УДК 004.056.53(045)

МОДЕЛЬ ЗАХИЩЕНОГО ДАТА-ЦЕНТРУ НА БАЗІ ТЕХНОЛОГІЇ CLOUD COMPUTING

Оксана Коваль, Сергій Бондаровець, Сергій Гнатюк

Стрімке зростання обсягів інформації створює нагальну потребу створення масштабних місць зберігання та накопичення даних. Задачу накопичення та зберігання інформації успішно розв'язують дата-центри – інструменти, які здатні забезпечити та автоматизувати будь-яку бізнес-діяльність. Наразі майже всі постачальники послуг використовують дуже перспективну технологію побудови дата-центрів – Cloud Computing («хмарні» обчислення), яка має низку переваг перед традиційними аналогами. Але проблема захищеності даних, які довіряють постачальнику, є настільки значною, що майже завжди є ризик втратити дані у «хмарі» назавжди. У статті було проведено аналіз існуючих моделей дата-центрів на базі технології Cloud Computing, що дало змогу виявити проблему забезпечення інформаційної безпеки. Зважаючи на це, у статті запропоновано модель захищеного дата-центру на базі технології Cloud Computing, показано її теоретичне обґрунтування та проведено відповідні симуляції, результатом яких є той факт, що розроблена модель вирішує проблему інформаційної безпеки в дата-центрі та може бути використана для побудови центрів обробки даних на базі технології Cloud Computing у різних галузях.

Ключові слова: *дата-центр, «хмарні» технології, інформаційна безпека, уразливість, захищеність, технологічна архітектура, модель загроз.*

Вступ. Інформатизація сучасного суспільства призводить до надзвичайно швидкого зростання кількості даних, які потрібно десь накопичувати, зберігати та обробляти. Для цих задач створюють дата-центри – потужні місця акумулювання інформації, які забезпечують зберігання, обробку, обчислення та передачу десятків ексабайтів. Це безперечно робить дата-центри популярними, зокрема враховуючи й те, що усі послуги надаються у якості оренди. Проте, наразі увага IT-корпорацій розвинених держав прикута до так званих «хмарних» обчислень, які, мають низку переваг та зможуть перетворити роботу дата-центрів на більш зручну та ефективну. «Хмарні» обчислення (Cloud Computing) – технологія надання обчислю-вальних ресурсів і даних для комп'ютерів та інших користувачів за запитом, тобто на вимогу. Згідно із статистикою міжнародної асоціації AFCOM близько 70% всіх існуючих у світі дата-центрів використовують «хмари» під час проведення обчислень. «Хмарні» сховища, безумовно, мають беззаперечну перевагу над звичайними «банками» даних, адже вони дозволяють створити розподілену мережу зберігання; виконувати відновлення після збоїв чи аварій, а також надійно захищати доступ до критично важливих застосунків. Також технологія Cloud Computing забезпечує злагоджену роботу систем зберігання даних, кластерів високої готовності, гіпервізорів, операційних систем, баз даних, програм та застосунків, тобто автоматизує реалізацію процесів у дата-центрах, а також перетворює процес на безперебійний (безперервний).

Незважаючи на такі явні переваги перед традиційними дата-центрами, технологія Cloud Computing має досить істотний недолік, який є значною перешкодою для вибору її як основи для архітектури дата-центру. Головною проблемою є питання довіри постачальнику, адже безпека даних може бути під загрозою та існує ризик масової втрати даних багатьма користувачами через технічний збій у постачальника хмарних послуг. Зважаючи на це, користувач не може довірити «хмарі» всі дані не лише для обробки, але й для зберігання.

1. Аналіз існуючих досліджень та постановка завдання

1.1. Типи сучасних дата-центрів

На сьогодні дата-центри надають велику кількість послуг, специфіка яких залежить вид типу дата-центру. Виділяють наступні типи дата-центрів [17, 21, 19]: *приватні хмарні провайдери; наукові обчислювальні центри; co-location центри* (один із прикладів багатокористувацьких дата-центрів, co-location простір може бути продано організаціям під стійку, шафу або кабіну); *«in-house» дата-центри* (знаходяться у володінні і керуються компаніями); *wholesale дата-центри* (провайдери, які продають чи здають в оренду простір дата-центру у більшому обсязі, ніж у co-location дата-центрах і, як правило, мають меншу кількість клієнтів); *виділений хостинг* (провайдер обслуговує та/або здає в оренду потужності серверів для окремих клієнтів); *віртуальний (shared) хостинг* (провайдер, клієнти якого ділять продуктивність сервера).

Важливішою характеристикою є набір компонентів дата-центру, а саме Tier (ярус, рівень),

тобто атрибут того, що він може запропонувати споживачеві: фізична інфраструк-тура, система охолодження, енергозабезпечення, зарезер-вування та час безперебійної роботи – усе це визначає надмірність всіє інфраструктури. Загалом таких рівнів є чотири, кожен з яких включає в себе попередні рівні та має більший час безперебійної роботи (uptime level) [9, 11].

Злагоджена робота усіх компонентів дата-центру залежить від його архітектури. Загальна архітектура складається з інженерної системи, системи безпеки, IT-інфраструктури та системи моніторингу, яка здійснює огляд та контроль над іншими системами [4]. Загальний опис рівнів дата-центрів показано в табл. 1.

Таблиця 1

Узагальнений опис Data Center Tiers

Tier 1	Незарезервовані компоненти потужності (єдині висхідні лінії зв'язку та сервери)
Tier 2	Tier 1 + надлишкові компоненти потужності
Tier 3	Tier 1 + Tier 2+подвійне живлення та декілька висхідних ліній зв'язку (uplinks)
Tier 4	Tier 1 + Tier 2 + Tier 3 +усі компоненти повністю відмовостійкі, включаючи uplinks, зберігання, охолодження, системи кондиціонування та вентиляції, сервери і т.д. все з подвійним живленням.

Необхідним аспектом дизайну дата-центру є використання багаторівневого підходу, адже це впливає на продуктивність, стійкість і масштабованість [7]. Іншим важливим аспектом архітектури дата-центру є гнучкість та швидкість розгортання і підтримка нових послуг. Проектування гнучкої архітектури, яка має можливість підтримки нових застосунків у стислі терміни може призвести до значної конкурентної переваги. Така конструкція вимагає твердого початкового планування і вдумливого розгляду в областях щільності портів, пропускної здатності висхідних ліній рівня доступу, істинної потужності сервера тощо [8]. На рис. 1 показано основну багаторівневу конструкцію архітектури.

