УДК 004.338:004.632:004.738.5
DOI https://doi.org/10.32782/2663-5941/2023.4/18

Стаценко Д.В.
Київський національний університет технологій та дизайну

Стаценко В.В.
Київський національний університет технологій та дизайну

Злотенко Б.М.
Київський національний університет технологій та дизайну

Романюк Є.О.
Київський національний університет технологій та дизайну

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглянути методи використання інформаційно-комунікативних технологій за допомогою яких можна підвищити захист інформації користувачів. Описано підходи, за допомогою яких дані можна відновити після їх зміни шкідливим програмним забезпеченням. В представленому матеріалі зазначені переваги використання приватних хмарних сховищ. В статті описані підходи до їх інтеграції та налаштування. Розглянуто різні методи технологій RAID для покращення ефективності приватних хмарних сховищ.

Сьогодні вартість інформації, що використовується в роботі та повсякденному житті, займає велике значення для її власників. Вона може багаторазово перевищувати вартість обладнання, що використовується для її зберігання. Відповідно використання сучасних інформаційних технологій для захисту інформації відіграє значну роль в приватному та професійному житті.

Складність та розгалуженість інформаційних інфраструктур призводить до збільшення потенційних загроз з боку зловмисників, які ставлять за мету отримання інформації, що зберігається на носіях комп'ютерних систем.

Хмарні технології все частіше обираються великою кількістю компаній для збереження даних, відповідно до чого зростає кількість постачальників даних послуг. Однак збереження інформації в таких системах залишається першочерговою. Проблеми, пов'язані з основними аспектами безпеки, а саме конфіденційністю, цілісністю та доступністю, розглядаються разом із пов'язаними з ними вразливими місцями.

Атаки на дані, що зберігаються на файлових серверах і робочих станціях, стають все більш поширеними. Стандартні методи безпеки не завжди задовольняють поставленим вимогам, а також можуть стати об'єктом кібератаки, якщо вони не налаштовані належним чином. В результаті чого, буде втрачена інформація від часу останнього резервного копіювання даних до моменту атаки. Стаття має на меті дослідити та запропонувати підходи, які можуть бути використані для зберігання, захисту та відновленню масивів даних. Наведені позитивні та негативні сторони запропонованих рішень.

Ключові слова: *інформаційно-комунікативні технології, хмарні сховища, RAID, захист інформації, шифрування, шкідливе програмне забезпечення.*

Постановка проблеми. У даному матеріалі розглянуті питання підвищення безпеки зберігання даних в інформаційно-комунікативних системах, що використовуються в різних комерційних компаніях. В результаті чого необхідність впровадження різноманітних інформаційних технологій для полегшення роботи. Файлові сервери на сьогодні є більш поширеними і використовуються в багатьох установах.

Одним із основних застосувань файлових серверів є зберігання цифрових даних компанії. Іншим застосуванням файлових серверів є необхідність легкого способу обміну інформацією між співробітниками компанії. Зазвичай дані, що зберігаються в комп'ютерних системах компанії, перевищують доступний обсяг апаратних носіїв.

Дискове сховище є важливим компонентом комп'ютерних систем для зберігання даних. Добре відомі, як провідні витрати в інформаційних проєктах, прогнозується їх щорічне зростання в більшості організаціях.

Аналіз останніх досліджень і публікацій. Із зростанням інфраструктури пов'язаної з інформаційно-комунікаційними технологіями зростає і обсяг необхідних для зберігання даних, що в свою чергу призводить до збільшення кількості розробленого шкідливого програмного забезпечення. В останні роки атаки на дані, що зберігаються на серверах і робочих комп'ютерах, постійно зростають [1–3].

