосконалювати та регулярно оцінювати заходи обробки вразливостей та врегулювання інцидентів;

26) затверджувати всі системні компоненти для усунення потенційних векторів атаки;

27) відокремлювати бази даних в хмарній інфраструктурі;

28) необхідно, щоб CSP впровадив технічні заходи, які мають базуватися на результатах аналізу ризиків, задля виявлення та протидії фізичним чи віртуальним атакам на мережу, використовуючи різні технології на своїх технічних запобіжних заходах, та повідомляти в систему SIEM всі дані з технічних гарантій, реалізованих таким чином, щоб ініціювалися автоматичні контрзаходи щодо корелюючих подій;

29) CSP має документувати, передавати інформацію, робити доступними та реалізовувати вимоги безпеки до підключення в мережі, враховуючи принаймні необхідність відокремлювати зони безпеки, трафік даних для адміністрування та моніторингу; дозволи на міжлокаційну комунікацію та зв’язок між мережами;

30) необхідно запровадити моніторинг підключень у мережі CSP, за якого розрізняють довірені та ненадійні мережі на основі оцінки ризику, розділяють їх на різні зони безпеки та відповідно до визначених вимог безпеки, налаштовують фізичне та віртуальне середовища; CSP повинен захищати всі журнали SIEM, проводити оцінку ризиків виявлених вразливих місць, сканування служб, протоколів та портів з визначеним інтервалом часу, а також принаймні раз на рік переглядати конфігурації моніторингу;

31) міжмережевий доступ повинен контролюватися шлюзами безпеки на кожному периметрі мережі на основі вимог користувачів хмарних послуг та оцінки безпеки, CSP повинен автоматично моніторити контроль периметрів мережі;

32) CSP повинен визначити та впровадити окремі мережі (фізично або логічно відокремлені) для адміністративного управління інфраструктурою та функціонування консолей управління, а також ті, що використовуються для переміщення або створення віртуальних машин; Якщо такої можливості немає, то адміністративні потоки повинні передаватися в суворо зашифрованому каналі з наявністю встановленого та налаштованого брандмауера для захисту інтерфейсів адміністрування, призначених для CSC та доступних у електронній комунікаційній мережі загального користування;

33) CSP повинен визначити, задокументувати та впровадити механізми розмежування на рівні мережі трафіка даних різних користувачів хмарних послуг, які під час реалізації використовують фізично відокремлені мережі або суворо зашифровані VLAN;

34) CSP повинен проводити своєчасне документування обладнання та серверів, логічної структури мережі, розподілу зон та географічного положення місць мережі та здійснювати повний огляд документації топології мережі щонайменше раз на рік;

35) при використанні програмно визначеної мережі CSP повинен забезпечити конфіденційність даних користувачів хмарних послуг, перевіряти функціональність функцій SDN перед наданням нових функцій SDN CSC або зміною існуючих функцій SDN, а також забезпечити, щоб конфігурація мереж відповідала політиці безпеки мережі;

36) CSP документує, повідомляє та впроваджує політику та процедури передачі даних, які містять посилання на класифікацію активів, з урахуванням захисту від несанкціонованого перехоплення, маніпулювання, копіювання, модифікації, перенаправлення або знищення.

5. Управління ідентифікацією, автентифікацією та заходами криптографічного захисту в технології хмарних обчислень:

1) необхідно забезпечити лише авторизований доступ до інформації;

2) впровадити політику управління обліковими записами користувачів хмарних послуг, яка б включала в себе положення щодо обов’язків управління, процедур блокування та скасування, вимог щодо документування;

3) забезпечити, щоб процедури блокування, розблокування та ануляції облікових записів відповідали положенням концепції безпеки інформації;

4) забезпечити своєчасне оновлення прав, наданих обліковим записам, при зміні статусу відповідного запису;

5) організувати регулярний перегляд прав доступу відповідно до актуального рівня ризиків;

6) додатково перевіряти облікові записи, яким надані привілейовані права доступу на предмет актуальності та необхідності;

7) упровадження механізмів автентифікації для надання доступу залежно від рівня доступу та актуального аналізу ризиків;

8) зберігати та обробляти облікові дані автентифікації для підтримки

гарантій проходження користувачами хмарних послуг автентифікації;

9) забезпечити розмежування доступу між різними категоріями активів;

10) політики для шифрування та управління ключами мають бути реалізовані з технічними та організаційними гарантіями для шифрування; криптографічна політика та процедури повинні відповідати найсучаснішим технологіям та базуватися на оцінці ризику;

11) CSP повинен визначити та впровадити надійні механізми шифрування для передачі всіх даних, а особливо даних користувачів хмарних послуг, через електронні комунікаційні мережі загального користування;

12) CSP повинен встановити процедури щодо зберігання даних користувачів хмарних послуг через документування та впровадження процедур і технічних запобіжних заходів для шифрування даних користувачів хмарних послуг під час зберігання, включаючи політику персоналізації та використання особистих та секретних ключів користувачів хмарних послуг;

13) мають бути встановлені процедури та технічні гарантії для безпечного управління ключами в зоні відповідальності CSP. Система управління ключами повинна бути ізольована від програмних рівнів та встановлено політику щодо безпечного зберігання ключів та інших таємниць, що використовуються для адміністрування.