1.2. Технологія Cloud Computing

Фактично хмарні обчислення (Cloud Computing) – це надання на вимогу клієнтів обчислювальних ресурсів (усіх від додатків до дата-центрів) через Інтернет на основі плати за використання [5]. Основні характеристики технології Cloud Computing [16]: само-обслуговування на вимогу; широкий доступ до мережі; об'єднання ресурсів; швидка еластичність.

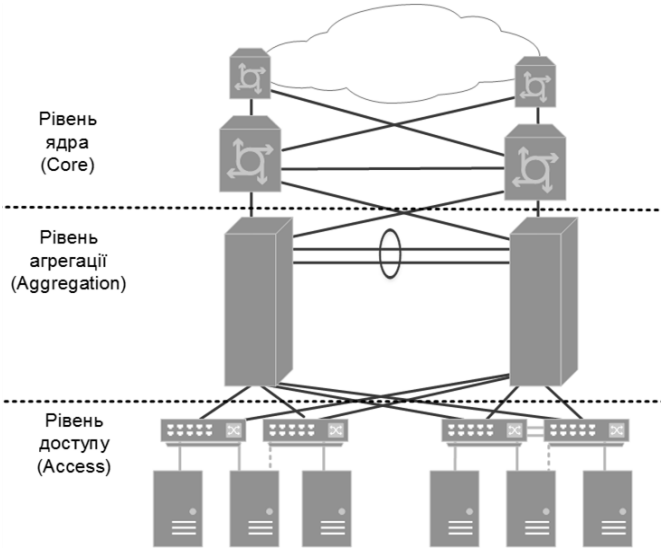


Рис. 1. Базова багаторівнева конструкція мережевої архітектури

Виділяють три основні сервісні моделі [18]:

1) Програмне забезпечення як сервіс (Software as a Service (SaaS)) забезпечує запуск «хмарних» застосунків на віддалених комп'ютерах в «хмарі», яка належить провайдеру [1].

2) Платформа як сервіс (Platform as a Service (PaaS)) забезпечує хмарне середовище всім необхідним для підтримки повного життєвого циклу застосунків шляхом надання доступу до використання інформаційно-технологічних платформ [3].

3) Інфраструктура як сервіс (Infrastructure as a Service (IaaS) забезпечує компанії обчислювальними ресурсами, включаючи сервери, мережі, пам'ять і просторами дата-центрів на основі плати за використання.

Крім цього, існують і різні *моделі розгортання хмарних технологій*: *1) приватна хмара (private cloud)* це інфраструктура, що працює виключно для однієї організації, навіть знаходячись під власним управлінням чи третьої особи [15]; *2) публічна хмара (public cloud)* знаходиться у володінні та управляється компаніями, що пропонують швидкий доступ через публічну мережу до доступних обчислювальних ресурсів [6]; *3) гібридна хмара (hybrid cloud)* – приватний хмарний фон, поєднаний із стратегічною інтеграцією та використанням послуг публічної хмари [12].

Вимоги до інформаційної безпеки «хмарних» дата-центрів засновані на еталонній моделі архітектури, яка описана в («Security Recommendations for Cloud Computing Providers (CPS)» Федерального агентства Німеччини з інформаційної безпеки (BSI). Ця еталонна архітектура (рис. 2) приблизно показує

компоненти, загальні для багатьох платформ хмарних обчислень [10, 13, 14, 20].

1.3. Сучасні моделі дата-центрів

У табл. 2 показано порівняльний аналіз досліджених моделей дата-центрів з точки зору їх архітектури та інформаційної безпеки. Умовні позначення: «+» – відповідність критерію; «–» – відсутність відповідності критерію; «?» – відсутність інформації у відкритих джерелах; К – конфіденційність; Ц – цілісність; Д – доступність.

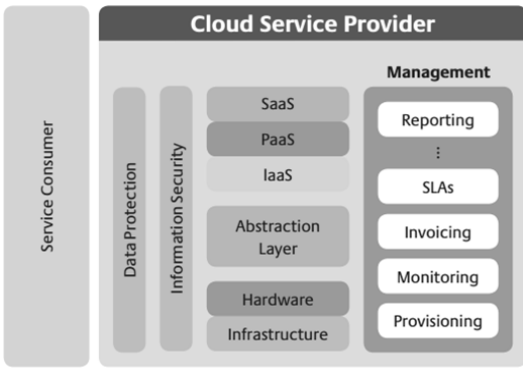


Рис. 2. Еталлона архітетура для платформи Cloud Computing

Таблиця 2

Аналіз відомих моделей реалізації дата-центрів

Моделі дата-центрів	Технологія	Компоненти	К	Ц	Д	Відсутність уразливостей
Воля Дата-центр	Saas	Tier 2/Tier 3	+	?	+	–
Data Center DataGroup	Saas	Tier 3	?	+	+	–
BEMOBILE	Saas	Tier 3 (комунікація Tier 4)	+	+	+	–
Amazon Data Center	Saas, PaaS, IaaS	Tier 4	+	?	+	–
Google Data Center	Saas, PaaS, IaaS	Tier 3+	?	?	?	–
Yandex Data Center	Saas	Tier 3	+	?	+	?
Tulip Data Center	IaaS	Tier 3+	+	+	+	+
Lakeside Tech. Center	IaaS	Tier 4	?	+	+	?
Microsoft Data Center	Saas, PaaS	Tier 4	+	?	+	–
Range International IG	PaaS, IaaS	Tier 4	?	?	+	?
Switch SuperNAP	SaaS, IaaS	Tier 3/ Tier 4	+	+	+	?
DuPont Fabros Tech.	Saas, PaaS, IaaS	Tier 4	+	?	+	+
Utah Data Center	Saas	Tier 3/ Tier 4	?	?	?	–

Аналізуючи табл. 2 з точки зору порівняння відомих прикладів реалізації моделей дата-центрів на базі технології Cloud Computing, можна зробити висновок, що розглянуті дата-центри побудовані на одній, або поєднують декілька з технологій (моделей послуг). Набір компонентів дата-центру відповідає вищим рівням Tier – це означає те, що інфраструктури майже або повністю відмовостійкі, системи життєзабезпечення мають резервні компоненти, а очікуваний час безперебійної роботи більше 99%.

