ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ В ДАТА-ЦЕНТРІ»

Виконав студент 6 курсу, групи БСДМ-51
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Андросов М.О.
(прізвище та ініціали)
Керівник Дмітрієв В.Є.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ
СТУДЕНТУ

Андросову Максиму Олексійовичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія захисту конфіденційних даних в дата-центрі»

керівник магістерської роботи Дмітрієв Віталій Євгенійович, ст. викладач
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
Законодавство украхни з захисту ;
кофіденційних даних
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту конфіденційних даних.
2.Вимоги до захисту даних в дата-центрах.
3. Прикладні стандарти захисту даних в дата-центрах.

5. Перелік графічного матеріалу
1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Основні положення про захист конфіденційної інформації.

4. Основні вимоги до дата-центрів.

5.Приклад реалізації захишеного дата-центру.

7. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту кофіденційних даних в дата-центрах.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	30.09.2022 р.	
3.	Аналіз положень про захист кофіденційних даних.	10.10.2022 р.	
4.	Аналіз параметрівзахисту дата-центрів.	10.11.2022 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	14.11.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Андросов М.О.
(підпис) прізвище та ініціали

Керівник магістерської роботи Дмітієв В.Є.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Андросов М.О. до захисту магістерської роботи
(прізвище та ініціали)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «технологія захисту конфіденційних даних в дата-центрі».

Магістерська робота і рецензія додаються.

Директор інституту _____ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Андросов М.О. за період навчання в інституті
(прізвище та ініціали студента)

ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Бреславська Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Андросов М.О.*** обрав тему роботи, метою якої було аналіз і дослідження вимог до захисту конфіденційних даних. Вимог що висуваються до дата-центрів в яких планується здійснюватись обробка конфіденційних даних. Також розглянути можливість покращення технології захисту. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Андросов М.О. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Андросова Максима Олексійовича на оцінку **«відмінно»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Дмітієв В.Є.
(підпис) (прізвище та ініціали)

“____” _____ 2022 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Андросов М.О.
(прізвище та ініціали)

допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Андросова Максима Олексыйовича 1
на тему: «Технологія захисту конфіденційних даних в дата-центрі»

Актуальність:
Сьогодні більшість сервісів і служб переходять на хостинг до дата-центрів. Дата-центри акумулюють в собі системи що являються бізнесом, та державні системи. Більшість систем обробляють персональні дані та іншу інформацію що підпадає під категорію конфіденційної. Тому робота, присвячена дослідженню та реалізації технологій захисту конфіденційних даних в дата-центрах, є актуальною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст актуальності проблеми безпеки інформації в дата-центрах.
2. Досліджено впливхарактеру інформації та режимів доступності дата центрів їх побудову.
3. Запропоновано модель побудови захищеного дата-центру на основі законодавчих актів і світових рекомендацій.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У магістерській роботі бажано було бнавести конкретні приклади побудованих дата-центрів, та провести аналіз їх надійності.
2. Доцільним будо-б показати визначені технічні і програмні рішення для дата-центрів.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку «**відмінно»**, а студент **Андросов Максим Олексійович** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека..

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

_____

РЕФЕРАТ

Текстова частина магістерської роботи: 80 сторінок, 4 таблиці, 5 рисунків, 31 джерело.

Об'єкт дослідження – дослідження загроз для дата-центрів.

Предмет дослідження – стандарти побудови системи технології захисту даних в дата-центрах.

Мета роботи – розробити варіант захищеного дата-центру поєднуючі стандарти і правила що використовуються у світі.

Мета дослідження – створення технології захисту конфіденційних даних в дата-центрах.

Для досягнення мети в роботі вирішені наступні завдання:

– дослідження законодавчої бази України в питанні захисту конфіденційних даних;

– дослідження світових тенденцій і Українських стандартів побудови системи захисту в дата-центрах;

– розроблений технології побудови захисту даних в дата-центрах що базується на стандартах України і світу.

В першому розділі розглянута законодавча база захисту конфіденційної інформації, та захист даних на обєктах ОКІ, до яких входять дата-центри в якиїх оброблються персональні дані.

В другому розділі розглядаються основні вимоги до дата-центрів для побудови відказостійкого ЦОДу.

В третьому розглядається технологія захисту інформації в дата-центрі та необхідність висування рекомендацій до побудови системи безпеки на основі світових стандартів.

КОНФІДЕНЦІЙНІ ДАНІ, ДАТА-ЦЕНТР, TIA, ISO/IEC, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ВІДКАЗОСТІЙКІСТЬ, БУДІВЛІ ДЛЯ РОЗМІЩЕННЯ

ДАТА-ЦЕНТРІВ

ABSTRACT

The text part of the master's thesis: 80 pages, 4 tables, 5 figures, 31 sources.

The object of the study is the study of threats to data centers.

The subject of the study is the standards for building a data protection technology system in data centers.

The goal of the work is to develop a version of the protected data center combining the standards and rules used in the world.

The purpose of the study is to create a technology for protecting confidential data in data centers.

To achieve the goal, the following tasks are written:

– research of the legislative framework of Ukraine in the matter of protection of confidential data;
– study of global trends and Ukrainian standards for building a protection system in data centers;
– developed technologies for building data protection in data centers based on Ukrainian and world standards.

In the first part, the legislative framework for the protection of confidential information and data protection at OKI facilities, which include data centers where personal data are processed, were reviewed.

In the second section, the current requirements for data centers for the construction of a fault-tolerant data center are considered.

In the third chapter, information protection technology in the data center and the need to put forward recommendations for the construction of a security system based on world standards are considered.

CONFIDENTIAL DATA, DATA CENTER, TIA, ISO/IEC, THREAT MODEL, ATTACKER MODEL, LIABILITY RESILIENCE, HOUSING BUILDINGS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 9
ВСТУП 9
1 ЗАКОНОДАВЧА СКЛАДОВА ВИМОГ ДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ 12
1.1 Нормативно-правова база в сфері захисту інформації 12
1.2 Захист ПД на ОКІ України 17
Висновки до розділу 25
2 ВИМОГИ І ПРАВИЛА ДО ДАТА-ЦЕНТРІВ 26
2.1 Поняття та задічі дата-центру 26
2.2 Стандарти побудови дата центрів 28
Висновки до розділу 35
3 ПРИКЛАД ПОБУДОВИ ДАТА-ЦЕНТАР 36
3.1 Структура дата-центра 36
3.2 Резервування дата-центрів 42
3.3 Модель порушника для Дата-центру 44
3.4 Модель загроз відносно хмарних сервісів 51
3.4 Профіль захищеності дата-центру 66
Висновок до розділу 73
ВИСНОВКИ 75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 76
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 80

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДІР – державні інформаційні ресурси;

ЗУ – Закон України;

ІТ – інформаційні технології;

ІКС – інформаційно-комунікаційна система;

КЗІ – криптографічний захист інформації;

КЗЗ – криптографічний засобів захисту;

КСЗІ – комплексна система захисту інформації;

ОКІ – об’єкт критичної інфраструктури;

ОС – операційна система;

ПЗ – програмне забезпечення ;

ТЗІ – технічний захист інформації;

ШПЗ – шкідливе програмне забезпечення;

ЦОД – центр обробки даних;

ДПП – державно-приватне партнерство;

ЛОС – локальна обчислювальна мережа;

МСЗД – мережа і система збереження даних;

KVM – Kernel -based Virtual Machine Середовище віртуалізації на ядрі Kernel;

IPS (англ. Intrusion Prevention System) - система запобігання вторгненням;

TR – апаратна система зв’язку;

DDoS (англ. Distributed Denial of Service) - Розподілена відмова в обслуговуванні;

ВСТУП

Актуальність дослідження. На даний момент в Україні надзвичайно широко використовуються дата-центри. Більшість державних і комерційних технічних інфроструктур здійснюють перехід до дата-центрів що зумовлене зручним корисуванням і зменшенням витрат на систему.

Оскільки рівень попит на розміщення сервісів в дата-центрах продовжить зростати і в подальшому необхідно усвідомлючати як правильно будувати систему захисту та відказостійкості для різних рівнів дата-центрів.

Об'єкт дослідження – дослідження властивостей захисту даних в дата-центрі.

Предмет дослідження – параметри якими повинен володіти дата-центр.

Мета роботи – даної дипломної роботи є створення технології захисту конфіденційних даних в дата-центрі.

Наукові завдання:

– досліджені нормативні асекти ї та складові частини захисту конфіденційної інформації(даних) в державі (РОЗДІЛ 1);

– досліджені основні вимоги при побудові дата-центрів для забезпечення захисту даних і вдказостійкості (РОЗДІЛ 2);

– розроблений технологія захисту в дата-центрі (РОЗДІЛ 3).

При написанні роботи використовувалися стандарти і рекомендації з побудови захищених систем і дата центрів Украхни і сміту.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в створення технології і побудови дата-центру що буде спроможній на захищати конфіденційні дані в різних умовах.

Апробація результатів. магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 ЗАКОНОДАВЧА СКЛАДОВА ВИМОГ ДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Нормативно-правова база в сфері захисту інформації

Законодавча складова завжди буде важливим елементом у врегулюванні питання необхідності захисту персональних даних та визначенні вимог до розпорядників персональних даних порядку захисту цих даних. Оскільки законодавча складова є без сумніву важлива, варто прийти розуміння, навіщо охороняти персональні данні.

Відповідно до ЗУ «Про захист персональних даних» [16] від 01.06.2010 № 2297-VI (у редації від 27.10.2022):

персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Відповідно до статті 24 цього Закону забезпечення захисту персональних даних у базах персональних даних:

Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від незаконної обробки, а також від незаконного доступу до них.

Забезпечення захисту персональних даних у базі персональних даних покладається на володільця цієї бази.

Володілець бази персональних даних в електронній формі забезпечує її захист відповідно до закону.

Відповідно до ЗУ «Про інформацію» [13] від 02.10.1992 № 2657-XII (у редації від 20.11.2022) що регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації:

захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та

належний порядок доступу до неї;

порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

Спираючись на Статтю 21. Інформація з обмеженим доступом.

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

Відповідно до Статті 1 : захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Розглядаючи питання захисту персональних даних, до цілей якого входить забезпечення інформаційної безпеки на ОКІ та зменшення ризиків і загроз щодо інформації, що обробляється, доцільно зазначити нормативно-правові засади забезпечення інформаційної безпеки передбачені Конституцією України, Законами України, Постановами Кабінету Міністрів України та іншими нормативно-правовими актами, що регулюють обіг інформації та її захист в цілому в державі.

Згідно з статтею 17 **Конституції України** [12]:

Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Згідно з **ЗУ "Про захист інформації в інформаційно-комунікаційних**

системах” від 5 липня 1994 року № 80/94-ВР [14] (у редакції 01.07.2022), що відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах:

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Відповідно до статті 9 (Забезпечення захисту інформації в системі):

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Згідно з Указом Президента України **“Про Положення про технічний захист інформації в Україні”** від 27 вересня 1999 року № 1229/99 (у редакції 04 травня 2008) [15]:

Технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій.

Нормативно-правові акти з технічного захисту інформації є обов'язковими для виконання всіма суб'єктами системи технічного захисту інформації.

Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

видання у межах своїх повноважень нормативно-правових актів із зазначених питань;

здійснення контролю за станом технічного захисту інформації.

Згідно з постановою Кабінету Міністрів України “Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах” від 29 березня 2006 р. № 373[18] захисту в ІКС підлягає:

відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація)

конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації” (2939-17) (далі - конфіденційна інформація);

службова інформація;

інформація, яка становить державну або іншу передбачену законом таємницю;

інформація, вимога щодо захисту якої встановлена законом.

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

У системі здійснюється обов'язкова реєстрація:

результатів ідентифікації та автентифікації користувачів;

результатів виконання користувачем операцій з обробки інформації;

спроб несанкціонованих дій з інформацією;

фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

результатів перевірки цілісності засобів захисту інформації.

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації.

Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі - система захисту), яка призначається для захисту інформації від:

несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

Захист інформації від несанкціонованих дій у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

1.2 Захист ПД на ОКІ України

Рішенням РНБО України від 29 грудня 2016 р. [17], Кабінету Міністрів України було доручено врегулювати питання щодо заборони державним органам, підприємствам, установам і організаціям державної форми власності закуповувати послуги (укладати договори) з доступу до мережі Інтернет у операторів (провайдерів) телекомунікацій та роботи з дата-центрами, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації. Відповідне рішення до цього часу не втілилося в окремий нормативно-правовий акт, оскільки суб’єкти ринку Інтернет-послуг та їх об’єднання блокують його прийняття на стадії громадського обговорення. Однак, з 2018 року оператори (провайдери) телекомунікацій та дата-центри отримують в Держспецзв’язку України атестати відповідності щодо забезпечення захисту інформації згідно з вимогами нормативних документів системи технічного захисту інформації в Україні, які дозволяють їм надавати послуги з доступу до мережі Інтернет та розміщення державних в дата-центрах державних ресурсів – “Захищений вузол Інтернет-доступу” – державним органам, підприємствам, установам і організаціям державної форми власності.

