ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056(477) doi.org/10.33298/2226-8553.2023.1.37.27

Богом'я В.І., Кочегаров В.С.

КІБЕРБЕЗПЕКА В ХМАРНИХ СЕРВІСАХ ЗА ДОПОМОГОЮ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ

Кібербезпека є актуальною в Україні, так як сучасний світ все більше залежить від технологій та інформаційних систем.

Крім того, в Україні триває війна на сході країни, і російські хакери та кіберзлочинці активно використовують кібератаки, щоб завдавати шкоди важливим об'єктам інфраструктури, урядовим установам та громадянам України.

Також, у зв'язку зі швидким розвитком технологій та збільшенням кількості цифрових сервісів, багато компаній та установ стають дедалі більш уразливими до кібератак. Це створює потребу у забезпеченні ефективного кіберзахисту.

Отже, хмарні сервіси - це важлива частина інфраструктури багатьох компаній та установ, які зберігають конфіденційну інформацію про клієнтів та користувачів. Проте, збільшення використання хмарних сервісів також призводить до зростання загроз для кібербезпеки. Одна з актуальних проблем - це забезпечення конфіденційності та захисту від зломів під час зберігання та передачі даних через хмарні сервіси. Хакери можуть використовувати різні методи для злому таких сервісів та отримання конфіденційної інформації. Забезпечення кібербезпеки в хмарних сервісах є важливим науковим завданням, яке потребує дослідження та вирішення. Застосування криптографічних методів для захисту конфіденційної інформації є одним з основних методів вирішення цього завдання. Врахування особливостей системи та використання оптимальних методів захисту є важливими факторами для успішного розв'язання проблеми.

Тому метою статті є аналіз можливостей щодо забезпечення безпеки зберігання та передачі конфіденційної інформації в хмарних сервісах за допомогою застосування криптографічних методів.

Ключові слова: *кібербезпека, хмарні сервіси, криптографічні методи, шифрувальні алгоритми, методи аутентифікації.*

Постановка проблеми

Кібербезпека є актуальною в Україні, так як сучасний світ все більше залежить від технологій та інформаційних систем [1-3]. Це створює нові можливості для злочинців, хакерів та інших зловмисників, які можуть використовувати кібератаки для отримання доступу до конфіденційної інформації, крадіжки коштів, розповсюдження шкідливих програм та інших злочинних дій.

Крім того, в Україні триває війна на сході країни, і російські хакери та кіберзлочинці активно використовують кібератаки, щоб провокувати невдачі та завдавати шкоди важливим об'єктам інфраструктури, урядовим установам та громадянам України.

Також, у зв'язку зі швидким розвитком технологій та збільшенням кількості цифрових сервісів, багато компаній та установ стають дедалі більш уразливими до кібератак [3-7]. Це створює потребу у забезпеченні ефективного кіберзахисту.

Отже, кібербезпека є важливою темою в Україні, яка потребує уваги та координації зусиль урядових та недержавних організацій для забезпечення безпеки інформаційного простору країни [6-9].

Хмарні сервіси – це важлива частина інфраструктури багатьох компаній та установ, які зберігають конфіденційну інформацію про клієнтів та користувачів. Проте, збільшення використання хмарних сервісів також призводить до зростання загроз для кібербезпеки.

Аналіз останніх досліджень і публікацій

Які теми є актуальними зараз для кібербезпеки. За результатом аналізу джерел інформації [1-9] авторами було визначено таки напрями дослідження кібербезпеці.

1. Захист від кібератак, включаючи додаткові заходи безпеки для захисту від розповсюдження вірусів, шкідливого програмного забезпечення і шпигунських програм.
2. Інтернет-безпека від фішингу та соціально-інженерних атак, що спрямовані на отримання конфіденційної інформації.
3. Безпека мережі Інтернет в розумному будинку (IoT), зокрема безпека підключених до мережі речей (smart things).
4. Захист корпоративних мереж від внутрішніх загроз, таких як витік даних, відправка конфіденційної інформації незаконним способом або крадіжка ідентифікаційних даних користувачів.
5. Боротьба з кібербулінгом та кібернасильством в мережі.
6. Кібербезпека в хмарних сервісах, зокрема зберігання і обробка конфіденційної інформації в хмарних сховищах.
7. Захист від кіберзлочинності в електронній комерції та онлайн-фінансах, зокрема злочинів, пов'язаних з крадіжкою ідентифікаційних даних та банківської інформації.
8. Захист від кібернападів на критичну інфраструктуру, таку як енергетичні системи, транспорт, банки та медичні заклади.
9. Боротьба з кіберзлочинністю в соціальних медіа, зокрема з метою запобігання крадіжки особистих даних користувачів та пропаганди дезінформації.
10. Використання штучного інтелекту та машинного навчання для виявлення та запобігання кібератак.

