УДК 004.72.056.52:004.4:[004.738.1.www.Amazon
DOI: 10.31673/2409-7292.2024.010002

Гайдур Г. І., Бригинець А. А.

ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ У СНЕПШОТАХ AMAZON ELASTIC BLOCK STORE

У статті розглядаються питання безпеки в середовищі Amazon Web Services (AWS) з акцентом на ризики, пов'язані з загальнодоступними снепшотами Elastic Block Store (EBS). Аналізується, як процеси ідентифікації користувачів і надання дозволів можуть сприяти виникненню ризиків безпеки та витоку конфіденційних даних. Детально описуються методи виявлення та моніторингу публічних снепшотів, а також надаються рекомендації щодо зміни дозволів і забезпечення безпеки облікових даних. Підкреслюється важливість проведення розслідувань при виявленні загальнодоступних снепшотів і розробляються стратегії запобігання подібним інцидентам, включно з навчанням персоналу та застосуванням політик конфіденційності. Освітлюється підхід AWS до безпеки, зокрема через інформування клієнтів про потенційні ризики, пов'язані з публічним доступом до снепшотів. Робота пропонує всебічний огляд проблем безпеки у середовищі AWS, зосереджуючись на управлінні даними та рекомендує конкретні заходи для забезпечення безпечного використання снепшотів EBS. Ілюструються потенційні вразливості за допомогою реальних прикладів, демонструючи значення правильного керування політиками доступу та обізнаного використання снепшотів для запобігання випадковому витоку даних. Особлива увага приділяється впливу відкритих снепшотів на різні галузі та необхідності проведення аудитів для ідентифікації потенційних загроз.

Ключові слова: Amazon Web Services (AWS), Elastic Block Store (EBS), безпека хмарних обчислень, конфіденційність даних, снепшот, управління дозволами, ризики безпеки.

Вступ

Amazon Web Services (AWS) надає потужну платформу для хмарних обчислень з численними функціями та послугами. Однією з таких послуг є снепшоти Elastic Block Store (EBS), яка дозволяє створювати та зберігати томи даних для віртуальних машин інстансів EC2.

Снепшоти EBS представляють собою знімки цих томів, які можна створювати для забезпечення резервного копіювання даних, відновлення до попередніх станів і обміну даними між регіонами та обліковими записами AWS. Однак неуважне керування снепшотами може призвести до серйозних проблем безпеки та витоку конфіденційних даних.

Постановка проблеми

При створенні образу машини Amazon (Amazon Machine Image, AMI) з інстансу EC2 з підтримкою Amazon Elastic Block Store (EBS), AWS створює снепшоти томів EBS, прикріплених до інстансу. Ці снепшоти потім асоціюються з AMI. Снепшоти EBS можуть бути використані для забезпечення миттєвого відновлення томів EBS, що корисно, якщо потрібно повернути дані до попереднього стану, а також вони можуть бути використані для передачі даних між регіонами і обліковими записами AWS.

Також важливо зазначити, що віртуальні машини на AWS можуть створюватися з абсолютно різною метою та зберігати абсолютно різноманітні дані, в тому числі і велику кількість конфіденційних. В першу чергу EBS снепшоти дуже часто використовуються для створення резервних копій томів EBS у певний момент часу. Це має вирішальне значення для захисту та відновлення даних у разі випадкового видалення, пошкодження даних або інших непередбачуваних ситуацій. Тобто можливо використовувати снепшоти EBS для бекапування томів до попереднього стану, що дозволяє швидко та ефективно відновлювати дані. Однак не варто забувати, що якщо зробити такі снепшоти публічними, будь-хто охочий зможе їх монтувати та отримати доступ до конфіденційної інформації, яка з високою ймовірністю наявна у резервній копії.

За схожим принципом працює копіювання EBS снепшотів в різні регіони AWS, забезпечуючи механізм міжрегіонального аварійного відновлення. Схожі загрози можуть виникнути також у разі масштабування інфраструктури підприємства, проведення тестувань, розробки та навчань персоналу та при міграції даних. Усі ці процеси включають у себе можливість завантаження снепшотів з їхнім необережним поширенням у відкритий доступ, що часто призводить до небажаних наслідків.