Основа нормативно-правової бази у сфері організації забезпечення безпеки об'єктів критичної інфраструктури складається з:

– Кодексу цивільного захисту України, Кримінального кодексу України;

– Законів України “Про національну безпеку України”, “Про боротьбу з тероризмом”, “Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання”, “Про об’єкти підвищеної небезпеки”, “Про основні засади забезпечення кібербезпеки України”, “Про правовий режим надзвичайного стану”, “Про правовий режим воєнного стану”,

– Указу Президента України від 16 січня 2017 року № 8 “Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури”, Указу Президента України від 26 травня 2015 року № 287 “Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України”, Указом Президента України від 15 березня 2016 року № 96 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”, резолюцією Ради безпеки Організації об'єднаних націй від 13 лютого 2017 року № 2341 щодо захисту критичної інфраструктури від терористичних атак;

– розпорядження Кабінету Міністрів України від 06.12.2017 № 1009 “Про схвалення Концепції створення державної системи захисту критичної інфраструктури”;

– Порядок формування переліку об’єктів критичної інформаційної інфраструктури (постанова Кабінету Міністрів України від 09.10.2020 № 943);

– Порядок внесення об’єктів критичної інформаційної інфраструктури до державного реєстру об’єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування (постанова Кабінету Міністрів України від 09.10.2020 № 943);

– Порядок віднесення об’єктів до об’єктів критичної інфраструктури (постанова Кабінету Міністрів України від 09.10.2020 № 1109); Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави (постанова

Кабінету Міністрів України від 09.10.2020 № 1109);

– Методика категоризації об’єктів критичної інфраструктури (постанова Кабінету Міністрів України від 09.10.2020 № 1109);

– постанова Кабінету Міністрів України від 23 грудня 2020 р. № 1295 “Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки”.

Найбільш універсальне визначення інформаційного ресурсу міститься в Законі України “Про національну програму інформатизації”[19].

Згідно зі ст. 1 Закону, інформаційний ресурс – це сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо).

Проте наведене поняття не враховує ознак, що перетворюють інформацію на ресурс, який включає такі складові характеристики: “інформація”, “інформаційний ресурс” як предмет і результат діяльності людини, як об’єкт права власності фізичних, юридичних осіб та держави, як об’єкт товарних відносин, як державний і національний ресурс. Крім того, важливими ознаками інформаційного ресурсу є те, що він може бути системоутворювальним і керованим чинником діяльності людини, суспільства і держави, позитивно впливати на соціально-економічний розвиток суспільства і держави та забезпечення національної безпеки. У разі браку цього ресурсу, низької його якості або негативної інформаційної експансії з боку інших країн завдавати шкоди суспільному життю; бути об’єктом кримінальних зазіхань і спеціальних заходів і засобів захисту; мати якості та ознаки, притаманні іншим ресурсам.

Державні інформаційні ресурси – це систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб’єктами владних повноважень.

Державні інформаційні ресурси є складовою національних інформаційних

ресурсів та мають споживчу цінність, а саме: політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо. Будь який суб'єкт інформаційних відносин України, має право доступу до державних інформаційних ресурсів згідно визначеної політики безпеки та чинного законодавства.

У Законі України "Про інформацію" [20] встановлено, що підставами виникнення права власності на інформацію можуть бути: створення інформації своїми силами і за свій рахунок; договір на створення інформації; договір, що містить умови переходу права власності на інформацію до іншої особи. Інформація, створена на кошти державного бюджету, є державною власністю.

Особливо важливим є визначення підстав для віднесення інформаційних ресурсів до категорії державних. Правова норма про те, що інформація, яка створена на кошти державного бюджету, є державною власністю, не є вичерпною. Отже, до державних інформаційних ресурсів доцільно було б відносити інформаційні ресурси створені, придбані, накопичені за рахунок коштів державного бюджету, позабюджетних державних фондів та платників податків. Як наслідок, бачимо, що державні інформаційні ресурси – це ресурси, які як елемент майна перебувають у власності держави. Державні інформаційні ресурси забезпечують виконання завдань державного управління; забезпечення прав та безпеки громадян; підтримки соціально-економічного розвитку країни, розвитку культури, науки, освіти, тощо.

Державні інформаційні ресурси [21]– це результати інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані і систематизовані на відповідних матеріальних носіях інформації, як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси, які обробляються й передаються у інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості і знання, які є об'єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і

задоволення потреб громадян, суспільства, держави та підлягають захисту згідно визначеної політики безпеки й чинного законодавства.

Державні інформаційні ресурси можуть бути розділені на дві групи[22]:

а) інформаційні ресурси, призначені для вирішення завдань конкретного органу управління певної ланки;

б) інформаційні ресурси, орієнтовані на зовнішнього користувача.

Останні формуються інформаційно-аналітичними структурами. Якщо вони мають загальне методичне керівництво, схожі завдання, які вирішуються на основі єдиних нормативних документів, то вони можуть бути названі державними інформаційними системами. До державних інформаційних ресурсів висуваються вимоги щодо актуальності та достовірності наведених у них даних; вичерпної повноти інформаційних джерел; компактності викладу; оперативності пошуку. Державні інформаційні ресурси мають типову структуру: обов'язкову – основну частину і вихідні дані та факультативну – довідково-бібліографічний апарат і додаткову інформацію.

В умовах впровадження електронного урядування надзвичайної ваги набувають державні електронні інформаційні ресурси. Першочерговими завданнями щодо державних електронних інформаційних ресурсів є [23]:

створення та ведення Національного реєстру електронних інформаційних ресурсів, зокрема реєстрація та облік державних електронних інформаційних ресурсів, формування і забезпечення доступності інформації про склад, розміщення і умови використання електронних інформаційних ресурсів;

систематизація, забезпечення доступу до наявних державних електронних інформаційних ресурсів та їх актуалізація;

формування та забезпечення ефективного використання державних електронних інформаційних ресурсів органами державної влади; вдосконалення нормативно-правової бази, зокрема визначення порядку і умов користування, оплати робіт, пов'язаних з формуванням, використанням та захистом державних електронних інформаційних ресурсів;

координація діяльності органів державної влади та підприємництва

(бізнесу) у сфері формування, використання та захисту державних електронних інформаційних ресурсів.

Встановлено правові та організаційні засади проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України [24], підприємств, установ і організацій незалежно від форм власності. Під оцінкою (оцінюванням) стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах розглядається сукупність заходів, спрямованих на виявлення загроз державним інформаційним ресурсам та запобігання несанкціонованим діям щодо інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Дані [25] напрацювання із сфери теоретичного обґрунтування інформаційних процесів поступово входять і в сферу методики організації сучасної інформаційної діяльності, і в сферу законотворчості, в практику формування системи інформаційного права, важливість і актуальність якої на етапі входження нашого суспільства в інформаційний етап розвитку важко переоцінити. Інформаційна основа діяльності в усіх сферах життя суспільства є фундаментом, або стратегічним ресурсом, соціального розвитку й прогресу. За значущістю та специфічністю інформаційний ресурс перевищує всі інші, але, як і всі інші, має свій життєвий цикл: “добування – нагромадження – систематизація – зберігання – використання – нарощування”.

В умовах актуалізації кіберзагроз та перетворення кібератак на інструмент міждержавного протистояння, а також засіб реалізації гібридної агресії з боку Російської Федерації, перед нашою державою виникла нагальна потреба – забезпечити у контексті розбудови національної системи кібербезпеки належний захист інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури.

Вочевидь, одним із перших кроків у цьому напрямку визначається

розроблення переліку об’єктів, що належать до критичної інформаційної інфраструктури держави, організація та проведення оцінки стану їх захищеності. Саме такі завдання, виконання яких повинно було завершитись до кінця 2016 року, були поставлені Урядом перед Державною службою спеціального зв’язку та захисту інформації України відповідно до п. 4 Плану заходів щодо захисту державних інформаційних ресурсів, затвердженому розпорядженням Кабінету Міністрів України від 5.11.14 р. № 1135-р [26].

Однак, протягом 2014 – 2016 років ці завдання повною мірою реалізовані не були. Натомість, на виконання вказаного розпорядження, Держспецзв’язку[27] спільно із зацікавленими державними органами було розроблено Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави (далі – Порядок), який визначав механізм, за яким відбуватиметься формування переліку таких систем, та повинен був стати “вагомим кроком у напряму підвищення рівня захисту інформації, що обробляється в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури держави”.

Відповідно до чинного законодавства [28], об’єктами критичної інфраструктури є підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей.

На сьогодні єдиний перелік зазначених об’єктів в Україні відсутній [29], а захист об’єктів, які згідно із світовою практикою відносять до категорії “критичної інфраструктури” регламентується численними нормативно-правовими актами, що носять переважно відомчий характер.

Загрози критичній інфраструктурі, зазвичай, розподіляють на три групи, що

включають аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії) [30]. протидія кіберзагрозам та заходи з кіберзахисту ІКС об'єктів критичної інфраструктури повинні реалізовуватись, перш за все, у рамках комплексної системи захисту критичної інфраструктури держави як один із її елементів.

Наразі в країні відбувається активний процес розбудови такої системи. Згідно із Законом України "Про основні засади забезпечення кібербезпеки України", а також Концепцією створення державної системи захисту критичної інфраструктури, затвердженій розпорядженням Кабінету Міністрів України від 6.12.17 р. №1009-р [31], передбачено розроблення переліку об'єктів критичної інфраструктури, методології та визначення критеріїв віднесення таких об'єктів до критичної інфраструктури, порядку їх паспортизації та категоризації.

Таким чином, формування переліку об'єктів критичної інфраструктури держави є першочерговим кроком, необхідним для визначення інформаційно-телекомунікаційних систем таких об'єктів, які потребуватимуть пріоритетного захисту від кібератак.

Центральним компонентом у визначенні критичної інфраструктури є інформаційна складова. Тож поняття "критична інформаційна інфраструктура" не повинно включати лише ІКС об'єктів критичної інфраструктури, як це передбачено Законом України "Про основні засади забезпечення кібербезпеки України", відповідно до якого, "об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури".

Це поняття повинно охоплювати також інші інформаційні системи, зокрема, національні електронні інформаційні ресурси, кібератака на які може призвести до значних негативних наслідків та суттєвої шкоди життєво важливим інтересам держави. Наприклад, Єдині та державні реєстри, які за формальними ознаками не є інформаційно-телекомунікаційними системами об'єктів критичної

інфраструктури, водночас, з урахуванням потенційних негативних наслідків для держави, до яких може призвести протиправний кібервплив на такі ресурси, повинні належати до критичної інформаційної інфраструктури та забезпечуватись підвищеним рівнем кіберзахисту.

Висновки до розділу

Персональні данні подлягають захисто відповідно до Конституції України та іншим законодавчам актам.

Основними володільцями баз даних що містять персональні дані являються державні органи до яких чітко визначено порядок захисту персональних даних. В сучасних реаліях більшість державних органів переносять свої інфраструктури в дата-центри, до яких відповідно також державною висуваються вимоги до системи захисту. Це пов’язано не тільки із розв’язанням гібридної війни проти України, але й динамікою соціальних, економічних, політичних і навіть технологічних процесів, що відбуваються у світі. Світові тенденції до посилення загроз природного та техногенного характеру, підвищення рівня терористичних загроз, збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об’єктів у східних та південних регіонах України внаслідок збройної агресії Російської Федерації зумовили актуалізацію питання захисту систем, об’єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки.

З огляду на те, що дата центри об’єднують в собі денілдька державних інформаціних систем, вони підпадають під ОКІ що містьть державні інофрмаційні ресурси, до яких також висуваються вимоги до стійкості систем.

2 ВИМОГИ І ПРАВИЛА ДО ДАТА-ЦЕНТРІВ

2.1 Поняття та задічі дата-центру

Дата-центр - це спеціалізована будівля для розміщення серверного устаткування клієнта з метою забезпечення надійності та безперебійності його роботи. Але головна особливість такого приміщення полягає в інфраструктурі. Центром обробки даних не буде будь-яка серверна або склад зі стійками. Тож що таке надійний дата-центр? Він повинен бути обладнаний надійною і відмовостійкою інфраструктурою, яка складається з:

- системи безперебійного і гарантованого електропостачання;
- системи диспетчеризації та моніторінгу;
- структурованої кабельної мережі.

Саме злагоджена робота всіх складових інженерної системи, а також цілодобова технічна підтримка можуть гарантувати клієнтові безперебійність роботи розміщеного обладнання.

Використання технологій хмарних обчислень дозволяє досягти ряд переваг, основними з них є:

- гнучкість;
- обчислювальна потужність;
- великий обсяг файлового сховища;
- різноманітність програмного забезпечення;
- повсякчасна можливість доступу до ресурсів в хмарі;
- можливість швидкого розгортання сервісів;
- можливість збільшення навантаження в хмарі;
- простота масштабування, резервування та самовідновлення;
- можливість управління навантаженнями та здійснення моніторингу в реальному часі.

Класифікація дата-центрів

Існує кілька підходів до класифікації дата-центрів. Серед них - за розміром, надійністю, а також за призначенням. Розглянемо два перші види класифікації.

Виходячи з розмірів, виділяють такі дата-центри:

Великі. Повністю автономний ЦОД з власною будівлею. Відповідно до системи класифікації Data Center Institute, до найбільш великих відносяться ЦОД із загальною територією більше 22 501 м², а також понад 9 тис. серверних стійок на його території.

Найбільшим дата-центром в світі сьогодні вважається Lakeside Technology Center. Розташований він у центрі Чикаго і його загальна площа становить близько 102 тис. м²

Середні. До даної категорії відносяться дата-центри загальною площею 501 - 2 000 м², а також кількістю серверних стійок 201 - 800.

Малі. Дата-центри з площею до 500 м² та загальною кількістю серверних стійок порядка 11-200.

Модульні. Дата-центр, який складається з модульних блоків і легко масштабується від одного серверного залу до необмежених потреб, завдяки нарощуванню окремих блоків модулів.

Контейнерні. Дата-центр в основі побудови якого використовуються стандартні ISO контейнери (в середньому розмір їх дорівнює 20-40 футів), в яких безпосередньо розміщуються сервери. Їх перевагою є мобільність, адже вони легко перевозяться автомобільним або іншим видом транспорту.

Класифікація по надійності грунтується на систематизації за рівнями від Uptime Institute (показники TIER).