Стосовно кожного дата-центру було проаналізовано систему забезпечення та моніторингу безпеки даних і, як показано у табл. 2, лише для трьох дата-центрів є достовірні та офіційні дані, які стосуються безпеки інформації (BEMOBILE, Tulip Data Center та Switch SuperNAP). Що стосується інших, то проаналізована інформація свідчить про гарантоване забезпечення лише окремих характеристик безпеки інформації. Але, наприклад, дані про Google Data Center та Utah Data Center є обмеженими в доступі, проте це не означає, що К, Ц чи Д не забезпечуються. Обмеження доступу до даних зумовлене в основному їх специфікою (Utah Data Center – дата-центр АНБ США). Тобто офіційних даних, які могли б підтвердити чи спростувати ефективність системи забезпечення інформаційної безпеки (як частини мережевої системи) в відкритих джерелах немає.

Не менш важливим критерієм є відсутність відомих уразливостей [2, 4]. Відповідно до табл. 2 майже для всіх дата-центрів були зафіксовані такі випадки, від потужного удару блискавки по будівлі дата-центру до багаторазових мережевих атак. Єдині дата-центри для яких уразливостей не виявлено (або дані про них приховані) – це Tulip Data Center та DuPont Fabros Technology. Загалом такий аналіз свідчить про наявність проблеми забезпечення безпеки інформації навіть за майже ідеальних інженерних та IT-інфраструктурних систем. Усунення цих недоліків вирішується створенням відповідної моделі. З огляду на це, ***метою роботи є*** розробка моделі захищеного дата-центру на базі технології Cloud Computing.

2. Основна частина дослідження

2.1. Розробка моделі захищеного дата-центру на базі технології Cloud Computing

Першим етапом розробки моделі є побудова технологічної архітектури, яка включає три основні «будівельні» блоки.

1) Блок 10 Gigabit Ethernet. Дата-центр розроблено з високою щільністю віртуальних машин, які поєднанні з великою кількістю процесорів. З точки зору мережі, зростання віртуальних машин та концентрації ядер сприятиме переходу до 10 Gigabit Ethernet як необхідного механізму для надавання серверів. Конкретні переваги переходу включають в себе конфігурацію політик в режимі реального часу, мобільну безпеку та політику мережі, безперервну роботу моделі управління, що встановлює управління і експлуатацію середовища для віртуальних машин та фізичних серверів тощо.

2) Блок Unified Fabric (уніфікована структура), який надає усім серверам (фізичним чи віртуальним) доступ до локальної мережі, мережі зберігання даних та IPC мережі, що дає змогу бути більше об'єднаним у мережу замовника для підвищення ефективності та економії витрат.

3) Блок Unified Computing (уніфіковане обчислення). Уніфікована структура дає змогу повністю віртуалізувати «хмарний» дата-центр з пулами комп'ютерних, мережевих та інших ресурсів. Цей блок перекриває storage silos (місткість для збереження даних) в класичному центрі обробки даних, що дозволяє ефективніше використовувати інфраструктури у повністю віртуалізованому середовищі і створює єдину архітектуру, використовуючи стандартні технології, які забезпечують сумісність і захист інвестицій.

На рис. 3 показано технологічну архітектуру, яка відображає «хмарний» дата-центр наступного покоління. На схемі зображені лише приклади складових блоків для дата-центру. Загалом закінчена архітектура містить не лише компоненти структури але й регулюється різними типами сервісних та регулятивних вимог.

