КОМП'ЮТЕРНІ НАУКИ

DOI https://doi.org/10.32782/2078-0877-2026-26-1-5
УДК 004.7:004.056

І. О. Воробйов, аспірант ORCID: 0009-0008-4097-5386
Д. В. Великодний, ст. викл. ORCID: 0000-0003-0044-5619
Сумський державний університет
e-mail: ivabyov@gmail.com

МЕТОДИ ПІДВИЩЕННЯ НАДІЙНОСТІ Й ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ ДО ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Анотація. У статті розглянуто комплекс методів підвищення надійності й інформаційної безпеки (ІБ) системи віддаленого доступу до телекомунікаційного обладнання для навчальних лабораторій. Сформовано модель загроз багатокористувацького середовища та визначено критичні вразливості доступності, ізоляції й керування доступом. Запропоновано резервування ключових сервісів і мережевих шляхів, балансування навантаження та self-healing контейнерних компонентів із централізованим моніторингом і журналюванням. Для зниження ризиків несанкціонованого доступу обґрунтовано використання TLS-шифрування, RBAC/MFA й сегментації мережі. Ефективність підходу підтверджено порівняльною оцінкою базової й удосконаленої системи за показниками часу відновлення, ізоляції користувачів і керованості інфраструктури.

Ключові слова: віддалений доступ, телекомунікаційне обладнання, надійність, інформаційна безпека, контейнеризація, RBAC, MFA, TLS, сегментація мережі, журналювання.

Постановка проблеми. Системи віддаленого доступу до телекомунікаційного лабораторного обладнання активно впроваджується в закладах вищої освіти, оскільки дає змогу забезпечити гнучкий, масштабований та індивідуально орієнтований доступ студентів до реальних мережевих стендів. Проте разом із перевагами віддалений доступ супроводжується низкою технічних та організаційних обмежень, що впливають на надійність і безпеку роботи таких систем.

Попри широке застосування віртуалізації, контейнеризації та хмарних технологій, значна частина чинних рішень орієнтована переважно на функціональність і зручність використання, тоді як питання відмовостійкості й інформаційної безпеки розглядаються фрагментарно. У більшості віддалених лабораторій відсутні цілісні механізми резервування критичних компонентів, автоматизованого відновлення працездатності й контролю цілісності конфігурацій обладнання. У разі збою окремого сервісу або серверного вузла функціонування системи може бути повністю або частково зупинене, що унеможливлює проведення лабораторних занять і доступ до інфраструктури.

Також значною проблемою залишається ідентифікація та автентифікація користувачів. Часто використовуються застарілі або недостатньо безпечні механізми авторизації, що створює ризики несанкціонованого доступу до лабораторних ресурсів. Крім того, недостатня ізоляція користувацьких сесій може призводити до конфліктів конфігурацій, порушення роботи стендів і небажаного впливу одних користувачів на інших. Окремі дослідження відзначають, що системи управління віддаленими лабораторіями вразливі до атак типу «людина посередині», підбору облікових даних, перевантаження сервісів і спроб втручання в мережеву топо-

логію. Брак інтегрованого моніторингу, журналювання дій користувачів та оперативного аналізу подій безпеки значно ускладнює виявлення інцидентів і реагування на них.

Аналіз останніх досліджень. Питання розроблення інфраструктур для віддаленого доступу до лабораторних ресурсів активно досліджуються у світовій науковій спільноті, особливо в контексті дистанційного навчання, хмарних технологій і віртуалізації. У роботах, присвячених управлінню віддаленими лабораторіями, акцент робиться на архітектурі систем, продуктивності сервісів, а також на безпечній взаємодії користувачів із реальним обладнанням. У публікації Safety and Security Considerations for Online Laboratory Management Systems автори підкреслюють, що більшість наявних платформ віддаленого доступу потребують удосконалення механізмів контролю доступу, шифрування трафіку й ізоляції робочих середовищ. Зазначається, що безпека таких систем має розглядатися комплексно – від моделювання загроз і захисту каналів передачі даних до аудиту дій користувачів і моніторингу аномалій [1].

Дослідники в роботі Remote Labs in Cybersecurity Education: Analyzing Requirements and Challenges звертають увагу на те, що віддалені лабораторії, особливо у сфері інформаційної безпеки, стикаються з проблемою масштабування та підтримання стабільної роботи при збільшенні кількості одночасних користувачів. Також визначено, що суттєвими є питання відмовостійкості, оскільки збої в роботі сервісів прямо порушують навчальний процес [2].

У ґрунтовному огляді Survey of Remotely Controlled Laboratories for Research and Education аналізується широкий спектр рішень, що використовуються в навчальних і дослідницьких лабораторіях. Автори виділяють тенденцію переходу від монолітних систем до гнучких модульних архітектур, які включають віртуалізацію, контейнеризацію та хмарні сервіси. При цьому звертається увага на значні відмінності між платформами щодо рівня безпеки, способів керування доступом і підтримки інцидент-менеджменту [3].