Аналіз наукових публікацій

У [1] зазначається, що у взаємопов'язаному світі, що розвивається, подібно до павутини, хмарні обчислення стали значним явищем. Цю концепцію можна порівняти з восьминогом, з головним сервером як головою і локальними машинами як щупальцями. Однак разом з цим розвитком з'явилося більше вразливостей у сфері безпеки. Посилення захисту від порушень безпеки стало критично важливим. Серед платформ, розроблених для вирішення цих проблем, виділяється і AWS (Amazon Web Services).

Велика кількість платформ наочно демонструє характер і гостроту проблеми. Всі ці платформи в тій чи іншій мірі виконують одне і те ж завдання - як зробити хмарні обчислення все більш безпечними та недосяжними. Згідно з дослідженням, за останні чотири-п'ять років кількість кібератак зросла на 67%, і кожні 14 секунд відбувається порушення безпеки [2]. AWS намагається бути конкурентоспроможним гравцем на ринку, тому впроваджує особливі сервіси, що не притаманні іншим провайдерам хмарних послуг.

Як зазначено у [3], снепшоти Amazon Elastic Block Store (EBS) – це концептуально нове рішення від Amazon Web Services, своєрідна копія даних у певний момент часу, яку можна використовувати для аварійного відновлення, міграції даних між регіонами та обліковими записами, а також для покращення відповідності вимогам до резервного копіювання.

Однак автори [4] вважають, що снепшоти EBS є “ключами від королівства”. Вони зберігають всі дані для хмарних додатків. “EBS снепшоти є секретними ключами до ваших додатків, і вони мають доступ до бази даних з інформацією про ваших клієнтів”, – зазначено у [4].

У 2018 році компанія Duo Security опублікувала статтю, в якій йдеться про те, що вони знайшли 116 386 загальнодоступних снепшотів EBS з 3 213 облікових записів [5]. На конференції DEFCON 27 (2019) Бен Морріс представив цікаве дослідження про загальнодоступні обсяги EBS, в якому він підтвердив 50 витоків даних і оцінив загальну кількість вразливостей у 750-1250 шт. у всіх регіонах AWS. При цьому витоку постраждав широкий перелік галузей, включно з великими компаніями у сфері технологій та охорони здоров'я. Витік даних включав несанкціонований доступ до вихідного коду, приватні SSH-ключі, персональні дані та паролі, а також інші різноманітні форми облікових даних [6, 7].

Однак [8] зазначає, що EBS снепшоти, апріорі, створюються у приватому доступі. Це означає, що користувач не може ділитися цим снепшотом з іншими акаунтами AWS, не вказавши це в явному вигляді. В цьому і полягає принадність AWS, враховуючи безпечний принцип проектування Fail-Safe Defaults (Відмовостійкі налаштування за замовчуванням). Це означає, що якщо не вказано явно, то доступ за замовчуванням заборонено. Проте існують процедури, за яких снепшот все ж повинен бути поширений у відкритий доступ, що і створює ризики конфіденційності даних, оброблюваних у снепшотах.

Експлуатація вразливості

Розглянемо гіпотетичний сценарій експлуатації такої вразливості. За цього сценарію уявімо, що зловмисник є співробітником деякої компанії А, який проходить стажування та вже має базові повноваження у AWS. Це є класичним сценарієм інсайдерської атаки, які, де-факто, вважаються найбільшими загрозами кібернетичній безпеці підприємств, організацій та державних структур. За даними [9] організації звітують, що 42% усіх інцидентів IT безпеки трапляються у результаті дій їхніх працівників.

Таким чином, інсайдер може з легкістю обійти існуючі засоби фізичного та технічного захисту інформації та при цьому вважатиметься правомірним користувачем автоматизованої системи. Наявність певних привілеїв забезпечується фактом обов’язку виконання щоденних робочих завдань. Отже, помітити зловмисну активність буде доволі складно та часозатратно. До того ж, працівники з достатнім рівнем технічних знань можуть спробувати ухилятися від засобів захисту прямо під час виконання зловмисних дій [10].