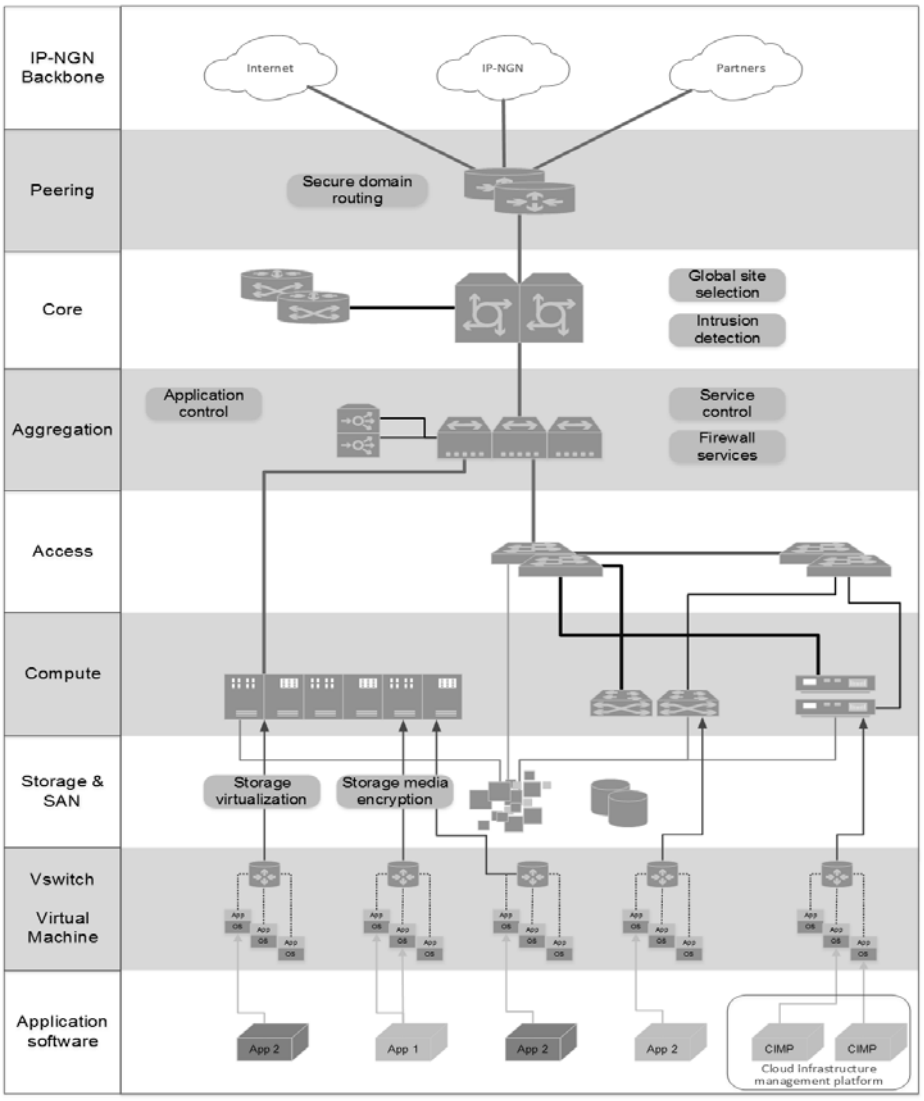


Рис. 3. Технологічна архітектура дата-центру на базі технології Cloud Computing

В архітектурі (рис. 3) запропоновано 9 ярусів мережі дата-центру: 1) програмного забезпечення (application software); 2) віртуальної машини та розподіленого віртуального комутатора (virtual machine, VSwitch); 3) зберігання та мережі зберігання даних (storage, SAN); 4) обчислення (compute); 5) доступу (access); 6) агрегації (aggregation); 7) ядра (core); 8) пірінгу (peering); 9) основи мережі Інтернет (IP-NGN backbone).

Кожен наступний рівень пов'язаний з попереднім за допомогою певного типу з'єднання. Від ярусу application software до ярусу Virtual machine&VSwitch зв'язок типу App to HW/VM (HW – hardware), далі дані застосунків від віртуальних машин поступають на розподілені віртуальні багаторівневі комутатори VSwitch.

Потім дані з мережі зберігання даних (SAN) та дані застосунків з VSwitch передаються на ярус обчислень за допомогою відповідно 4G FC (fibre chanel – оптоволоконний канал) та VSwitch to HW. Результати обчислень поступають на ярус доступу через 4G FC, 10G FCoE (Fibre Channel over Ethernet) та 1G Ethernet, а з цього ярусу до рівня агрегації через 10G Ethernet. На цьому ярусі відбувається контроль застосунків і сервісів та встановлюються сервіси фаєрвола (IDS, SSL, anti-DDoS).

Наступний ярус – це ядро, де також застосовуються процедури глобального місця вибору розташування та виявлення вторгнень. На ярусі пірінгу (взаємозв'язку окремих мереж з метою обміну трафіком між користувачами кожної мережі) відбувається захищена маршрутизація домену. Останній ярус – це мережа Інтернет, використовується тип з'єднання 10G Ethernet.

Поряд з технологічною складовою архітектури дата-центрів, важливе місце займає також питання довіри до моделі інфраструктури «хмарних» обчислень. На рис. 4 показано структуру захищеного дата-центру на базі технології Cloud Computing з позиції захищеності, а саме моделі загроз та заходів, які потрібно прийняти для мінімізації ризиків. Структура відображає також повний контроль, дотримання вимог та угод про рівень послуг.

Ключова ідея цієї моделі полягає у тому, що інформаційна безпека не повинна бути другорядною чи просто частиною загальної безпеки – вона має поширюватись та бути реалізованою на всіх рівнях архітектури.

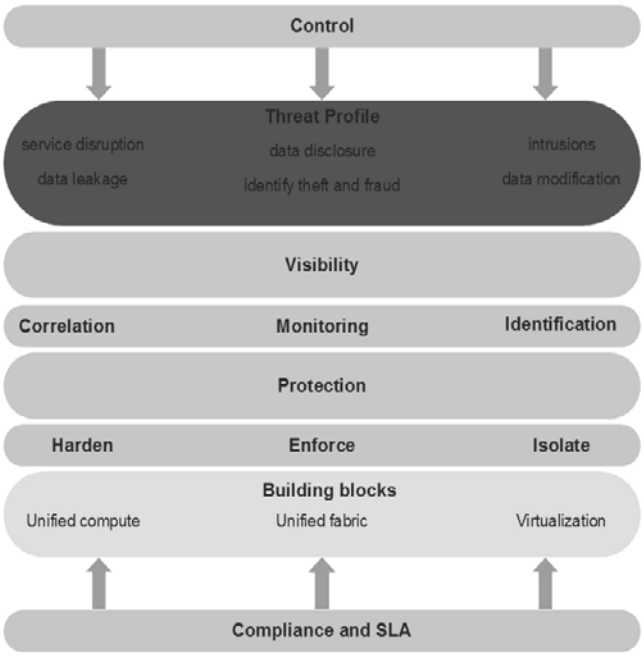


Рис. 4. Структура захищеного дата-центру на базі технології Cloud Computing

Побудова захищеної архітектури «хмарного» дата-центру включає в себе впровадження шести рівнів безпеки, а саме: 1) фізичний захист; 2) захист серверів; 3) захист даних; 4) захист додатків та платформ; 5) захист мережі; 6) захищена система шифрування та управління ключами.

На рис. 5 відображено співвідношення рівнів захисту «хмарного» дата-центру та їх взаємодія:

Рис. 5. Рівні захищеної архітекрути «хмарного» дата-центру з позиції інформаційної безпеки

2.2. Експериментальне дослідження моделі захищеного дата-центру

Система симуляції CloudSim

Платформа CloudSim – це узагальнене і масштабований засіб симуляції, що дозволяє здійснювати повноцінне моделювання і симуляцію хмарних обчислювальних систем і інфраструктур, у тому числі і побудову дата-центрів з використанням «хмари». Вона є розширенням базової функціональності платформи GridSim, забезпечуючи можливість

моделювання сховища даних, веб-сервіси, розподіл ресурсів між віртуальними машинами.

