DOI: 10.18372/2225-5036.29.18074

ДОСЛІДЖЕННЯ ПРОБЛЕМ КЛАСИФІКАЦІЇ ТА БЕЗПЕЧНОГО ЗБЕРІГАННЯ ДАНИХ

Олег Гарасимчук, Олег Дейнека

Національний університет «Львівська політехніка»

ДЕЙНЕКА Олег Романович, аспірант
Рік та місце народження: 1986 рік, м. Львів, Україна.
Освіта: Національний університет «Львівська політехніка», 2008 рік.
Посада: аспірант кафедри захисту інформації, з 2023 року
Наукові інтереси: засоби захисту інформації
E-mail: deinekaoleg.86@gmail.com.
Orcid ID: 0009-0005-9156-3339.

ГАРАСИМЧУК Олег Ігорович, к.т.н., доц.
Рік та місце народження: 1979 рік, м. Бережани, Тернопільська обл., Україна.
Освіта: Національний університет «Львівська політехніка», 2001 рік.
Посада: доцент кафедри захисту інформації з 2008 року.
Наукові інтереси: комплексні системи санкціонованого доступу, генерування псевдовипадкових чисел та послідовностей, генерування пуассонівських імпульсних послідовностей, методи і засоби захисту інформації, проектування комплексних систем захисту інформації, бази даних та знань, сигнальні процесори в системах захисту інформації.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографії, навчальний посібник, патенти, тези та матеріали доповідей на конференціях.
E-mail: oleh.harasymchuk@gmail.com.
Orcid ID: 0000-0002-8742-8872.

Анотація*. З розвитком технологій і ростом обсягів даних все більше постає проблема, як ці дані класифікувати та організувати їх безпечне зберігання. Мета даної статі полягає в ознайомленні з аналізом та потребами безпечного зберігання даних за наступними критеріями: обсяг даних, термін зберігання, доступність та швидкодія, безпека та конфіденційність. Технологічні прогрес а також економічні чинники змінюють сучасні тенденції зберігання даних у напрямку хмарних рішень, а особливо у розподіленні між різними гравцями збереження даних із використанням хмарних рішень для пониження ризиків втрати. В даній статті ми проаналізовані джерела загроз для великих даних, а саме кіберзлочини, соціальний інжиніринг, фізичні та внутрішні загрози, віруси та шкідливе програмне забезпечення. Проаналізовані основні принципи конфіденційності та безпечного зберігання великих обсягів даних.*

Ключові слова*: SOC2 Type 2, Big Data, класифікація даних, зберігання даних, конфіденційність, джерела загроз, кібератаки, DDOS.*

Постановка проблеми

В сучасному світі щодня обробляється велика кількість різноманітних даних, а тому їх класифікація та надійне зберігання стали надзвичайно важливими завданнями, оскільки інформація є ключовим активом для багатьох організацій та підприємств. З розвитком технологій та ростом обсягів даних збільшується необхідність у безпечному та ефективному їхньому зберіганні [1-5]. В даній публікації ми розглянемо основні проблеми та виклики, пов'язані з зберіганням та класифікацією великих обсягів даних та сучасні підходи до їх вирішення.

Аналіз останніх досліджень і публікацій

Аналізуючи провідні аудиторські компанії можна спостерігати різкий ріст попиту на стандарт SOC 2 Type [6-9] який являє собою звіт про те що компанії відповідають критеріям оцінки контролів стосовно безпеки, доступності, цілісності, конфіденційності та приватності. Інтерес спостерігається як від компаній, що надають сервіс так і від клієнтів, що планують

його отримувати. Обидві сторони отримують вигоду від цього. Сторона котра відповідає даній оцінці показує процеси та контроль відповідності згідно із стандартом. Клієнтська сторона розуміє як компанія забезпечує безпеку згідно стандарту [10]. Ринок показує що різні домени цікавляться такими звітами. Компанії IT, охорони здоров'я, фінансові, фармацевтичні, банківські установи впроваджують безпечні процеси пов'язані з збереженням персональних клієнтських даних які відповідають критеріям стандарту. Згідно досліджень усі великі публічні та непублічні компанії мають даний звіт SOC2 Type2 на рівні різних продуктів чи компаній і в свою чергу забезпечують все, що вписано у вимогах до стандарту. Можна переглянути ці звіти у відомих компаніях Microsoft Azure, AWS, GCP [11-13].

