МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НАУКОВО-ПРАКТИЧНИЙ ВИМІР В УМОВАХ ВОЄННИХ ВИКЛИКІВ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов’язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

ISBN 978-617-8430-05-4

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

Казакова Надія Феліксівна
Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук, професор

Кулешова Євгенія Романівна
Національний університет «Одеська юридична академія»,
аспірант кафедри кібербезпеки

ВИБІР ТИПУ ХМАРНИХ ПОСЛУГ ТА РИЗИК ВИТОКУ ЧУТЛИВОЇ ІНФОРМАЦІЇ

У сучасному світі, де інформація є найважливішим активом, її захист набуває критичного значення. Ми живемо у час, коли дані переміщуються зі швидкістю світла, а їхнє зберігання та обробка вимагають все більших обсягів та складності. Таке середовище створює ідеальні умови не тільки для інновацій та прогресу, але й для нових видів загроз.

Витік чутливої інформації може стати причиною значних фінансових втрат, підриву довіри та навіть національної безпеки. Неважливо, чи це стосується особистих даних, фінансової інформації компанії, комерційних секретів або державних таємниць – витік може мати незворотні наслідки [1].

Ризик витоку чутливої інформації відноситься до потенційної небезпеки, коли конфіденційні дані можуть стати доступними для неправомірного використання або публічного розголошення без дозволу власника або осіб, яким ця інформація довірена.

Несанкціоноване розголошення інформації може призвести до репутаційних та фінансових втрат для організації. Інформація, яка має бути доступна лише обмеженому колу осіб у зв'язку з їхніми службовими обов'язками, часто потрапляє до зловмисників або шахраїв через недбалість, хабарництво або незаконні дії третіх осіб.

Це може стосуватися різних типів інформації, включаючи особисті дані, фінансові звіти, комерційні секрети, державні таємниці, інтелектуальну власність тощо.

Основні причини ризику витоку інформації можна подивитись в табл. 1.

Таблиця 1

Причини ризиків витоку інформації

№	Причина	Опис
1.	Технічні вразливості	Недоліки в програмному забезпеченні або апаратному забезпеченні, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до систем
2.	Людський фактор	Помилки або навмисні дії співробітників, які призводять до витоку інформації (наприклад, використання слабких паролів, передача інформації третім особам)
3.	Фізичний доступ	Несанкціонований фізичний доступ до приміщень або обладнання, де зберігається чутлива інформація
4.	Мережеві атаки	Використання шкідливого програмного забезпечення, фішингу, атак типу «людина посередині» та інших методів для витоку або перехоплення даних
5.	Втрата або крадіжка обладнання	Втрата або несанкціоноване вилучення носіїв даних (наприклад, ноутбуків, смартфонів, зовнішніх жорстких дисків)

Джерело: складено за даними [2]

Мінімізація ризиків витоку чутливої інформації вимагає комплексного підходу, включаючи технічні засоби захисту (шифрування, застосування брандмауерів, антивірусного програмного забезпечення), організаційні заходи (політики безпеки, навчання персоналу) та фізичний захист.

Вибір типу хмарних послуг є критичним рішенням для будь-якої організації, що прагне максимізувати ефективність своїх IT-ресурсів, забезпечуючи при цьому належний рівень безпеки своєї чутливої інформації. Хмарні послуги можна класифікувати на три основні типи: публічні, приватні та гібридні хмари, кожен з яких має свої переваги, недоліки та особливості ризику.

Публічні хмари – публічні хмарні послуги надаються через інтернет і доступні для широкого кола користувачів. Вони зазвичай є найбільш коштовно-ефективним варіантом, оскільки дозволяють користувачам платити лише за використані ресурси, без необхідності інвестувати в обладнання або обслуговування. Ризики:

– Витік даних – через спільне використання ресурсів і велику кількість користувачів, публічні хмари можуть бути більш схильними до витоків даних.
– Кібератаки – висока популярність публічних хмар зробила їх привабливими цілями для хакерів.

Приватні хмари – це ексклюзивні мережі, створені спеціально для однієї організації. Вони забезпечують більший контроль над даними та кращу безпеку, але вимагають значних інвестицій у створення та утримання. Ризики:

– Висока вартість – великі початкові інвестиції та витрати на обслуговування.
– Управління та обслуговування – вимагає висококваліфікованих IT-фахівців для управління інфраструктурою.

Гібридні хмари – комбінують елементи публічних та приватних хмар, дозволяючи організаціям оптимізувати свої IT-ресурси для різних задач, балансуючи між вартістю, ефективністю та безпекою. Ризики:

– Комплексність управління – управління гібридною хмарою може бути складним через необхідність інтеграції різних платформ і сервісів.
– Сумісність та інтеграція – можуть виникати труднощі з інтеграцією між приватними та публічними компонентами хмари [3].