У роботі Remote Laboratory for Computer Networks розглядається практична реалізація лабораторії мережевого обладнання з використанням консольного доступу (SSH, telnet) і базових механізмів авторизації. Автори підкреслюють, що такі рішення мають низку обмежень, зокрема недостатню гнучкість і відсутність механізмів ізоляції користувацьких конфігурацій, що впливає на надійність роботи стенду [4].

Аналіз корпоративних рішень у сфері безпечного віддаленого доступу, представлений у роботі. Дослідження безпечних методів і засобів віддаленого доступу в корпоративному сегменті демонструє, що використання багатофакторної автентифікації, тунелювання трафіку та централізованого журналювання є базовими вимогами до сучасних систем. Водночас автори зазначають, що навіть у комерційному секторі недостатньо уваги приділяється аспектам відмовостійкості й автоматизованому відновленню роботи сервісів після збоїв [5].

Узагальнюючи результати наведених досліджень, можна зробити висновок, що більшість робіт детально розглядають питання організації віддаленого доступу, але приділяють обмежену увагу комплексному поєднанню надійності й інформаційної безпеки; існує значний розрив між академічними рекомендаціями та реальними інструментами, що застосовуються в навчальних лабораторіях; практично відсутні системи, що інтегрують контейнеризацію, автоматизоване резервування, моніторинг інцидентів і багаторівневий захист у єдину платформу.

Це підкреслює актуальність розроблення методів, спрямованих на створення комплексної відмовостійкої та захищеної інфраструктури для віддаленого доступу до телекомунікаційного обладнання, саме на цьому й зосереджено дослідження.

Формулювання мети статті (постановка завдання). Метою роботи є обґрунтування комплексу методів підвищення надійності й інформаційної безпеки системи віддаленого доступу до телекомунікаційного обладнання з урахуванням контейнеризації та хмарної інфраструктури. Для досягнення мети поставлено такі завдання:

• визначити основні загрози та вразливості систем віддаленого доступу;
• сформувати вимоги до відмовостійкої архітектури (резервування, балансування, self-healing, моніторинг);
• запропонувати методи інформаційної безпеки (далі – ІБ) (RBAC/MFA, TLS, сегментація, аудит);
• розробити інтегровану модель поєднання відмовостійкості й інформаційної безпеки;
• оцінити ефективність підходу за ключовими показниками (доступність, час відновлення, керованість, стійкість до атак).

Основна частина. Основний матеріал зосереджений на формуванні узгодженого набору методів підвищення надійності й інформаційної безпеки системи віддаленого доступу до телекомунікаційного обладнання. Методи згруповано за напрямами: відмовостійкість (резервування, балансування, self-healing, моніторинг) і кіберзахист (шифрування, контроль доступу, сегментація, аудит).

Інформаційна безпека системи базується на застосуванні контролю доступу, шифруванні каналів зв'язку, сегментації мережі й аудиту дій користувачів відповідно до рекомендацій сучасних стандартів інформаційної безпеки [10].

Архітектура системи віддаленого доступу до телекомунікаційного обладнання має забезпечувати поєднання трьох ключових властивостей: стабільності роботи, захищеності каналів взаємодії та можливості масштабування. Сучасні підходи базуються на використанні мікросервісної моделі, контейнеризації та сегментації мережі, що дає змогу розподілити окремі функціональні модулі та мінімізувати вплив збоїв на загальну роботу платформи (рис. 1).

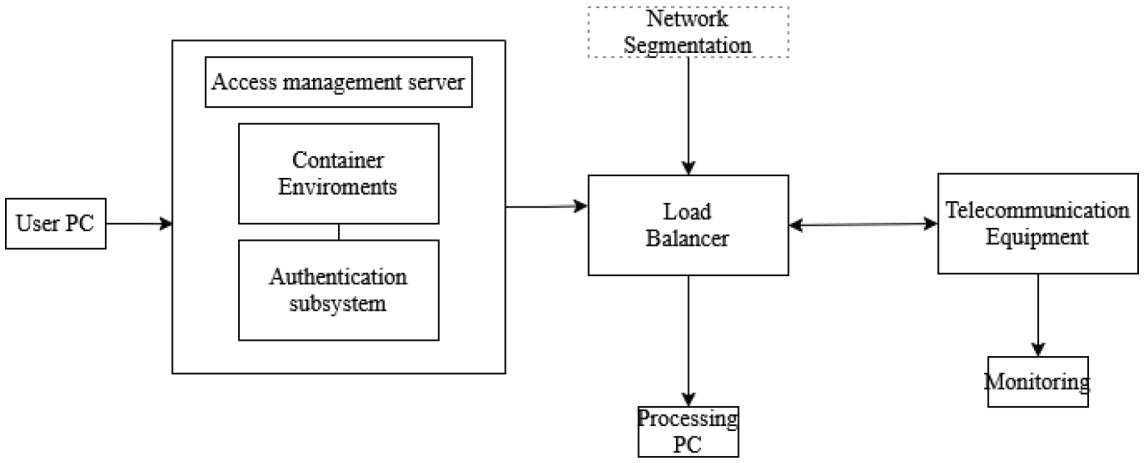

Рис. 1. Узагальнена архітектура системи віддаленого доступу до телекомунікаційного обладнання

Типова архітектура включає такі компоненти:

1. Сервер керування доступом. Відповідає за маршрутизацію підключень, управління сесіями та взаємодію з лабораторним обладнанням; доцільним є поділ на окремі сервіси (API, маршрутизація, керування сесіями).