Виходячи з надійності виділяють 4 рівня дата-центрів:

TIER I гарантує відмовостійкість системи на рівні 99,671% (допустимий простий в рік 28,8 годин);

TIER II передбачає рівень доступності сервісу 99,749% (22 години простоїв на рік), а також передбачає дублювання активного обладнання (ІБП, кондиціонерів);

TIER III характеризується стійкістю до відмов на рівні 99,982% (1,6 годин простою в рік), наявністю повної схеми резервування системи кондиціонування, електроживлення та комунікації;

TIER IV (гарантує максимальну доступність сервісу - всього 0,4 години простою в рік).

2.2 Стандарти побудови дата центрів

TIA 942 – Telecommunications Industry Association – Telecommunications Infrastructure Standard for Data Centers**:**

Цей стандарт розроблений асоціацією телекомунікаційної промисловості США і, впершу чергу, стосується питань організації структурованих кабельних систем в ЦОД, і в меншій мірі питань відмовостійкості та інших інженерних підсистем.

Носить рекомендований характер.

Є пошагові інструкції та рекомендовані схеми (помощь інженеру). «Делай як тут написано і отримаєш хороший результат».

Відповідність стандарту заявляється власником об'єкта або виконавцем проекту (на рівні «Я робив, як ви сказали, чесне слово»).

Зазвичай, на відповідність стандарту перевіряється тільки проектна документація.

Один раз реалізований об'єкт не втрачає з часом рівня.

Урівні варіюються від I до IV

Принципово, і стандарту TIA 942, і методології Uptime Institute класифікація за рівнями однакова. Грубо описати їх можна так:

Tier I – без резервування. Наявність 99.671%.

Tier II – резервування критичних вузлів. Наявність 99.741%.

Tier III – резервування критичних вузлів, шляхів отримання

електроенергії та трас доставки холодоносія. При цьому є можливість виведення будь-якого вузла з експлуатації для його обслуговування із збереженням повної функціональності об'єкта загалом. Наявність 99.982%

Tier IV – це найбільш стійкий до відмов, де допускається одна аварія (а не плановий виведення вузла з експлуатації) в один момент часу. Як приклад аварії – критична людська помилка. По суті, це два Tier-другі, які побудовані в одній будівлі навколо серверних стійок. Доступність 99.995%, що забезпечує даунтайм лише 26 хвилин на рік.

Як приклад: якщо ми робимо систему з доставкою рідкого теплоносія по трубах, Tier III треба робити подвійне кільце, а Tier II можна обійтися одним. При цьому рівень резервування чилерів та фанкойлів може бути однаковим.

Те саме стосується електроживлення та інших систем. На рівні IV ще крутіше: наприклад, ДБЖ та траси харчування повинні бути не просто задубльовані, але ще й рознесені в різні приміщення: якщо перший блок вибухне (аварійний випадок, а не планова зупинка), то другий не повинен постраждати. Якщо прориває трубопровід у якомусь місці, це ніяк не впливає на електроніку, що дублює, – є фізичний поділ систем.

Якщо говорити простіше, то рівні виглядають так: перший працює і може відмовити, другий загалом нормально працює і витримує частину найпоширеніших відмов, третій виживає в будь-яких некритичних умовах, четвертий придатний для роботи у військових умовах.

При цьому для США вартість об'єкта коливається так: 30, 50, 65 і 100 тисяч доларів за стійку (це дуже приблизні цифри для оцінки співвідношення витрат між рівнями). В Україні, зазвичай, ще дорожче. Таким чином, якщо вибирати між Tier II та Tier III, бюджет збільшується не дуже суттєво, а ось аптайм – більш ніж. Але питання навіть не у витратах, а тому, наскільки правильно все спроектовано та захищено від експлуатаційних проблем на місці.

Навіщо ці стандарти потрібні?

Задумалися про стандарти класифікації дата-центрів ще на початку 90-х:

тоді в Uptime Institute почали прописувати на папері основні принципи будівництва стійких до відмов об'єктів.

Завданням Uptime Institute було вивчення методології будівництва безвідмовних високотехнологічних об'єктів та розслідування кожної проблеми, яка спричинила відмову в ЦОДі. На момент старту компанія мала задокументований досвід будівництва ЦОДів та їх «теплих лампових аналогів» ще з часів 70-х, причому ті обчислювальні центри були дуже масштабними і цілком стійкими до відмови. За цими центрами також була статистика основних проблем: починаючи від знаменитого метелика до різного роду дрібних ремонтів.

У результаті приблизно в 95-му році було запропоновано класифікацію ЦОД за рівнями, виходячи з їхньої відмовостійкості. Ця класифікація була запропонована для того, щоб замовники могли обирати ту інфраструктуру, яка відповідає їхнім потребам відповідно до завдання. Грубо кажучи, якщо замовник будує кол-центр, то йому не обов'язково думати про доступність у чотири дев'ятки (99,99% аптайму), а от якщо ЦОД, де крутяться системи, критичні для бізнесу банку, то так, тоді варто. Саме ця класифікація була врахована в першій редакції TIA 942. У 96-му році з'явився перший документ, що описує вимоги до інженерної інфраструктури обчислювальних центрів методології Uptime Institute.

Основні чотири рівні були введені на основі статистики відмов та досвіду організації. Рівень стійкості до відмови вказував можливий аптайм, причому без проміжних етапів: тобто ніяких II+ і III+ не було і немає – навіть якщо недотягнув через один не задубльований вентиль на не дуже важливій резервній системі до трійки – все одно присвоюється двійка. Власне, так надається рівень і зараз, тому слова про Tier II+ – це особиста фантазія власника, і вона не має відношення до самого стандарту.

Основні поняття, якими оперують документи – це резервування, можливість обслуговування вузлів без зупинки функціонування об'єкта загалом плюс стійкість до збоїв та аварій. При цьому постулюється ряд вельми

незвичайних для нашої реальності речей: наприклад, за стандартом Uptime вважається, що на рівнях I та II мережеве харчування від міської мережі може бути основним джерелом отримання електроенергії, а для рівнів III та IV – ні. Місто на цьому рівні стандарту раптово перестає бути надійним і розглядається лише як економічно ефективне додаткове джерело живлення. При цьому система ДГУ має забезпечувати роботу на повній потужності, без обмежень щодо тривалості.

Мета створення TIA – допомога інженерам-проектувальникам, щоб вони не вигадували щось своє, а проектували так, як запропоновано у стандарті, що враховує досвід створення багатьох великих об'єктів. Стандарт ілюструє та описує кращі техніки та рішення. Зі свого боку, Uptime фокусується на принципах, при реалізації яких можна досягти заданої стійкості до відмови.

Ось у чому різниця: TIA дуже детально показує, як потрібно організовувати структуровані кабельні системи, інформаційні зв'язки та іншу інженерку (що логічно, оскільки в цих речах підказки із best practice досить важливі).

При цьому Uptime не робить акценту на електроживленні, наприклад, а розглядає вплив усіх інженерних систем на відмовостійкість обладнання в ЦОД в цілому. Або ще (спростовуючи одну з найпоширеніших помилок): Uptime, насправді, ніяк не регламентує вибір майданчика.

Що підлягає захисту

Забезпечення інформаційної безпеки ЦОД є комплексом різних технічних заходів, які допомагають запобігти витоку даних і захистити файли від несанкціонованого доступу. І найбільш «захищеними» компонентами в цьому випадку є:

Ресурси (тобто, безпосередньо самі дані).

Дії зі збору, переробки, зберігання та подальшої передачі інформації.

Користувачі сервера.

IT-інфраструктура, включаючи всі технічні та програмні інструменти обробки.

Які фактори становлять загрозу

Складання політики безпеки інформації вимагає побудови особливої моделі загроз і порушників. Тобто необхідно скласти список факторів, які несуть загрозу для IT-інфраструктури та нормальної роботи ЦОД.

Загрозою для дата-центру можуть стати різні явища:

Природні лиха.

Порушення термінів постачання обладнання.

Терористичні акти.

Події техногенного чи соціального характеру.

Збої та відмови програмних та технічних засобів.

Внутрішні порушення ІБ співробітниками тощо.

Цей список можна продовжувати нескінченно, оскільки безпека ЦОДу порушується навіть при банальних перебоях в електроживленні.

Аналіз ризиків включає не просто виявлення можливих загроз, а й оцінку масштабів їх наслідків. Це допоможе скласти план дій для забезпечення ІБ, розподілити завдання по важливості та спланувати бюджет для купівлі необхідних технічних та програмних засобів.

ІБ організується з урахуванням вимог законодавчих стандартів, нормативних документів та інших регуляторів. Варто зазначити, що безпека не є додатковим джерелом доходу, а лише мінімізує ризики і дозволяє підвищити рівень обслуговування клієнтів.

Захист інженерних компонентів

Великий ризик для роботи ЦОД несуть перебої в електроживленні та можливі відмови системи охолодження. На щастя, такі загрози вдалося повністю нейтралізувати.

Відбувається це за рахунок впровадження «розумної» системи управління, яка поєднує в собі нові системи охолодження, вентиляції та електроживлення, суміщені з контролерами для цілодобового моніторингу.

Захист приміщення

Якщо в дата-центрі реалізується послуга оренди, то, крім інформаційної

безпеки, буде потрібний фізичний захист обладнання. Важливо запобігти несанкціонованому доступу до обладнання та захистити його від зовнішнього впливу.

Для цього застосовуються обгороджені частини приміщення, які обов'язково перебувають під постійним відеоспостереженням. Також організовується система пожежогасіння, яка самостійно активується у разі пожежі, що починається, і задимлення.

Зараз стали впроваджуватись і більш досконалі технології захисту. Наприклад, сервіс контролю та управління став повністю інтелектуальним, а сам доступ забезпечується під час сканування біометрії.

Додатковий захист від зовнішніх загроз (наприклад, від вибухів та пожеж у будівлі) забезпечують кімнати та сейфи безпеки. Вони серверне обладнання надійно захищене від будь-яких загрозливих чинників.

Людський фактор

Інформаційна безпека ЦОДів, що забезпечується різними датчиками стеження та розумним відеоспостереженням, на жаль, не дозволяє вирішити абсолютно всіх проблем. Головний фактор ризику залишається – це фахівці, які допущені до роботи в дата-центрі.

На функціонування центру обробки даних може спричинити нецільова експлуатація системи персоналом. Для запобігання подібним факторам використовуються спеціальні системи управління.

Додаткового захисту вимагає і сам персонал, оскільки саме працівники ЦОД є вразливим місцем у всій системі безпеки. На жаль, нерідкі випадки, коли злочинці починають використовувати способи соціальної інженерії. Мінімізація ризиків у разі відбувається з допомогою навчання персоналу навичкам ІБ.

Захист каналів передачі даних

Більшість дата-центрів сьогодні надають послуги не лише «колокейшну», а й оренди хмарних ресурсів. Отже, потрібно забезпечувати захист кількох каналів зв'язку.

Атаки на cloud-технології сьогодні відбуваються все частіше – майже 50%

ЦОДів стикаються з ними щороку. Небезпека DDoS-атак полягає у можливій установці вірусів-шифрувальників та блокуванні інфраструктури компанії.

Найчастішими є загрози злому, крадіжки чи видалення даних, що зберігаються на хмарних сервісах.

Захист інформації досягається за допомогою інструментів для виявлення та усунення шкідливого коду. Також багато ЦОД використовують системи з функціями IPS.

Багато російських data-центрів застосовують зовнішні додатки, що дозволяють перерозподіляти трафік на інші вузли, а потім проводити його фільтрацію в хмарі.

Захист віртуального середовища

Для підтримки безпеки ЦОД обов'язково враховується специфіка об'єкта, що захищається. Наприклад, ризики значно вищі при використанні віртуальних серверів. Через взаємопов'язану інфраструктуру завершена атака на одного з клієнтів може загрожувати безпеці його «сусідів».

Найчастіше використовуються автоматизовані засоби безпеки, оскільки вони дозволяють досягти масштабування всіх рівнях і автоматизувати контроль доступу. Застосовуються інструменти для фільтрації мережевого трафіку на декількох рівнях.

Потрібно усунути «сліпі зони» на ступені віртуалізації ресурсів, що використовуються, в іншому випадку комплексні заходи для ІБ можуть виявитися малоефективними.

Рівні захищеності інформації

Сьогодні найбільш затребуване застосування інтегрованих та багаторівневих систем ІБ. До їх складу входить макросегментація на рівні мережного екрану та мікросегментація використовуваних міжмережевих екранів.

Наступний рівень захисту полягає у виявленні проблем усередині сегментів. У дата-центрі здійснюється аналіз та перевірка динаміки трафіку, яка дозволяє виявити можливі шкідливі активності (наприклад, сканування каналу, DDoS-атаки, несанкціоноване скачування файлів тощо). Через великі обсяги трафіку

зробити це «вручну» проблематично, тому застосовуються просунуті алгоритми. Ці інструменти дозволяють розпізнати шкідливе програмне забезпечення навіть у шифрованому трафіку.

Останній рівень – забезпечення захищеності пристроїв у локальній мережі, тобто безпосередньо самих серверів та віртуальних машин. Для цього використовуються встановлювані агенти для аналізу операцій введення-виводу, зміни, видалення та інших дій з файлами. Для аналізу безпеки застосовуються алгоритми Big Data, які допомагають виявити аномалії та порушення логіки.

Звісно, часом удається обійтися без агентів установки. Багато способів захисту інформації є безагентними, тобто інтегруються в ОС на рівні гіпервізора.

Для дата-центрів, що займаються автоматизацією виробничих процедур, пов'язаних із високою небезпекою (наприклад, на атомних електростанціях), представлених заходів часто буває недостатньо. Тому можуть застосовуватись додаткові методики автоматизації.

