

УДК 78.031.4:004.67:930.25(477)(045)
DOI: <https://doi.org/10.31318/2522-4212.2024.19.319765>

Олександр Кропивний

ORCID: <https://orcid.org/0000-0001-7601-7878>
Аспірант Кафедри історії української музики та музичної фольклористики
Національної музичної академії України імені П. І. Чайковського
Вул. Архітектора Городецького, 1-3/11, 02000 Київ, Україна
Тел.: +38 050 7717182; e-mail: ok@accordion.in.ua



АУДІОВІЗУАЛЬНІ КОЛЕКЦІЇ МУЗИЧНОГО ФОЛЬКЛОРУ В УМОВАХ ВОЄННОГО ЧАСУ: ПРОЄКТ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ ДЛЯ ЗБЕРІГАННЯ ЦИФРОВИХ ДАНИХ

У статті представлено досвід розробки та впровадження серверної інфраструктури для зберігання цифрових аудіовізуальних колекцій українського музичного фольклору. Особливу увагу приділено технічним аспектам збереження, резервного копіювання та забезпечення доступності даних в умовах воєнного часу. Основою запропонованої системи є мобільна архітектура, що забезпечує швидке переміщення серверів та їх відновлення без втручання адміністратора.

Реалізація системи базується на використанні файлової системи ZFS для забезпечення надійності та цілісності даних, а також технології RAIDZ для захисту від апаратних збоїв. Важливу роль відіграє застосування принципу резервного копіювання 3-2-1, що включає створення кількох копій даних на різних носіях, зокрема в хмарному середовищі. Для віддаленого доступу до даних застосовано протокол WireGuard, що забезпечує безпечний VPN-зв'язок між користувачами та серверами.

Запропонована серверна інфраструктура вирішує ключові проблеми, з якими стикаються українські етномузикологи та культурні інституції під час роботи з цифровими архівами: зберігання великих обсягів аудіовізуальних даних, організація автоматизованого резервного копіювання та можливість оперативного доступу до колекцій. Особливістю системи є її здатність до масштабування, що дозволяє використовувати її як на локальному рівні, так і в рамках загальноукраїнського цифрового репозиторію.

Апробацію пропонованих підходів проведено на матеріалах Лабораторії етномузикології Національної музичної академії та приватних записах її співробітників. Практичні дії демонструють ефективність створеної інфраструктури для забезпечення збереження культурної спадщини, особливо в умовах нищівних загроз під час війни.

Ключові слова: український музичний фольклор, етномузикологія, Лабораторія етномузикології (Київ), репозиторій, архівування, цифровий архів, серверна інфраструктура, мережеве сховище

Скорочення, використані у статті

ІМФЕ – Інститут мистецтвознавства, фольклористики та етнології імені М. Т. Рильського Національної академії наук України, м. Київ

ЛЕК – Лабораторія етномузикології, Київ = ПНДЛ (див. нижче)

НМАУ – Національна музична академія України імені П. І. Чайковського, м. Київ

ПНДЛ – Проблемна науково-дослідна лабораторія етномузикології НМАУ

ЦР УМФ – цифровий репозиторій українського музичного фольклору

Вступ

Одним із ключових завдань українських етномузикологів упродовж останніх років є збереження, оцифрування та каталогізація аудіовізуальних колекцій — як інституційних, так і приватних. Особливий

сплеск уваги до цієї теми, що спостерігався з початку активної фази російсько-української війни у 2022 році, триває досі. Останнім часом зростає кількість проєктів, присвячених архівній тематиці в етномузи-

кології: це наукові публікації й виступи (А. Вовчак, І. Довгалюк, Л. Добрянська, О. Коробов та інші) та громадські ініціативи, наприклад акція «Відкритий лист до ІМФЕ» від київської спільноти любителів фольклору.

Незадовго до початку воєнних дій, коли стало зрозуміло, що вторгнення є неминучим, та в перші місяці після впровадження воєнного стану на території України в лютому 2022 року, розпочалася низка акцій з евакуації матеріальних фондів та резервного копіювання цифрових фольклорних колекцій. Оскільки всі ці роботи відбувалися в очікуванні наступу ворожих сил, а іноді в безпосередній близькості до територій ведення бойових дій, вони були дещо хаотичними, несистемними та спрямованими на захист суб'єктивно найцінніших об'єктів.

Евакуація фізичних носіїв інформації відбувалася силами самих утримувачів колекцій, тоді як копіювання цифрових даних майже повністю спиралося на ініціативи, налагоджені сторонніми особами та організаціями, здебільшого закордонними. Серед таких ініціатив, які відбувалися після початку широкомасштабної війни на території України, можемо навести¹:

- 24 лютого 2022: дистанційне резервне копіювання фондів Проблемної науково-дослідної лабораторії етномузикології Національної музичної академії України імені П. Чайковського (далі – Лабораторія етномузикології / ЛЕК) до мережевого сховища, наданого Литовською академією музики і театру, ініціатива Варси Люткуте-Закарене (Varsa Lutkutė-Zakariene);

- 25 лютого 2022: масштабне резервне копіювання до хмарного сховища (технологія Google Drive), наданого Університетом Індіани за сприяння Американського фольклорного товариства (США), ініціатива спільноти українських фольклористів та любителів фольклору, куратор та посередник – Ірина Волошина (Вовчак, 2022б);

- березень-червень 2022: низка засідань робочих груп, присвячених збереженню та захисту цифрової інформації, організатори – Ірина Клименко, Андрій Вовчак (Барышнікаў, 2022; Вовчак, 2022а; Маханець, 2022);

- 11 березня 2022: ініціатива Університету Альберти (Канада) «U-ART Українським вченим — Термінова архівація даних в Канаді» (Canadian Institute of Ukrainian Studies, 2022);

- 22 березня 2022: проєкт «Збереження української культурної спадщини онлайн (Saving Ukrainian Cultural Heritage Online, SUCHO)», ініціатори Квінн Домбровські (Quinn Dombrowski) зі Стенфордського університету (Stanford University), Анна Е. Кіяс (Anna E. Kijas) з Університету Тафтса (Tufts University) та Себастьян Майсторович (Sebastian Majstorovic) з Австрійського центру цифрових гуманітарних наук і культурної спадщини (Austrian Centre for Digital

Humanities and Cultural Heritage) (RISM Editorial Team, 2022).

Зважаючи на складні умови того часу, відсутність належної підготовки та аналізу ситуації, технічну необхідність українських утримувачів колекцій про технології, які використовуються, а також через неможливість прямої та чіткої комунікації ініціаторів з великим числом задіяних користувачів, відразу почали виникати як технічні, так і правові та етичні проблеми².

Станом на кінець 2024 року можемо констатувати, що за період воєнних дій 2022–2024 років не було завдано непоправної шкоди цифровим матеріалам, що належать учасникам згаданих вище ініціатив, а матеріали в наданих цифрових сховищах стали одними з багатьох резервних копій невисокої якості (зважаючи на згадані проблеми та недоліки).

На початку 2022 року українські інституції і приватні утримувачі фольклорних аудіовізуальних колекцій не мали необхідної інфраструктури для зберігання цифрових даних, а також не володіли методиками резервного копіювання та роботи з цифровими даними, тому потребували допомоги сторонніх партнерів, швидко (й тому поверхнево) освоюючи нові принципи роботи. У час умовного «затишшя» активних бойових дій чимало українських дослідників розпочало власні більш системні та сплановані активності із систематизації та резервного копіювання цифрових фондів, а також розробку технічних рішень для реалізації цих задумів, як от купівля нової техніки чи отримання безкоштовних хмарних сховищ для інституцій за програмою Google Workspace for Education (Google, н.д.) тощо.