Програмне забезпечення-вимагач – це тип зловмисного програмного забезпечення, яке намагається заблокувати доступ користувача до робочої станції або даних, які зберігаються на неї. Метою програм-вимагачів є блокування жертві доступу до її власних ресурсів шляхом блокування ОС або шифрування певних файлів, які здаються цінними для жертви, наприклад фотографій, електронних таблиць або презентацій [4]. Щоб відновити цей доступ, вимагачі потребують викуп. Сума запитуваного викупу та призначення платежу залежить від типу вірусу. Викуп в основному коливається від 300 доларів до 2000 доларів за розшифровку інформації та повернення доступу. Поширення криптовірусів досягається в основному за допомогою шкідливого програмного забезпечення типу «троянський кінь» і масових електронних повідомлень в яких також знаходяться віруси. Для виявлення типу програми вимагача існує декілька методів [5].

Компанії з антивірусного програмного забезпечення вкладають все більше ресурсів і зусиль у розробку програмного забезпечення, яке допомагає розшифровувати інформацію, але це потребує певного часу в залежності від типу вірусного ПЗ. Сьогодні існує десятки програм-вимагачів, для яких не розроблено інструментів відновлення.

Криптовіруси атакують певні типи файлів, що залежить від типу та версії шкідливого ПЗ. Більш інтелектуальні алгоритми, крім локальних файлів, шифрують файли, доступні на підключених мережевих дисках, а також сканують локальну мережу на наявність незахищених ресурсів – спільних папок і дисків з дозволом на читання і запис, що робить файлові сервери вразливими.

Хмарне сховище – це одна з хмарних служб інформаційно-комунікативних технології, яка дозволяє користувачам віддалено зберігати та керувати своїми даними на хмарних серверах. Воно представляє собою модель мережевого онлайн-сховища, де дані зберігаються на кількох віртуальних серверах [6]. Характеристики хмарних обчислень можуть створити серйозний ризик для даних, оскільки одні й ті ж ресурси використовуються різними користувачами [7].

Метою статті є дослідження та порівняння існуючих інформаційно-комунікаційних технологій для збереження та відновлення даних користувачів, які використовуються в межах організацій.

Виклад основного матеріалу. Хмарне сховище – це модель мережевого онлайн-сховища, де дані зберігаються на кількох віртуальних серверах, які зазвичай розміщені третіми сторонами, а не на виділених серверах [6]. Це дозволяє користувачам зберігати свої дані на віддалених дисках і отримувати доступ до них у будь-який час із будь-якого місця [8].

Архітектура хмарного сховища (рис. 1) складається з [8] інтерфейсу, який експортує API для доступу до сховища. У традиційних системах зберігання цим API є протокол SCSI; але в хмарі ці протоколи постійно розвиваються. Логіка зберігання за інтерфейсом – це рівень проміжного ПЗ. Він реалізує різноманітні функції, такі як реплікація та зменшення даних, замість традиційних алгоритмів розміщення даних. Серверна частина реалізує фізичне зберігання даних за допомогою або внутрішнього протоколу, який реалізує певні функції, або традиційної серверної частина фізичних дисків.

Загалом розрізняється три основні типи хмар: публічні, приватні та гібридні.

Загальнодоступні (публічні) хмари – це тип послуг SaaS. Найпоширенішими з них є Google Drive, Microsoft One Drive, pCloud, DropBox,