Висновки до розділу

Сумуючи вищесказане приходмо до висновку що основною задачою забезпечення безпеки в дата-центрах вважається забезпечення відмовостійкості системи.

Важливим елементом в забезпеченні захисту дата-центрів являється забезпечення електричних розв’язок та резервування даних.

Аналізуючи небезпеку яка являжється зовнішньою на систему це завжи загроза DDoS атак, які вирішуються резервуванням і впровадженням IPS системи та налагодження Firewall в Демілітаризованій зоні.

3 ПРИКЛАД ПОБУДОВИ ДАТА-ЦЕНТАР

3.1 Структура дата-центра

Основні елементи

До телекомунікаційних зон дата-центру належать: кімната введення, головна розподільча зона (MDA), горизонтальна розподільча зона (HDA), місце зонного розподілу (ZDA) та апаратна зона (EDA).

Кімната введення – це місце, що використовується для поєднання структурованої кабельної системи дата-центру та міжбудинкових кабелів, як належать провайдеру доступу, так і споживачеві. Тут розташовані належні провайдеру розмежувальна арматура та обладнання. Кімната введення може розташовуватися поза машинного залу, якщо дата-центр розміщений у будівлі, де знаходяться офіси спільного призначення або приміщення, що не входять до дата-центру. Кімната введення може бути розташована поза машинним залом також з міркувань підвищення безпеки, т.к. у цьому випадку виключається необхідність впускання в машинний зал техніків провайдера доступу. Дата-центри можуть мати не одну, а кілька кімнат введення метою забезпечення додаткового резервування або для того, щоб уникнути перевищення максимальної довжини ділянок кабелю, що йде до проводки, передбаченої провайдером. Кімната введення сполучається з машинним залом через головну розподільча зона. Кімната введення може розташовуватися поруч із головною розподільчою зоною або може бути об'єднана з нею.

Головна розподільча зона містить основну (головну) кросс-панель (MC), яка є центральним пунктом розподілу структурованої кабельної системи і може містити горизонтальну кросс-панель (HC), коли апаратні зони обслуговуються прямо з головної розподільної зони. Це місце знаходиться усередині машинного залу; у розрахованих на багато користувачів дата-центрах воно може

розташовуватися в спеціально виділеній кімнаті, з міркувань безпеки. Кожен дата-центр повинен мати хоч одну головну розподільну зону. Центральний маршрутизатор, центральний комутатор ЛОМ, центральний комутатор мережі системи зберігання даних (SAN, ССХД), а також установчу АТС часто розміщують у головній розподільній зоні, оскільки це місце є ядром кабельної інфраструктури дата-центру. Підготовче обладнання (наприклад, мультиплексори M13), що належить провайдеру доступу, також часто розташовується в головній розподільній зоні, а не в кімнаті введення, це виключає необхідність виділяти другу

кімнату введення через обмеження, що накладаються на довжину контуру.

Головна розподільна зона може обслуговувати одну або кілька горизонтальних розподільчих зон або апаратних зон у межах дата-центру та одну або кілька апаратних системи зв'язку, розташованих поза дата-центром

Документ SP-3-0092: (Стандарт TIA-942, редакція 7.0, лютий 2005) чених для підтримки допоміжних офісних кімнат, операційного центру та інших допоміжних приміщень.

Горизонтальна розподільча зона використовується для обслуговування апаратних зон у тих випадках, коли горизонтальна крос-панель (HC) не знаходиться в головній розподільчій зоні. Тому, коли вона використовується, горизонтальна розподільна зона може включати горизонтальну крос-панель (HC), яка є центральним розподільчим пунктом для кабельного розведення до апаратних зон. Горизонтальна розподільча зона знаходиться всередині машинного залу, але може розташовуватися у спеціально виділеній кімнаті всередині машинного залу з метою забезпечення додаткової безпеки. У горизонтальній розподільній зоні зазвичай знаходяться комутатори локальних мереж, комутатори мережі системи зберігання даних (SAN, ССХД), а також KVM-комутатори (KVM switches) для кінцевого обладнання, розміщеного в апаратних зонах. Дата-центр може містити частини машинного залу, що знаходяться на декількох поверхах, причому кожен поверх обслуговується власною горизонтальною крос-панеллю. Невеликі дата-центри можуть не потребувати горизонтальної розподільчої зони,

оскільки весь машинний зал загалом зможе обслуговувати головна розподільча зона.

Однак дата-центр типу А матиме кілька горизонтальних розподільчих зон.

Апаратна зона (EDA) – це місце, виділене для кінцевого обладнання, включаючи комп'ютерні системи та апаратуру зв'язку. Ці зони не повинні обслуговувати задачі кімнат введення, головної розподільної зони та горизонтальної розподільчої зони.

Допускається мати в горизонтальному кабельному розведенні опціональну точку прямого з'єднання (interconnection), що називається місцем зонного розподілу. Це 6 місце розташовується між зоною горизонтального розподілу та апаратною зоною, що дозволяє часто здійснювати реконфігурацію та підвищує гнучкість системи.

Типова топологія дата-центра

Типовий дата-центр містить одну кімнату введення зовнішніх сервісів, можливо одну або кілька апаратних систем зв'язку, одну головну розподільну зону і кілька горизонтальних розподільчих зон. Топологія такого дата-центру представлена на рис. 3.1.

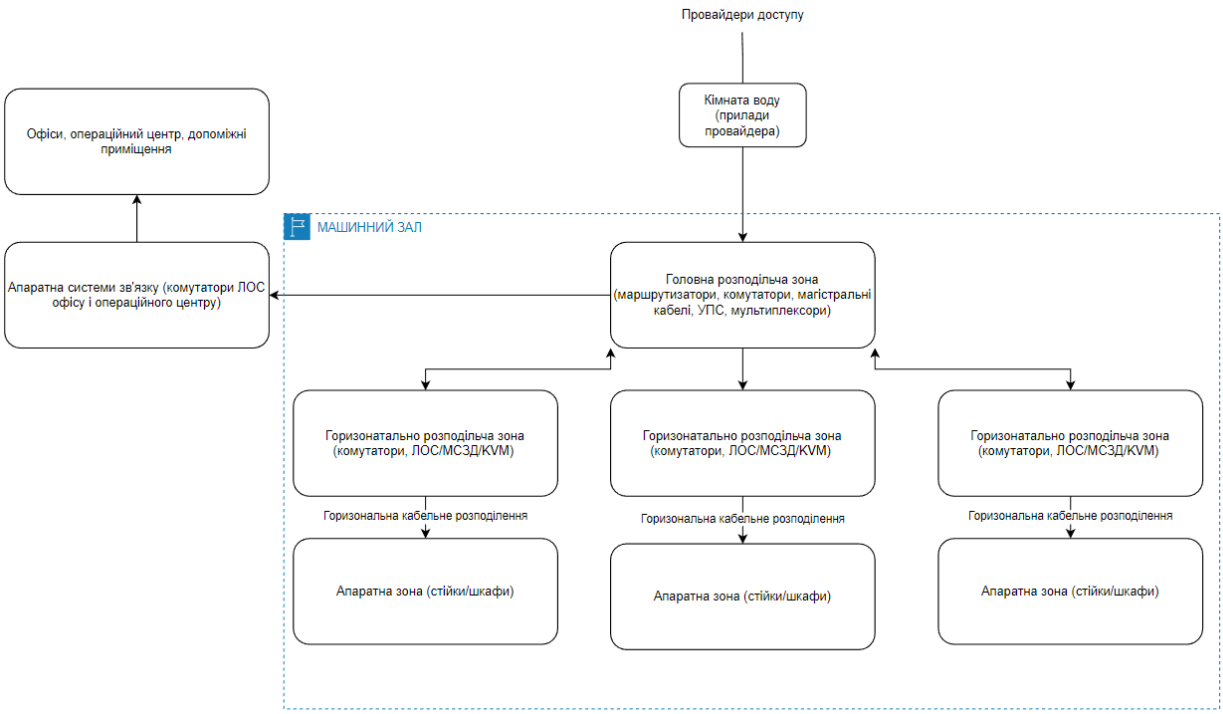

Рис. 3.1 Типова топологія дата-центру

Машинний зал є простір з регульованим навколишнім середовищем,

яке служить єдиної мети – в ньому розміщують обладнання та кабельну розгортку, що мають безпосереднє відношення до комп'ютерних систем та інших телекомунікаційних систем. Машинний зал має відповідати вимогам стандарту NFPA 75.

Поверховий розміщення обладнання повинен бути сумісний з вимогами щодо постачальників апаратури та обладнання, таким як:

– вимоги до навантаження на перекриття, з урахуванням обладнання, кабелів, шнурів та носіїв (статична зосереджена навантаження, статична рівномірно розподілене навантаження, динамічне навантаження при коченні);

– вимоги до службових вільних проходів (вимоги до проходів, або коридорів, з кожної сторони обладнання, необхідного для належного обслуговування цього обладнання);

– вимоги до повітряного потоку;

– вимоги до встановлення (монтажні вимоги);

– вимоги до потужності постійного струму та обмеження за довжиною контуру;

– вимоги до довжини зв'язності обладнання (наприклад, максимально допустимі довжини каналів зв'язку з периферійним обладнанням та пультами управління).

Кімната введення являє собою простір, переважно виконане у вигляді окремої кімнати, в якій обладнання, що належить провайдеру доступу, сполучається з кабельною системою дата-центру. Тут зазвичай знаходиться апаратура провайдера, і саме тут провайдери доступу зазвичай передають лінії зв'язку користувачеві. Ця точка передачі називається точкою розмежування. Саме тут відповідальність провайдера доступу за лінію зв'язку зазвичай закінчується, а відповідальність користувача починається.

У кімнаті введення будуть знаходитися зовнішні кабельні канали, захисні блоки мідних зовнішніх кабелів, обладнання провайдера доступу та термінальне обладнання для кабельної розводки, що йде до машинного залу.

Головна розподільча зона (MDA) – це центральне місце, де знаходиться точка розподілу для структурованої кабельної системи у дата-центрі. Дата центр повинен мати, принаймні, одну головну розподільну зону. Центральні маршрутизатори та центральні комутатори мереж дата-центрів часто розміщують у головній розподільчій зоні або поблизу неї.

У дата-центрах, що використовуються кількома організаціями, наприклад, дата-центрах, де зберігаються бази даних Інтернету або практикується спільне розміщення обладнання, головну розподільчу зону слід розташовувати в безпечному місці.

Горизонтальна розподільча зона (HDA) – це простір, який підтримує кабельну розводку, що йде до апаратної зони. У цій же зоні зазвичай розташовуються комутатори локальних мереж, комутатори мережі системи зберігання даних (SAN, МСЗД), пульт управління, а також KVM, які підтримують кінцеве обладнання. Головна розподільна зона може виконувати функції горизонтальної розподільної зони для близько розташованого зони обладнання або навіть для всього машинного залу, якщо машинний зал невеликий.

На кожному поверсі має бути принаймні одна горизонтальна розподільна зона. Можуть бути потрібні додаткові горизонтальні розподільні зони для підтримки обладнання, що знаходиться за межами обмежень, що накладаються на довжину горизонтального кабелю.

Максимальна кількість підключень до однієї горизонтальної розподільної зони слід вибирати виходячи з можливостей кабельних лотків, з урахуванням вільного місця, що залишається у лотках для розведення кабелів у майбутньому.

У дата-центрах, що використовуються кількома організаціями, наприклад, дата-центрах, де зберігаються бази даних Інтернету або практикується спільне розміщення обладнання, горизонтальну розподільну зону слід розташовувати в безпечному місці.

Апаратні зони – це місця, виділені для кінцевого обладнання, зокрема для комп'ютерних систем та телекомунікаційної апаратури. Сюди не належать апаратні приміщення системи зв'язку, кімнати введення зовнішніх сервісів,

головна розподільча зона та горизонтальні розподільні зони.

Кінцеве обладнання - це зазвичай обладнання для підлоги або обладнання, що монтується в шафах або стійках. Горизонтальні кабелі термінуються в апаратних зонах на віконцях, змонтованих у шафах або стійках. Для кожної шафи або стійки з обладнанням слід передбачити достатню кількість мережевих розеток та віконців, щоб мінімізувати довжину шнурів перемикання та шнурів живлення.

Між одиницями обладнання, що знаходяться в апаратній зоні, допускається пряме кабельне з'єднання «точка-точка» (point-to-point cabling). При такому з'єднанні одиниць обладнання в апаратній зоні не слід застосовувати кабелі довжиною понад 15 м (49 футів), причому їх слід використовувати лише між одиницями обладнання, що знаходяться в сусідніх стійках або шафах в тому самому ряду

У дата-центрах апаратна система зв'язку (TR) – це місце, де відбувається розведення кабелів до зон поза машинним залом. Зазвичай TR розташована поза машинним залом, але при необхідності її можна поєднати з головною розподільчою зоною або горизонтальною розподільчою зоною.

Документ SP-3-0092: (Стандарт TIA-942, редакція 7.0, лютий 2005)

1 У дата-центрі може бути кілька апаратних систем зв'язку, якщо зони неможливо підтримувати з однієї апаратної системи зв'язку.

3 Апаратна система зв'язку повинна відповідати технічним вимогам відповідно до документу ANSI/TIA-569-B.

Допоміжні зони дата-центру

Допоміжні (підсобні) зони дата-центру – це місця поза машинним залом, які призначені для підтримки обладнання дата-центру. Сюди можна зарахувати операційний центр, офіси допоміжного персоналу, кімнати охорони, кімнати електриків, механіків, складські приміщення, приміщення для підготовки обладнання перед монтажем, навантажувальні платформи.

Операційний центр, кімната охорони та офіси допоміжного персоналу повинні бути забезпечені кабельним розведенням, подібним до розведення в стандартних офісних зонах за документом ANSI/TIA/EIA-568-B.1.