Серед подібних ініціатив найближчими автору є проєкти, які реалізує київський осередок етномузикологів, об'єднаних навколо ЛЕК. На основі роботи з колекціями ЛЕК було розроблено концепцію інституційного цифрового репозиторію українського музичного фольклору (ЦР УМФ), загальні положення якої описано в попередніх публікаціях автора (Кропивний, 2022; 2023а; 2023б). У цих роботах більше уваги приділено теоретичним аспектам концепції, ніж її технічним особливостям.

Відсутність напрацьованих технічних методик роботи із цифровими аудіовізуальними архівами музичного фольклору стала очевидною для українських етномузикологів під час подій весни 2022 року, тож розробка технічної інфраструктури для зберігання таких даних є нагальною потребою.

У цій статті автор має **на меті**:

² Наприклад, ті, хто використовував технологію Google Drive від Університету Індіани, неодноразово скаржилися, на те, що завантажені файли «безслідно зникають»; при завантаженні матеріалів до сховища Synology через Web-GUI застосунок частина файлів не завантажувалася без попереджень про це; на початку своєї роботи ініціативи з резервного копіювання фондів до сторонніх сховищ мали неврегульований правовий статус завантажених матеріалів; існують резервні копії, створені сторонніми особами, до яких правласники не мають прямого доступу etc.

¹ Список не є вичерпним і обмежується лише найбільш масштабними проєктами, до яких автор був безпосередньо причетний.

а) проаналізувати стан цифрової колекції ЛЕК на тепер (2024);

б) окреслити передумови створення нової серверної інфраструктури ЛЕК;

в) запропонувати нові для української етномузикології підходи до зберігання й резервного копіювання цифрових даних;

г) детально описати програмні та апаратні рішення, застосовані для реалізації нової інфраструктури.

Цифровий фонд ЛЕК. Сучасний стан

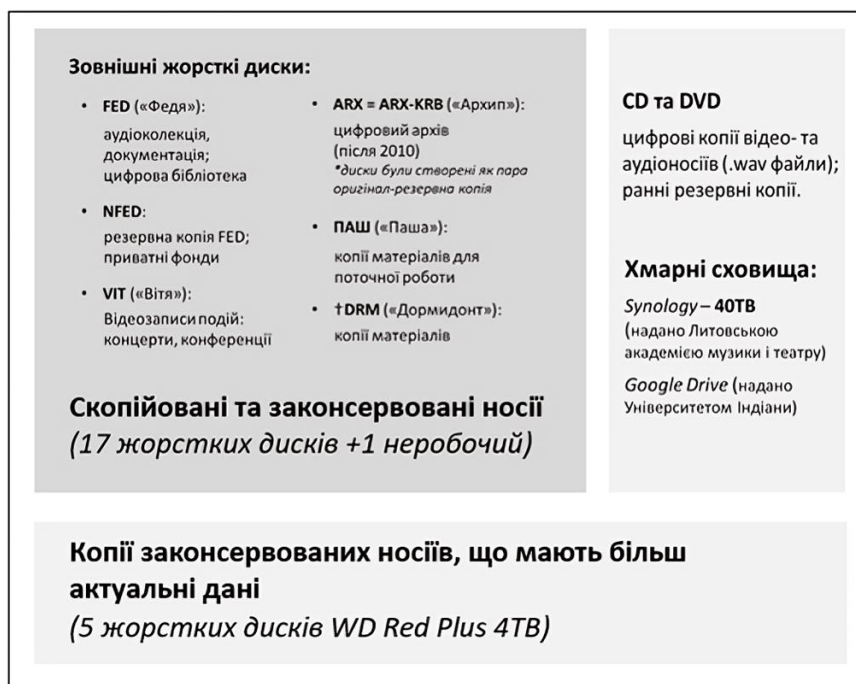
Упродовж понад 30 років діяльності ЛЕК як структурного підрозділу НМАУ («спадкоємця» Кабінету народної творчості при Київській державній консерваторії, що діяв з 1965 року), силами її співробітників було утворено одну з найбільших в Україні аудіовізуальних колекцій українського музичного фольклору. Попри неясний правовий статус матеріалів, якими оперує ЛЕК (більшість із них – приватні колекції окремих дослідників), уся колекція опрацьовується за спільною методикою, має однакові принципи впорядкування даних і метаданих.

Історичні етапи формування колекції ЛЕК описано в публікаціях її співробітників (Бут, 2004; Клименко, 2008; Данилейко, 2010; Гончаренко, 2010) та ін. Способи опрацювання архівних даних у ЛЕК не були сталими, а постійно адаптувалися до технічного прогресу, поступово наближаючись до сучасних стандартів упорядкування цифрових аудіовізуальних колекцій.

Станом на 2024 рік цифрову колекцію ЛЕК докладно описано на рівні метаданих та захищено від втра-

ти даних: існує кілька рівнів резервних копій, що зберігаються в різних місцях, а також на кількох хмарних сховищах, що забезпечує ці цифрові дані від втрати. Проте питання доступу до них, зокрема віддаленого, до недавнього часу лишалося невирішеним.

Розглянемо детальніше структуру цифрових носіїв, якими оперує ЛЕК (Ілюстрація 1). Її загальний опис подано в статті (Кропивний, 2023б). Основним блоком цифрових носіїв ЛЕК, створеним на початку формування колекції (умовні «оригінали»), є 17 робочих жорстких дисків з різним об'ємом та характеристиками, а також серія копій на CD та DVD. Наразі ці носії, скопійовані та законсервовані, зберігаються як «недоторкані». Інформацію з них протягом 2022–2024 років було скопійовано на сучасніші жорсткі диски з однаковими параметрами (WD Red Plus 4 TB), завантажено до хмарного сховища Google Drive, а також перенесено до прототипу серверної системи, що є основним об'єктом розгляду в цій статті.



Ілюстрація 1. Структура цифрових носіїв ЛЕК

«Ущільнення» цифрового фонду до меншої кількості носіїв спростило доступ до даних, проте основною проблемою все ще лишалася неможливість одночасного доступу до всіх наявних матеріалів колекції через технічні обмеження та неможливість одночасного підключення значної кількості носіїв. Віддалений доступ до колекції теж було утруднено, незважаючи на наявність копії матеріалів у хмарному сховищі Google Drive – давалися взнаки нові технічні обмеження та особливості Google Drive, не пристосованого для роботи з «важкими» аудіовізуальними матеріалами.

Вирішити більшість проблем, котрі постали перед адміністраторами й користувачами цифрової колекції ЛЕК, може проєкт серверної системи для зберігання цифрових даних, який має:

а) об'єднати наявну цифрову інформацію в одному просторі;

б) забезпечити якісне автоматичне резервне копіювання;

в) вирішити проблеми, обумовлені обмеженнями традиційних файлових систем;

г) надати можливість зручного віддаленого доступу до цифрової колекції.

Засадничі принципи збереження даних

Серед методів убезпечення цифрових даних від втрати можемо назвати:

а) резервування носіїв багатодискової системи зберігання даних, що дозволяє зберегти інформацію за виходу з ладу окремих носіїв (жорстких дисків) системи;

б) резервне копіювання даних;

в) забезпечення цілісності даних у процесі їх запису та оперування ними.

Сукупне застосування цих методів дозволяє створити комплексну систему захисту даних, що мінімізує ризики втрати інформації.