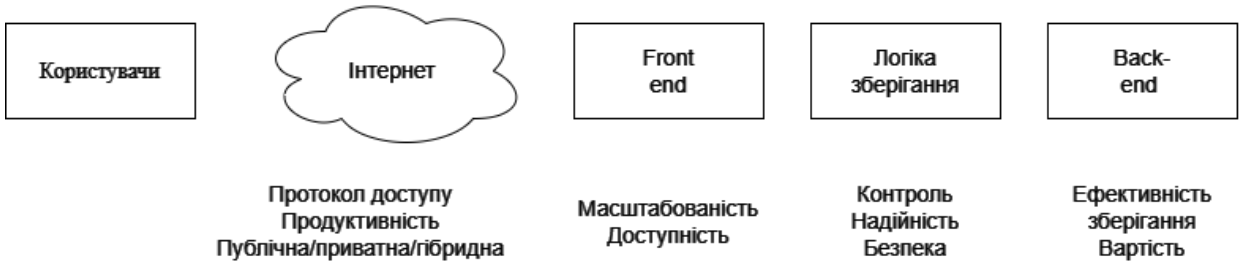

Рис. 1. Архітектура хмарного сховища

Amazon Cloud, Apple iCloud та інші. Ці типи хмар добре підходять для зберігання та обміну неконфіденційними даними, але вони не є рекомендованим варіантом для зберігання та обміну конфіденційною та конфіденційною інформацією через відсутність контролю над серверами, на яких зберігаються дані.

Гібридна хмара – це інфраструктура, яка поєднує в собі дві або більше різних хмарних інфраструктур (приватних, загальнодоступних, державних), які мають унікальні об'єкти, але з'єднані між собою стандартними або спеціалізованими технологіями від фірм виробників, які дозволяють передавати дані або програми між компонентами.

У приватній хмарі служби та інфраструктурні ресурси підключені до локальної мережі. Користувачі бачать надані ресурси як послуги SaaS, але при цьому потрібно сформувати організацію, яка буде підтримувати інфраструктуру даного сховища. Щоб захистити інформацію, системи захисту розміщуються в локальній комп'ютерній мережі організації. Відповідно до чого, доступ до файлів або комп'ютерної станції має знаходитись в цій мережі, або потрібно використовувати віртуальну приватну мережу (VPN).

Переваги приватних хмар наступні: масштабованість; захист; високий рівень безпеки, оскільки система випускається тільки для потреб організації і ніхто інший не має до неї доступу; простіше управління структурою; легкий контроль доступу користувачів до певних ресурсів.

Параметри резервного копіювання для файлових серверів зазвичай передбачають створення резервних копій, що в деяких випадках не є достатньо гнучким способом захисту. У разі зараження криптовірусом це призведе до втрати даних за період від останнього резервного копіювання до моменту зараження. У таких випадках приватні хмари, безсумнівно, надають великі переваги, такі як контроль версій і підтвердження видалення.

У випадках, коли використовується файловий сервер, надання доступу відбувається за іншою процедурою, оскільки для захисту інформації сервер зазвичай під'єднаний безпосередньо лише до локальної мережі, а доступ до збереженої інформації здійснюється з публічної мережі, для чого використовуються VPN. Також можна реалізувати приватні хмари лише в локальній мережі, якщо дані, що зберігаються, надто конфіденційні.

Недоліком локальних користувачів є те, що вони зберігають копії даних на машинах, на яких вони встановлені та налаштовані. Ці копії зберігаються в незашифрованому вигляді. Однак локальні користувачі також використовуються в ситуаціях, коли однакові великі файли спільно використовуються різними користувачами.

Наприклад, відділ попереднього друку, який не працює з локальними копіями даних або не копіює необхідні файли для роботи на локальному комп'ютері, то при середньому розмірі файлу 100 МБ генерується 100 МБ трафіку для кожного індивідуально відкритого файлу. При збереженні файл необхідно передати на сервер, а потім розглянути можливість збереження, що у свою чергу інколи навантажує мережу та сповільнює роботу інших користувачів.

Під час використання локального клієнта користувач один раз згенерує 100 МБ трафіку на сервер, щоб зберегти локальну копію сервера, а потім вона буде прочитана локальною файловою системою. При збереженні трафік на сервер не зменшиться, але синхронізація версій файлів на локальному комп'ютері і сервері стане «невидимою» для користувачів і це не заважатиме роботі інших людей на сервері. Крім того, збереження файлу на локальний диск буде швидшим, ніж збереження через мережу, відповідно синхронізація займе таку саме кількість часу, скільки при роботі через змонтований диск.