Пульти операційного центру та пульти охорони потребують більшого числа кабелів, ніж стандартні робочі місця. Необхідна кількість кабелів, слід визначати за допомогою співробітників операційного центру та за участю технічного персоналу. Операційний центр може вимагати також кабельного розведення для великих стінних або стельових дисплеїв (моніторів або телевізійних екранів).

У кімнатах електриків, кімнатах механіків, складських приміщеннях, кімнатах для підготовки обладнання до монтажу та у навантажувальних платформ слід встановити хоча б по одному настінному телефону на кожне приміщення. Кімнати електриків і механіків повинні мати принаймні одне підключення для передачі даних для доступу до системи керування об'єктом.

3.2 Резервування дата-центрів

Дата-центри, які обладнані різнотипними телекомунікаційними пристроями, можуть виявитися здатними продовжувати роботу навіть за умов катастрофи, яка інакше перервала б телекомунікаційний сервіс дата-центру. На цей Стандарт встановлює чотири рівні, що відповідають різного ступеня готовність інфраструктури дата-центру. На рисунку 3.2 представлені різні резервні компоненти телекомунікаційної інфраструктури, які можна додати до базової інфраструктури.

Надійність телекомунікаційної інфраструктури можна підвищити, передбачивши резервні зони перехресного з'єднання та фізично розділені кабельні канали. Звичайна практика для дата-центрів – мати кілька провайдерів доступу, що надають послуги, а також мати резервні маршрутизатори, резервне центральне розподіл (core distribution) та кінцеві комутатори (edge switches). Хоча така топологія мережі забезпечує певний рівень резервування, але все ж таки одне тільки дублювання сервісів та апаратури не забезпечує виключення єдиних точок відмов.

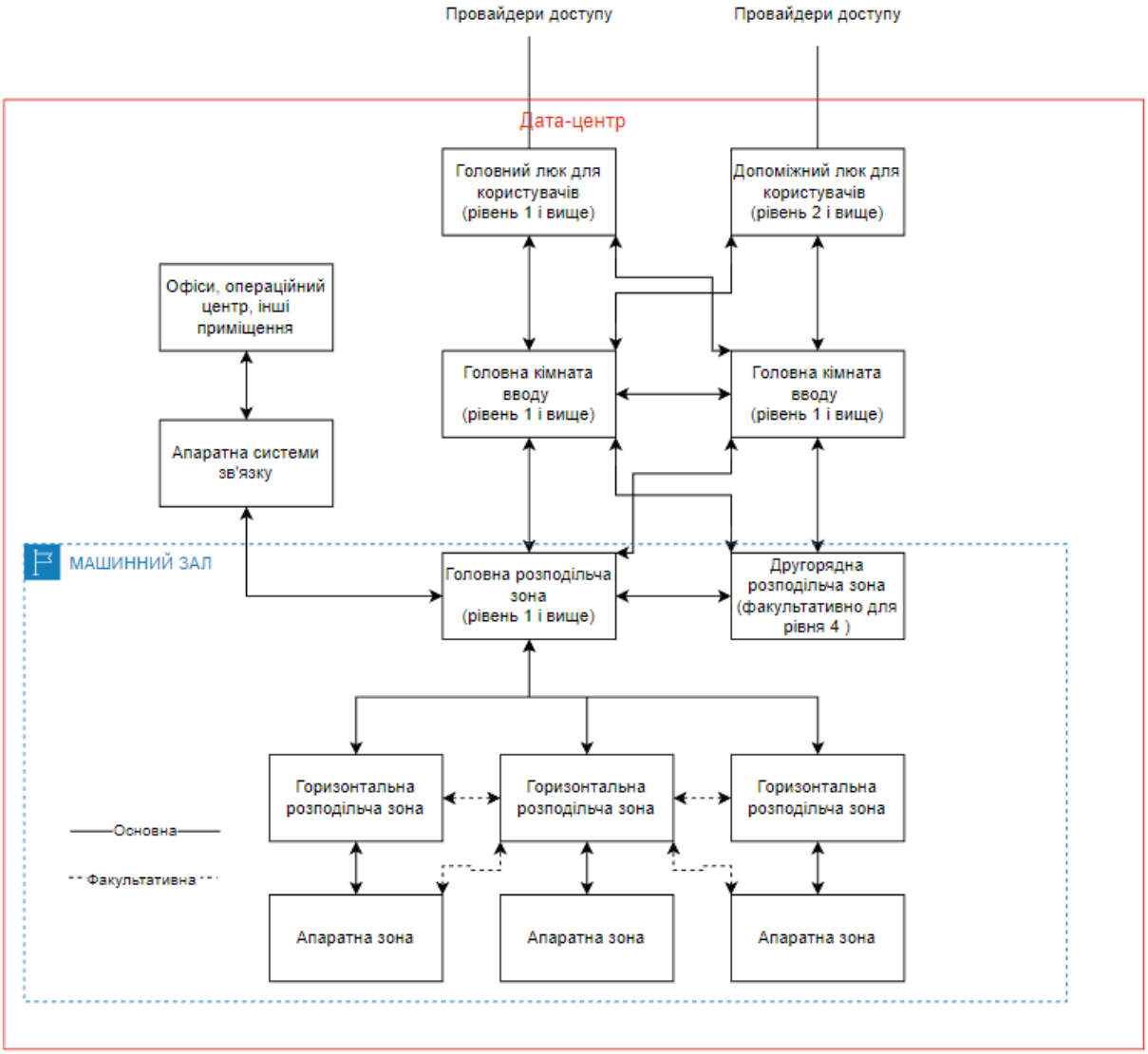

Рис. 3.2 Резервування телекомунікаційної мережи

Резервні сервіси провайдерів доступу

З метою забезпечення безперервності послуг зв'язку, що надаються дата-центру провайдерами доступу, можна залучити кілька провайдерів, використовувати кілька провайдерських центральних офісів, а також передбачити кілька різних кабельних трас від провайдерів доступу до дата-центру.

Наявність кількох провайдерів забезпечить безперервність зв'язку у разі масштабної аварії у провайдера або у разі його фінансового краху, здатного вплинути на Сервіс.

Але все ж таки одне лише використання кількох провайдерів доступу не гарантує безперервності сервісу, оскільки провайдери часто спільно займають

площу в центральних офісах та спільно використовують трубопровідні траси.

Користувачеві слід забезпечити таке положення, при якому сервіси постачаються з різних провайдерських центральних офісів і кабельні траси до цих центральних офісів йдуть різними маршрутами. Ці траси мають бути фізично віддалені один від одного на відстань не менше 20 м (66 футів) у всіх точках по всій довжині цих трас.

3.3 Модель порушника для Дата-центру

При побудові застосовується методика, що ґрунтується спочатку на побудові моделі порушника, виявленні усіх можливих загроз та визначенні способів їх реалізації, а на останок – побудові моделі загроз. Побудовані моделі порушника та загроз дозволяють сформулювати вимоги до системи захисту інформації в середовищі хмарних обчислень.

Орієнтуючись на [3], під моделлю порушника будемо розуміти абстрактний формалізований чи неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо.

Складність побудови моделі порушника для інформаційно-комунікаційної системи (ІКС) хмарних обчислень полягає в необхідності врахування моделі розгортання хмари, моделі надання послуг, власника та рівень контролю інформації, а також рівень контролю провайдера та користувачів над інфраструктурою хмари [3]. Також така модель має бути ще адекватною реальному порушнику.

Аналіз моделі хмари NIST (рис. 3.3) показує, що по відношенню до ІКС хмари порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи). Особливу небезпеку в середовищі хмарних обчислень становлять внутрішні порушники. Навіть при наданні послуг на рівні IaaS [3], внутрішня інфраструктура хмари, в тому числі і середовище

передачі даних, контролюється провайдером хмарних послуг.

На рисунку 3.4 наведена розроблена на основі рис. 1 модель порушника.

В таблиці 3.1 наведено запропонований відносно хмарних сервісів на основі [3] та рисунку 3.3 профіль порушника. Він включає такі основні категорії, як: категорія осіб; характер дій; рівень доступу та можливостей; рівень ознайомленості; методи та засоби, що використовуються, та мету дій.

На основі наведеного відносно хмарних сервісів профілю порушника розроблено та запропоновано модель загроз (рис. 3.4), у якій у формалізованій формі також міститься модель порушника. У ній формалізація зроблена на основі даних таблиці 3.1.

В табл. 3.2 наведено запропонований основний перелік загроз для середовища хмари, модель якої наведено на рис. 3.3, та порушника, профіль якого наведено в табл. 1

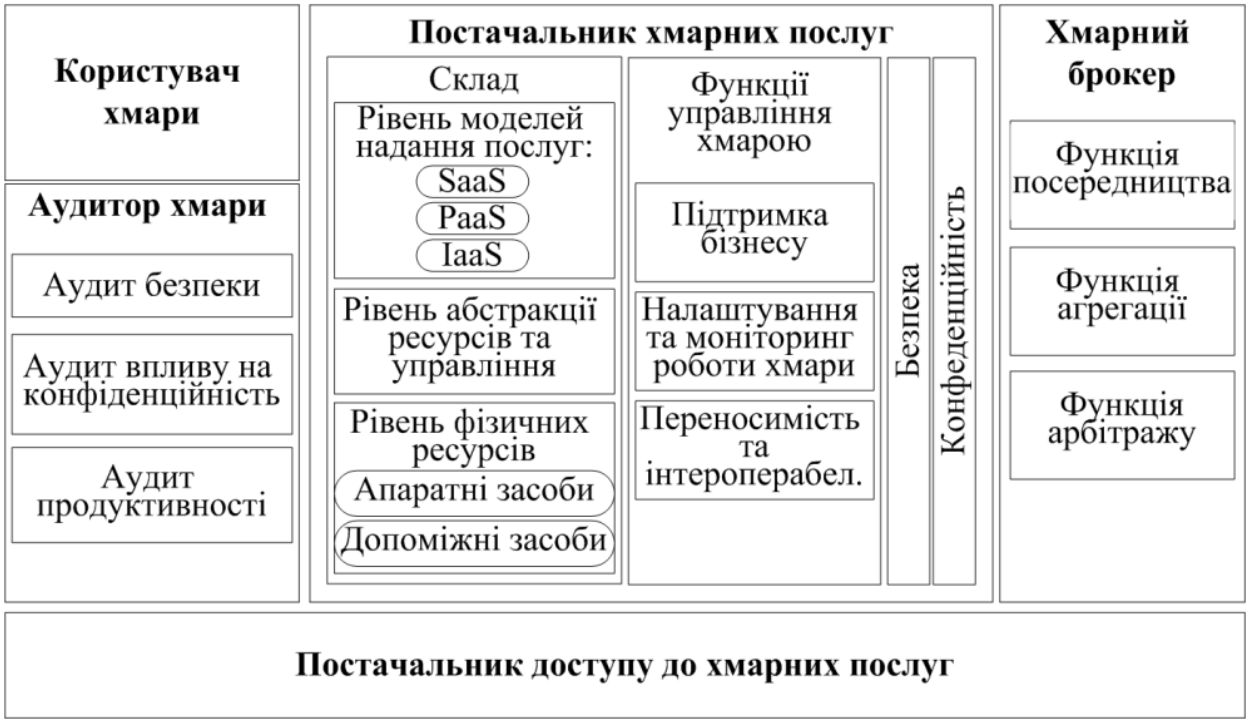

Рис.3.3 Модель хмарних обчислень (сервісів) NIST

Наведена на рисунок 3.3 модель визначає:

– категорії осіб, з числа яких може бути порушник;

– припущення про рівень можливостей, кваліфікацію, рівень

ознайомлення з системою, характер дій порушника;

– методи та засоби, що може використовувати порушник;

– мета, яку перед собою ставить порушник;

– елементи системи, які порушник буде атакувати.

За категорією осіб порушниками можуть бути:

– внутрішні порушники: працівники провайдера хмарних послуг, працівники користувача, сторонні особи, що отримують доступ до ресурсів ІКС хмари. Для їх визначення слід детально розглянути можливості несанкціонованого доступу до ресурсів ІКС кожного із працівників провайдера та користувача, а також можливості сторонніх осіб щодо несанкціонованого доступу до ресурсів ІКС з урахуванням наявної системи організаційного обмеження їх доступу;

– зовнішні порушники: інші особи, що не мають безпосереднього доступу до ресурсів ІКС хмари. Для їх визначення слід детально розглянути можливі канали витоку інформації та вразливі місця системи.

За рівнем можливостей порушників, згідно, розділимо на чотири класи:

– перший рівень припускає можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації

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

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

– четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів ІКС хмари, з можливістю включення до складу ІКС хмари власних засобів з новими функціями обробки інформації.

Таблиця 3.1

Профіль порушника відносно хмарних сервісів

№	Категорія	Значення (Позначення)
1.	Категорія осіб	внутрішній (В)
		зовнішній (З)
2	Характер дій	випадковий (В)
		пасивний (П)
		активний (А)
3	Рівень доступу та можливостей	перший рівень (1)
		другий рівень (2)
		третій рівень (3)
		четвертий рівень (4)
4	Рівень ознайомленості	користувач (К)
		спеціаліст (С)
		адміністратор системи (А)
		спеціаліст з найвищим рівнем знань (Н)
		адміністратор безпеки (Б)
5	Методи та засоби	агентурні (Р)
		штатні (Ш)
		пасивні (П)
		активні (А)
6	Мета дій порушника	отримання атрибутів доступу персоналу чи користувачів АС (О)
		отримання несанкціонованого доступу до обчислювальних ресурсів хмари (НСД)
		проникнення на територію хмарного ЦОД з метою впливу на фізичне обладнання (ВФ)
		зміна режимів функціонування чи виводу з ладу фізичних ресурсів АС (М)
		встановлення засобів технічної розвідки (ТР)
		встановлення технічних засобів нав’язування (ТЗН)
		встановлення програмних закладок розвідки (ПЗР)
		встановлення програмних засобів нав’язування (ПЗН)

За рівнем ознайомлення з системою, порушників будемо класифікувати за такими рівнями, як [2, 11]:

– що не володіють спеціальними знаннями з обчислювальної техніки та програмування, проектування та експлуатації хмарної ІКС, а є лише користувачами сервісу;

– що володіють базовим або високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації хмарних ІКС, а також базовим або високим рівнем знать про системи захисту хмарних ІКС;

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

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

– що володіють інформацією про функції та механізм дії засобів захисту в визначеній ІКС хмари.