Загальний алгоритм реалізації такого типу атаки зображений на рис. 1.

© Гайдур, Г. І., & Бригинець, А. А. (2024). Захист конфіденційних даних у снепшотах Amazon Elastic Block Store. Сучасний захист інформації, 1(57), 15–21. https://doi.org/10.31673/2409-7292.2024.010002.

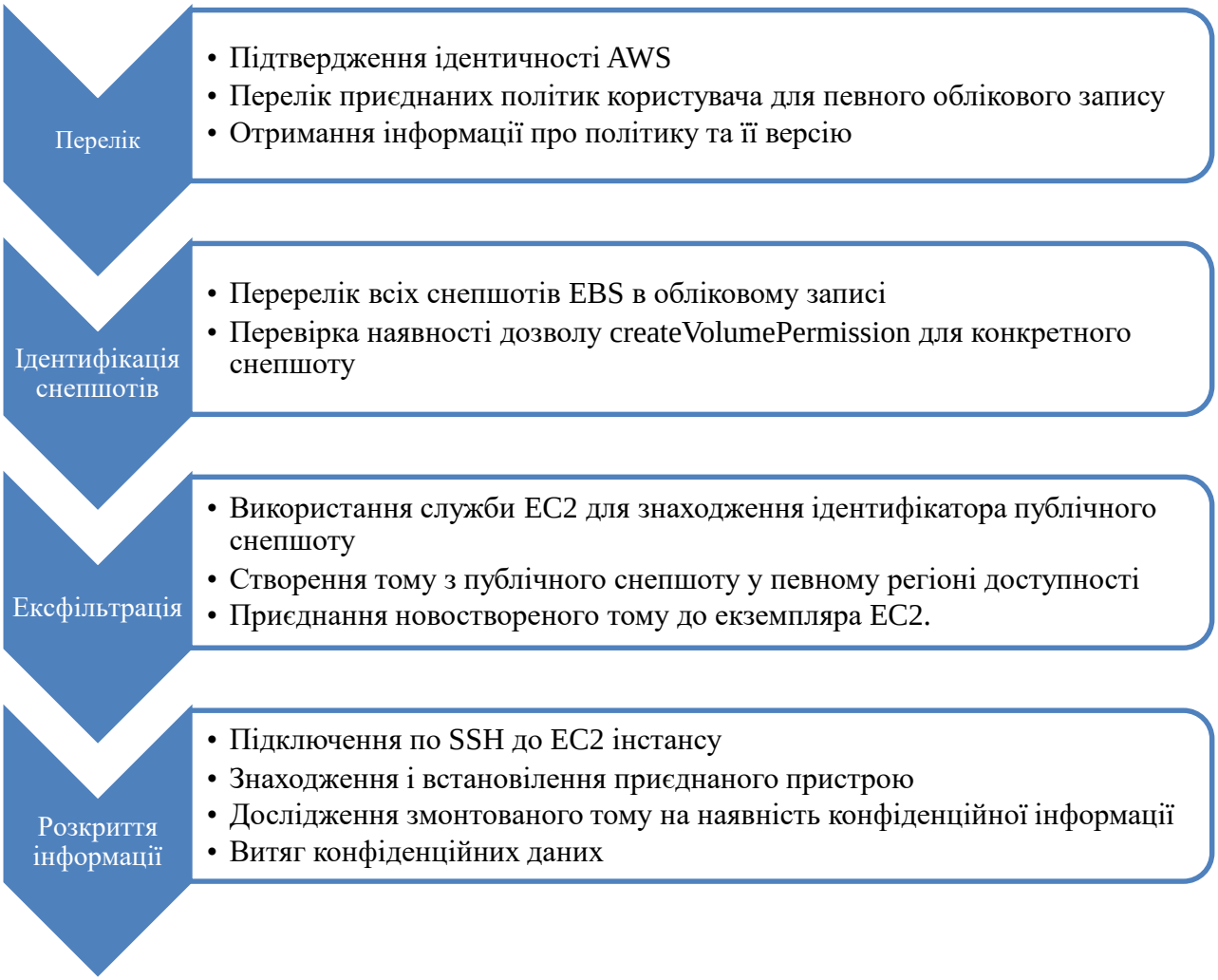

Рис. 1. Алгоритм експлуатації вразливості

Тепер перейдемо до детального розгляду алгоритму експлуатації вразливості, який демонструє конкретні кроки, що можуть бути використані для виявлення та використання слабких місць у захисті конфіденційних даних в AWS [11].

Для початку необхідно визначити користувача IAM, від імені якого ми працюємо, та унікальний ідентифікатор облікового запису AWS. Далі необхідно перевірити наявність прикріплених користувацьких політик, щоб визначити дозволи, надані нашому користувачеві IAM, це може бути виконано командою

```
aws iam list-attached-user-policies --user-name [username].
```

Це допоможе знайти свідчення про існування політики з певною назвою. Щоб перевірити деяку політику далі, потрібно отримати її версію. Припустимо, що версія 7 (v7) є останньою версією політики. Нехай політика також надає дозволи для ec2:DescribeSnapshotAttribute і ec2:DescribeSnapshots. Хоча перший з них обмежується одним снепшотом EBS, другий застосовується до всіх снепшотів EBS в обліковому записі AWS. Щоб перерахувати всі доступні снепшоти, виконаємо:

```
aws ec2 describe-snapshots --owner-ids [ID].
```