Для **резервування носіїв** (жорстких дисків=HDD) у системі зберігання даних широко застосовується технологія RAID та її аналоги, що дозволяє об'єднувати кілька дисків у єдину систему для підвищення надійності та доступності даних. У разі виходу з ладу одного чи кількох дисків залежно від конфігурації RAID (наприклад, RAID 1, RAID 5, RAID 6) дані лишаються доступними завдяки дублюванню або розподіленому зберіганню з додаванням контрольної інформації. Це забезпечує додатковий рівень захисту від втрати інформації внаслідок апаратних несправностей.

Основні конфігурації RAID:

RAID 0 (Striping). Дані розподіляються між кількома дисками для підвищення продуктивності. Підходить для тих задач, у яких швидкість роботи з даними є важливішою за їх захищеність. За виходу з ладу одного з дисків масиву вся інформація втрачається.

RAID 1 (Mirroring). Копіювання даних на два або більше дисків. Є найнадійнішою конфігурацією, проте дозволяє використовувати не більше 50% загального об'єму носіїв.

RAID 5 (Striping with Parity). Дані та їх копії розподіляються між кількома дисками (мінімум три). Дозволяє витримати найкращий баланс між швидкістю й надійністю, «витримує» збій одного диска без втрати даних.

RAID 6 (Double Parity). «Витримує» збій двох дисків із масиву без втрати даних (у масиві має бути мінімум чотири диски).

Крім цих основних конфігурацій RAID існують варіанти їх поєднання для збільшення швидкості або надійності дискового масиву, як от RAID 50, 60, 51, 61 тощо, які застосовують у разі специфічних задач.

Важливо, що RAID, хоча й значно покращує надійність зберігання даних, не є повноцінною альтернативою резервному копіюванню, а лише захищає від втрати даних у разі виходу з ладу одного чи кількох дисків (залежно від конфігурації), не забезпечуючи захисту від інших ризиків, таких як людський фактор, програмні збої, фізичні пошкодження обладнання тощо (Storage Networking Industry Association, 2006).

Ключовим інструментом захисту даних, який дозволяє відновити їх у разі збою системи, помилок користувачів чи інших несподіваних подій, є **резервне копіювання**. Для ефективної організації системи резервного копіювання особливо важливо дотримувати-

ся принципів, що забезпечують надійність, доступність і цілісність даних. Одним із варіантів організації резервного копіювання є правило 3-2-1, сформульоване фотографом Пітером Кроугом у 2009 році (Krogh, 2009). Завдяки своїй простоті та ефективності це правило стало загальноприйнятим, у тому числі рекомендується до використання Агентством з кібербезпеки та безпеки інфраструктури США (CISA) (Університет Карнегі-Меллона, 2012).

Правило 3-2-1 передбачає три основні вимоги до організації резервного копіювання:

3. **Три копії даних**. Уся інформація має складатися з основних даних та двох резервних копій. Збереження кількох копій знижує ризик втрати інформації через технічні неполадки або інші непередбачувані фактори.

2. **Два різні типи носіїв**. Резервні копії повинні зберігатися на різних типах носіїв, наприклад, жорстких дисках, твердотільних накопичувачах (SSD), оптичних носіях або ж у хмарних сховищах. Такий підхід зменшує ймовірність одночасного виходу з ладу кількох носіїв унаслідок проблем, специфічних для кожного виду носіїв.

1. **Одна копія поза основним місцем зберігання**. Одна з резервних копій повинна зберігатися в іншому фізичному або віртуальному місці, як от віддалений сервер, хмарне сховище або інше безпечне місце. Це дозволяє захистити дані від локальних катастроф, таких як пожежі, затоплення, крадіжки чи пошкодження внаслідок бойових дій чи терористичних атак.

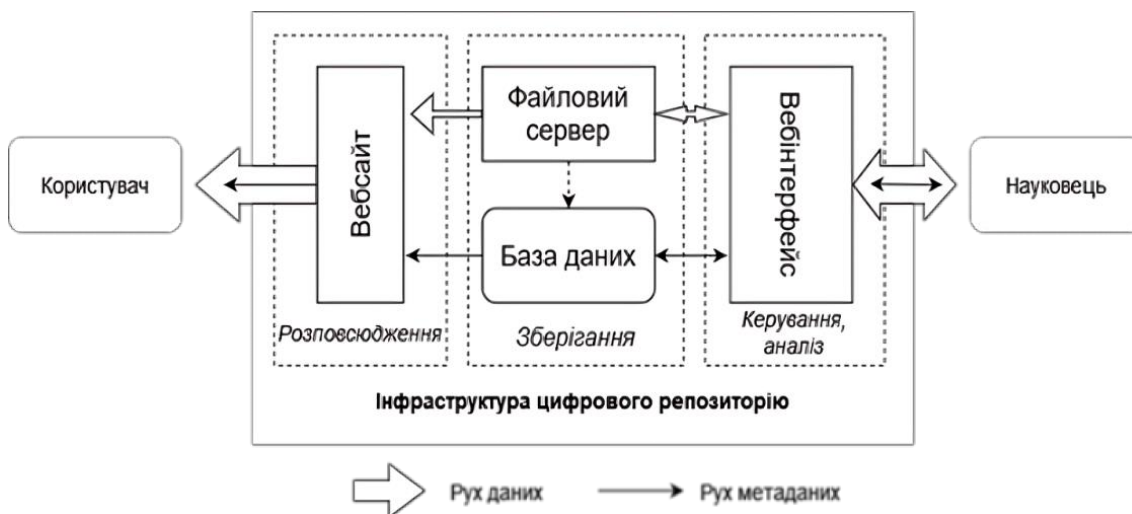
Крім резервного копіювання та резервування носіїв, одним із важливих аспектів є **забезпечення цілісності даних**. Пошкодження даних можуть статися в результаті різних факторів, таких як фізичні збої, програмні помилки або атаки шкідливого програмного забезпечення. Тому використання механізмів для забезпечення цілісності є критичним для всіх систем зберігання даних. У переліку засобів, що забезпечують цілісність даних, існують як апаратні, так і програмні рішення. Серед спеціалізованого апаратного забезпечення для підтримки цілісності даних можемо виділити ECC-пам'ять (Error-Correcting Code Memory), апаратні RAID-контролери з підтримкою контролю цілісності даних та SSD із вбудованими механізмами перевірки цілісності.

До програмних засобів забезпечення цілісності даних можемо віднести застосування сучасних файлових систем, таких як ZFS та Vtrfs, що включають в себе вбудовані механізми для забезпечення цілісності даних. Вони використовують контрольні суми для перевірки та виявлення пошкоджень даних при запису й читанні, крім того, ці файлові системи підтримують технологію *copy-on-write* (COW), що дозволяє уникати пошкоджень даних при несподіваних збоях, оскільки замість перезапису старих даних створюється їх нова копія. ZFS також має механізм самовідновлення (self-healing), що дозволяє автоматично виправляти пошкоджені дані (Oracle, 2013).

Загальна структура серверної системи

Концепція Цифрового репозиторію українського музичного фольклору (ЦР УМФ), згадувана в попередніх публікаціях автора (Кропивний, 2022, 2023а, 2023б), передбачає існування системи зберігання даних як окремої частини загальної інфраструктури цифрово-

го репозиторію (Ілюстрація 2). Окрім зазначеної основної функції власне зберігання даних ця частина системи повинна забезпечувати також і захист інформації – завдяки резервному копіюванню, захисту цілісності даних і резервуванню носіїв (система RAID).