Одна з актуальних проблем – це забезпечення конфіденційності та захисту від зломів під час зберігання та передачі даних через хмарні сервіси. Хакери можуть використовувати різні методи для злому таких сервісів та отримання конфіденційної інформації.

Існує велика кількість досліджень в галузі оптимізації налаштувань криптографічних алгоритмів. У [9-19] автори проводять огляд різних методів оптимізації криптографічних алгоритмів, включаючи генетичні алгоритми, алгоритми на основі машинного навчання та інші.

У [9,11, 18] запропоновано гібридний підхід до оптимізації криптографічних

алгоритмів для пристроїв з обмеженими ресурсами. Автори використовують генетичний алгоритм для пошуку оптимальних налаштувань алгоритмів шифрування.

У [9-12] автори використовують методи машинного навчання для оптимізації криптографічних алгоритмів. Вони досліджують взаємозв'язок між різними параметрами алгоритмів і їх ефективністю та використовують ці знання для підвищення ефективності.

У [12-19] автори використовують методи колективного інтелекту для оптимізації хеш-функцій. Вони використовують різні методи оптимізації, включаючи ройовий інтелект, для пошуку оптимальних параметрів алгоритмів.

Але у цих дослідженнях остається не повністю визначеними питання особливостей забезпечення кібербезпеці в хмарних сервісах.

Мета статті

Забезпечення кібербезпеки в хмарних сервісах є важливим науковим завданням, яке потребує дослідження та вирішення. Застосування криптографічних методів для захисту конфіденційної інформації є одним з основних методів вирішення цього завдання. Врахування особливостей системи та використання оптимальних методів захисту є важливими факторами для успішного розв'язання проблеми [9]. Тому метою статті є аналіз можливостей щодо забезпечення безпеки зберігання та передачі конфіденційної інформації в хмарних сервісах.

При цьому актуальною є тема: "Застосування криптографічних методів для захисту

конфіденційної інформації в хмарних сервісах".

Методи досліджень

Одним з методів для вирішення цієї проблеми є застосування криптографічних методів для захисту даних, які зберігаються в хмарі. Наприклад, шифрування даних перед їх передачею в хмару та зберігання даних в шифрованому вигляді в хмарі. Крім того, можна використовувати механізми аутентифікації, контролю доступу та аудиту, щоб захистити хмарні сервіси від несанкціонованого доступу.

На погляд авторів, основні методи вирішення проблеми:

1. Використання симетричного та асиметричного шифрування для захисту даних.
2. Використання механізмів аутентифікації, контролю доступу та аудиту.
3. Розробка алгоритмів шифрування, які можуть працювати з даними, не викладаючиїх у відкритий доступ.

Особливості вирішення наукового завдання полягають у врахуванні того, що зберігання та передача даних в хмарній інфраструктурі можуть здійснюватися за допомогою різних технологій та протоколів. Тому важливо підібрати оптимальні методи для конкретної системи та врахувати всі можливі загрози [6-9].

Для вирішення проблеми можна використовувати різні алгоритми шифрування, такі як AES, RSA, SHA-256, та інші. Однак, вибір алгоритму повинен залежати від типу даних, які зберігаються в хмарному сервісі, та рівня безпеки, який потрібен для їх захисту.

Наприклад, для захисту фінансових даних можна використовувати AES-256, а для захисту паролів та іншої особистої інформації - RSA.

Виклад основного матеріалу дослідження

Як можна покращити застосування криптографічних методів, якщо вони вже давно відомі. За рахунок можна підвищити ефективність використання криптометодів?

Хоча криптографічні методи досить давно відомі, вони все ще є найбільш ефективними засобами захисту конфіденційної інформації. Однак, стандарти захисту даних не стоять на місці, а постійно розвиваються, оскільки з’являються нові загрози та вразливості. Тому існує постійна потреба в дослідженнях та покращенні криптографічних методів.