Мета та постановка завдання

Обробка і зберігання великих обсягів даних стають все важливішими завданнями в сучасному високо розвинутому в інформаційному плані світі. Це спричинило напрацювання деяких цікавих сучасних тенденцій і підходів щодо даного процесу [14-18]. Метою даної статі є ознайомлення з аналізом та потребами безпечного зберігання даних за наступними критеріями: обсяг даних, термін зберігання, доступність та швидкодія, безпека та конфіденційність.

Виклад основного матеріалу дослідження

Можемо виділити наступні деталі аналізу та фактори, які впливають на потреби у зберіганні даних:

1. Обсяг даних: сучасні організації накопичують величезні обсяги даних. Це може бути інформація про клієнтів, фінансові дані, виробничі дані, медичні записи, дані з давачів IoT та інше. Аналіз потреб в зберіганні даних починається з оцінки обсягів інформації, яку необхідно зберігати;

2. Зростання обсягів даних: обсяги даних постійно зростають. Це може бути через збільшення кількості клієнтів, розширення бізнесу або накопичення нових видів даних. Організації повинні передбачити цей зріст та планувати відповідне збільшення потужностей зберігання;

3. Терміни зберігання: законодавство та регулюючі органи можуть встановлювати терміни зберігання даних для різних видів інформації. Наприклад, фінансові дані можуть вимагати зберігання протягом декількох років, після чого їх можна буде видаляти. Аналіз цих вимог важливий для правильного управління даними;

4. Доступність і швидкодія: деякі дані повинні бути доступними негайно, тоді як інші можуть зберігатися на довгостроковому терміні. Аналіз потреб у зберіганні даних включає розгляд різних рівнів доступності і швидкодії, які необхідні для різних типів інформації;

5. Забезпечення безпеки: зберігання даних має включати в себе заходи забезпечення безпеки, такі як шифрування, резервне копіювання і контроль доступу. Аналіз потреб включає в себе ідентифікацію ризиків та визначення необхідних заходів для їх зменшення;

6. Технологічні можливості: ринок технологій для зберігання даних постійно змінюється. Аналіз потреб повинен враховувати нові технології, такі як хмарне зберігання, кордонні обчислення, блокчейн та інші інновації, які можуть покращити зберігання даних;

7. Бюджетні обмеження: обсяг інвестицій, доступних для зберігання даних, також відіграє важливу роль у визначенні потреб. Організації повинні бути готові раціонально використовувати свої бюджети та розглядати різні варіанти зберігання, включаючи аутсорсинг та оптимізацію;

8. Аналіз даних: потреби в зберіганні даних пов'язані з потребами в аналізі цих даних. Для багатьох організацій важливо не лише зберігати дані, але і швидко та ефективно аналізувати їх для прийняття рішень. Це може вимагати спеціалізованих інструментів та відповідної інфраструктури;

9. Конфіденційність даних: потреби в класифікації даних на предмет публічні, конфіденційні, секретні дані і розмежування доступів до цих даних у межах організації згідно рольових моделей чи організаційної ієрархії. Це може вимагати спеціалізованих інструментів та інфраструктури.

Враховуючи ці фактори, аналіз потреб у зберіганні великих обсягів даних стає складним завданням, яке вимагає стратегічного планування та постійного моніторингу.

Огляд сучасних тенденцій, підходи та специфіка у надійному зберіганні даних великих обсягів

Хмарне зберігання стає все популярнішим. Багато організацій обирають мультихмарність, використовуючи різні хмарні середовища для зберігання даних [16-18]. Це зменшує ризик втрати даних через відмову одного постачальника. Також, кордонні обчислення (Edge Computing) стають дедалі важливішими для обробки даних ближче до їх джерела. Шифрування даних стає все більш важливим аспектом зберігання даних. Всі дані, які передаються до хмари або зберігаються на серверах, повинні бути зашифровані, щоб забезпечити їх конфіденційність. Шифрування на рівні даних та шифрування з використанням ключів допомагають забезпечити захист від несанкціонованого доступу. Технологія блокчейн використовує розподілені мережі для надійного зберігання та захисту даних [14]. Вона набуває популярності як засіб для децентралізованого зберігання та безпеки даних. У світі великих даних (Big Data), розподілена обробка даних і машинне навчання стають ключовими. Технології, такі як Apache Hadoop [19-20] та Apache Spark [21], дозволяють аналізувати великі обсяги даних у реальному часі і виявляти патерни за допомогою машинного навчання. Особлива увага приділяється безпеці даних та захисту від кіберзагроз. Системи вия-