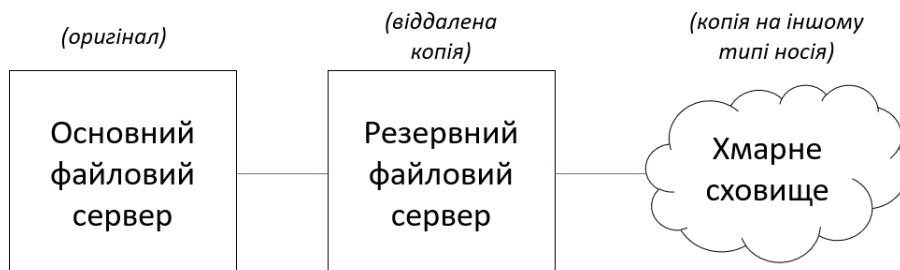


Ілюстрація 2. Інфраструктура Цифрового репозиторію українського музичного фольклору (Кропивний, 2023а).

Відповідно до принципу резервного копіювання «3-2-1» серверна система для зберігання аудіовізуальних матеріалів має складатися не менше, як із трьох елементів: основного носія, резервної копії на іншому типі носія та віддаленої резервної копії. Зважаючи на те, що ЛЕК має доступ до хмарного сховища об'ємом 40 ТБ, наданого НМАУ, можемо вважати його частиною серверної системи, що виконуватиме функцію

«копії на іншому типі носія», а також «віддаленої копії».

Основний і резервний файлові сервери повинні мати схожі параметри: їхня ємність має бути однаковою, інші ж параметри, такі як загальна продуктивність системи чи окремих жорстких дисків, у резервного сервера можуть бути нижчими, зважаючи на особливості його функціонування.



Ілюстрація 3. Спрощена схема серверної системи зберігання даних.

Основний і резервний файлові сервери мають бути розміщені в різних локаціях, максимально віддалених одна від одної задля уникнення ризику пошкодження чи відключення їх обох у результаті локальної аварії чи надзвичайної ситуації.

Кожен сервер бажано забезпечити якісним підключенням до мережі Інтернет (оптоволоконна лінія зі швидкістю до 500 мбіт/с, за відсутності такої – не

менше 100 мбіт/с, резервуванням лінії зв'язку та живлення для уникнення ризику відключення системи або її пошкодження внаслідок нестабільної роботи мереж. Результати практичних вимірів швидкості системи залежно від пропускної здатності лінії підключення до мережі Інтернет та специфічних налаштувань MTU можемо бачити на Ілюстрації 5).

Програмне забезпечення

Зважаючи на необхідність розробки масштабованої системи, яка могла б однаково добре працювати на обладнанні різних класів та з різними об'ємами інформації, особливу увагу слід приділити програмній частині проекту. Серед поставлених завдань слід виділити:

- 1) вибір операційної системи (систем);
- 2) вибір оптимальної файлової системи (систем);
- 3) вибір програмного забезпечення для організації мережевого доступу до серверів;
- 4) вибір програмного забезпечення для організації резервного копіювання.

Одним із ключових етапів розробки програмної частини проекту є *вибір операційних систем* для основного та резервного серверів. Враховуючи традиційні принципи організації схем резервного копіювання, зокрема правило «3-2-1», основний і резервний сервери мають використовувати максимально відмінне програмне забезпечення. Це дозволяє мінімізувати ризик їх одночасного виходу з ладу через програмні помилки, атаки шкідливого програмного забезпечення чи інші фактори вразливості.

Головна відмінність між функціональним призначенням основного й резервного серверів полягає у рівні їх навантаження. Основний сервер безпосередньо взаємодіє з користувачами, тому вимоги до його продуктивності, стабільності та безпеки є значно вищими ніж до резервного. Своєю чергою, резервний сервер відповідає виключно за процеси резервного копіювання, унаслідок чого його навантаження є значно меншим.

У процесі вибору програмного забезпечення, включно з операційною системою, основну увагу слід приділяти саме основному серверу. Завдання резервного сервера зводиться до роботи спеціалізованого програмного забезпечення для резервного копіювання, а також VPN-клієнта, що забезпечує доступ до віртуальної мережі основного сервера.

1. Серед багатьох *операційних систем*, доступних нині на ринку, виділимо такі:

а) системи сімейства **GNU/LINUX** – Unix-подібні операційні системи, представлені низкою дистрибутивів, серед яких найпоширенішими є Ubuntu, Debian, CentOS тощо. Основною їх перевагою є відкритий вихідний код, що сприяє широкій гнучкості, адаптації до специфічних потреб і швидкому виправленню вразливостей. Більшість таких систем є безкоштовними для користувача. Linux характеризується високим рівнем безпеки й стабільністю, що робить його особливо популярним для серверів;

б) система **Windows Server** – продукт корпорації Microsoft, орієнтований переважно на корпоративний сегмент. Серед переваг цієї системи – тісна інтеграція з іншими продуктами Microsoft. Однак Windows Server має ряд недоліків, як от високі ліцензійні витрати, підвищені вимоги до апаратного забезпечення та меншу стабільність у порівнянні з Unix-подібними системами;

в) система **FreeBSD** – Unix-подібна операційна система, яка особливо цінується за стабільність, продуктивність та безпеку. Завдяки оптимізації вона ідеально підходить для серверів, мережевого обладнання та вбудованих систем. Ліцензія BSD є однією з найгнучкіших для комерційного використання, що сприяє її популярності серед компаній, які створюють власні програмні продукти. Проте FreeBSD є менш поширеною, ніж Linux чи Windows, що обмежує доступність технічної підтримки та специфічного програмного забезпечення (Tanenbaum & Vos, 2023).

Найбільш апробованою та традиційною для високонантажених серверів операційною системою наразі вважають GNU/LINUX¹. Вона не вимагає ліцен-

зійних відрахувань, а також активно розробляється спільнотою, тому є найпридатнішою для організації файлового сервера. Вибір же конкретного дистрибутива залежатиме більше від досвіду та особистих вподобань розробників системи. Оскільки найбільш знайомими для автора є дистрибутиви на базі Debian (deb based), такі як власне Debian та Ubuntu Server, зупинимо вибір саме на них. Обидві системи є досить схожими за архітектурою та за процесами налаштування, тому може бути використана будь яка з них.

Можливим варіантом операційної системи для резервного сервера є комерційні базовані на Linux системи, що поставляються в комплекті з обладнанням (як от QTS, Synology DSM тощо), або ж уже означені системи Debian/Ubuntu.

2. Серед сучасних *файлових систем* виокремимо:

а) **NTFS (New Technology File System)** – основна файлова система для операційних систем Windows, розроблена компанією Microsoft. Особливістю NTFS є її орієнтація на системи сімейства Windows і слабка підтримка Linux. Файлова система має низку особливостей, що лімітують її використання для колекцій музичного фольклору, а її закритий код обмежує гнучкість налаштувань.

б) **Ext3/Ext4 (Third Extended File System / Fourth Extended File System)** – є стандартними файловими системами для багатьох дистрибутивів Linux. Ext4 прийшла на заміну Ext3, зберігши сумісність, але додавши нові функції. Ext4 забезпечує кращу продуктивність і ефективність роботи з великими файлами та надійність. Крім того, її особливостями є підтримка великих розмірів файлових систем (до 1 ЕБ) і швидке монтування. Серед недоліків – відсутність функції знімків файлової системи (snapshot), що є однією з найважливіших функцій для файлового сервера, а також менша гнучкість у порівнянні з більш сучасними системами, такими як *Btrfs* або *ZFS*.

в) **Btrfs (B-Tree File System)** – сучасна файлова система для Linux, орієнтована на гнучкість і управління великими обсягами даних. Вона має функції для роботи зі знімками, перевірки цілісності даних, дедуплікації тощо. Проте, Btrfs вважається менш стабільною для критичних систем порівняно з Ext4 чи ZFS, а також складна в налаштуванні та подальшій підтримці.