Загалом проблеми пов'язані з безпекою в хмарних сховищах охоплює три аспекти: конфіденційність, цілісність і доступність (CIA). Ці аспекти є основними міркуваннями при розробці заходів безпеки для забезпечення максимального захисту [9]. Забезпечення доступу до захищених даних обмежено певним рівнем користувача, авторизованого на доступ до них.

Основна відмінність між файловими серверами та приватними хмарами полягає в тому, що файлові сервери не мають захисту масивів даних, тоді як приватні хмари мають контроль версії та подвійне видалення. На файлових серверах захист від таких атак програм-вимагачів пов'язаний із резервним копіюванням даних. У разі криптовірусної атаки це призведе до втрати даних з останньої резервної копії.

Контроль версій може забезпечити безпеку у кількох випадках зараження програмами-вимагачами. Деякі криптовіруси не видаляють файли, а шифрують лише частину метаданих файлу, не видаляючи оригінальну копію, а перезаписуючи його без зміни імені та/або розширення. У таких ситуаціях незашифровані файли можна відновити за допомогою контролю версій, вбудованого в описані приватні хмари.

Режим подвійного видалення може захистити інформацію від криптовірусів, які шифрують цілі файли та видаляють незашифровані дані. У підході подвійного видалення, після видалення файл

автоматично потрапляє до кошика, індивідуального для кожного користувача. Видалені файли потраплять у папку «Видалені» користувача, який видалив файли, а не до папки «Видалені» користувача, якому належать файли.

Щоб відновити файли, комп'ютерну мережу спочатку потрібно очистити від програм-вимагачів, після чого видалені файли можуть бути відновлені відповідним користувачем з розділу «Видалені файли» у веб-інтерфейсі. Основна проблема в даному випадку полягає в тому, що потрібно мати великий дисковий простір. Наприклад для відновлення даних об'ємом 5 ТБ, при активації модуля для зберігання інформації на сервері в зашифрованому вигляді, що збільшує розмір до 35%, відповідно сервер зберігатиме 6,75 ТБ.

Коли система заражена вірусом даного типу, відбувається шифрування поточних файлів, що додатково збільшує їх розмір, а розмір зашифрованих файлів залежить від використовуваного алгоритму шифрування. У загальному випадку розмір не збільшується більше ніж на 50%, тобто зашифровані файли досягнуть розміру 10 ТБ. Після того, як файли зашифровано, вихідні незашифровані файли переміщуються до «Видалених файлів», відповідно загальний простір, який займуть заражені та неінфіковані файли, становитиме 16,75 ТБ. Це означає, що потрібно мати приблизно 10 ТБ вільного хмарного простору, щоб забезпечити постійне відновлення інформації. Якщо вільне місце на диску сервера, для запуску операції, відсутнє, процедура виконується методом черги, і файли з «Видалених файлів» видаляються, згідно з правилом, першим буде видалено перший, введений у «Видалений файл».

Один з методів для зменшення об'єму необхідного для виконання операції автоматичного резервного відновлення видалених файлів у приватних хмарних сервісах розроблено доповнення «Захист від програм-вимагачів». Після її активації автоматично створюється список із розширеннями, які потенційно можуть містити шкідливого програмне забезпечення та запобігає виконанню вкладених файлів та інших вірусів. У модулі міститься база даних більшості відомих шкідливих ПЗ, тому рекомендується постійно оновлювати даний додаток.

На першому етапі встановлення приватної хмари необхідно визначити та розрахувати потужність обладнання, яке встановлене в організації. На другому етапі відбувається перенесення наявних даних у вибрану приватну хмару. Створюються основні користувачі для системи, у якій зберігаються файли та з якої користувачі надають спільний доступ іншим, щоб під час роботи з людьми в приватній хмарі право власності на файл завжди належало основним користувачам. Це дозволяє легко видалити користувача з системи при звільненні співробітника організації, без видалення файлів основного користувача. Існує декілька способів переміщення даних із файлового сервера або спільних каталогів у приватну хмару.

1. Підключення головного користувача до сервера через WebDAV і копіювання даних вручну.