Щоб мінімізувати ризики витоку чутливої інформації при виборі типу хмарних послуг, організації мають приділити особливу увагу кільком ключовим аспектам. Перш за все, необхідно розробити та строго дотримуватися політик безпеки. Це включає в себе застосування шифрування даних для захисту від несанкціонованого доступу, впровадження многофакторної аутентифікації для забезпечення додаткового рівня верифікації користувачів, а також проведення регулярних аудитів для виявлення та виправлення потенційних вразливостей у системі безпеки.

Важливим кроком є також обережний вибір провайдера хмарних послуг. Варто віддавати перевагу провайдерам з надійною репутацією, які дотримуються визнаних стандартів безпеки. Такий підхід дозволяє забезпечити, що ваші дані будуть захищені відповідно до найкращих практик галузі.

Останній, але не менш важливий аспект – це навчання персоналу. Підвищення обізнаності співробітників про методи захисту інформації є ключовим для запобігання випадкам витоку через людський фактор. Вчасне та цілеспрямоване навчання допомагає створити культуру безпеки в організації, де кожен співробітник розуміє свою роль у захисті чутливих даних.

Врахування цих аспектів сприяє створенню надійного та безпечного хмарного рішення, яке зможе захистити чутливу інформацію від різноманітних загроз.

Вибір між різними типами хмарних послуг залежить від конкретних потреб бізнесу, його розміру, галузі та специфіки чутливої інформації, якою він володіє. Оцінка потенційних ризиків та розробка стратегії їх мінімізації є ключовими кроками для забезпечення ефективного та безпечного використання хмарних технологій.

Список використаних джерел

1. Шадська У. Захист персональних даних: що потрібно знати. 2020. URL: https://zmina.info/articles/zahyst-personalnyh-danyh-shho-potribno-znaty/

2. Чифліклій І. І. Розробка та дослідження системи запобігання витоку інформації. Одеса : ОНПУ, 2021. 76 с.

3. Березніков А. Види хмарних сервісів: який обрати та огляд хмарних провайдерів. 2018. URL: https://denovo.ua/blog/vidi-hmarnih-servisiv-yakij-obrati-ta-oglyad-hmarnih-provajd-8

Ключові слова: хмарні послуги, чутлива інформація, витік інформації, ризики, безпека.
Keywords: cloud services, sensitive information, information leakage, risks, security.

Ахмаметьєва Ганна Валеріївна
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент

ПРОБЛЕМИ РОЗПОВСЮДЖЕННЯ ФЕЙКОВИХ МУЛЬТИМЕДІА В МЕРЕЖІ INTERNET

Широкомасштабне поширення технологій інтернет зв'язку в сучасному світі з одного боку призводить до використання простих та зручних інструментів спілкування, обміну повідомленнями та мультимедійних даних, будь то зображення, відео, аудіо-файли та голосові повідомлення, з іншого відбувається неконтрольоване розсилання фейкових мультимедіа в соціальних мережах, месенджерах, чатах, форумах тощо. Якщо для офіційних медіа, ресурсів новин, крупних мультимедійних платформ проблеми поширення недостовірної інформації можуть бути вирішені на рівні закону та внутрішньої політики щодо перевірки ресурсів на порушення авторських прав та/або підтвердження достовірності викладених фактів, то в групових чатах месенджерів це майже ніким не контрольовано.

Згідно [1] «недостовірною вважається інформація, яка не відповідає дійсності або викладена неправдиво, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені)». Під це визначення також можуть потрапити цілком оригінальні та достовірні дані, які дійсно мали місце, але час та локація їх скоєння навмисно чи ненавмисно змінені, наприклад, через постійні пересилання з груп у групи масштабної кількості відео через деякий час в пам'яті взагалі стирається розуміння, коли та до якої події відноситься інформація. Особливо це актуально для коротких відео-роліків, аудіо-записів, де взагалі не зрозуміло, з якої країни або міста ведеться запис. Часто з метою впливу на людські маси беруть старі відео- та аудіо файли, зображення, які видаються за нові та актуальні, притому оригінальність та цілісність таких файлів може бути взагалі не порушена.

В мультимедійних даних відомості щодо власника, пристрою та моделі апарату, яким був здійснений запис, дата, час запису, та деякі інші властивості можуть зберігатися у метаданих, однак існує чимало програм та онлайн-ресурсів, що дозволяють їх змінювати, зокрема [2-4] для різних офісних документів, зображень і відео.

Це вимагає розроблення спеціальних методів вбудовування спеціальних міток та маркерів безпосередньо в мультимедійні файли. Таку задачу дозволяє вирішити використання стеганографічних методів, зокрема методів вбудовування невидимих ідентифікаційних заголовків та цифрових водяних знаків.

Обов'язковими даними, що підлягають вбудовуванню, є:

– відомості щодо пристрою, якими велася зйомка/запис;