Слідом треба визначити, хто має дозвіл createVolumePermission на цьому снепшоті. Цей дозвіл дозволяє створювати томи зі снепшоту, що потенційно може призвести до витоку даних [12].

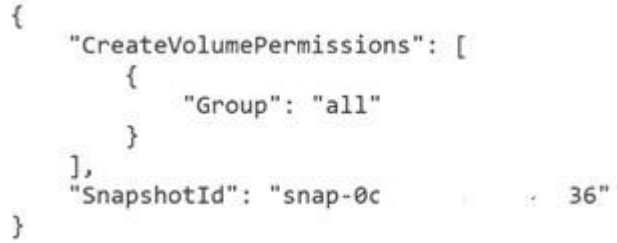

Рис. 2. Перегляд дозволів на снепшот

Ми бачимо, що снепшот є загальнодоступним, про що свідчить те, що для поля «Група» встановлено значення "всі". Тому стає можливим створення тому із загальнодоступного снепшота і подальше його прикріплення до EC2 у обліковому записі AWS [13].

Після успішного приєднання тому до EC2, можна під'єднатися по SSH до цього снепшота і монтувати том. Усередині тому можуть знаходитися конфіденційні дані, в т. ч. різні облікові дані. Налаштування AWS CLI з отриманими обліковими даними дозволяє отримати доступ до S3-бакету, розкриваючи додаткову конфіденційну інформацію.

Захист від вразливості

Необхідно підкреслити, що потреба у створенні загальнодоступних снепшотів EBS в Amazon Web Services не є поширеною практикою для більшості бізнес-операцій. Проте, наявність можливості зробити снепшот публічним відкриває шлях до його використання, часто навіть ненавмисно. Це особливо актуально для користувачів, які не мають достатньої експертизи в цій сфері або тих, хто може випадково вибрати публічну конфігурацію без усвідомлення потенційних ризиків. Такі випадки підкреслюють важливість проведення регулярних навчань для співробітників компаній, акцентуючи на політиці конфіденційності та безпеки даних, щоб мінімізувати ризик витоку конфіденційної інформації через необережне управління снепшотами [14].