2. Використання клієнта синхронізації. При налаштуванні клієнта синхронізації з новим користувачем встановлюється локальний каталог, у якому будуть зберігатися файли. Важливо вибрати параметр, який вказує, де зберігати локальні файли. Це призведе до того, що клієнт синхронізації автоматично завантажить їх у приватну хмару, і якщо цей параметр не вибрано, файли, розташовані у вказаному каталозі, будуть видалені.

При створенні нових користувачів необхідно врахувати їх ієрархію доступу. Для належної конфігурації та гнучкості ієрархії рекомендовано використання методів створення груп і організації в них користувачів. При цьому користувач може бути членом кількох груп.

Наступний етап налаштування приватних хмар організацій є налаштування механізмів доступу користувачів до файлу. Розглянуті приватні хмари мають декілька варіантів доступу до даних – через браузер, клієнт синхронізації та WebDAV. Деяким організаціям може знадобитися поєднання різних методів доступу до даних.

Таким чином опорними точками для впровадження приватної хмари в існуючу інформаційну інфраструктуру організації є:

1. вибір типу приватної хмари.
2. розрахунок необхідної потужності комп'ютерних систем.
3. встановлення та налаштування приватної хмари.
4. перенесення даних у приватну хмару.
5. додавання користувачів і створення ієрархії.
6. обмін інформацією з новоствореними користувачами.
7. налаштування доступу робочої станції до приватної хмари.

В порівнянні з файловими серверами приватні хмари крім зберігання інформації мають систему автентифікації користувачів, за допомогою якої можна визначити, чи може користувач лише читати файл, редагувати його та ділитися ним з іншими користувачами, що в разі файл-серверів може виконувати лише системний адміністратор. Дані можуть зберігатися в зашифрованому вигляді на сервері, а також доступ до них через зашифрований зв'язок. Також, за замовчуванням вони мають

контроль версій, який може не тільки захистити дані від деяких типів програм-вимагачів, але й від зловмисника, який видаляє самі дані у файлі і як вже зазначалося є функція подвійного видалення.

Доступність хмарного сховища означає час безперебійної роботи системи та здатність системи працювати безперервно. Для підвищення доступності системи використовуються різні методи. У хмарі дані зберігаються за допомогою RAID (надлишкового масиву незалежного диска). Він забезпечує спосіб зберігання тих самих даних у різних місцях на кількох дисках. Функції RAID у сховищі даних RAID – це технологія, яка об'єднує незалежні фізичні диски в один жорсткий диск з метою підвищення швидкості читання/запису або підвищення надійності збережених даних, або обох. Існує 2 реалізації RAID [10]: Апаратний RAID потребує контролера RAID, який керує введенням/виведенням, частіше за все, він використовується для хост-серверів. Даний тип має високу продуктивність, але вартість його висока. Програмний RAID: операційна система контролює вхід/вихід, він реалізований на комп'ютерах для підвищення продуктивності за урахуванням невисокої вартості необхідного обладнання.

RAID використовує багато різних архітектур, які називаються рівнями, кожен рівень має різні сценарії диска та техніки зберігання, залежно від балансу між відмовостійкістю та продуктивністю. У рівнях хмарної архітектури RAID описується, як дані розподіляються між дисками, існує 7 рівнів RAID з різними функціями, створених на двох базових рівнях RAID 0 і RAID 1 [10].

RAID 0 складається принаймні з 2 подібних дисків, що створює масив із n дисків ($n \geq 2$). Дані рівномірно розподіляються та записуються на всі пристрої в масиві. Кожен диск зберігає 1/n даних. Розмір масиву визначається, як розмір найменшого диска, помножений на кількість дисків. До переваг даного рівня відноситься швидкість передачі читання/запису, відповідно кожен диск має читати/записувати 1/n даних. Недоліки полягають в тому, що надійність в такій системі знижується, якщо один диск виходить з ладу, усі дані в масиві RAID 0 втрачаються.