Запропонована модель захищеного дата-центру реалізується на платформі CloudSim таким чином:

1) встановлюється провайдер сервісу та Інтернет провайдер контенту для зберігання даних у середовищі «хмарних» обчислень та використання «хмарних» сервісів;

2) запускається модуль аналізу часу, вартості та ресурсів використання дата-центру;

3) застосовується евристичний алгоритм планування завдання для виконання їх в режимі реального часу;

4) ефективне забезпечення ресурсів та вимірювання продуктивності роботи на основні зазначеного алгоритму;

5) CloudSim використовує «Green computing», що дозволяє нівелювати простої сервера для збереження рівня енергії;

6) велика увага приділяється безпеці гіпервізора в «хмарі», враховуються атаки на віртуальні машини;

7) включення модулів захисту «хмарних» обчислень, застосовуючи інструменти для моделювання розподілених атак відмови інфраструктури та інструмент аналізу впливу DDoS атак;

8) використання запропонованої ієрархічної моделі дата-центру (розробленої у п. 2.1) шляхом порівневого (поетапного) підключення різних ярусів архітектури;

9) застосування політик безпеки: від політики захищеної локації віртуальних машин до системи моніторингу.

У табл. 3 відображено характеристики розробленої моделі дата-центру на базі технології Cloud Computing з точки зору архітектури.

Таблиця 3

Характеристики розробленої моделі «хмарного» дата-центру «DCM»

Дата-центр	Технологія	Компоненти	Модель «хмари»
DCM	IaaS, SaaS	Tier 3	Гібридна

На рис. 6. зображена схема симуляції дата-центру на платформі CloudSim, реалізація якої відбувається у режимі реального часу симуляції. Повноцінна модель захищеного дата-центру на базі технології Cloud Computing будується шляхом підключення до базової моделі дата-центру різних рівнів захисту: шифрування та управління ключами; захист від шкідливого програмного забезпечення; конфігурований файєрвол; віддалене управління з використанням SSH, TLS/SSL, IPSec; багаточинникова аутентифікація; використання регулярних резервних копіювань; використання політик віртуальних машин тощо.

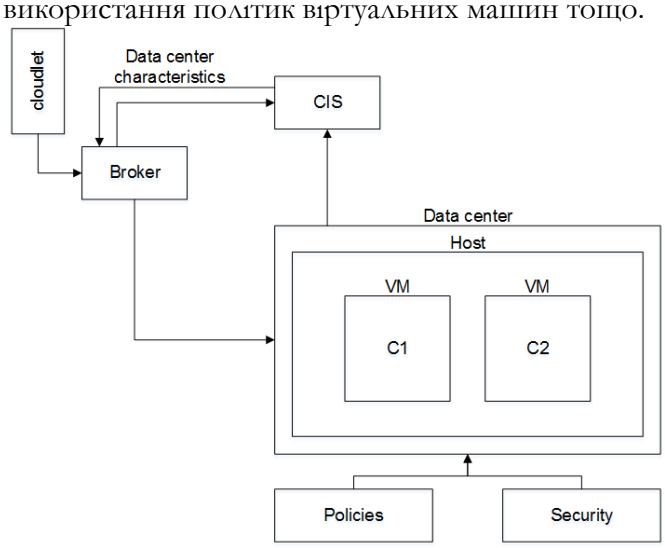
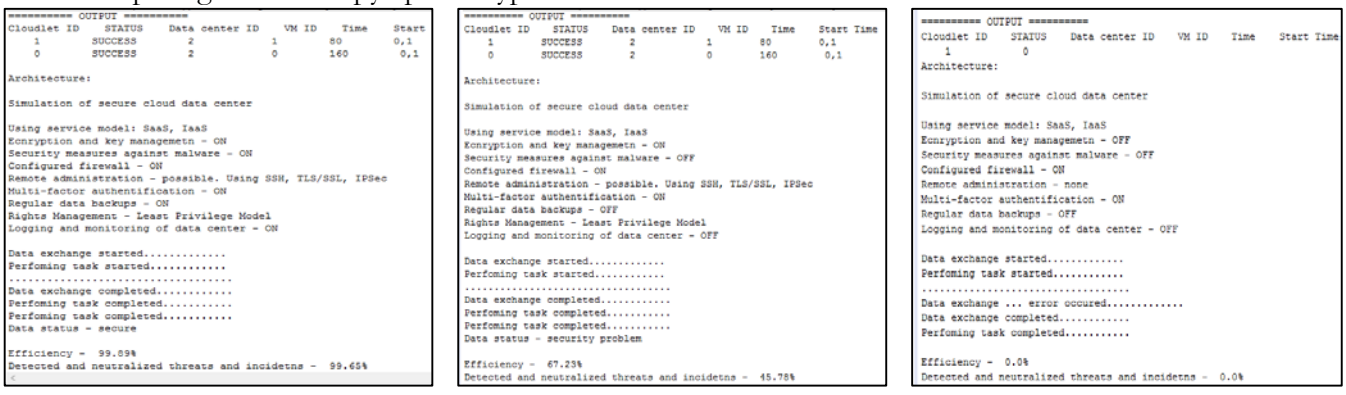


Рис. 6. Схема роботи процесу моделювання

Для дослідження розробленої системи було проведено три експерименти (рис. 7).



а *б* *в*

Рис. 7. Підключення до базової моделі: всіх рівнів захисту (а), вибіркових рівнів захисту (б), без застосування жодних рівнів захисту (в)

Порівняння результатів проведення симуляцій на платформі CloudSim наведено у табл. 4:

Таблиця 4

Порівняння результатів проведення симуляцій

№ експе-рименту	Рівні захисту	Ефек-тивність	Детектовані та знешкоджені атаки
1	100%	99,89%	99,65%
2	<50%	67,23%	45,78%
3	0%	0,0%	0,0%

Результати експериментів свідчать про те, що при підключені усіх рівнів захисту ефективність (під якою розуміємо «швидкодію + захищеність даних») та рівень детектованих і знешкоджених атак становить майже 100%; під час проведення другого експерименту при підключені менше 50% рівнів захисту ефективність роботи і рівень детектованих та знешкоджених атак зменшились майже у половину; а під час проведення третього експерименту, коли рівні захисту взагалі не підключались, то ефективність роботи і рівень детектованих та знешкоджених атак, як і результати симуляції – нульові.

Система симуляції OPNET IT

Платформа OPNET IT (Riverbed Modeler) – інструмент для створення сценаріїв інфраструктур з використанням «хмарних» обчислень та подальшого їх моделювання. З використанням цієї системи симуляції було реалізовано розроблену модель, з позиції технологічної архітектури, з підключенням деяких вбудованих засобів захисту основних компонентів: «хмари», серверів, клієнта.