г) **ZFS (Zettabyte File System)** – файлова система, розроблена компанією Sun Microsystems, яку вважають однією з найдосконаліших файлових систем, особливо для серверів і сховищ даних. Поєднує в собі файлову систему і менеджер томів. Перевагами ZFS є надійність і контроль цілісності даних завдяки перевірці контрольних сум, наявність функцій знімків і клонів файлової системи, підтримка великих обсягів даних і висока продуктивність. Серед недоліків – високі вимоги до оперативної пам'яті. Важливою функцією файлової системи ZFS є підтримка RAID-Z та DRAID – аналогів RAID з покращеним управлінням пам'яттю та стійкістю до помилок. RAID-Z може бути одно-, дво- або тривірневим, що дозволяє відновлювати дані у разі виходу з ладу одного або більше дисків (Oracle, 2013).

¹ Система є домінуючою в інтернет-інфраструктурі, використовується в 70% веб серверів (Gitnux, 2024).

Відповідно до заявлених характеристик, найоптимальнішим вибором є файлова система ZFS, оскільки вона поєднує високий рівень надійності й масштабованості, має вбудовані механізми контролю цілісності даних і можливість створення знімків, що дозволяє ефективно управляти великими обсягами інформації. Окрім того, система забезпечує ефективні механізми відновлення даних, що робить її стійкою до пошкоджень, а також має вбудовану функцію резервування носіїв, аналогічну RAID.

3. Важливою умовою функціонування пропонованої серверної системи в умовах воєнного стану та нестабільності комунікацій є її *мобільність*, можливість швидкої зміни місця розташування фізичних серверів. Для реалізації такої можливості часто застосовують віртуальні приватні мережі (VPN), які дозволяють не бути прикріпленими до певної локації, а також уникнути використання спеціального підключення до мережі Інтернет (розблоковані вхідні порти, статична IP адреса тощо). Використовуючи VPN, серверна система може працювати, будучи підключеною до «побутової» лінії, наданої інтернет-провайдером і не вима-

гатиме переналаштування при підключенні до іншої лінії чи в разі зміни фізичного розташування.

Серед протоколів і програмних реалізацій VPN (як от OpenVPN, IKEv2/IPsec, L2TP/IPsec, PPTP, WireGuard тощо) найпридатнішим для застосування є протокол WireGuard – завдяки своїй «легкій» кодовій базі, найвищій швидкості з'єднання та використанню сучасних криптографічних алгоритмів. WireGuard є ефективнішим і безпечнішим порівняно з іншими протоколами (Donenfeld, 2020).

4. Для реалізації *автоматичного резервного копіювання* можливо використовувати як власноруч розроблені скрипти з використанням таких утиліт, як rsync і cron, так і готові програмні продукти, як от Bacula, Duplicity, Timeshift, Syncology тощо. Спосіб реалізації автоматичного резервного копіювання не є критично важливим для системи та може бути обраним залежно від досвіду та особистих уподобань розробників. Позаяк сценарії автоматичного резервного копіювання повинні виконуватися резервним файловим сервером, слід зважати на можливість підтримки конкретних утиліт операційною системою та апаратним забезпеченням резервного сервера.

Апаратне забезпечення

Програмне забезпечення та принципи його роботи, описані в цій публікації, можна застосовувати в системах різних рівнів – як малого приватного, так і широкомасштабного, а продуктивність та об'єм конкретного варіанту серверної системи буде визначене можливостями апаратного забезпечення.

У 2022 році київською робочою групою зі збереження архівів українського музичного фольклору було «складено варіант апаратного забезпечення, ... виходячи з того набору техніки, що був доступний на ринку на кінець 2022 року.

Основні складові та характеристики цього варіанту:

- Серверна система на базі HPE Apollo 4200 G9:
Центральний процесор: 2x E5-2680,
Оперативна пам'ять: 256GB DDR4,
Мережеві адаптери: Ethernet 1Gb 2-port RJ45 + LOM 2x 10Gbit SFP+
- Дискова система: HP Smart Array P840ar + BBU.
- Комплект жорстких дисків Seagate Exos 7E8 Enterprise (ST8000NM001A) в кількості 28 шт. загальним об'ємом 224 ТБ» (Кропивний, 2023а).

Результатом напрацювань робочої групи був гіпотетичний проєкт загальноукраїнського сховища польових фольклорних матеріалів, що могло би забезпечити потреби більшості українських інституцій та окремих дослідників, що були власниками аудіовізуальних колекцій українського фольклору. Унаслідок відсутності фінансування цей проєкт не був реалізований, а подальша робота з його розвитку була призупинена.

Прикладом реалізованого проєкту, що становить основний об'єкт дослідження в цій публікації, є серверна

система, уведена в експлуатацію в тестовому режимі протягом 2024 року в ПНДІ етномузикології НМАУ (ЛЕК). Через відсутність державного фінансування обладнання для створення системи було придбане за приватні кошти автора статті, тому для цього варіанту системи було обрано найдоступніші компоненти, які відповідали мінімальним технічним вимогам. Загальний об'єм системи було визначено на рівні ~30 ТБ. Це число було вираховано, виходячи з приблизного розміру цифрової колекції ЛЕК із додатковим резервом для нових цифрових копій, адже процес оцифрування аналогових носіїв ще не був завершений.

Для реалізації проєкту було використано таке обладнання:

- Основний файловий сервер:
QNAP TS-464-8G, RAM: 16GB, SSD: 256GB+1TB,
4x HGST Ultrastar He12 12TB
- Резервний файловий сервер:
QNAP TS-462-4G,
4x WD Red Plus 12TB

В якості хмарного сховища застосовано частину простору у хмарному сховищі Google Drive обсягом 40 ТБ, наданому НМАУ безкоштовно за програмою Google Workspace for Education (Google, н. д.).

Цей варіант реалізації системи продемонстрував свою перспективність і високу продуктивність, незважаючи на мінімальну потужність використаного апаратного забезпечення. Станом на осінь 2024 року проєкт серверної системи є готовим до повноцінного введення в експлуатацію.

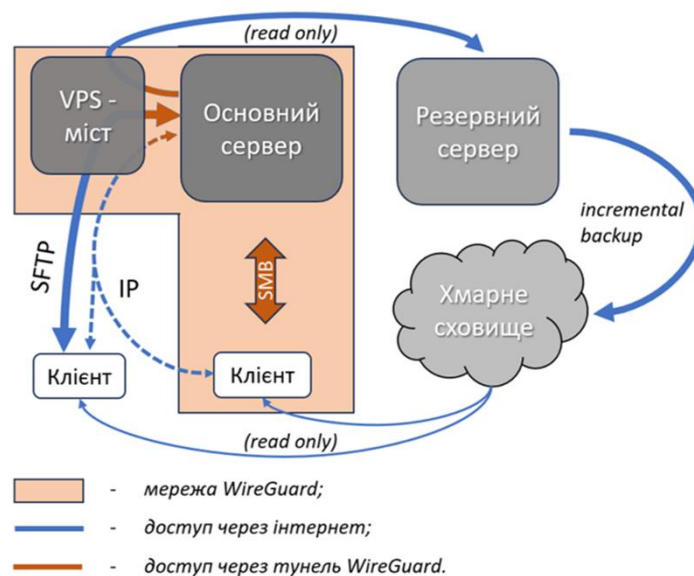
Особливості реалізації концепції

Основною користувацькою функцією є простий і швидкий віддалений доступ до сховища архівних матеріалів без необхідності розуміння будови та принципів роботи системи. Окрім цього головного завдання, при розробці та під час тестування системи основну увагу було надано таким її особливостям:

- мобільність фізичних серверів, важлива в умовах воєнного стану для їх швидкої евакуації у разі потреби;
- можливість автоматичного старту системи після збоїв / відключень без втручання користувачів або адміністратора;
- дискретність системи для зменшення ризиків втрати інформації через вихід з ладу певної частини системи або отримання несанкціонованого доступу до неї;
- використання захищених ліній зв'язку «сервер-користувач» та «сервер-сервер»;

- автоматична схема резервного копіювання, що працює без втручання користувачів та адміністратора;
- можливість створення «моментальних знімків» файлової системи як вручну, так і автоматично за розкладом для відновлення втрачених даних;
- можливість надання індивідуальних прав доступу та квот для кожного окремого користувача;
- підтримка кількох різних технологій забезпечення доступу до серверів.