RAID 1відноситься до найпростіших рівнів RAID. Він забезпечує надійність даних. Як і попередній рівень, RAID 1 потребує принаймні 2 диска для роботи. Дані зберігаються двічі на 2 дисках (метод дзеркала), при цьому, якщо один диск виходить з ладу, другий залишається працездатним. Відповідно до чого, диск, який вийшов з ладу, можна замінити, не турбуючись про втрату даних. RAID 1 не є високопродуктивним; однак це важливо для адміністрацій та осіб, які керують важливими даними. Ємність масиву RAID 1 дорівнює розміру одного диска. На рисунку 2 показані моделі RAID 0 та RAID 1.

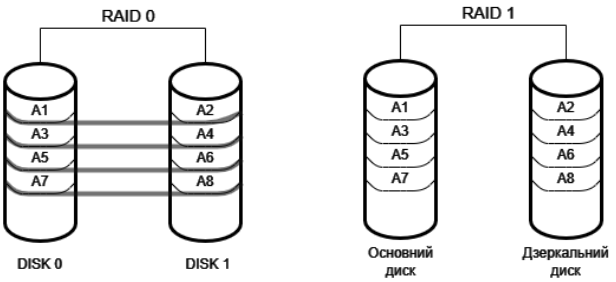

Рис. 2. Структурні моделі RAID 0 та RAID 1

Наступна модель, RAID 10, поєднує в собі підходи RAID 1 та RAID 0. Для створення масиву даного типу потрібно мінімум 4 диски. Дані записуються на 4 диски одночасно: за допомогою технології «смугастість» (RAID 0) на 2 дисках і за допомогою метода «дзеркала» (RAID 1) на двох інших. Метод RAID 10 має високу швидкість і при цьому рівень безпеки більший ніж в RAID 0, в зв'язку з тим, що працездатність залишається навіть коли один з дисків виходить з ладу. На рисунку 3 показано модель RAID 10.

До недоліків RAID 10 можна віднести високу вартість, ефективний простір становить 50% від загального розміру 4 дисків.

Головним недоліком приватних хмар у порівнянні з файловими серверами є те, що для зберігання одних і тих же даних і роботи тієї ж кількості користувачів з системою потрібно більше обчислювальних ресурсів. Інтеграція приватної хмари

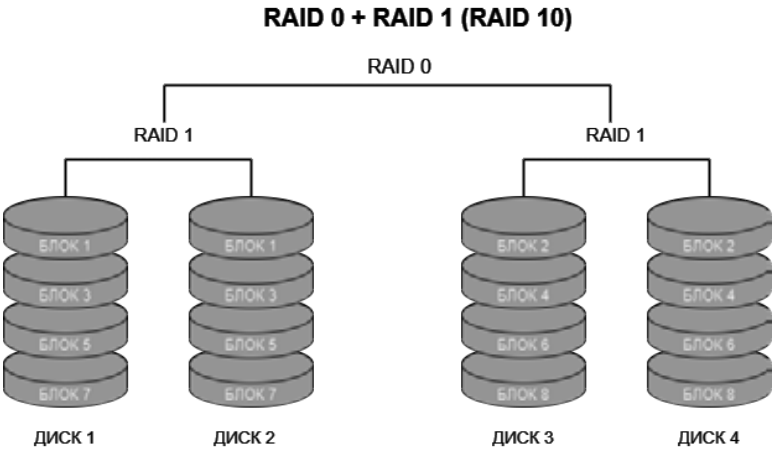

Рис. 3. Структурна модель RAID 10

може бути складним завданням, для вирішення якого потрібен більш кваліфікований персонал.