Спрощену технологічну модель, перенесену на платформу OPNET IT, показано на рис. 8

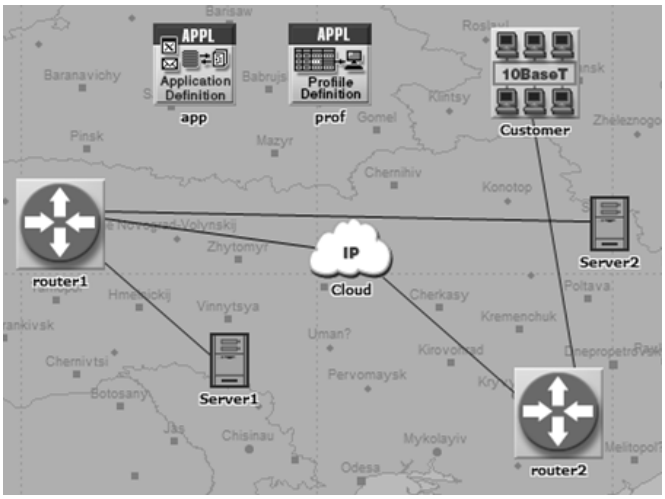


Рис. 8. Адаптована до середовища симуляції модель захищеного дата-центру

Використовуючи вбудовані властивості компонентів системи OPNET IT підключаємо рівні захисту. На жаль, не всі рівні захисту, описані в п. 2.1, можна включити, зважаючи на специфіку платформи OPNET IT.

Наступний крок – конфігурування процесу симуляції, визначення часу, протягом якого вона буде відбуватися, та власне запуск. Під час запуску симуляції її час адаптується до реального часу (наприклад, час симуляції 1 година на платформі OPNET IT насправді буде відбуватися 1 хв.). Лог-файли результатів симуляції відображають лише загальна дані: прогрес, швидкість, час (рис. 9).

```
156 | Speed: Average (827,711 events/sec.); Current (712,253 events/sec.)
157 | Time : Elapsed (6.6 sec.); Remaining (38 sec.)
158 | DES Log: 8 entries
159 |---------------------------------------------------------------
160 |---------------------------------------------------------------
161 | Progress: Time (11 min. 11 sec.); Events (6,000,143)
162 | Speed: Average (828,176 events/sec.); Current (833,334 events/sec.)
163 | Time : Elapsed (7.2 sec.); Remaining (35 sec.)
164 | DES Log: 8 entries
165 |---------------------------------------------------------------
166 |---------------------------------------------------------------
167 | Progress: Time (11 min. 59 sec.); Events (6,500,148)
168 | Speed: Average (833,458 events/sec.); Current (902,534 events/sec.)
169 | Time : Elapsed (7.8 sec.); Remaining (32 sec.)
170 | DES Log: 8 entries
```

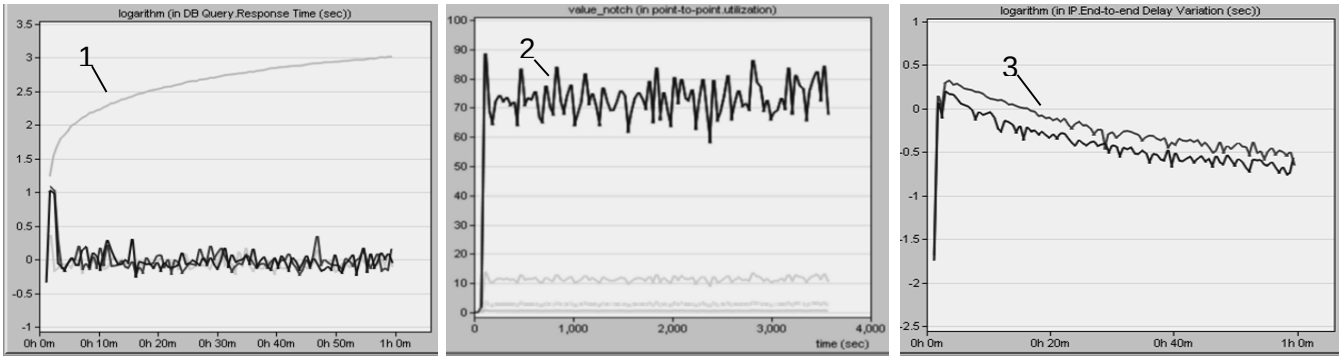
Рис. 9. Результат симуляції у вигляді лог-файла

Аналогічно до методики проведення симуляції у системі CloudSim було проведено три експерименти з різними умовами, тобто кожного разу використовувалися різна кількість рівнів захисту. Після проведення всіх експериментів у вбудованому редакторі платформи OPNET IT були побудовані та порівняні такі графіки (рис. 10): ефективність роботи сервера за умов підключення захисту та без, результати роботи мережі з використанням засобів захисту та без них, результати симуляції відносно кінцевого споживача.

На рис. 10 (а) зображено криву ефективності роботи серверу з використанням усіх рівнів захисту (1), а інші криві – ефективність без включення таких засобів. Отже, з використанням засобів захисту, ефективність та захищеність серверу набагато більша.

На рис. 10 (б) зображено криву ефективності роботи мережі з використанням усіх рівнів захисту (2), а інші криві – ефективність без включення таких засобів. Очевидно, що з використанням засобів захисту, ефективність та захищеність мережі набагато вища.

На рис. 10 (в) зображено криву ефективності роботи дата-центру з кінцевим споживачем за умови використанням усіх рівнів захисту (3), а інші криві – ефективність без включення таких засобів. За умов включення засобів захисту, ефективність роботи дата-центру з кінцевим споживачем більша та відбувається за допомогою захищеної комунікації.



а *б* *в*

Рис. 10. Графіки ефективності роботи: серверу дата-центру (а), мережі дата-центру (б), дата-центру з кінцевим споживачем (в)

Провівши усі відповідні симуляції, отримані результати було порівняно з відомими моделями дата-центрів (див. табл. 2) та визначено, що розроблена модель захищеного дата-центру позбавлена виявлених під час аналізу недоліків.