AWS демонструє високу відповідальність щодо питань безпеки, регулярно інформуючи своїх клієнтів про наявність загальнодоступних снепшотів у їхніх облікових записах. Такі сповіщення виступають як важливий елемент проактивної безпеки, спонукаючи користувачів перевіряти та коригувати налаштування доступу до своїх снепшотів. AWS акцентує увагу на тому, що публічний доступ до снепшотів є небажаним через потенційні ризики безпеки, зокрема ризик витоку конфіденційної інформації. На веб-сторінках, присвячених редагуванню дозволів AMI та змінам дозволів, чітко вказується на нерекомендований характер таких параметрів. Це підкреслює важливість усвідомленого управління доступом до снепшотів, підвищуючи загальний рівень безпеки даних в середовищі AWS (рис. 3).

Як згадувалося раніше, команда нижче може ідентифікувати загальнодоступні снепшоти, що стане у нагоді для їх локалізації та подальшого прийняття рішення щодо їх видалення або встановлення налаштування приватного доступу, як показано далі.

```
aws ec2 describe-snapshots --owner-id self --restorable-by-
user-ids all --no-paginate
```

Якщо буде виявлено, що незашифрований снепшот у обліковому записі AWS став загальнодоступним, можна [15–16]:

• Зробити його приватним: необхідно змінити дозволи снепшота, щоб зробити його приватним, дозволивши доступ до нього лише авторизованим обліковим записам AWS.

• Змінити всі облікові дані, які були в снепшоті: якщо в загальнодоступному снепшоті зберігалися конфіденційні облікові дані або інформація, дуже важливо змінити ці дані, щоб запобігти несанкціонованому доступу або зловживанню ними.

• Провести розслідування того, як снепшот став загальнодоступним: це важливо для виявлення потенційних ризиків у системі безпеки та запобігання подібним інцидентам у майбутньому.

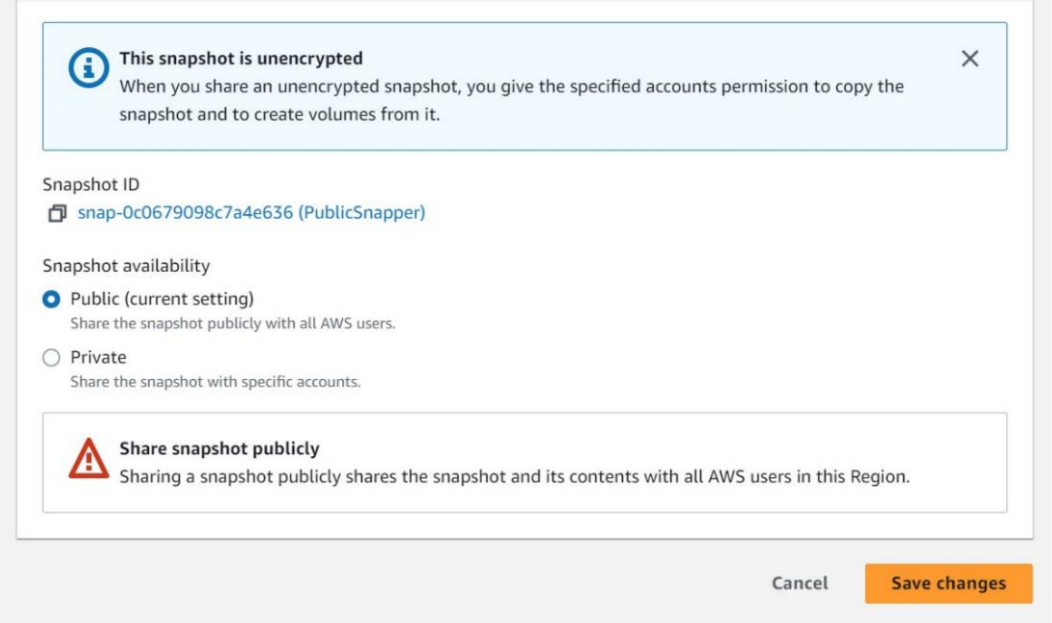

Рис. 3. Сповіщення про те, що публічний доступ до снепшоту не є рекомендованим параметром

Що стосується виявлення та моніторингу публічних снепшотів, документація Stratus Red Team від DataDog надає зразки подій CloudTrail, які допоможуть відстежити та реагувати на інциденти [3]. Ці події включають:

• Снепшот оприлюднено: ця подія спрацьовує, коли снепшот публікується у відкритий доступ. Моніторинг цієї події може допомогти виявити несанкціонований доступ до снепшоту в режимі реального часу.