Наукова новизна дослідження полягає в тому, що можна вдосконалювати існуючі криптографічні методи, шляхом покращення шифрувальних алгоритмів, зменшення розміру ключів та покращення методів аутентифікації.

Одним із напрямків покращення криптографічних методів є використання квантової криптографії, яка використовує квантову механіку для шифрування та декодування даних. Ця технологія може забезпечити більш високий рівень безпеки, оскільки атаки на квантові системи є важким завданням [12, 14].

Для підвищення ефективності використання криптографічних методів, важливо враховувати особливості конкретної системи та вибирати оптимальні методи захисту, що залежать від типу даних, які зберігаються в хмарному сервісі, та рівня безпеки, який потрібен для їх захисту. Також важливо підтримувати існуючі криптографічні методи у відповідному стані та забезпечувати їх правильне використання.

Для покращення застосування криптографічних методів вважаємо за доцільне розглянути наступні напрямки дослідження [12-15]:

1. Розробка нових криптографічних алгоритмів. Наукова новизна полягає в розробці алгоритмів, які забезпечують більшу стійкість до атак, швидкість обчислення та підтримку різних платформ.

2. Вдосконалення існуючих криптографічних алгоритмів. Це може бути досягнуто за допомогою змін параметрів алгоритму, зокрема, довжини ключа, або змін режиму роботи алгоритму.

3. Дослідження вразливостей і побудова атак на криптографічні методи. Це дозволить підвищити рівень стійкості криптографічних методів, виявити слабкі місця та недоліки, які можуть бути використані зловмисниками для злому криптозахисту.

4. Дослідження криптографічних протоколів, зокрема, їхньої захищеності від різних типів атак. Це дозволить покращити ефективність використання криптографічних протоколів в різних сферах застосування.

5. Розробка нових методів криптографічного ключа. Це може включати в себе використання біометричних даних, генерацію ключа на основі фізичних параметрів пристрою, або використання квантової криптографії.

Новітні дослідження в криптографії дають можливість підвищити ефективність використання криптографічних методів за рахунок розробки нових алгоритмів, удосконалення існуючих методів, вдосконалення протоколів

Є кілька підходів, які можуть бути використані для покращення ефективності використання криптографічних методів [15-18]. Ось кілька з них:

1. Використання нових алгоритмів криптографії: розробка нових алгоритмів криптографії є одним із підходів до покращення ефективності застосування криптометодів. Це може включати розробку алгоритмів з більшою потужністю шифрування, швидкішею роботи та більшою стійкістю до атак.

2. Оптимізація налаштувань криптографічних алгоритмів: у багатьох випадках ефективність криптографічних методів може бути покращена за рахунок оптимізації налаштувань алгоритмів. Наприклад, можна змінити довжину ключа, вибір алгоритму шифрування або використовувати більш потужні системи обчислювальної техніки для забезпечення більшої швидкості обробки даних.

3. Використання комбінованих методів шифрування: одним із способів підвищення стійкості застосування криптографічних методів є використання комбінованих методів шифрування. Це означає, що використовуються два або більше методів шифрування, щоб забезпечити більшу стійкість до атак.

Покращення процесу ключового управління: управління ключами є важливою частиною застосування криптографічних методів. Покращення процесу ключового управління може забезпечити більшу стійкість до атак, а також допомогти уникнути втрати ключів.

Зміна довжини ключа – один з основних способів оптимізації налаштувань криптографічних алгоритмів. Довжина ключа повинна бути достатньою для забезпечення безпеки, проте не повинна бути занадто великою, оскільки це може знизити продуктивність криптосистеми.

Для визначення оптимальної довжини ключа необхідно враховувати рівень потенційної загрози, ступінь вірогідності атак та кількість інформації, яка повинна бути захищена. Для більшої безпеки можна використовувати довші ключі, але це може знизити швидкість обробки даних та потребувати більш потужних обчислювальних ресурсів [13,14].

Існує багато досліджень, які присвячені визначенню оптимальної довжини ключа для різних криптографічних алгоритмів. Наприклад, Національний інститут стандартів та технологій (NIST) США регулярно оновлює рекомендації щодо довжини ключа для різних криптографічних алгоритмів.

Також, існують спеціальні програмні засоби, що дозволяють проводити тестування на міцність криптосистеми при різних довжинах ключа та вибрати найбільш оптимальну довжину для конкретного застосування [14, 15].