Висновки

У цій статті було проаналізовано сучасні підходи до побудови дата-центрів, що дало змогу виявити основні особливості їх побудови з точки зору архітектури та інформаційної безпеки. Було виділено та досліджено моделі дата-центрів на базі технології Cloud Computing, виявлено проблему забезпечення інформаційної безпеки за майже ідеальних інженерних та інфраструк-турних рішень. Виявлені недоліки були усунуті за допомогою розробки моделі захищеного дата-центру на базі технології Cloud Computing, яка за рахунок використання технологічної архітектури, високошвидкісної комунікації, уніфікованих структур та обчислень дозволяє забезпечити захищеність дата-центру на базі технології Cloud Computing і провести відповідні симуляції. Розроблена модель може бути використана для побудови дата-центрів у різних галузях. Крім того, були сформульовані практичні вимоги, які можуть бути використані архітекторами при розробці та проектуванні різних дата-центрів (особливо на базі технології Cloud Computing).

ЛІТЕРАТУРА

[1]. Безопасность как головная боль облачных вычислений [Електронний ресурс] / А. Иванов. – Режим доступу: World Wide Web. – URL: http://www.cnews.ru/reviews/free/saas/articles/articles12.shtml.

[2]. Безопасность облачных вычислений [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://ru.thales-esecurity.com/solutions/by-business-issue/cloud-computing-security

[3]. Модели "облачных" технологий [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://wiki.vspu.ru/workroom/adb91/index

[4]. Угрозы облачных вычислений и методы их защиты [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://habrahabr.ru/post/183168/

[5]. Boniface M. Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds / M. Boniface // 5th International Conference on Internet and Web Applications and Services (ICIW (Barcelona, Spain: IEEE, 2010), P. 155-160.

[6]. Breaking down what's in your cloud SLA [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://searchcloudcomputing.techtarget.com/essentialguide/Breaking-down-whats-in-your-cloud-SLA.

[7]. Data Center Architecture Overview [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_1.html.

[8]. Data Center Design Models Overview [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_1.html#wp1058588.

[9]. Data Center Tiers Explained [Електронний ресурс] / B. Hatton. – Режим доступу: World Wide Web. – URL: http://webcache.googleusercontent.com/search?q=cache:http://www.thedatacave.com/data-center-tiers-explained&gws_rd=cr&ei=VEvoVsSRKcL8swG78ZH4 BQ.

[10]. Dodani M. Architected Cloud Solutions Revealed / M. Dodani // Journal of Object Technology. – 2010. – Vol. 9 (2). – P. 27-36.

[11]. Explain: Tier 1 / Tier 2 / Tier 3 / Tier 4 Data Center [Електронний ресурс] / V. Gite. – Режим доступу: World Wide Web. – URL: http://www.cyberciti.biz/faq/data-center-standard-overview.

[12]. Hybrid cloud: is it right for your business? [Електронний ресурс] / D. Athow. – Режим доступу: World Wide Web. – URL: http://www.techradar.com/news/internet/cloud-services/hybrid-cloud-is-it-right-for-your-business--1261343.

[13]. NIST Cloud Computing Reference Architecture [Електронний ресурс] / Dr.FangLiu, JinTong,Dr.JianMa. – Режим доступу: World Wide Web. – URL: http://collaborate.nist.gov/ twiki-cloud-computing/pub/CloudComputing/ ReferenceArchitectureTaxonomy/NIST_CC_Reference_Architecture_v1_March_30_2011.pdf.
[14]. Security Recommendations for Cloud Computing Providers. White Paper / Federal Office for Information Security. – GmbH.: Druckpartner Moser Druck, 2011. – 71 p.
[15]. Self-Run Private Cloud [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.govconnection.com/IPA/PM/Info/ Cloud-Computing/Self-Run-Private-Cloud.htm.
[16]. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology [Електронний ресурс] / NIST Computer Security Division, Information Technology Laboratory. Електрон.дані. – Gaithersburg: National Institute of Standards and Technology. – 2011. – Режим доступу: World Wide Web. – URL: http://nvlpubs.nist.gov/ nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
[17]. Understanding the Different Types of Data Center Facilities [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.cyrusone.com/blog/understanding-the-different-types-of-data-center-facilities.
[18]. What is cloud computing [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.ibm.com/cloud-computing/what-is-cloud-computing.html.
[19]. What type of data center do you need? [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.compassdata centers.com/type-data-center-need/
[20]. Whitepaper Cloud Computing Use Cases Version 3.0, produced by the Cloud Computing Use Case Discussion Group [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://opencloudmanifesto.org/cloud_computing _use_cases_whitepaper-3_0.pdf.
[21]. 4 types of data centers [Електронний ресурс] / A. Lesser. – Режим доступу: World Wide Web. – URL: https://gigaom.com/2012/10/15/4-types-of-data-centers/