Для підключення серверів через «побутову» лінію доступу до мережі Інтернет, вільного їх переміщення без переналаштування, а також для захисту трафіку можливе застосування схеми роботи через мережу VPN зі шлюзом (Ілюстрація 4); тоді з'являється потреба у ще одному елементі системи – VPS сервері, що має статичні основну та резервну IP адреси, а також функціонує в умовах дата-центру.



Ілюстрація 4. Інфраструктурна схема серверної системи.

VPS-шлюз (Virtual Private Server) є центральним елементом запропонованої мережевої архітектури. Завдяки наявності кількох статичних IP-адрес, VPS функціонує як основний сервер для мережі VPN на базі WireGuard, через який забезпечується взаємозв'язок усіх інших компонентів системи. VPS виконує роль шлюзу (мосту), який гарантує зв'язок між клієнтами, основним сервером і резервним сервером. Додатково VPS може використовувати свою резервну IP-адресу (floating IP) для перенаправлення трафіку від клієнтів до основного сервера.

Основний сервер – головне місце зберігання даних, що є частиною мережі WireGuard, підключеною до VPS для забезпечення шифрованого з'єднання з клієнтами та резервним сервером. Основний сервер дозволяє клієнтам здійснювати доступ до розміщеної на ньому інформації через протокол SMB через VPN-з'єднання або через SFTP у разі підключення поза VPN за резервною IP адресою VPS-шлюзу.

Крім забезпечення доступу користувачів основний сервер також надає доступ до своїх даних для резервного сервера в режимі read-only (лише для читання). Це

означає, що резервний сервер може отримувати дані для резервного копіювання, але не має права змінювати чи видаляти інформацію на основному сервері.

Резервний сервер відіграє ключову роль у створенні й зберіганні резервних копій. Він підключається до основного сервера і отримує інформацію лише в режимі read-only для гарантування цілісності даних на основному сервері. Також резервний сервер має повний доступ до хмарного сховища, що дозволяє йому виконувати операції з «хмарними» резервними копіями (зберігання, оновлення, видалення). За допомогою автоматичних скриптів сервер без втручання людини інкрементно¹ оновлює обидві резервні копії – як власну, так і хмарну. Резервний сервер залишається невідомим для користувачів, що слугує додатковим ступенем захисту інформації від умисного пошкодження чи знищення.

Хмарне сховище використовується для зберігання на іншому типі носія віддалених резервних копій, отри-

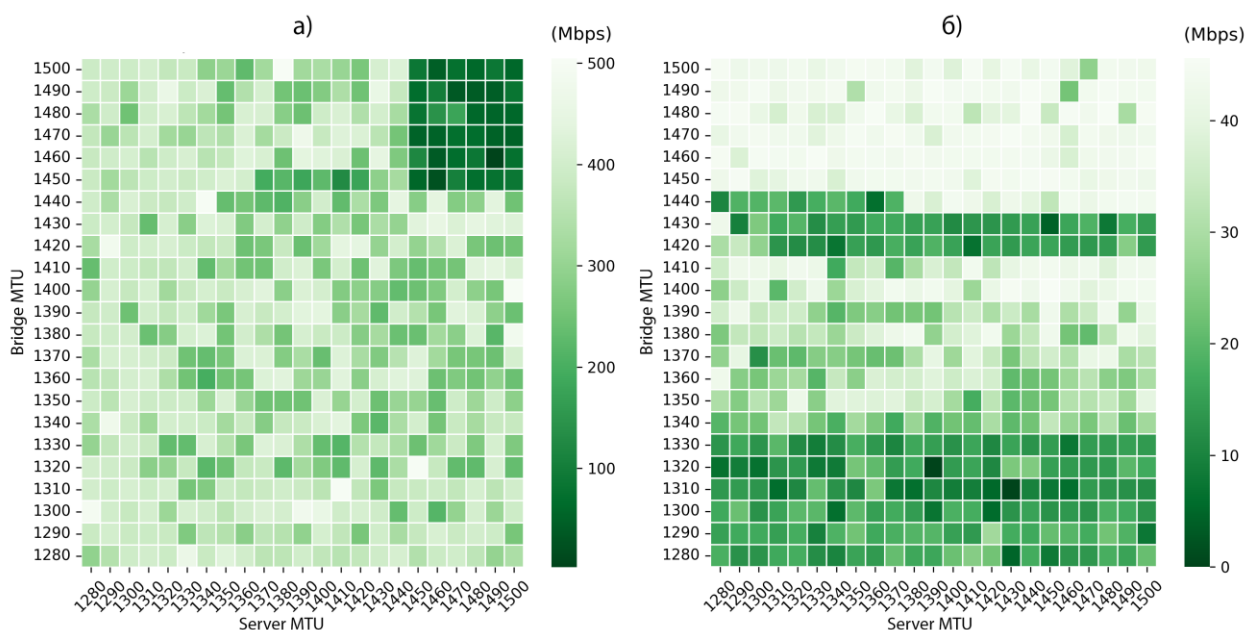
¹ Інкрементне резервне копіювання – метод, завдяки якому копіюється лише та інформація, що змінилася після останнього резервного копіювання.

маних з резервного сервера. Клієнти також можуть мати read-only доступ до хмарного сховища, що дозволяє їм лише переглядати або завантажувати інформацію чи надавати до неї такий доступ стороннім особам, але не вносити зміни до резервних копій. Можливість змінювати, оновлювати чи видаляти інформацію в хмарному сховищі має лише резервний сервер.

Результатом подібної інфраструктурної схеми є **дискретність системи**, яка унеможливує втрату даних унаслідок компрометації одного з її елементів, оскільки жоден окремих елемент не має прямого дос-

тупу до обох інших одночасно. На рівні ж основного сервера максимально знижується ризик втрати інформації через людський фактор (оскільки можливе її відновлення за допомогою функції моментальних знімків файлової системи ZFS) чи вихід із ладу носія інформації (резервування RAIDZ).

Основним *недоліком* цієї схеми є дещо знижена швидкість роботи порівняно з більш традиційними рішеннями, проте за умов високошвидкісного підключення до мережі Інтернет та тонкого налаштування мережі, цей недолік не є суттєвим (ілюстрація 5).



Ілюстрація 5. Швидкість доступу до основного сервера залежно від ширини його лінії підключення та значень MTU: а) лінія 600 Mbit/s; б) лінія 50 Mbit/s.

Висновки. Перспективи

У статті представлено докладний план реалізації проекту серверної системи, призначеної для зберігання аудіовізуальних колекцій українського музичного фольклору. Наразі описано та апробовано найпростіший варіант утілення запропонованої концепції у межах, достатніх для колекції певного закладу. Утім, система має перспективи для розширення, оскільки її програмна частина та загальні принципи функціону-

вання є універсальними та можуть бути застосовані у зв'язці з апаратним забезпеченням будь-якого рівня й уміщувати фактично будь-який об'єм інформації.