Одним з відомих досліджень на цю тему є «Key Lengths» від NIST, який надає рекомендації щодо довжини ключа для різних криптографічних алгоритмів, таких як AES, RSA, SHA-2 і ін.

Отже, зміна довжини ключа – це важлива техніка оптимізації криптографічних алгоритмів.

Звичайно, у кожної методики є свої особливості та переваги, і не можна однозначно сказати, який саме метод є найбільш ефективним. Тому важливо враховувати контекст та конкретну ситуацію, в якій будуть використовуватись криптографічні методи.

Однак, можна виділити кілька загальних принципів, які можуть допомогти підвищити ефективність використання криптографічних методів [15-18]:

1. Використання достатньо складних ключів: чим складніший ключ, тим важче його

розшифрувати зловмиснику.

2. Використання асиметричних шифрувань: такі шифри використовують два ключі, один з яких відкритий, а інший - закритий. Відправник може відправити повідомлення, зашифроване публічним ключем отримувача, тоді як лише власник приватного ключа зможе розшифрувати його.

3. Використання протоколів аутентифікації та авторизації: такі протоколи дозволяють перевірити ідентичність користувача та його дозволи на доступ до ресурсів.

4. Використання стійких алгоритмів шифрування: на сьогоднішній день найбільш стійкі алгоритми шифрування - AES, RSA, SHA.

Регулярне оновлення ключів та алгоритмів: оновлення ключів та алгоритмів забезпечує стійкість криптографічного захисту в часі.

У наукових дослідженнях з криптографії шукають нові методи шифрування, які були більш стійкими та ефективними за вже відомі методи. Наприклад, дослідження в галузі квантової криптографії ведуть до створення нових алгоритмів [18, 19].

Хмарні сервіси застосовуються в різних галузях промисловості, і для кожної з них існують конкретні виклики з кібербезпеки, які потрібно вирішувати. Одним з прикладів може бути промисловість медичних технологій, де зберігається та обробляється конфіденційна інформація про пацієнтів. У цьому випадку, кібербезпека в хмарних сервісах медичних технологій включає в себе захист від несанкціонованого доступу до медичних даних, забезпечення цілісності та конфіденційності даних, а також відновлення даних в разі їх втрати або пошкодження.

Інший приклад може бути промисловість фінансових технологій, де хмарні сервіси використовуються для зберігання та обробки фінансової інформації клієнтів. У цьому випадку, кібербезпека включає в себе захист від кібератак на банківські системи, забезпечення захисту від фішингу та інших видів шахрайства, а також забезпечення дотримання вимог регуляторних органів щодо захисту фінансових даних [19].

Хмарні сервіси стали надзвичайно популярними в сучасному світі, оскільки вони дозволяють користувачам зберігати та обробляти дані у віддалених центрах обробки даних, що зменшує потребу у власних серверах та обладнанні. Однак, це також створює нові виклики для кібербезпеки, оскільки користувачі повинні довіряти свої дані та інфраструктуру хмарних сервісів третім сторонам [19].

Висновки й перспективи подальших досліджень

Аналіз, що проведений авторами дозволяє визначити найбільш важливіші заходи для усунення негативних наслідків вторгнень. Тому організація кібербезпеки в хмарних сервісах повинне включати такі заходи:

Аутентифікація та авторизація: Користувачі повинні проходити процес аутентифікації та авторизації, щоб мати доступ до хмарних сервісів. Для цього можуть використовуватись різні методи, такі як двофакторна аутентифікація, біометричні методи аутентифікації та інші.

Шифрування: Важливо шифрувати дані, які зберігаються в хмарних сервісах, щоб забезпечити їх конфіденційність та недоступність для сторонніх осіб. Крім того, можна використовувати шифрування даних під час їх транспортування до та з хмарних сервісів.

Захист від вірусів та шкідливих програм: Хмарні сервіси повинні мати захист від вірусів та шкідливих програм, які можуть завдати шкоди інфраструктурі та даним користувачів.

Моніторинг та виявлення вторгнень: Хмарні сервіси повинні мати систему моніторингу та виявлення вторгнень, щоб вчасно виявляти та реагувати на можливі загрози.

Захист від DDoS-атак: Хмарні сервіси можуть бути піддаються DDoS-атакам, які спрямовані на перевантаження систем та призводять до відмови в обслуговуванні. Для захисту від цих атак, можуть використовуватись різні методи, такі як захист на рівні мережі, на рівні додатку, а також використання технологій CDN (Content Delivery Network).