REFERENCES

[1]. Security as a headache of cloud computing [E-resource] / A. Ivanov. – Mode access: World Wide Web. - URL: http://www.cnews.ru/reviews/free/saas/ articles/articles12.shtml.
[2]. Cloud Security [E-resource]. – Access mode: World Wide Web. - URL: http://ru.thales-esecurity.com/ solutions/by-business-issue/cloud-computing-security.
[3]. Models of cloud technologies [E-resource]. – Access mode: World Wide Web. – URL: http://wiki.vspu.ru /workroom/adb91/index
[4]. Threats of Cloud Computing and methods of their protection [E-resource]. – Access mode: World Wide Web. - URL: https://habrahabr.ru/post/183168/
[5]. Boniface M. Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds / M. Boniface // 5th International Conference on Internet and Web Applications and Services (ICIW (Barcelona, Spain: IEEE, 2010), P. 155–160.
[6]. Breaking down what's in your cloud SLA [E-resource]. – Access mode: World Wide Web. – URL: http://searchcloudcomputing.techtarget.com/essentialguide/Breaking-down-whats-in-your-cloud-SLA
[7]. Data Center Architecture Overview [E-resource]. – Access mode: World Wide Web. – URL: http://www.cisco.com/c/en/us/td/docs/solutions /Enterprise/Data_Center/DC_Infra2_5/DCInfra_1.html
[8]. Data Center Design Models Overview [E-resource]. – Access mode: World Wide Web. – URL: http://www.cisco.com/c/en/us/td/docs/solutions /Enterprise/Data_Center/DC_Infra2_5/DCInfra_ 1.html#wp1058588.
[9]. Data Center Tiers Explained [E-resource] / B. Hatton. – Access mode: World Wide Web. – URL: http://webcache.googleusercontent.com/ search?q=cache:http://www.thedatacave.com/data-center-tiers-explained&gws_rd=cr&ei=VEvoVsSR KcL8swG78ZH4 BQ.
[10]. Dodani M. Architected Cloud Solutions Revealed / M. Dodani // Journal of Object Technology. – 2010. – Vol. 9 (2). – P. 27-36.
[11]. Explain: Tier 1 / Tier 2 / Tier 3 / Tier 4 Data Center [E-resource] / V. Gite. – Access mode: World Wide Web. – URL: http://www.cyberciti. biz/faq/data-center-standard-overview/
[12]. Hybrid cloud: is it right for your business? [E-resource] / D. Athow. – Access mode: World Wide Web. – URL: http://www.techradar.com/ news/ internet/cloud-services/hybrid-cloud-is-it-right-for-your-business—1261343.
[13]. NIST Cloud Computing Reference Architecture [E-resource] / Dr.FangLiu,JinTong,Dr.JianMa. – Access mode: World Wide Web. – URL: http://collaborate.nist.gov/twiki-cloud-computing/ pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_CC_Reference_Architecture_v1_March_30_2011.pdf.
[14]. Security Recommendations for Cloud Computing Providers. White Paper / Federal Office for Information Security. – GmbH.: Druckpartner Moser Druck, 2011. – 71 p.
[15]. Self-Run Private Cloud [E-resource]. – Access mode: World Wide Web. – URL: http://www.gov connection.com/IPA/PM/Info/Cloud-Computing/ Self-Run-Private-Cloud.htm.
[16]. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology [E-resource] / NIST Computer Security Division, Information Technology Laboratory. – Gaithersburg: National

Institute of Standards and Technology. – 2011. – Access mode: World Wide Web. – URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
[17]. Understanding the Different Types of Data Center Facilities [E-resource]. – Access mode: World Wide Web. – URL: http://www.cyrusone.com/blog/understanding-the-different-types-of-data-center-facilities/
[18]. What is cloud computing [E-resource]. – Access mode: World Wide Web. – URL: http://www.ibm.com/cloud-computing/what-is-cloud-computing.html.
[19]. What type of data center do you need? [E-resource]. – Access mode: World Wide Web. – URL: http://www.compassdatacenters.com/type-data-center-need/
[20]. Whitepaper Cloud Computing Use Cases Version 3.0, produced by the Cloud Computing Use Case Discussion Group [E-resource]. – Access mode: World Wide Web. – URL: http://opencloudmanifesto.org/cloud_computing_use_cases_whitepaper-3_0.pdf.
[21]. 4 types of data centers [E-resource] / A. Lesser. – Access mode: World Wide Web. – URL: https://gigaom.com/2012/10/15/4-types-of-data-centers/

МОДЕЛЬ ЗАЩИЩЕННОГО ДАТА-ЦЕНТРА НА БАЗЕ ТЕХНОЛОГИИ CLOUD COMPUTING

Стремительный рост объемов информации создает неотложную необходимость создания масштабных мест хранения и накопления данных. Задачу накопления и хранения информации успешно решают дата-центры – инструменты, которые способны обеспечить и автоматизировать любую бизнес-деятельность. Сейчас почти все поставщики услуг используют очень перспективную технологию построения дата-центров – Cloud Computing («облачные» вычисления), которая имеет ряд преимуществ перед традиционными аналогами. Но проблема защищенности данных, которые доверяют поставщику, настолько значительной, что почти всегда есть риск потерять данные в «облаке» навсегда. В статье был проведен анализ существующих моделей дата-центров на базе технологии Cloud Computing, что позволило выявить проблему обеспечения информационной безопасности. Исходя их этого, в статье предложена модель защищенного дата-центра на базе технологии Cloud Computing, показано ее теоретическое обоснование и проведены соответствующие симуляции, результатом которых является тот факт, что разработанная модель решает проблему информационной безопасности в дата-центре и может быть использован для построения центров обработки данных на базе технологии Cloud Computing в различных сферах.

Ключевые слова: дата-центр, «облачные» технологии, информационная безопасность, уязвимость, защищенность, технологическая архитектура, модель угроз.

SECURED DATA CENTER MODEL BASED ON CLOUD COMPUTING TECHNOLOGY

The rapid growth of information creates an urgent need for the establishment of large-scale storage and accumulation of data. The task of information collecting and storing is successfully resolved by data centers – tools that are able to secure and automate any business activity. Currently, almost all the service providers use a very promising technology for data centers – Cloud Computing, which has several advantages over traditional data centers. The problem of data protection that is trusted to the vendor, is so great that usually the risk of losing data in the «cloud» forever. In this paper, there is an analysis of existing models of data center technology based on Cloud Computing, which helped to identify the problem of information security. Therefore, in the paper there is proposed the model of secure data center based on technology of Cloud Computing, showed its theoretical foundation and conducted appropriate simulation, the result of which is the fact that the developed model solves the problem of information security in the data center and can be used in creation data centers based on technology Cloud Computing in different spheres.

Keywords: data center, «cloud» technology, information security, vulnerability, security, technology architecture, threats model.

Коваль Оксана Сергіївна, студентка бакалаврату кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: oksanakoval@mail.ua
Коваль Оксана Сергеевна, студентка бакалавраата кафедры безопасности информационных технологий Национального авиационного университета.
Koval Oksana, Bachelor Student of IT-security Academic Dept in National Aviation University.

Бондаровець Сергій Сергійович, студент бакалаврату кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: bondss29@gmail.com
Бондаровец Сергей Сергеевич, студент бакалавраата кафедры безопасности информационных технологий Национального авиационного университета.
Bondarovets Serhii, Bachelor Student of IT-security Academic Dept in National Aviation University.

Гнатюк Сергій Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua
Гнатюк Сергей Александрович, кандитат технических наук, доцент, доцент кафедры информационных технологий Национального авиационного университета.
Gnatyuk Sergiy, PhD in Eng, Associate Professor of IT-security Academic Dept in National Aviation University.