Цей процес має тригер на подію ModifySnapshotAttribute, коли requestParameters.createVolumePermission показує, що до снепшоту EBS було надано доступ до нового або невідомого облікового запису AWS (рис. 4). У випадку публікації снепшоту саме у відкритий доступ, подія буде також містити поле {"groups":"all"}.

```
"requestParameters": {
  "snapshotId": "snap-01b3f7d87a02559a1",
  "attributeType": "CREATE_VOLUME_PERMISSION",
  "createVolumePermission": {
    "add": {
      "items": [{ "userId": "111111111111" }]
    }
  }
}
```

Рис. 4. Тригерна подія

• Снепшот скопійовано або використано зловмисником: ця подія спрацьовує, коли зловмисник копіює снепшот у власний обліковий запис AWS або створює з нього том EBS.

Моніторинг цієї події може допомогти вам виявити і відреагувати на потенційні порушення безпеки.

На цьому етапі ініціюється подія SharedSnapshotCopyInitiated, що відповідає створенню SharedSnapshotVolume. У цьому контексті, важливо звернути увагу на поле userIdentity.accountId, яке відображає ID облікового запису особи, що ініціювала процес. З іншого боку, recipientAccountId представляє собою ID облікового запису, у якому первісно було створено снепшот і який, відповідно, виступає в ролі жертви в даному сценарії. Особливу увагу слід звернути на факт того, що подія SharedSnapshotCopyInitiated є ключовим моментом у процесі, оскільки саме вона відзначає початок копіювання снепшоту. Цей процес є важливим з погляду безпеки даних, адже він відображає дії, які потенційно можуть бути здійснені з метою несанкціонованого доступу або поширення інформації (рис. 5).


```
{
  "userIdentity": {
    "invokedBy": "ec2.amazonaws.com",
    "type": "AWSAccount",
    "accountId": "999999999999"
  },
  "eventSource": "ec2.amazonaws.com",
  "eventVersion": "1.08",
  "eventTime": "2022-09-27T07:58:49Z",
  "service": "cloudtrail",
  "eventName": "SharedSnapshotCopyInitiated",
  "eventType": "AwsServiceEvent",
  "eventCategory": "Management",
  "awsRegion": "us-east-1",
    "serviceEventDetails": {
    "snapshotId": "snap-12345"
  },
  "readOnly": false,
  "managementEvent": true,
  "recipientAccountId": "111111111111"
 }
```


Рис. 5. Логування події копіювання снепшоту

Уважний моніторинг подій CloudTrail дозволяє проактивно реагувати на будь-які інциденти, пов'язані з публікацією снепшотів, що є критично важливим для забезпечення безпеки ресурсів AWS. Цей процес включає в себе не лише виявлення подій, але й аналіз контексту, в якому вони відбуваються, виявлення потенційних загроз і невідповідностей у діях користувачів. Завдяки цьому можна ефективно ідентифікувати спроби несанкціонованого доступу або розповсюдження конфіденційної інформації. Ключовим аспектом є також своєчасність реакції на виявлені інциденти. Вживання коригувальних заходів, таких як оновлення політик безпеки, обмеження доступу до ресурсів або ревізія прав доступу, може значно знизити ризики, пов'язані з безпекою даних. Такий підхід не лише запобігає потенційним загрозам, але й підвищує загальний рівень безпеки робочого середовища в AWS.