Захист від витоку даних: Хмарні сервіси повинні мати заходи для захисту від витоку даних, оскільки це може призвести до серйозних наслідків для користувачів та організацій. Для цього можуть використовуватись методи шифрування даних, моніторингу доступу до

даних та аудиту дій користувачів.

Резервне копіювання: Хмарні сервіси повинні забезпечити можливість резервного копіювання даних, щоб уникнути їх втрати в разі збоїв або атак на систему.

Тестування на проникнення: Організації повинні проводити тестування на проникнення (penetration testing) своєї інфраструктури та додатків, щоб виявляти можливі уразливості та захищати їх від атак.

Захист від інсайдерських загроз: Організації повинні забезпечити захист від інсайдерських загроз, тобто внутрішніх загроз, що можуть виникати з боку співробітників. Для цього можуть використовуватись різні методи, такі як обмеження доступу до даних, моніторинг дій користувачів та навчання співробітників правилам кібербезпеки.

ЛІТЕРАТУРА

1. ISO/IEC 17788 - 2014. Information technology - Cloud computing - Overview and vocabulary. - Publ. 2014-10-15. - Geneva: ISO, 2014. - 10 p.

2. Закон України «Про захист персональних даних»;

3. Закон України «Про доступ до публічної інформації»;

4. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційнотелекомунікаційних системах (Постанова Кабінету Міністрів України від 29.03.06 № 373);

5. Концепція технічного захисту інформації в Україні (Постанова Кабінету Міністрів України від 8.10.97 №1126);

6. Положення про технічний захист інформації в Україні (Указ Президента України від 27.09.99 № 1229/99).

7. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі"

8. Хмарне сховище чи локальні сервери: 9 критеріїв, які слід врахувати під час вибору. https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers

9. Kozyura V. D., Khoroshko V. O., Shelest M. YE., Tkach YU. M., Usov YA.YU. Kompleksni systemy zakhystu informatsiyi v informatsiyno-telekomunikatsiynykh systemakh [Complex systems of information protection in information and telecommunication systems]. Nizhyn: FOP Luk'yanenko V.V. TPK «Orkhideya», 2019. 144 p.

10. How to Protect Your Data from Unauthorized Access, Retrieved from https://cypressdatadefense.com/blog/unauthorized-data-access

11. Cloud Data Center Trends To Watch For In 2015 [Електронний ресурс] / Sarah Tanksalvala-Режим доступу: World Wide Web.- URL: https://www.forbes.com 2015/

12. What Companies Growing More than 50 Percent Faster Are Investing In [Електронний ресурс] / Laura Pevehouse - Режим доступу: World Wide Web. - URL: https://www.delltechnologies.com/en-us/blog/what-companies-growingmore-than-50-percent-faster-are-investing-in

13. Хмарні обчислення, Integrity Systems.[Електронний ресурс]. Доступно: http://integritysys.com.ua/solutions/pricatecloud-solution. Дата звернення: Січ. 27, 2020.

14. А.Е. Кононюк, Фундаментальна теорія хмарних технологій. Київ. Освіта України. 2018. Кн. 2. 528 стор.

15. Краткая история облачных технологий [Електронний ресурс] / Анна Полякова - Режим доступу: World Wide Web. - URL: https://rb.ru/story/cloudcomputing-history/

16. Six Advantages of Cloud Computing [Електронний ресурс] - Режим доступу : World Wide Web. - URL: https://docs.aws.amazon.com/whitepapers/latest/awsoverview/six- advantages-of-cloud-computing.html

17. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021

[Електронний ресурс] - Режим доступу :World Wide Web. - URL: https://www.gartner.co/en/ newsroom/press-releases/2020-11-17-gartnerforecasts-worldwide- publi c-cloud-end-user-spending-to-grow-18 -percent-in-2021

18. 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

19. OWASP is pleased to announce the release of the OWASP Top 10 - 2017 [Електронний ресурс] - 2017 - Режим доступу : World Wide Web. - URL: https://owasp.blogspot.com/2017/11/owasp-is-pleased-to-announce-releaseof.html

REFERENCE

1. ISO/IEC 17788 – 2014. Information technology – Cloud computing – Overview and vocabulary. Publ. 2014-10-15. Geneva: ISO, 2014. 10 p.