влення вторгнень (IDS) та захисту від вторгнень (IPS) стають більш інтелектуальними та розширеними [22-24]. Крім того, кіберстрахування [25] стає важливим компонентом захисту від кіберризиків. Не менш важливою стає екологічна сторона зберігання даних. Зелена IT та сталий розвиток включають зменшення споживання енергії та впливу на навколишнє середовище в дата-центрах. Зберігання та обробка даних стають більш доступними для кінцевих користувачів завдяки платформам самообслуговування та інтерактивній аналітиці. Аналітика даних також вдосконалюється, включаючи обробку природної мови (NLP) та використання графових баз даних. І, нарешті, резервне копіювання даних стає більш розширеним та ефективним завдяки continuous data protection (CDP) [26] та резервному копіюванню у хмарному середовищі. Ці сучасні тенденції та підходи допомагають організаціям забезпечувати безпеку, доступність та ефективність у зберіганні даних великих обсягів, що має дуже актуально в сучасному інформаційному світі. Шифрування в цьому контексті відіграє важливу роль у забезпеченні конфіденційності та безпеки даних.

Аналіз джерел загроз та атак на дані, що зберігаються і визначення можливих наслідків від їх реалізації

Зі збільшенням обсягів даних, що зберігаються виникає необхідність детального аналізу джерел потенційних загроз та можливих атак на ці дані. Аналіз цих аспектів є критичним для забезпечення безпеки та конфіденційності інформації. Ось докладніше про кожне з цих джерел загроз [27].

Кіберзлочинці: зловмисники та хакери є однією з найбільших загроз для даних. Вони можуть використовувати різноманітні методи, включаючи вразливості програмного забезпечення, соціальний інжиніринг та атаки на мережевий рівень, щоб отримати несанкціонований доступ до системи зберігання. Дії кіберзлочинців можуть мати серйозні наслідки для організацій та індивідів. Нижче розглянемо деякі із можливих наслідків від дій кіберзлочинців:

1. Втрата конфіденційної інформації: Кіберзлочинці можуть вкрасти конфіденційні дані, такі як особисті дані користувачів, фінансову інформацію, комерційні та важливі бізнес-дані. Ця втрата може призвести до порушення конфіденційності та порушення законів про захист даних;

2. Втрата репутації: якщо інформація про порушення безпеки стає відомою громадськості, це може серйозно підірвати репутацію організації. Клієнти можуть втратити довіру до компанії, що може вплинути на її прибутковість та імідж;

3. Фінансові втрати: кіберзлочинці можуть завдати фінансових збитків організації шляхом вимагання викупу за відновлення доступу до заблокованих даних (ransomware), штрафів за порушення законів про захист даних, а також через крадіжку фінансових активів;

4. Недоступність сервісів: кіберзлочинці можуть використовувати атаки, такі як DDoS (деніал-сервіс) для створення недоступності важливих веб-сайтів та онлайн-сервісів. Це може призвести до втрати прибутку та негативного впливу на користувачів;

5. Втрата інтелектуальної власності: кіберзлочинці можуть вкрасти інтелектуальну власність, таку як патенти, розробки та конфіденційні інформаційні ресурси. Це може призвести до втрати конкурентної переваги та фінансових втрат;

6. Втрата довіри: індивіди, які стають жертвами кіберзлочинців, можуть втратити довіру до онлайн-сервісів та цифрового середовища загалом, що може вплинути на їхню онлайн-активність та поведінку.

Загалом, дії кіберзлочинців можуть призвести до серйозних наслідків як для організацій, так і для індивідів, і тому вони однозначно підкреслюють важливість заходів забезпечення безпеки даних, що зберігаються та здатності реагувати на ці загрози.