6. Управління конфігураціями в технології хмарних обчислень:

1) CSP повинен документувати, впроваджувати та передавати політику та процедури управління змінами ІТ-систем, що підтримують хмарний сервіс з урахуванням визначених аспектів управління змінами;

2) CSP проводить класифікацію та визначає пріоритетність змін, базуючись на оцінці ризику, щодо потенційного впливу на відповідні компоненти системи, вживає відповідних заходів щодо пом’якшення наслідків, якщо ризик високий, та надає уповноваженим органам CSC значущу інформацію про зміни;

3) CSP проводить кваліфікованими працівниками або автоматизованими процедурами тестування запропонованих змін перед розгортанням з урахуванням збереження конфіденційності даних користувача хмарних послуг протягом усього процесу. Необхідно дотримуватися процедури тестування та відповідно до ступеня серйозності помилок та вразливостей ініціювати дії щодо своєчасного виправлення або їх пом'якшення;

4) перш ніж зміни стануть доступними CSC у виробничому середовищі CSP їх затверджує на основі визначених критеріїв із залученням CSC до процесу затвердження відповідно до вимог договору;

5) для моніторингу змін виконуються розподіл ролей та прав серед уповноваженого персоналу або компонентів системи, реєстрація всіх змін з можливістю відстеження ініціатора зміни, а також автоматичний контроль зміни у виробничому середовищі;

6) CSP повинен впровадити процедури контролю версій для відстеження

залежностей окремих змін та відновлення уражених компонентів системи до попереднього стану в результаті помилок або виявлених вразливостей зі збереженням конфіденційності, цілісності та доступності даних користувачів хмарних послуг;

7) CSP розробляє та документує політику та процедури розвитку хмари з урахуванням безпеки з найперших етапів проєктування, базуючись на визнаних стандартах, методах та керівних принципах, включаючи автоматизовані засоби;

8) для розробки безпечного ланцюга постачання CSP повинен вести перелік залежностей від апаратних та програмних продуктів, задокументувати та впровадити політику щодо використання сторонніх програм та програм з відкритим кодом, надавати користувачам хмарних послуг свій список залежностей за запитом та проводити оцінку ризику під час закупівель;

9) CSP повинен забезпечити належний захист конфіденційності та цілісності вихідного коду на всіх стадіях розробки, вести контроль версій, впровадити безпечне середовище розробки та тестування і включати амортизаційні ресурси як частину політики резервного копіювання;

10) CSP повинен забезпечити відокремлення виробничих середовищ (фізично або логічно) від середовищ розробки, випробувань або попереднього виробництва та захист конфіденційності даних, що містяться у виробничих середовищах; коли невиробничі середовища діють через загальнодоступні мережі, вимоги до безпеки повинні бути еквівалентними тим, які визначені для виробничого середовища;

11) розробка особливостей безпеки враховує документування підвищених вимог для тестування та проєктну документацію для функцій захисту, а також необхідність документування процесу та результатів випробувань;

12) CSP застосовує відповідні процедури для перевірки хмари на наявність вразливостей, які інтегровані в процес розробки та містять види діяльності, залежно від оцінки ризику; CSP регулярно проводить перевірку коду, оцінку ступеня серйозності виявлених вразливостей та щорічні огляди коду та тести на проникнення експертами з предметних питань;

13) при передачі підряднику розробки хмари або її компонентів, CSP та підрядник повинні домовитися про підписання договорів щодо специфікацій з регулювання безпеки та недотримання існування відомих вразливих місць. Перед наданням субпідряду на розробку хмарного сервісу або його компонентів CSP повинен провести оцінку ризику з урахуванням встановлених аспектів. CSP проводить документування нагляду та контролю за сторонніми розробниками та тестування розробленого підрядником проєкту;

14) використовувати механізми обробки помилок та механізми входу при доступі до інформації про хмари;

15) управління сесіями має відповідати найсучаснішому рівню техніки та містити механізми реагування на період бездіяльності;

16) використовувати мережу передачі даних, у якій рівень управління мережею віддалений від пристроїв передачі даних і реалізований програмно;

17) забезпечити заходи захисту для хмарних послуг з надання та управління віртуальними машинами та контейнерами;

18) місця обробки і зберігання даних повинні обиратися користувачем хмарних послуг та надаватися CSP.