Висновки. Останнім часом кількість шкідливого програмного забезпечення зросла, особливо віруси типу «вимагач» призводе до блокування або втрати цінної інформації. Використання інформаційно-комунікативних технологій таких, як приватна хмара, розглянуті в цьому матеріалі, є одним з способів, за допомогою якого можна підвищити захист даних. Описано підходи, за допомогою яких інформацію користувачів можна відновити після шифрування. Також описано основні переваги використання розглянутих рішень у порівнянні зі стандартними файловими серверами. Наведено підходи до інтеграції та налаштування приватної хмари в існуючу інформаційну інфраструктуру організації. Представлені та запропоновані різні методи технологій RAID для покращення ефективності доступності хмарних сховищ. Наведені позитивні та негативні сторони запропонованих рішень.

Список літератури:

1. Mohurle S., Patil M. A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science,* Volume 8, No. 5, May-June 2017, ISSN No. 0976-5697.

2. Richardson R., North M. Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, Vol. 13 No. 1 2017.

3. Стаценко Д.В., Стаценко В.В., Осипенко В.В., Злотенко Б.М., Кулік Т.І. Сучасні тенденції кіберзагроз у комп'ютерних системах та мережах. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. 2021. с. 156-161.

4. Tailor J.P., Patel A.D. A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control. *Int. J. Res. Sci. Innov.,* vol IV, no. November, pp. 2321-2705.

5. Kok SH, Azween Abdullah A., Jhanjhi NZ, Supramaniam M. Ransomware, Threat and Detection Techniques: A Review. *IJCSNS International Journal of Computer Science and Network Security*, VOL.19 No. 2, February 2019, pp. 136-146.

6. Balbudhe Pravin O., Balbudhe Pradip O. Cloud storage reference model for cloud computing. *International Journal of IT, Engineering and Applied Sciences Research (IJIEASR)*, 2(3):83, March 2013.

7. Chandan P., Surajit D. Cloud computing security analysis: Challenges and possible solutions. *In International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, page 3, 2016.

8. Spoorthy V., Mamatha M., Santhosh Kumar B. A survey on data storage and security in cloud computing. *International Journal of Computer Science and Mobile Computing*, 3(6):307-311, June 2014.

9. Yahya F., Chang V., Walters R.J., Wills G.B. Security challenges in cloud storage. *In IEEE 6th International Conference on Cloud Computing Technology and Science*, pages 1052-1054, 2014.

10. Le Quang Minh, Huy Anh Phan, Anh Chuyen Nguyen, Khanh Duong Le. Research on enhancing security in cloud data storage. *In ICTA: International Conference on Advances in Information and Communication Technology*, pages 511-512, 2016.

Statsenko D.V., Statsenko V.V., Zlotenko B.M., Romaniuk I.O. USING INFORMATION AND COMMUNICATION TECHNOLOGIES FOR INFORMATION PROTECTION

The article considers the methods of using information and communication technologies, which can be used to improve the protection of user information. Describes approaches by which data can be recovered after it has been altered by malicious software. The presented material indicates the advantages of using private cloud storage. The article describes approaches to their integration and configuration. Different methods of RAID technologies to improve the performance of private cloud storage are considered.

Today, the value of information used in work and everyday life is of great importance to its owners. It can many times exceed the cost of the equipment used for its storage. Accordingly, the use of modern information technologies to protect information plays a significant role in private and professional life.

The complexity and branching of information infrastructures leads to an increase in potential threats from attackers who aim to obtain information stored on computer system media.

Cloud technologies are increasingly being chosen by a large number of companies for data storage, and accordingly, the number of data service providers is increasing. However, the preservation of information in such systems remains a priority. Issues related to the fundamental aspects of security, namely confidentiality, integrity, and availability, are addressed along with their associated vulnerabilities.

Attacks on data stored on file servers and workstations are becoming more common. Standard security methods do not always meet the requirements and can also become the target of a cyber attack if they are not configured properly. As a result, information will be lost from the time of the last data backup to the moment of the attack. The article aims to explore and propose approaches that can be used to store, protect and recover data sets. The positive and negative aspects of the proposed solutions are given.

Key words: *information and communication technologies, cloud storage, RAID, information protection, encryption, malicious software.*