Внутрішні загрози: іноді загрози можуть виникати зсередини організації, від співробітників або адміністраторів, які мають доступ до даних. Несанкціонований доступ, недбале оброблення або навіть зловживання привілеями можуть призвести до втрати інформації та інших ризиків.

Внутрішні загрози, які виникають зсередини організації, можуть мати серйозні наслідки для безпеки та конфіденційності даних. Ось докладніше про можливі наслідки таких внутрішніх загроз:

1. Втрата конфіденційної інформації: інсайдери, такі як співробітники або адміністратори, можуть мати доступ до конфіденційної інформації та використовувати її несанкціоновано або навіть викрити порушення безпеки. Це може призвести до витоку конфіденційних даних;

2. Пошкодження даних: інсайдери можуть наносити шкоду даним, видаляти або модифікувати інформацію. Це може призвести до втрати цілісності даних та навіть до непридатності для використання;

3. Зловживання привілеями: співробітники або адміністратори можуть зловживати своїми привілеями та отримувати доступ до даних, до яких вони не мають права доступу. Це може призвести до порушення конфіденційності та безпеки даних;

4. Порушення політик безпеки: внутрішні загрози можуть порушувати політики безпеки організації, такі як використання слабких паролів, передача інформації по незахищеним каналам або неналежне оброблення даних;

5. Втрата репутації: якщо внутрішнє порушення безпеки стає відомим громадськості, це може пошкодити репутацію організації та втратити довіру клієнтів та партнерів;

6. Правові наслідки: внутрішні загрози можуть підпадати під кримінальну відповідальність, що може призвести до їхнього судового переслідування та покарання відповідно до законів;

7. Втрати фінансів: втрати, пов'язані з інцидентами безпеки, включаючи штрафи та витрати на відновлення та відшкодування, можуть призвести до фінансових втрат для організації.

Усі ці наслідки підкреслюють важливість вжиття заходів для виявлення та запобігання внутрішнім загрозам, а також розробки відповідних стратегій забезпечення безпеки даних в організації. Але тут варто зазначити, що забезпечення від внутрішніх загроз вимагає постійного моніторингу, розвитку політик безпеки та навчання співробітників щодо правил обробки даних та їх безпечного зберігання.

Соціальний інжиніринг: атаки, що використовують соціальний інжиніринг [28-29], полягають у впливі на людей, щоб отримати доступ до системи. Це може включати в себе маніпуляцію або обман співробітників організації для отримання доступу до конфіденційних даних.

Наслідки від соціального інжинірингу :

1. Витік конфіденційної інформації: атаки соціального інжинірингу можуть призвести до витоку конфіденційних даних, таких як паролі, особисті ідентифікаційні дані або корпоративні секрети;

2. Порушення конфіденційності: зловмисники можуть зловживати довірою співробітників, отримувати доступ до систем та витягувати конфіденційну інформацію, що може бути використана для недобросовісних цілей;

3. Фінансові втрати: якщо атака соціального інжинірингу спрямована на фінансові активи, це може призвести до великих фінансових втрат для організації.

Фізичний доступ: зловмисники можуть намагатися отримати фізичний доступ до обладнання, що зберігає дані. Це може становити загрозу, особливо якщо обладнання не захищено від фізичних атак.

Можливі наступні наслідки від несанкціонованого фізичного доступу до обладнання, що використовується для зберігання даних:

1. Крадіжка обладнання: зловмисники можуть намагатися вкрасти фізичне обладнання, на якому зберігаються дані. Це може призвести до втрати даних та порушення доступу до них;

2. Пошкодження обладнання: зловмисники можуть наносити шкоду серверам, комп'ютерам або мережевому обладнанню, що може призвести до недоступності системи та втрати інформації;

3. Зловживання фізичним доступом: якщо зловмисники отримують фізичний доступ до обладнання, вони можуть здійснювати несанкціоновані дії, включаючи встановлення шкідливого програмного забезпечення або крадіжку даних;

4. Порушення безпеки приміщення: фізичний доступ також може включати в себе порушення безпеки приміщення, такі як проникнення до серверних кімнат або зламування замків.

Кібератаки та віруси: різні види кібератак, такі як деніал-сервіс атаки (DDoS) [30], можуть призвести до недоступності системи. Віруси та шкідливе програмне забезпечення можуть пошкодити дані або заблокувати доступ до них.