Аналіз показує, що незалежно від моделі розгортання хмари та моделі надання послуг найнебезпечнішими порушниками в ІКС хмари є адміністратори хмари та адміністратори безпеки хмари. Порушення з боку цих осіб можуть бути як ненавмисними, так і зловмисними. При цьому якщо «випадковий порушник» здійснює загрози ІКС під час виконання своїх функціональних обов’язків внаслідок помилкових дій, за рахунок неуважності чи недбалості, то порушник, що здійснює зловмисне порушення, чітко розуміє свої дії та має змогу проаналізувати їх вплив. Також необхідно брати до уваги, що порушник в середовищі хмари може здійснювати активні чи пасивні загрози ресурсам ІКС чи АС. Під активною загрозою слід розуміти навмисні та не навмисні несанкціоновані дії порушника, що призвели до зміни стану ІКС (АС), а під пасивною загрозою – дії, що призвели до несанкціонованого проникнення в систему без зміни її стану.

За характером дій порушників можна класифікувати на [2, 3]:

– «випадковий порушник» – це користувачі, обслуговуючий персонал, які не навмисно подолали засоби управління (адміністрування) доступом до

об’єкту захисту, виконали непередбачені дії відносно цього об’єкту, чим спричинили порушення політики безпеки до об’єкта захисту;

– «пасивний порушник» – авторизований користувач, або обслуговуючий персонал хмари, який навмисно порушив політику безпеки послуги, але не вживає рішучих дій. З метою прихованого подолання засобів управління (адміністрування), використовує атрибути доступу інших користувачів;

– «активний порушник» – порушник, який не приховує своїх дій та може використовувати всі доступні методи та засоби для порушення властивості захищеної інформації. До таких дій відносяться дії, що спрямовані на подолання організаційного обмеження доступу, охоронної сигналізації, управління доступом до фізичних ресурсів, фізичний доступ до засобів оброблення, зберігання чи передавання інформаційних об’єктів з метою виведення їх з ладу, зміни режимів функціонування, крадіжки чи пошкодження носіїв тощо;

– «віддалений порушник» – порушник, що використовує засоби віддаленого доступу до інформаційних об’єктів: виток інформації технічними каналами, спеціальний вплив на інформацію по технічним каналам, мережне обладнання локальних чи розподілених мереж, в тому числі і засоби телекомунікаційних мереж.

За методами та засобами, що використовує порушники, їх можна класифікувати як таких, що використовують [2, 3]:

– виключно агентурні методи одержання відомостей;

– пасивні технічні засоби перехоплення інформаційних сигналів;

– для реалізації спроб НСД виключно штатні засоби АС або недоліки проектування КСЗІ;

– способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

Також при подальших дослідженнях будемо вважати, що метою

зловмисника, при здійсненні порушення, може бути наступне [1–3]:

– авторизація та отриманні атрибутів доступу з найбільшими правами до ресурсів ІКС з метою їх використання для ознайомлення з конфіденційною інформацією, її модифікації чи знищення, використання обчислювальних ресурсів хмари в своїх власних цілях;

– пошук та/або здобуття атрибутів доступу особи з персоналу чи користувачів АС, які мають атрибути доступу з найбільшими правами, з метою заволодіння їх атрибутами доступу. Здобуття атрибутів особи може бути реалізовано шляхом використання технічних засобів, крадіжок, купівлі, чи отримання іншим шляхом;

– проникнення на місця розміщення тих чи інших компонентів, елементів чи ресурсів АС (обчислювальних ресурсів, інформаційних ресурсів, базового, прикладного програмного забезпечення та програмного забезпечення системи ТЗІ, включаючи носії резервних копії, ресурсів вводу/виводу, телекомунікаційного обладнання, включаючи мережу передачі даних) шляхом подолання перешкод (огорожі, елементів будівельних конструкцій, охорони чи охоронної сигналізації та ін.) та нанесення збитків шляхом знищення матеріальних та інформаційних цінностей;

– зміна режимів функціонування чи виводу з ладу ресурсів АС;

– установка фізичних засобів (апаратурних закладок) чи інших засобів технічної розвідки в місцях розміщення елементів АС (в тому числі і віддалених, наприклад в елементах комунікаційної мережі зв’язку) для знімання інформації;

– установка фізичних чи інших засобів (апаратурних закладок) в місцях розміщення елементів АС (в тому числі і віддалених, наприклад, в елементах комунікаційної мережі зв’язку) для генерації несправжніх сигналів, інформаційних символів чи повідомлень;

– установка програмних засобів (програмних закладок) знімання інформації з метою її того чи іншого використання;

– установка програмних засобів (програмних закладок чи вірусів) для модифікації як програмних засобів, так і інформації АС, шляхом генерації

(впровадження) програмних вірусів, несправжніх сигналів, інформаційних символів чи повідомлень з метою перевантаження систем АС і порушення, таким чином, доступності компонентів АС чи АС в цілому;

– здійснення спроб несанкціонованого доступу до обчислювальних ресурсів, інформаційних рес урсів, базового та прикладного програмного забезпечення та програмного забезпечення системи ТЗІ як власне АС, так і її телекомунікаційної підсистеми шляхом подолання системи управління доступом.

Важливим також є визначення та використання в моделі того, яким чином загрози можуть бути реалізовані при хмарних обчисленнях. Ґрунтуючись на [3, 11], будемо вважати, що вони реалізуються наступними способами:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, віброакустичні, акустоелектричні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів, як на стороні користувача так і провайдера хмарних послуг.

3.4 Модель загроз відносно хмарних сервісів

Наведені вище потенційні можливості порушника дозволили розробити модель загроз відносно хмарних сервісів (обчислень). Детально опис такої моделі загроз наведена в табл. 3.2. В ній на основі рис. 3.4 вказується об’єкт, для якого реалізується загроза, мета порушника, ймовірність загрози та мета здійснення захисту

Класифікація загроз за ймовірністю була проведена з урахуванням рекомендацій [1]. Згідно цих рекомендацій, найбільшу ймовірність мають загрози, що здійснюються на компоненти хмарної інфраструктури, які мають інтерфейси доступу з зовні та/або знаходяться в віртуалізованому середовищі.

Аналіз моделі загроз, зображеної на рис. 3.4, показав, що найбільшу небезпеку становлять загрози управління хмарою (З.9) та її безпекою (З.1), а також загрози гіпервізору (З.6).

На основі розроблених моделей хмарних обчислень, порушника та загроз ІТС хмарних обчислень(сервісів) з суттєвим урахуванням [2–4, 6] визначено, що найбільш проблемними з точки зору перекриття є загрози відносно ключів та ключової інформації.

На рис. 3.5 наведено визначений в процесі досліджень та даних табл. 3.1, 3.2, а також рис. 3.3, 3.4, перелік загроз ключовим даним (ключам), які необхідно за стосовувати для криптографічного захисту інформації в процесі хмарних обчислень. Детально опис моделі загроз наведений в табл. 3.3.

Враховуючи в аналізі наведенні дані в роботі [6], приймемо що в середовищі хмари відносно ключових даних можуть існувати та реалізовуватись зі сторони порушника такі загрози:

– компрометація ключів та ключової інформації;
– несанкціоноване знищення ключів та ключової інформації;
– перехоплення та запам’ятовування ключів та ключової інформації;
– нав’язування помилкових або хибних ключів та ключової інформації;
– нав’язування слабких ключів або напів слабких ключів;
– підміна ключів або ключової інформації;
– отримання несанкціонованого доступу до ключів чи ключової інформації;
– отримання можливості несанкціонованого використання ключів тощо.

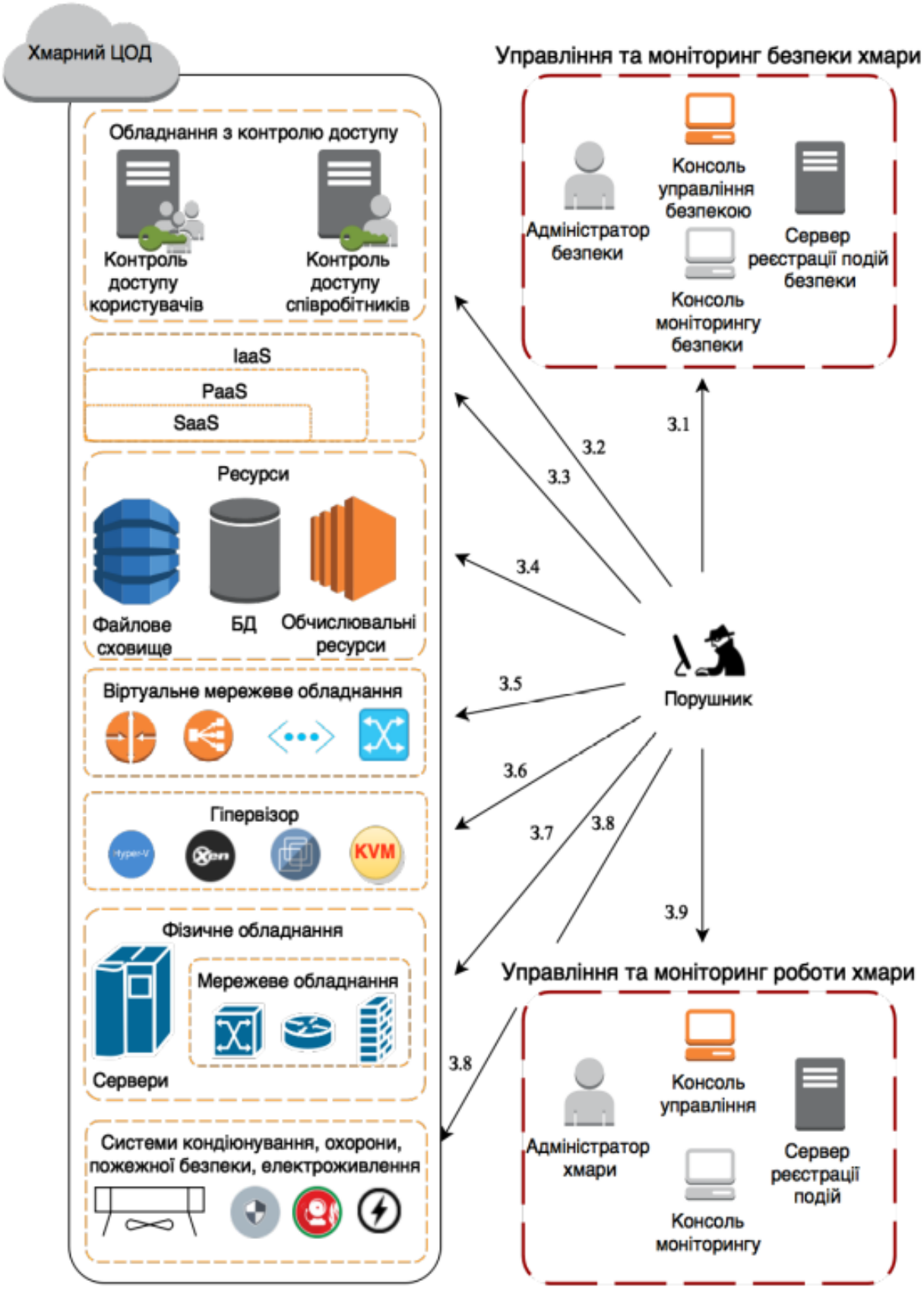

Рис. 3.4 Модель загроз для ІТС хмарних обчислень

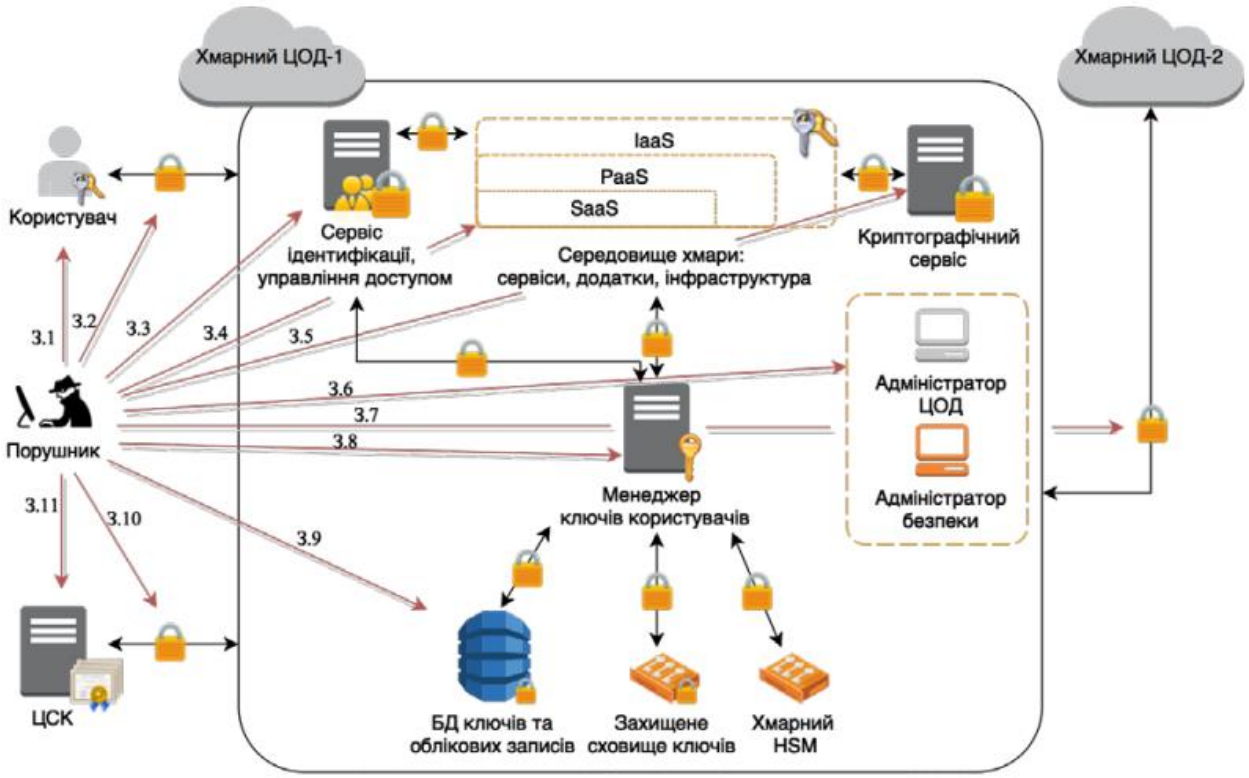

Рис. 3.5 Загрози ключам в середовищі хмари

Зважаючи на пропозиції та визнані критерії, що наведені в [1, 3, 6], приймемо в якості основного критерію ймовірність реалізації загрози. Також приймемо, що вона може оцінюватись як: низька, середня та висока.