7. Правила реагування на інциденти при забезпеченні безперервності в технології хмарних обчислень:

1) визначити політику для реагування на інциденти безпеки, у тому числі їх документування, збір даних, аналіз типових випадків та тестування;

2) забезпечувати ефективну та впорядковану обробку випадків безпеки;

3) задокументувати усі випадки інцидентів безпеки та надавати користувачам хмарних послуг інформацію про них;

4) повідомляти користувачів хмарних послуг про вразливості системи, пов’язані із зареєстрованими інцидентами безпеки;

5) інформувати користувачів хмарних послуг про стан та вжиті дії щодо інциденту безпеки;

6) проводити аналіз інцидентів безпеки, визначити, впровадити та підтримувати сховище інформації про інциденти безпеки та заходи, вжиті для їх вирішення;

7) проводити захист інформації, пов’язаної з інцидентами в галузі безпеки, та вимагати проведення додаткової експертизи інцидентів безпеки;

8) встановити безперервність надання хмарних послуг з визначенням керівника та відповідальних осіб за забезпечення безперервності бізнесу;

9) запровадити процедури визначення наслідків будь-якої несправності або переривання роботи хмари;

10) створити систему безперервності надання хмарних послуг, включаючи відповідні плани на випадок непередбачених ситуацій;

11) вести регулярні перевірки та тестування системи безперервності надання хмарних послуг;

12) визначити варіанти використання способів боротьби із загрозами кіберзахисту при хмарних обчисленнях, які ще не виникли;

13) квантову загрозу кіберзахисту необхідно пом’якшувати шляхом розгортання в хмарних обчисленнях нових криптографічних інструментів, які є стійкими до квантових та класичних атак тощо. Якщо термін загрози більший за суму терміну зберігання та часу міграції постквантової криптографії, то організації повинні захистити свої хмарні активи протягом необхідних років від квантових атак;

14) забезпечувати ідентифікацію та документування хмарних інформаційних активів та їх поточний криптографічний захист від існуючих та потенційних класичних та квантових атак;

15) визначити суб'єктів загрози та провести оцінку їх часу для технології

хмарних обчислень, необхідного для отримання доступу до квантової технології;

16) визначити час існування активів технології хмарних обчислень і час, необхідний для перетворення технічної інфраструктури хмари в квантово-безпечний стан;

17) визначити значення квантового ризику за допомогою обчислення, чи стануть активи вразливими перш, ніж хмара зможе їх захистити;

18) визначити та розставити пріоритети заходів, необхідних для підтримки обізнаності та переведення технологій хмарних обчислень організації в квантово-безпечний стан;

19) обґрунтувати, розробити та застосувати варіанти захисту від квантових загроз технології хмарним обчисленням на цей момент часу;

20) проводити внутрішній та зовнішній аудит системи внутрішнього контролю стану використання для технології хмарних обчислень стандартизованих криптографічних перетворень та криптографічних протоколів;

21) квантова оцінка ризику має забезпечувати організацію знаннями, необхідними для розуміння ступеня їх квантового ризику кіберзахисту та термінів, за яких можуть виникнути квантові загрози; це забезпечить організацію основою для проактивного вирішення квантових ризиків, побудови шляху до квантово-безпечного стану, а також для впровадження та підтвердження квантово-безпечних рішень;

22) оцінювати основні переваги та недоліки фізичних реалізацій квантових комп’ютерів при їх застосуванні для технології хмарних обчислень, тобто масштабованість, сумісність з різними обчислювальними моделями, типовий час декогерентності, швидкість і точність, з якою вентилі можуть бути застосовані, тощо;

23) проводити квантову оцінку ризику як ідеальний підхід для виявлення та визначення пріоритетів загроз і вразливостей, а також закладання основи для надійного та економічно ефективного розвитку хмари та технологій, щоб вони були стійкими до квантових атак;

24) квантова оцінка ризику не повинна замінювати звичайну оцінку системи внутрішнього контролю, для чого необхідно:

проводити квантову оцінку ризику як частину регулярного процесу оцінки ризику або після нього;

зрозуміти позицію надавачів електронних комунікаційних мереж та/або послуг та безпеки щодо квантових обчислень, на які з їхніх продуктів це вплине, а також про те, як вони підготуються до управління цим ризиком;

оцінити квантову готовність як частину поточних процесів закупівлі мереж і систем безпеки, обговорити стан квантового планування поточних надавачів;

співпрацювати з інформованим партнером, щоб відстежувати розвиток квантових обчислень і квантово-безпечних рішень, а також створити план квантової готовності для організації.

8. Запити від державних органів щодо розслідувань в технології хмарних обчислень:

1) необхідність оцінювання інциденту правоохоронними органами перед розслідуванням експертами у предметній галузі;

2) інформувати користувачів хмарних послуг про розкриття даних при поточному розслідуванні;

3) забезпечення анонімності та автоматичного контролю доступу до даних користувачів хмарних послуг з боку CSP при запитах правоохоронних органів.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв'язку
лейтенант Ігор МАЛЬЧЕНЮК