Можливі наступні наслідки від кібератак, включаючи DDoS:

1. Недоступність сервісу: DDoS-атаки можуть спричинити недоступність важливих онлайн-сервісів, включаючи веб-сайти, електронну пошту та інші ресурси. Це може призвести до втрати прибутку та негативного впливу на користувачів;

2. Втрата репутації: коли онлайн-сервіси стають недоступними через DDoS-атаку, це може вплинути на репутацію організації та спричинити втрату довіри клієнтів;

3. Фінансові втрати: для багатьох організацій недоступність сервісів може призвести до фінансових втрат, особливо якщо бізнес залежить від онлайн-присутності;

4. Порушення безпеки: DDoS-атаки також можуть бути використані як відволікання для інших кібератак, спрямованих на порушення безпеки та доступу до конфіденційних даних.

Віруси та шкідливе програмне забезпечення: це ще один критично важливий вид загроз. Він може привести до наступних наслідків:

1. Пошкодження даних: віруси та шкідливе програмне забезпечення можуть пошкодити або знищити дані на комп'ютерах та серверах. Це може призвести до втрати важливої інформації, яка там зберігається;

2. Зловживання доступом: деяке шкідливе програмне забезпечення може намагатися отримати несанкціонований доступ до системи або користувацьких облікових записів;

3. Шпигунство: деяке вірусне програмне забезпечення може слугувати для відстеження активності користувача та витоку конфіденційних даних;

4. Захоплення ресурсів: деякі види вірусів можуть використовувати ресурси комп'ютера, що призводить до повільної роботи системи;

5. Втрати фінансів: відновлення від атак вірусів та шкідливого програмного забезпечення може призвести до витрат на видалення вірусів та відновлення функціональності.

Загалом, кібератаки та віруси можуть завдати серйозної шкоди інформації, системам та організаціям, і підкреслюють важливість захисту та виявлення таких загроз за допомогою антивірусного програмного забезпечення, мережевих заходів безпеки та засобів моніторингу.

Конфіденційність і безпека зберігання великих обсягів даних

З інтенсивним збільшенням обсягів даних, які зберігаються, виникає загострення проблеми забезпе-

чення конфіденційності та безпеки інформації. Ця проблема вимагає певних дій та заходів:

1. Захист від несанкціонованого доступу: збільшення обсягів даних призводить до збільшення ризику несанкціонованого доступу до інформації. Це може бути використано кіберзлочинцями або зловмисниками для отримання конфіденційних даних, що може веде до витоку інформації та порушення конфіденційності користувачів;

2. Шифрування даних: щоб забезпечити конфіденційність, організації використовують методи шифрування даних. Однак із зростанням обсягів даних важливо забезпечити ефективне та масштабоване шифрування, що не призводить до великих затрат на обчислювальні ресурси;

3. Мультифакторна ідентифікація: для забезпечення безпеки даних важливо використовувати системи мультифакторної ідентифікації, які вимагають два або більше методів підтвердження особи. Це може включати в себе паролі, біометричні дані, токени та інші фактори;

4. Реагування на кіберзагрози: з інтенсивним збільшенням обсягів даних зростає й ризик кіберзагроз, таких як віруси, троянці, різновиди шкідливих програм, які можуть атакувати системи зберігання. Для боротьби з цими загрозами організації повинні регулярно оновлювати та підтримувати свої заходи безпеки;

5. Законодавство та регулювання: у багатьох країнах існують закони та регулювання, які вимагають від організацій зберігати та обробляти дані відповідно до встановлених стандартів безпеки. Виконання цих норм обов'язкове та може призвести до санкцій у разі їх порушення;

6. Класифікація інформації: організації повинні класифікувати інформацію на рівні конфіденційності, зазначаючи, які документи є внутрішніми, конфіденційними, секретними тощо. Це допомагає визначити рівні захисту та правила доступу;

7. Політика доступу: встановлення чітких правил доступу до документів інформації на різних рівнях конфіденційності. Лише уповноважені особи повинні мати доступ до внутрішніх і секретних документів;

8. Аудит і моніторинг: організації повинні вести облік доступу до конфіденційної інформації та регулярно перевіряти системи на наявність слабких місць в захисті;

9. Навчання та усвідомлення: персонал повинен бути навчений правилам безпеки інформації та розуміти важливість дотримання цих правил;

10. Документація: всі процедури і правила, пов'язані зі зберіганням конфіденційної інформації, мають бути документовані і доступні для уповноважених осіб.