Саме можливість масштабування проекту дозволяє використовувати його і як систему зберігання невеликого обсягу даних окремого дослідника чи інституції, так і як частину масштабного цифрового репозитору – регіонального чи навіть загальноукраїнського.

Цитована література

- Барышнікау, Я. (2022). *Практичне прямианенне прадукту Kobo Toolbox для збору і захоування палявых фольклорных матэрыялаў*. Доповідь на семінарі робочої групи з захисту фондів українського фольклору. Отримано 23 листопада 2024 р. з <https://lek.media/files/bar.mp4>
- Бут, О. (2004). Комп'ютерні технології в музичній фольклористиці: методичні рекомендації. *Проблеми етномузикології*, 2, 328–337. Київ.
- Вовчак, А. (2022а). *З досвіду архівної організації польових фольклорних фіксацій*. Доповідь на семінарі робочої групи з захисту фондів українського фольклору. Отримано 23 листопада 2024 р. з <https://lek.media/files/vov.mp4>
- Вовчак, А. (2022б). Українсько-американський проєкт резервного копіювання фольклорних архівних документів. *Етномузика*, 18, 192–205. Львів.
- Вовчак, А., & Довгалюк, І. (2024). *Фольклористична практика. Засади підготовки і проведення фольклористичного польового дослідження, упорядкування, транскрибування й архівування зібраного фольклорного матеріалу: Навчально-методичний посібник*. Львів: ГАЛИЧ-ПРЕС. 240 с.
- Гончаренко, К. (2010). *База даних звукозаписів українського музичного фольклору: розробка параметрів опису та створення концепційної моделі (за матеріалами фонотеки аудіопублікацій ПНДЛ музичної етнографії при НМАУ)*. (Магістерська робота). Національна музична академія України ім. П. І. Чайковського: Кафедра музичної фольклористики. Київ. 111 с.
- Данилейко, І. (2010). Аудіофонд Київської лабораторії етномузикології: польові записи 2004–2010 років. *Проблеми етномузикології*, 5, 232–241 +карта К48. Київ.

- Клименко, І. (2008). Аудіофонд українського фольклору, 1982–2008: Засади устрою і перспективи електронної архівації. *Проблеми етномузикології*, 3, 53–105. Київ: НМАУ ім. П. І. Чайковського.
- Кропивний, О. (2022). Цифровий репозиторій українського музичного фольклору: передумови створення, шляхи реалізації концепту, загальні особливості структури. *Проблеми етномузикології*, 17, 79–87. <https://doi.org/10.31318/2522-4212.2022.17.270908>
- Кропивний, О. (2023а). На шляху формування цифрових архівів (репозиторіїв) музичного фольклору в Україні (розробка інфраструктури робочого середовища). *Музикознавча думка Дніпропетровщини*, 24, 229–247. <https://doi.org/10.33287/222313>
- Кропивний, О. (2023б). Від ієрархічної моделі даних до цифрового репозиторію: Перехідний етап упорядкування колекції українського музичного фольклору Київської лабораторії етномузикології. *Етномузіка*, 19 (1), 143–159. Львів. <https://doi.org/10.33398/2523-4846-2023-19-1-143-159>
- Маханець, О. (2022). *Керування та впорядкування цифрових архівів: досвід роботи з Collective Access*. Доповідь на семінарі робочої групи з захисту фондів українського фольклору. Отримано 23 листопада 2024 р. з <https://lek.media/files/mah.mp4>
- Canadian Institute of Ukrainian Studies. (2022, 11 березня). Ukraine Archives Rescue Team. University of Alberta. Отримано 23 листопада 2024 р. з <https://www.ualberta.ca/en/canadian-institute-of-ukrainian-studies/publications-and-resources/ukraine-archives-rescue-team.html>
- Carnegie Mellon University. (2012). *Data backup options*. Produced for US-CERT, a government organization. Отримано 23 листопада 2024 р. з https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf
- Donenfeld, J. A. (2020). *WireGuard: Next generation kernel network tunnel*. Отримано 23 листопада 2024 р. з <https://www.wireguard.com/papers/wireguard.pdf>
- Gitnux. (2024). *Linux statistics: Usage and market share in 2024*. Отримано 23 листопада 2024 р. з <https://gitnux.org/linux-statistics/>
- Google. (н.д.). *Education Fundamentals*. Google for Education. Отримано 23 листопада 2024 р. з <https://edu.google.com/workspace-for-education/editions/education-fundamentals/>
- Krogh, P. (2009). *The DAM book: Digital asset management for photographers* (2nd ed., p. 207). O'Reilly Media.
- Oracle. (2013). *Oracle® Solaris ZFS Administration Guide*. Отримано 23 листопада 2024 р. з https://docs.oracle.com/cd/E26505_01/pdf/E37384.pdf
- RISM Editorial Team. (2022, 22 березня). Rescuing music data: Saving Ukrainian cultural heritage online (SUCHO). RISM. Отримано 23 листопада 2024 р. з https://rism.info/electronic_resources/2022/03/22/rescuing-music-data-saving-ukrainian-cultural-heritage-online-sucho.html
- Storage Networking Industry Association. (2006). Common RAID Disk Data Format Specification Version 1.2. Storage Networking Industry Association. Отримано 23 листопада 2024 р. з <https://www.snia.org/sites/default/files/SNIA-DDFv1.2.pdf>
- Tanenbaum, A. S., & Bos, H. (2023). *Modern operating systems: Global edition* (5-те вид., с. 1185). Pearson.

References

- Baryshnikau, Ya. (2022). Praktychnaye prymyanenne praduhtu Kobo Toolbox dlya zboru i zakhovannya palyavykh falklornykh materyyalau [Practical Application of the Kobo Toolbox Product for Collecting and Storing Field Folklore Materials]. Presentation at the Seminar of the Working Group on the Protection of Ukrainian Folklore Collections. Retrieved November, 23, 2024 from <https://lek.media/files/bar.mp4> [in Belarusian].
- But, O. (2004). Kompiuterni tekhnolohii v muzychnii folklorystytsi: metodychni rekomendatsii [Computer Technologies in Music Folkloristics: Methodical Recommendations]. *Problemy etnomuzykolohii [Problems of Music Ethnology]*. Iss. 2, 328–337. Kyiv. [in Ukrainian].
- Canadian Institute of Ukrainian Studies. (2022, March 11). *Ukraine Archives Rescue Team*. University of Alberta. Retrieved November, 23, 2024 from <https://www.ualberta.ca/en/canadian-institute-of-ukrainian-studies/publications-and-resources/ukraine-archives-rescue-team.html> [in English].
- Carnegie Mellon University. (2012). *Data backup options*. Produced for US-CERT, a government organization. Retrieved November, 23, 2024 from https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf [in English].
- Danyleiko, I. (2010). Audiofond Kyivskoi laboratorii etnomuzykolohii: polovi zapysy 2004–2010 rokiv [Kyiv ethnomusic laboratory audio fund: field records of 2004–2010s]. *Problemy etnomuzykolohii [Problems of Music Ethnology]*. Iss. 5, 232–241 +map K48. Kyiv. [in Ukrainian].
- Donenfeld, J. A. (2020). *WireGuard: Next generation kernel network tunnel*. Retrieved November, 23, 2024 from <https://www.wireguard.com/papers/wireguard.pdf> [in English].
- Gitnux. (2024). *Linux statistics: Usage and market share in 2024*. Retrieved November, 23, 2024 from <https://gitnux.org/linux-statistics/> [in English].
- Google. (n.d.). *Education Fundamentals*. Google for Education. Retrieved November, 23, 2024 from <https://edu.google.com/workspace-for-education/editions/education-fundamentals/> [in English].
- Honcharenko, K. (2010). *Baza danykh zvukozapysiv ukrainskoho muzychnoho folkloru: rozrobka parametriv opysu ta stvorennia kontseptsii noi modeli (za materialamy fonoteky audiopublikatsii PNDL muzychnoi etnohrafii pry NMAU) [The Database of Ukrainian Musical Folklore Sound Recordings: Development of Description Parameters and Creation of the Conceptual Model (Based on the Materials of the Audio Library of Audio Publications of the Problematic Scientific Research Laboratory of Music Ethnology)]*. (Master's degree). Tchaikovsky National Music Academy of Ukraine: Department of Musical Folklore. Kyiv. 111 p. [in Ukrainian].
- Klymenko, I. (2008). Audiofond ukrainskoho folkloru, 1982–2008: Zasady ustroiu i perspektyvy elektronnoi arkhivatsii [Audio Fund of Ukrainian Folklore, 1982–2008: Principles of Organization and perspectives of Electronic Archiving]. *Problemy etnomuzykolohii [Problems of Music Ethnology]*. Iss. 3, 53–105. Kyiv. [in Ukrainian].
- Krogh, P. (2009). *The DAM book: Digital asset management for photographers* (2nd ed., p. 207). O'Reilly Media. [in English].
- Kropyvnyi, O. (2022). Tsyfrovy repozytorii ukrains'koho muzychnoho folkloru: peredumovy stvorennia, shlyakhy realizatsii kontseptsii, zahal'ni osoblyvosti [Digital repository of ukrainian musical folklore: prerequisites for creation, implementation