Висновки

У роботі розглядається комплексний підхід до захисту конфіденційних даних у EBS снепшотах Amazon Web Services. Підкреслюється, що необережне розподілення доступу до снепшотів може призвести до серйозних витоків конфіденційної інформації. Інциденти з загальнодоступними снепшотами EBS, які використовуються для несанкціонованого доступу до чутливих даних, висвітлюють ці ризики. Рекомендується застосування комплексних

стратегій захисту, які включають обмеження доступу до снепшотів, застосування інструментів моніторингу, таких як CloudTrail, та розроблення процедур для швидкого реагування на інциденти безпеки. Висвітлюється важливість освіти та тренінгів для співробітників, щоб підвищити обізнаність та компетентність у питаннях безпеки.

Таким чином, наголошується на потребі інтегрованого підходу до безпеки в AWS, забезпечуючи захист даних на всіх рівнях управління хмарними ресурсами.

Перелік посилань

1. Hussain, Z. Security with AWS. (date of access: 06.12.2023) URL: https://www.researchgate.net/publication/348237177_Security_with_AWS.
2. Mukherjee, S. Benefits of AWS in Modern Cloud. SSRN Electronic Journal. 2019. URL: https://doi.org/10.2139/ssrn.3415956 (date of access: 06.12.2023).
3. Amazon EBS Snapshots. URL: https://aws.amazon.com/ebs/snapshots/ .
4. Whittaker, Z. Hundreds of exposed Amazon cloud backups found leaking sensitive data. URL: https://techcrunch.com/2019/08/09/aws-ebs-cloud-backups-leak/ .
5. Piper, S. Beyond S3: Exposed Resources on AWS. Duo Security. URL: https://duo.com/blog/beyond-s3-exposed-resources-on-aws (date of access: 08.11.2023).
6. DEFCON Conference. xBen Benmap Morris - Finding Secrets in Publicly Exposed Ebs Volumes - DEF CON 27 Conference, 2019. YouTube. URL: https://www.youtube.com/watch?v=HXM1rBk_wXs (date of access: 08.11.2023).
7. Exfiltrate EBS Snapshot by Sharing It - Stratus Red Team. *Home - Stratus Red Team*. URL: https://stratus-red-team.cloud/attack-techniques/AWS/aws.exfiltration.ec2-share-ebs-snapshot/ (date of access: 14.11.2023).
8. Kumar, S. Creating secure snapshots for Instances & volumes. URL: https://www.linkedin.com/pulse/creating-secure-snapshots-instances-volumes-santhosh-kumar-k/.
9. Insider Threat: 74% of security incidents come from the extended enterprise, not hacking groups. URL: https://www.clearswift.com/about-us/pr/press-releases/insider-threat-74-security-incidents-come-extended-enterprise-nothacking-groups.
10. Mazzarolo, G. & Jurcut, A. (2019). Insider threats in Cyber Security: The enemy within the gates. URL: https://www.researchgate.net/publication/337438838_Insider_threats_in_Cyber_Security_The_enemy_within_the_gates.
11. Dineva, K. (2021). AWS Certified Cloud Practitioner Certificate. 10.13140/RG.2.2.36605.08161.
12. Бондар, Н. О. Захист персональних даних користувачів з використанням хмарних сервісів AWS / Н. О. Бондар, Ю. М. Колтун // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. 13-ї міжнар. наук.-техн. конф., 26-27 квітня 2023 р., Баку–Харків–Жиліна : [у 2 т.]. Т. 2: секція 2 / Нац. ун-т оборони Азербайджанської Республіки [та ін.]. – Харків: Impress, 2023. – С. 89.
13. Blazor Web Assembly. Run Blazor-based .NET Web applications on AWS Serverless. – [Електронний ресурс]. Режим доступу: https://aws.amazon.com/ru/blogs/developer/run-blazor-based-net-webapplications-on-aws-serverless/
14. Using multi-factor authentication (MFA) in AWS [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html.
15. Маслова Н. Hadoop-рішення для захисту даних великих обсягів / Н. Маслова, О. Половинка // Фізико-математичне моделювання та інформаційні технології, 2021, Вип. 33. – С. 23-27, [Електронне видання]. – Режим доступу: http://www.fmmit.lviv.ua/index.php/fmmit/issue/view/32.
16. AWS Identity and Access Management Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-ug.pdf.

Надійшла 28.12.2023