Загальна проблема конфіденційності та безпеки вимагає постійного вдосконалення технологій та методів захисту, а також особливої уваги до масштабованості та ефективності заходів, оскільки збільшення обсягів даних ускладнює завдання забезпечення безпеки інформації.

Висновки. У сучасному світі, зберігання великих обсягів даних стає надзвичайно актуальною проблемою. Споживачі та організації постійно генерують великі обсяги інформації, і ця тенденція зростає. Щоб забезпечити ефективне та безпечне зберігання цих даних, важливо розглянути виклики та стратегії, які використовуються в цій галузі. Світовою тенденцією в зберіганні даних є розширення можливостей доступу до інформації. Проте ризик з втратою даних за допомогою різних факторів залишається дуже високий. Міжнародні стандарти інформаційної безпеки рекомендують як можна забезпечити конфіденційність та доступність різних типів даних, що може допомогти дійти до певних рішень та з допомогою стандартів провести аудит на правдоподібність. Обсяги інформації продовжать зростати, і разом з цим зростатиме і важливість забезпечення безпеки та прозорості її зберігання. Розробка нових стратегій та технологій для забезпечення цього стане актуальним завданням для галузі зберігання даних у майбутньому.

Список літератури

[1]. Kai, Z. (2021). Research on network data storage Technology based on Autonomous Controllable system. In 2021 International Conference on Computer Engineering and Artificial Intelligence (ICCEAI), Shanghai, China, pp. 183-186. https: // doi.org /10.1109/icceai52939.2021. 00035.

[2]. Русин, Б. П., Погрелюк, Л. В., Висоцька, В. А., Осипов, М. М., Варецький, Я. Ю., & Капшій, О. В. (2019). Архітектура системи дедублікації та розподілу даних у хмарних сховищах під час резервного копіювання. Інформаційні технології та комп'ютерна інженерія, 45(2), pp. 40-63. https://doi.org/10.31649/1999-9941-2019-45-2-40-63.

[3]. Yatskiv, V., Kulyna, S., Yatskiv, N., & Kulyna, H. (2020). Protected Distributed Data Storage Based on Residue Number System and Cloud Services. 10th International Conference on Advanced Computer Information Technologies (ACIT), pp. 796-799. https://doi.org/10. 1109/acit49673. 2020.9208849.

[4]. Aujla GS, Chaudhary R, Kumar N, Das AK, Rodrigues JJ. SecSVA: secure storage, verification, and auditing of big data in the cloud environment. IEEE Commun Mag. 2018; 56(1), pp. 78-85.

[5]. Vyas J, Modi P. Providing confidentiality and integrity on data stored in cloud storage by hash and meta–data approach. Int J Adv Res Eng Sci Tech. 2017; 4: pp. 38-50.

[6]. https: // www.schgroup.com/wp-content/uploads / 2021/08/SCH-Group-A-Comprehensive-Guice-to-SOC-Reports-eBook.pdf

[7]. https: // provectus.com/wp-content/uploads/ 2022 / 05 / Provectus-IT-Inc.-SOC-2-Type-I-Report-Final. pdf.

[8]. https: // www. logicmanager.com / resources/ complian-ce-management/download-soc-2-compliance-checklist/.

[9]. https: // securitycheckbox.com / blog /2016/ soc2-controls-free-download-xls-csv/.

[10]. https://secureframe.com/hub/soc-2/compliance-documentation.

[11]. https: // learn.microsoft.com / en-us / azure/ compliance / offerings / offering-soc-2#azure-and-soc-2-type-2.

[12]. https: // aws.amazon.com / compliance /soc-faqs/.

[13]. https: // cloud.google.com / security/compliance/soc-2.

[14]. Ren, Y.; Huang, D.; Wang, W.; Yu, X. BSMD: A blockchain-based secure storage mechanism for big spatio-temporal data. Future Gener. Comput. Syst. 2023, 138, pp. 328-338.