- paths of the concept, general features]. *Problemy etnomuzykologii* [Problems of Music Ethnology]. Iss. 17, 79–87. Kyiv. DOI: <https://doi.org/10.33287/222313> [in Ukrainian].
- Kropyvnyi, O. (2023a). Na shliakhu formuvannia tsyfrovyykh arkhiviv (repozytoriiv) muzychnoho folkloru v Ukraini (rozrobka infrastruktury robochoho seredovyscha) [Towards the establishment of digital musical folklore archives (repositories) in Ukraine (development of the workspace infrastructure)]. *Muzykoznavcha dumka Dnipropetrovshchyny* [Musicological Thought of Dnipropetrovsk region]. Iss. 24, 229–247. DOI: <https://doi.org/10.33287/222313> [in Ukrainian].
- Kropyvnyi, O. (2023b). Vid hierarchichnoi modeli danykh do tsyfrovoho repozytoriiu: Perekhidnyi etap uporiadkuvannia kolektsii ukrainskoho muzychnoho folkloru Kyivskoi laboratorii etnomuzykologii [Hierarchical Data Model to Digital Repository: Transition Stage in Organizing the Ukrainian Musical Folklore Collection of the Kyiv Laboratory of Ethnomusicology]. *Etnomuzyka* [Ethnomusic]. Iss. 19(1), 143–159. Lviv. DOI: <https://doi.org/10.33398/2523-4846-2023-19-1-143-159> [in Ukrainian].
- Makhanets, O. (2022). *Keruvannia ta vporiadkuvannia tsyfrovyykh arkhiviv: dosvid roboty z Collective Access* [Management and Organization of Digital Archives: Experience with Collective Access]. Presentation at the Seminar of the Working Group on the Protection of Ukrainian Folklore Collections. Retrieved November, 23, 2024 from <https://lek.media/files/mah.mp4> [in Ukrainian].
- Oracle. (2013). *Oracle® Solaris ZFS Administration Guide*. Retrieved November, 23, 2024 from https://docs.oracle.com/cd/E26505_01/pdf/E37384.pdf [in English].
- RISM Editorial Team. (2022, March 22). *Rescuing music data: Saving Ukrainian cultural heritage online (SUCHO)*. RISM. Retrieved November, 23, 2024 from https://rism.info/electronic_resources/2022/03/22/rescuing-music-data-saving-ukrainian-cultural-heritage-online-sucho.html [in English].
- Storage Networking Industry Association. (2006). Common RAID Disk Data Format Specification Version 1.2. Storage Networking Industry Association. Retrieved November, 23, 2024 from <https://www.snia.org/sites/default/files/SNIA-DDFv1.2.pdf> [in English].
- Tanenbaum, A. S., & Bos, H. (2023). *Modern operating systems: Global edition* (5th ed.). Pearson. 1185 p. [in English].
- Vovchak, A. (2022a). *Z dosvidu arkhivnoi orhanizatsii polovyykh folklornykh fiksatsii* [Experience in archival organization of field folklore recordings]. Presentation at the Seminar of the Working Group on the Protection of Ukrainian Folklore Collections. Retrieved November, 23, 2024 from <https://lek.media/files/vov.mp4> [in Ukrainian].
- Vovchak, A. (2022b). Ukrainsko-amerykanskiy proekt rezervnoho kopiuvannia folklornykh arkhivnykh dokumentiv [Ukrainian-American Project of Backup for Folklore Archival Documents]. *Etnomuzyka* [Ethnomusic]. Iss. 18, 192–205. [in Ukrainian].
- Vovchak, A., & Dovhalyuk, I. (2024). *Folklorystychna praktyka. Zasady pidhotovky i provedennia folklorystychnoho polovoho doslidzhennia, uporiadkuvannia, transkrybuвання y arkhivuvannia zibranoho folklornoho materialu: Navchalno-metodychnyi posibnyk* [Folkloristic Practice: Principles of Preparing and Conducting Folklore Field Research, Organizing, Transcribing, and Archiving Collected Folklore Material: A Teaching and Methodological Guide]. Lviv: HALYCH-PRES. 240 p. [in Ukrainian].

Oleksandr Kropyvnyi

ORCID: <https://orcid.org/0000-0001-7601-7878>

PhD student, Department of Ukrainian Music History and Music Folk Studies
Ukrainian National Tchaikovsky Academy Of Music
Architect Horodetskyi St., 1-3/11, 01001 Kyiv, Ukraine
Tel.: +38 050 7717182; e-mail: ok@accordion.in.ua

AUDIOVISUAL COLLECTIONS OF MUSICAL FOLKLORE IN WARTIME: A PROJECT OF SERVER INFRASTRUCTURE FOR DIGITAL DATA STORAGE

The article presents the experience of developing and implementing a server infrastructure for storing digital audiovisual collections of Ukrainian musical folklore. Particular attention is given to the technical aspects of preservation, backup, and ensuring data accessibility during wartime. The proposed system is based on a mobile architecture that enables quick relocation and recovery of servers without administrator intervention.

The implementation of the system relies on the use of the ZFS file system to ensure data reliability and integrity, as well as RAIDZ technology to protect against hardware failures. A key role is played by the application of the 3-2-1 backup principle, which involves creating multiple copies of data on different storage media, including in the cloud environment. For remote data access, the WireGuard protocol is used, providing secure VPN connections between users and servers.

The proposed server infrastructure addresses key challenges faced by Ukrainian ethnomusicologists and cultural institutions in working with digital archives: storing large volumes of audiovisual data, organizing automated backups, and enabling prompt access to collections. A distinctive feature of the system is its scalability, allowing it to be used both locally and as part of a nationwide digital repository.

The proposed approaches were tested using materials from the Laboratory of Ethnomusicology at the National Music Academy and private recordings of its staff. Practical results demonstrate the effectiveness of the developed infrastructure in preserving cultural heritage, especially under the devastating threats posed by war.

Keywords: Ukrainian musical folklore, ethnomusicology, The Laboratory of Ethnomusicology (Kyiv), repository, archiving, digital archive, server infrastructure, network storage