На основі аналізу переліку загроз та моделі загроз ключовим даним можна зробити висновки про те, що порушник може з високою ймовірністю здійснювати:

– компрометацію, знищення, отримання несанкціонованого доступу чи несанкціоноване використання ключів відносно користувача;

– перехоплення, нав’язування та підміну ключів через канали зв’язку між користувачем та хмарою;

– отримання несанкціонованого доступу до ключів через сервіси ідентифікації, автентифікації, авторизації та керування правами доступу;

– отримання несанкціонованого доступу чи несанкціоноване використання ключів через хмарне середовище – сервісів додатків та, інфраструктуру;

– найбільшу небезпеку в середовищі хмарних обчислень для ключових даних користувача представляють адміністратори хмарних сервісів, які мают доступ до середовища в якому розгорнуто хмарні додатки користувача.

Для захисту від вказаних загроз на рівні користувача необхідно використовувати захищені з необхідним рівнем носії ключів.

На рівні каналів зв’язку між користувачем та хмарою використовувати захищені канали зв’язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються.

На рівні сервісів ідентифікації, автентифікації, авторизації та керування правами доступом використовувати надійні протоколи автентифікації з стійкими криптографічними алгоритмами, також методи багатофакторної автентифікації.

На рівні хмарного середовища, тобто сервісів додатків та інфраструктури – використовувати для

здійснення криптографічних операцій захищені відповідним чином криптографічні модулі – HSM.

Також на основі табл. 3.3 можна визначити методи та механізми криптографічного та іншого захисту в середовищі хмарних обчислень для середнього та низького рівнів ймовірностей реалізації загроз

Під час розробки комплексної системи захисту для хмари, в процесі аналізу моделі загроз виникає необхідність отримати значення ризику виникнення

загроз з метою використання найбільш оптимальних методів захисту, а також оцінки використаних методів в побудованій системі.

В загальному випадку існує два показники, які отримують в процесі аналізу ризиків: якісний та кількісний.

За визначення стандарту ISO/IEC 27005 під ризиком розуміється вплив невизначеності на цілі, що характеризується комбінацією ймовірності подій та їх наслідків. Значення ризику R може бути задано наступним виразом:

$$R = R_i * C_j \tag{3.1}$$

де R_i – ймовірність успішної реалізації і-й загрози, C_j – оцінка збитку викликаного впливом інциденту ІБ на активи при успішній реалізації і-й загрози.

Під загрозою розуміється будь-які обставини або події, що виникають у середовищі хмарних обчислень, які можуть бути причиною порушення політики безпеки інформації і (або) нанесення збитків автоматизованій системі.

Стандарт ISO/IEC 31010 описує основні методи з оцінки ризиків, сферу їх застосування та можливості, вхідні та вихідні дані, а також переваги та недоліки цих методів.

На сьогодні існує декілька методологій та підходів по оцінці ризиків. В першу чергу оцінка ризиків може бути виконана використовуючи кількісний (ISAMM, Mehari), якісний (EBIOS, Octave, IT-Grundshutz) або змішаний підхід (CRAMM, MEGERIT). Кількісні методи використовують вимірні, об'єктивні дані для визначення вартості активів, імовірність втрати і пов'язаних з ними ризиків. В ході оцінки з використанням кількісного підходу обчислюються числові значення для кожного з компонентів, зібраних в ході оцінки ризиків та аналізу витрат і переваг. В свою чергу, якісні методи ґрунтуються на використанні відносного показнику ризику або вартості активу на основі рейтингу або поділу на категорії, такі як низький, середній, високий, не важливо, важливо, дуже важливо, чи за шкалою від 1 до 10. Якісна модель дозволяє оцінити дії й імовірності виявлених ризиків більш швидким та дешевшим способом порівняно з кількісним. Якщо вимагається більш детальний та точний аналіз на основі окремих отриманих якісних оцінок можна провести кількісний аналіз. Такий аналіз з комбінації якісного та кількісного підходів являє собою змішаний підхід з сукупністю переваг і недоліків вище згаданих методів.

Окремих стандартів, що описують аналіз ризиків ключових систем в хмарі станом на 2015 не існує, але в якості керуючих документів по аналізу ризиків в середовищі хмарних обчислень можуть бути застосовані наступні стандарти: ISO 27001, ISO 27005, ISO 17799. В цих стандартах теоретично описуються і даються методичні вказівки процесу оцінки ризиків, в тому числі і для ключових систем. В наведених стандартах не визначено та не дається конкретних технологій з

проведення оцінок, тому в якості інструментів для проведення аналізу можуть бути використані різні програмні додатки, наприклад такі як Cobra (Великобританія), RiskWatch (США), ГРИФ (Росія).

Окрім зазначених вище стандартів існує публікація NIST NISTIR 7956, що розглядає питання та проблеми управління ключами в хмарних сервісах.

Низка закордонних та вітчизняних публікацій [8–10] відзначають наступні особливості при проведенні оцінки ризиків хмарних обчислень:

– загалом існуючи підходи до оцінки ризиків можуть бути використанні в середовищі хмарних обчислень, за умови урахування особливостей функціонування та інфраструктури хмари;

– розробка та використання методів оцінки повинна будуватися на принципах адаптивності, тобто враховувати принцип невизначеності складу хмарної інфраструктури та можливості її динамічної зміни;

– невизначеність та динамічна зміна конфігурації хмари потребує методик з поточного аналізу вразливостей хмари;

– суттєвим недоліком існуючих методик є ускладнене отримання прогнозів про стан середовища хмарних обчислень, що в умовах високої невизначеності є важливим фактором, в результаті знижується загальний рівень захищеності хмарної ІТС;

– також недоліком існуючих методик є складність їх застосування до каналів НСД в хмарі, через їх відмінність для кожної з реалізації моделі хмарних обчислень;

– наявність можливості користувачами використання своїх власних пристроїв для взаємодії з середовищем хмари призводить до розмиття поняття контрольована зона;

– при проведенні аналізу ризиків у хмарній ІТС, відповідно до традиційних підходів, часто відсутня можливість отримання будь-яких кількісних експертних оцінок про ймовірність реалізації загроз, через незнання географії, умов функціонування та рівня захищеності ресурсів.

Задачу вибору методу з аналізу ризиків в середовищі хмари ускладнюють

такі особливості хмарного середовища, як: розподілена складна архітектура, наявність адміністраторів, які контролюють обслуговуюче обладнання та розгорнуту інфраструктуру, конфігурація системи, що складається з різних вузлів та може динамічно змінюватися, відсутність контролю середовища користувачами тощо. Керуючись зазначеними вище особливостями середовища хмари, а також відсутністю статистичних даних з реалізації загроз, з широкого кола методів було обрано два, що найбільш повно дозволяють провести аналіз та отримати оцінки з ризиків інформаційної безпеки в хмарному середовищі.

В якості методів, що дозволяють провести аналіз та класифікацію загроз, пропонується використовувати метод попереднього аналізу небезпек (PHA), що дозволяє провести аналіз на попередніх стадіях проектування з недостатньою кількістю інформації, ранжування небезпек та ризику або метод CHAZOP, який виконує всебічний та систематичний аналіз на завершальному етапі розробки системи або коли вона вже побудована. По причині складності використання методу CHAZOP його доцільно застосовувати тільки у випадках, коли необхідно виконати повний аналіз системи. В якості кількісного методу оцінки ризиків пропонується до застосування використання байесовського підходу, який дозволяє отримати апостеріорну ймовірність на основі апріорних ймовірностей, при цьому є можливість уточнення результатів при отриманні нових даних, що важливо при динамічній зміні кількості вузлів в системі та її архітектури [9].

Таблиця 3.2

Загрози в середовищі хмари

Загроза	**Об’єкт для якого реалізується загроза**	**Мета**	**Ймовірність загрози**	**Методи захисту**
3.1	Управління та моніторинг безпеки хмари	Отримання несанкціонованого доступу до хмари	низька	Використання систем з контролю доступу, політики безпеки, атестація персоналу
3.2	Обладнання з контролю доступу	Отримання несанкціонованого доступу до хмарних ресурсів чи управління хмарою	висока	Використання захищених носіїв ключа для автентифікації
3.3	Середовище хмари: сервіси, додатки та інфраструктура	Порушення сервісами, додатками та об’єктами інфраструктури прав доступу. Несанкціонований доступ до функцій управління інфраструктурою, даних сервісів та додатків користувача хмари. Зараження шпигунським ПЗ та вірусами	висока	Використання технологій розмежування та обмеження доступу, контроль над цілісністю об’єктів та їх моніторинг

Продовження таблиці 3.2

Загрози в середовищі хмари

Загроза	**Об'єкт для якого реалізується загроза**	**Мета**	**Ймовірність загрози**	**Методи захисту**
3.4	Ресурси хмари	Отримання несанкціонованого доступу до файлів, записів БД або використання обчислювальних ресурсів	висока	Впровадження механізмів обмеження доступу, шифрування даних, моніторинг роботи
3.5	Віртуальні мережі в межах хмарної інфраструктури	Прослуховування трафіку, порушення цілісності, доступності, організація атак DDoS, несанкціоноване підключення до мережі	висока	Використання засобів захисту даних в мережі, систем виявлення та протидії мережевим атакам, моніторинг роботи
3.6	Гіпервізор	Повний контроль над розгорнутим віртуальним середовищем	низька	Захист гіпервізора та контроль доступу до його налаштувань

Продовження таблиці 3.2

Загрози в середовищі хмари

Загроза	**Об'єкт для якого реалізується загроза**	**Мета**	**Ймовірність загрози**	**Методи захисту**
3.7	Фізичне обладнання	Встановлення засобів несанкціонованого доступу, модифікації та знищення інформації. Порушення доступності ЦОД	низька	Використання систем контролю доступу, політики безпеки, атестація персоналу. Встановлення контрольованої зони
3.8	Допоміжні системи (живлення, охорони, безпеки, охолодження)		низька	
3.9	Управління та моніторинг роботи хмари	Отримання несанкціонованого доступу до налаштувань хмари	середня	Використання технологій розмежування та обмеження доступу, моніторинг дій адміністраторів
3.10	Зв'язки між хмарними ЦОД	Порушення доступності ЦОД, отримання несанкціонованого доступу до інформації, що передається мережею	низька	Використання надійних протоколів з стійкими криптограф. алгоритмами

Таблиця 3.3

Загрози ключам в середовищі хмари

Загроза	**Об’єкт для якого реалізується загроза**	**Мета**	**Ймовірність загрози**	**Методи захисту**
3.1	Користувач	Компрометація, знищення, отримання несанкціонованого доступу чи несанкціоноване використання ключів	висока	Використання захищених носіїв ключа
3.2	Канал зв’язку між користувачем та хмарою	Перехоплення, нав’язування, підміна ключів	висока	Використання захищеного каналу зв’язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються
3.3	Сервіс ідентифікації, автентифікації, авторизації та керування правами доступу	Отримання несанкціонованого доступу до ключів; Отримання можливості несанкціонованого використання ключів.	висока	Використання надійних протоколів автентифікації з стійкими криптографічними алгоритмами. Використання багатофакторної автентифікації

Продовження таблиці 3.3

Загрози ключам в середовищі хмари

Загроза	**Об’єкт для якого реалізується загроза**	**Мета**	**Ймовірність загрози**	**Методи захисту**
3.4	Хмарне середовище: сервіси додатки, інфраструктура	Отримання несанкціонованого доступу до ключів; Отримання можливості несанкціонованого використання ключів.	висока	Використання HSM для здійснення криптографічних операцій
3.5	Криптографічний сервіс	Компрометація, знищення, підміна, нав’язування, отримання несанкціонованого доступу чи несанкціоноване використання ключів	середня	Використання HSM для здійснення криптографічних операцій

Продовження таблиці 3.3

Загрози ключам в середовищі хмари

Загроза	**Об’єкт для якого реалізується загроза**	**Мета**	**Ймовірність загрози**	**Методи захисту**
3.6	Адміністратор ЦОД та адміністратор безпеки	Компрометація, отримання несанкціонованого доступу чи несанкціоноване використання ключів адміністраторів з метою отримання вищих повноважень в системі	низька	Використання захищених носіїв ключа
3.7	Канал зв’язку між відокремленими хмарними ЦОД	Перехоплення, нав’язування, підміна ключів	середня	Використання захищеного каналу зв’язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються
3.8	Менеджер ключів користувачів	Компрометація, знищення, підміна, нав’язування, отримання несанкціонованого доступу чи несанкціоноване використання ключів	середня	Використання надійного сервісу автентифікації

Продовження таблиці 3.3

Загрози ключам в середовищі хмари

Загроза	**Об’єкт для якого реалізується загроза**	**Мета**	**Ймовірність загрози**	**Методи захисту**
3.9	Засоби зберігання ключів	Компрометація, знищення, підміна, отримання несанкціонованого доступу до ключів	низька-середня	Використання захищених апаратних модулів зберігання ключів та/або HSM
3.10	Канал зв’язку між хмарним ЦОД та ЦСК	Перехоплення, нав’язування, підміна ключів та результатів перевірки ключів	низька	Використання надійних протоколів з стійкими криптографічними алгоритмами
3.11	ЦСК	Компрометація, отримання несанкціонованого доступу чи несанкціоноване використання ключів з метою компрометації сервісів, що надаються ЦСК	низька	Створення КСЗІ для ЦСК, проходження експертизи та відповідність державним та міжнародним стандартам

3.4 Профіль захищеності дата-центру

Для доступу до обробки персональних данних до дата-центрів висуваються вимоги з визначеним профілем захищеності.