[15]. Яцків, В.В., Кулина, С.В. (2019). Метод надійного зберігання даних на основі надлишкової системи залишкових класів. Вісник Хмельницького національного університету. Технічні науки, 6, С. 98-104. http://journals.khnu.km.ua/vestnik/wp-content/ uploads/2021/01/20-9.pdf.

[16]. Rafique, A.; Van Landuyt, D.; Beni, E.H.; Lagaisse, B.; Joosen, W. CryptDICE: Distributed data protection system for secure cloud data storage and computation. Inf. Syst. 2021, 96, 101671 p.

[17]. Reena, M. and Nargunam, A.S., 2019. Secured Storage of Big Data in Cloud. International Journal of Recent Technology and Engineering (IJRTE), 8(2S3), pp. 6-10.

[18]. Li, Yibin & Gai, Keke & Qiu, Longfei & Qiu, Meikang & Zhao, Hui. (2016). Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing. Information Sciences, pp. 387.

[19]. Ab, Anantha Babu. (2018). Apache Hadoop, 10.13140/RG.2.2.30673.48483.

[20]. Anwesh Bhattacharyya. Beginning Apache Hadoop Administration, 252 p.

[21]. B. Chambers, M. Zahariaю Spark: The Definitive Guide, Big Data Processing Made Simple. Published by O'Reilly Media 2018. 601 p.

[22]. Коробейнікова, Т & Цар, О. (2023). Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. Grail of Science. С. 317-325.

[23]. Butt, Saad. (2022). Cognitive Analysis of Intrusion Detection System. Journal of Siberian Federal University. Engineering & Technologies. 15. 10.17516/1999-494X-0377.

[24]. Harasymchuk O, Bloshchenko O., Ramsh V. Analysis of principles and systems for detecting remote attacks through the internet. Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej. 2020.

[25]. Prykaziuk, Nataliia & Gumenyuk, Ludmila. (2020). Cyber-Insurance as an important tool of enterprise protection in the digitization economy. Efektyvna ekonomika. 10.32702/2307-2105-2020.4.6.

[26]. Laden, Guy & Ta-Shma, Paula & Yaffe, Eitan & Factor, Michael & Fienblit, Shachar. (2007). Architectures for Controller Based CDP. pp. 107-121.

[27]. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – К І І В і П НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

[28]. Sokolov, V. Y., & Kurbanmuradov, D. M. (2018). Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(1), С. 6-16.

[29]. Корченко О., Горніцька Д. Гололобов А. "Розширена класифікація методів соціального інжинірингу." Ukrainian Scientific Journal of Information Security 20 (2014): С. 197-205.

[30]. Laktionov, I., Kmit, A., Opirskyy, I., & Harasymchuk, O. (2022). Дослідження інструментів захисту інтернет-ресурсів від DDoS-атак під час кібервійни. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), С. 91-111.

УДК 004.056.5

Deineka O., Harasymchuk O. Rresearch on classification issues and secure data storage

***Abstract**. In the modern world, the storage of large volumes of data has become an extremely relevant issue. Consumers and organizations continuously generate large amounts of information, and this trend is increasing. To ensure effective and secure storage of this data, it is important to consider the challenges and strategies used in this field. A global trend in data storage is expanding access to information. However, the risk of data loss through various factors remains very high. International information security standards recommend ways to balance confidentiality with accessibility for different types of data, which can help make informed decisions. Auditing for accuracy and reliability is also suggested by these standards. The volume of information will continue to grow, and with it, the importance of ensuring the security and transparency of its storage. Developing new strategies and technologies to achieve this will be a significant task for the data storage industry in the future.*

***Key words:** SOC2 Type 2, Big Data, data classification, data storage, confidentiality, threats, cybersecurity, DDOS.*

Дейнека Олег Романович, аспірант, спеціальності «Кібербезпека та захист інформації» Національного університету «Львівська політехніка».

Oleg Deineka, Postgraduate the Department of Information Security, National University "Lviv Polytechnic".

Гарасимчук Олег Ігорович, к.т.н., доцент, доцент кафедри захисту інформації Національного університету «Львівська політехніка».

Oleh Harasymchuk, Ph.D., Associate Professorat the Department of Information Security, National University "Lviv Polytechnic".

Отримано *3 жовтня 2023 року*, затверджено редколегією *30 жовтня 2023 року*