2. Law of Ukraine "On Protection of Personal Data". https://zakon.rada.gov.ua/go/2297-17.

3. Law of Ukraine "On access to public information". https://zakon.rada.gov.ua/laws/show/2939-17#Text.

4. Rules for ensuring the protection of information in information, telecommunication and information-telecommunication systems (Resolution of the Cabinet of Ministers of Ukraine dated 03.29.06 No. 373). https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

5. The concept of technical protection of information in Ukraine (Resolution of the Cabinet of Ministers of Ukraine dated 10.8.97 No. 1126). https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text.

6. Regulations on technical protection of information in Ukraine (Decree of the President of Ukraine dated 27.09.99 No. 1229/99). https://zakon.rada.gov.ua/laws/show/1229/99#Text.

7. ND TZI 3.7-003-05 "Procedure for the creation of a comprehensive information protection system in the information and telecommunications system". https://tzi.ua/ua/nd_tz_3.7-003_-2005.html.

8. Cloud storage or local servers: 9 criteria to consider when choosing. https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers.

9. Kozyura V. D., Khoroshko V. O., Shelest M. YE., Tkach YU. M., Usov YA.YU. Kompleksni systemy zakhystu informatsiyi v informatsiyno-telekomunikatsiynykh systemakh [Complex systems of information protection in information and telecommunication systems]. Nizhyn: FOP Luk'yanenko V.V. TPK "Orkhideya", 2019. 144 p.

10. How to Protect Your Data from Unauthorized Access, Retrieved from https://cypressdatadefense.com/blog/unauthorized-data-access.

11. Cloud Data Center Trends To Watch For In 2015 [Electronic resource] / Sarah Tanksalvala - https://www.forbes.com/sites/huawei/2015/04/16/cloud-data-center-trends-towatch-for -in-2015.

12. What Companies Growing More than 50 Percent Faster Are Investing In [Electronic resource] / Laura Pevehouse – https://www.delltechnologies.com/en-us/blog/what-companies-growing-more-than-50-percent-faster -are-investing-in.

13. Cloud computing, Integrity Systems. [Electronic resource]. Available: http://integritysys.com.ua/solutions/pricatecloud-solution.

14. A.E. Kononyuk, Fundamental theory of cloud technologies. Kyiv. Education of Ukraine. 2018. Book 2. 528 pages.

15. Brief history of cloud technologies [Electronic resource] / Anna Polyakova. https://rb.ru/story/cloudcomputing-history.

16. Six Advantages of Cloud Computing [Electronic resource]. https://docs.aws.amazon.com/whitepapers/latest/awsoverview/six-advantages-of-cloud-computing.html.

17. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021 [Electronic resource]. https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartnerforecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021.

18. Using multi-factor authentication (MFA) in AWS [Electronic resource]. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html.

19. OWASP is pleased to announce the release of the OWASP Top 10 – 2017 [Electronic resource]. https://owasp.blogspot.com/2017/11/owasp-is-pleased-to-announce-releaseof.html.

Bohomia V.I., Kochegarov V.S.

CYBERSECURITY IN CLOUD SERVICES USING CRYPTOGRAPHIC METHODS

Cybersecurity is relevant in Ukraine, as the modern world increasingly relies on technology and information systems. Additionally, Ukraine is currently at war in the east of the country, and Russian hackers and cybercriminals actively use cyberattacks to cause damage to important infrastructure objects, government institutions, and citizens of Ukraine.

Furthermore, with the rapid development of technology and the increasing number of digital services, many companies and institutions are becoming increasingly vulnerable to cyberattacks. This creates a need for effective cybersecurity.

Therefore, cloud services are an important part of the infrastructure of many companies and institutions that store confidential information about clients and users. However, the increased use of cloud services also leads to an increase in cybersecurity threats. One of the current problems is ensuring confidentiality and protection against breaches during data storage and transmission through cloud services. Hackers can use various methods to hack such services and obtain confidential information.

Ensuring cybersecurity in cloud services is an important scientific task that requires research and solution. The use of cryptographic methods to protect confidential information is one of the main methods of solving this task. Taking into account the characteristics of the system and using optimal protection methods are important factors for successfully solving the problem.

Therefore, the purpose of this article is to analyze the possibilities of ensuring the security of storage and transmission of confidential information in cloud services using cryptographic methods.

Keywords: *cybersecurity, cloud services, cryptographic methods, encryption algorithms, authentication methods.*