Функціональний профіль захищеності На ЦОД «Парковий»:

(КА-2, КВ-1, ЦА-1, ЦА-2, ЦВ-1, ЦО-1, ДР-2, ДС-3, ДЗ-1, ДЗ-2, ДВ-3, НР-2, НР-4, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1) НД ТЗІ 2.5-004-99

Таблиця 3.4

Профіль захищеності дата-центру

Послуга	Значення
КА-2. Базова адміністративна конфіденційність	Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта користувача і захищеного об'єкта
	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити — конкретних користувачів і/або групи користувачів, які мають право ініціювати процес

Продовження таблиці 3.4

Профіль захищеності дата-центру

Послуга	Значення
КА-2. Базова адміністративна конфіденційність	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту
КВ-1. Мінімальна конфіденційність при обміні	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься
	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності
	КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається
ЦА-1 Мінімальна адміністративна цілісність	Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта
	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження
	КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт

Продовження таблиці 3.4

Профіль захищеності дата-центру

Послуга	Значення
ЦА-1 Мінімальна адміністративна цілісність	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту
ЦА-2 Базова адміністративна цілісність	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта процесу і захищеного об'єкта
	КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт
	КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити — конкретних користувачів і/або групи користувачів, які мають право ініціювати процес
ЦВ-1 Мінімальна цілісність при обміні	Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності
	КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається
ЦО-1 Обмежений відкат	Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься

Продовження таблиці 3.4

Профіль захищеності дата-центру

Послуга	Значення
ЦО-1 Обмежений відкат	Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу
ДР-1 Недопущення захоплення ресурсів	Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів КС
	Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу
	Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження
	Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку окремого користувача
ДС-3 Стійкість без погіршення характеристик обслуговування	Розробник повинен провести аналіз відмов компонентів КС
	Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів КС
	Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги
	Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування
	КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента

Продовження таблиці 3.4

Профіль захищеності дата-центру

Послуга	Значення
ДЗ-1 Модернізація	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації КС
	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) КС. Модернізація КС не повинна призводити до необхідності ще раз проводити інсталяцію КС або до переривання виконання КЗЗ функцій захисту
ДЗ-2 Обмежена гаряча заміна	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати множину компонентів КС, які можуть бути замінені без переривання обслуговування
	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент
ДВ-3 Вибіркове відновлення	Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС
	Після будь-якої відмови КС або переривання обслуговування, що не призводить до необхідності заново інсталювати КС, КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути КС до нормального функціонування або, в гіршому випадку, функціонування в режимі з погіршеними характеристиками обслуговування
	Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження
	Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування

Продовження таблиці 3.4

Профіль захищеності дата-центру

Послуга	Значення
НР-2 Захищений журнал	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються
	КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки
	Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події
	КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації
НР-4 Детальна реєстрація	КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки
	КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій
НИ-2 Одиночна ідентифікація і автентифікація	Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ
	Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму

Продовження таблиці 3.4

Профіль захищеності дата-центру

Послуга	Значення
НИ-2 Одиночна ідентифікація і автентифікація	КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування
НК-1 Однонаправлений достовірний канал	Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ
	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем
НО-2 Розподіл обов'язків адміністраторів	Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції
	Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі
	Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі
НЦ-1 КЗЗ з контролем цілісності	Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ
	В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження
	Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ

Продовження таблиці 3.4

Профіль захищеності дата-центру

Послуга	Значення
НТ-2 Самотестування за запитом	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ
	КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження
НВ-1 Автентифікація вузла	Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації

Висновок до розділу

Підсумовуючи вищевикладене можна зробити наступні висновки:

1. Розроблена модель загроз хмарних сервісі дозволяє зробити висновок про те, що найбільшу ймовірність реалізації мають загрози, що здійснюються на компоненти хмарної інфраструктури, які мають інтерфейси доступу з зовні та/або знаходяться в віртуалізованому середовищі. С точки зору найбільшої небезпеки та найбільших втрат системи у разі реалізації загроз слід виділити згідно рис. 2 загрози управління хмарою (З.9) та її безпекою З.1, а також загрози гіпервізору (З.6).

2. Визначений в результаті аналізу перелік загроз та розроблена модель загроз ключовим даним дозволили зробити висновки про те, що порушник з

високою ймовірністю може реалізовувати ряд наведених в підрозділі 5. 1. загроз, але найбільша небезпеку в середовищі хмарних обчислень для ключових даних користувача виникає при використанні їх в середині розгорнутою інфраструктури, без застосування криптографічних сервісів та HSM.

3. Розроблений профіль порушника, що включає категорію осіб, характер дій, рівень доступу та можливостей, рівень ознайомленості, методи та засоби, що використовуються та мету дій порушника. Його використання дозволяє формалізувати процес побудування моделі загроз хмари та аналіз можливостей порушника.

4. Результати аналізу моделі загроз ключовим даним дозволили запропонувати методи та механізми захисту, дані відносно яких наведені в табл. 3.3. До основних механізмів можна віднести використанням захищених сховищ ключів для безпечного зберігання ключів, та криптографічних сервісів та хмарних HSM для безпечного використання ключів в хмарі.

5. Проведені результати досліджень дозволили з урахуванням особливостей функціонування хмар обрати методи оцінки ризиків згідно стандарту ISO/IEC 31010, за рахунок яких досягається найбільша повнота та якість проведення оцінки.

6. Профіль захищеності для хмарних дата-центрів проектує використання Європейських стандартів в реалії що можуть використовуватись для обробки державних інформаційних ресурсів і персональних даних що підлягають захисту.

ВИСНОВКИ

Виходячи з усього вище сказаного, можна зробити загальний висновок про те наскільки важливе збереження персональних данних, особливо це стосується даних що входять до державних інформаційних ресурів.

Зважаючи на те що державні інформаційні системи мають тенденцією переїзду в дата-центри, важливо розуміти всю критичніть потреби захисту інформації в дата-центрах.

Дата-центри, як обєкти критичної інфратруктури потребуєть захисту зі сторони Держави та контролю захищеності інформації в системі, проте не тільки на відмовостійкість, а й з точки зору моделі загроз і моделі порушника.

Розроблений профіль порушника, що включає категорію осіб, характер дій, рівень доступу та можливостей, рівень ознайомленості, методи та засоби, що використовуються та мету дій порушника. Його використання дозволяє формалізувати процес побудування моделі загроз хмари та аналіз можливостей порушника.

Законодавча база що стосується дата-центрів має конкретно визначений профіль захищеності для обробки данних, виконання яких відповідно до законодавства дозволяє виконувати задачі, пов’язані з обробкою персональних даних в них.

Проте побудови системи запхисту на основі законодавства України недостатн для надійного захисту персональних даних. Для більшого рівня безпеки і гарантії збереження конфіденційності, цілісності та доступності конфіденційної інформації рекомендую застосовувати Європейські в Американьскі стандарти як доповнення до Українських. Такі як ISO/IEC 31010, TIA, ISO/IEC 27k.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Haeberlen, T. Cloud Computing Benefits, risks and recommendations for information security [Electronic resource] / T. Haeberlen, L. Dupré // Available at: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/at_download/file.

2. Jansen, W. Cloud Hooks: Security and Privacy Issues in Cloud Computing [Text] / W. Jansen // 44th Hawaii International Conference on System Sciences (HICSS) – 2011. – P. 1–10. doi: 10.1109/hicss.2011.103.

3. Jansen, W. Guidelines on Security and Privacy in Public Cloud Computing. [Electronic resource] / W. Jansen, F. Grance, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf // Available at: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

4. Hashizume, K. An analysis of security issues for cloud computing [Text] / K. Hashizume, D. Rosado, E. Fernández-Medina, E. Fernandez // Journal of Internet Services and Application – 2013. – Vol. 4, Issue 5. – P. 15–28. doi: 10.1186/1869-0238-4-5.

5. Chandramouli, R. Analysis of Protection Options for Virtualized Infrastructures in Infrastructure as a Service Cloud [Text] / R. Chandramouli // Fifth International Conference on Cloud Computing, GRIDs, and Virtualization, Venice, Italy, 2014. – P. 37–43.

6. Chandramouli, R. NIST Cryptographic Key Management Issues & Challenges in Cloud Services [Electronic resource] / R. Chandramoli, S. Chokhani, M. Iorga. – National Institute of Standards and Technology, 2013. – 31 p. doi: 10.6028/nist.ir.7956.

7. Luna, J. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards [Text] / J. Luna, N. Suri, M. Iorga and A. Karmel // IEEE Cloud Computing. – 2015. – Vol. 2, Issue 3. – P. 32–40. doi:

10.1109/mcc.2015.52.

8. Choo, K. A Cloud Security Risk-Management Strategy [Text] / K. Choo // IEEE Cloud Computing. – 2014. – Vol. 1, Issue 2. – P. 52-56. doi: 0.1109/mcc.2014.27.

9. Зикратов, И. А. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода [Текст] / И. А. Зикратов, С. В. Одегов // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 121–126.

10. Juliadotter, N. Cloud Attack and Risk Assessment Taxonomy [Text] / N. Juliadotter, K. Choo // IEEE Cloud Computing. – 2015. – Vol. 1, Issue 2. – P. 14-20. doi: 10.1109/mcc.2015.2.

11. Аулов, І. Ф. Аналіз формальної модели безпеки хмари NIST [Текст]: Всеукр. межвед. науч.-техн. сб. / І. Ф. Аулов, І. Д. Горбенко // Радиотехника. – 2014. – Вып. 176. – С. 131–137.

12. Конституція України від 28 червня 1996 року. Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

13. Закон України “Про інформацію” від 2 жовтня 1992 року № 2657-XII. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

14. Закон України “Про захист інформації в інформаційно-комунікаційних системах” від 5 липня 1994 року № 80/94-ВР. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

15. Указ Президента України “Про Положення про технічний захист інформації в Україні” від 27 вересня 1990 року № N 1229/99. Режим доступу: https://zakon.rada.gov.ua/laws/show/1229/99#Text.

16. Закон України “Про захист персональних даних” від 01 червня 2010 року № 2297-VI. Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

17. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”: Указ Президента України від

13.02.17 р. № 32. URL: https://www.president.gov.ua/documents/ 322017-21282.

18. Постанова Кабінету Міністрів України “ Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах ” від 29 березня 2006 р. № 373.

19. Бойко В.О. Монографія. Досвід Німеччини у функціонуванні платформ державно-приватного партнерства в сфері кібербезпеки. 2018 р.

20. Довгань О.Д. Інформаційні ресурси: національні та державні, зміст, поняття. 2015.Журнал ‘Інформація і право’. Випуск 15. С. 85-91.

21. Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів // Наукоємні технології. – 2013. – № 3(19). – (Технічні науки). – С. 299-304.

22. Приймак Ю.Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг // Державне управління: теорія та практика. – 2009. – № 2. Режим доступу: www.academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf.

23. Концепція створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів: Розпорядження Кабінету Міністрів України від 05.09.12 р. № 634-р. Режим доступу: http://zakon2.rada.gov.ua/laws/show/634-2012-%D1%80.

24. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 02.12.14 р. № 660. - Режим доступу : http://zakon.rada.gov.ua/go/z0090-15.

25. Марутян Р. Національні інформаційні ресурси як першооснова інформаційного суверенітету України // Актуальні проблеми міжнародної безпеки : український вимір. – К.: ВД “Стилос“, 2010. – С. 496.

26. Про затвердження плану заходів щодо захисту державних інформаційних ресурсів: Розпорядження Кабінету Міністрів України від

5.11.14 р. № 1135-р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1135-2014-%D1%80.

27. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, Адміністрація Держспецзв'язку. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=2A9C287BFE0D1CA5AB75C3EFEC060867.app1?art_id=261878&cat _id=240232.

28. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-19. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2163-19.

29. Щодо створення державної системи захисту критичної інфраструктури: аналітична записка Національного інституту стратегічних досліджень. – Режим доступу : http://www.niss. gov.ua/articles/ 2490.

30. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки: аналітична записка. – (Національний інститут стратегічних досліджень). – Режим доступу: http://www.niss.gov.ua/articles/2532.

31. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України від 6.12.17 р. № 1009-р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1009-2017-%D1%80.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)