2. Підсистема автентифікації та авторизації. Забезпечує перевірку облікових даних і розмежування прав доступу з використанням RBAC/ABAC; рекомендовано застосовувати MFA й сучасні протоколи (OAuth 2.0 тощо).

3. Система контейнеризації. Надає ізольовані робочі середовища для користувачів (Docker/аналог), що зменшує взаємний вплив сесій і підвищує відтворюваність експериментів.

4. Мережева інфраструктура лабораторії. Охоплює маршрутизатори, комутатори, міжмережеві екрани й інше телекомунікаційне обладнання; доступ організовується через захищені канали.

5. Моніторинг і журналювання. Відстежує стан сервісів і ресурсів, фіксує події доступу та дії користувачів; дані використовуються для реагування на інциденти й підтримки стабільності.

Ключовим елементом такої архітектури є ізоляція компонентів, що зменшує площу можливих вразливостей і полегшує оновлення програмних модулів [8]. Завдяки контейнеризації система може працювати в розподіленому середовищі, а збільшення кількості користувачів компенсується горизонтальним масштабуванням окремих вузлів.

Важливим аспектом архітектури є наявність захищених каналів зв'язку між серверами й обладнанням. Застосування шифрування, сегментації мережі та політик доступу дає змогу зменшити ризики несанкціонованого втручання й перехоплення даних [7]. Архітектура має включати також резервні компоненти, що забезпечують безперервність роботи платформи навіть у разі часткової відмови обладнання.

Модель загроз для системи віддаленого доступу до телекомунікаційного обладнання формується на основі аналізу типових ризиків, притаманних розподіленим сервісам, мережевим інфраструктурам і платформам із багатокористувацьким режимом роботи. Особливість таких систем полягає в тому, що вони поєднують програмні компоненти, канали передачі даних і реальне мережеве обладнання, яке безпосередньо реагує на некоректні команди або несанкціоноване втручання [6] (рис. 2).

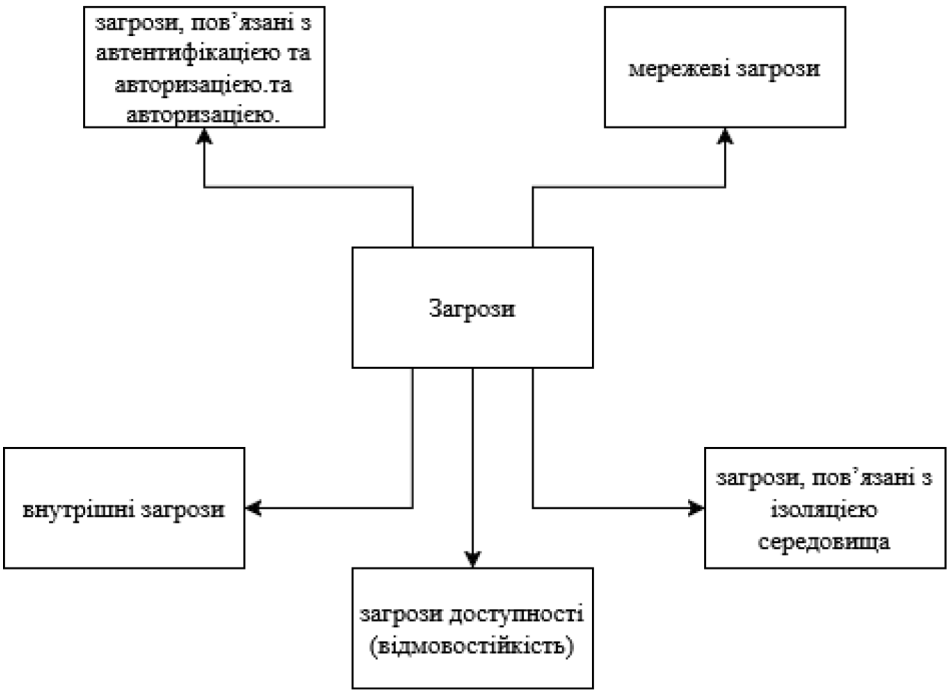

Рис. 2. Узагальнена модель загроз для системи віддаленого доступу

Основні групи загроз включають таке:

1. Загрози, пов'язані з автентифікацією та авторизацією. Атаки на облікові дані, повторне використання сесій і несанкціоноване підвищення привілеїв; знижується шляхом MFA та коректної політики прав доступу [9].

2. Мережеві загрози. Перехоплення трафіку, модифікація команд, атаки типу «людина посередині», сканування інфраструктури; критичною є наявність шифрування й сегментації мережі.

3. Загрози, пов'язані з ізоляцією середовища. Недостатня ізоляція контейнерів/сесій або помилки конфігурації можуть вплинути на інших користувачів чи змінити стан реального обладнання.

4. Загрози доступності (відмовостійкість). Перевантаження, відмови вузлів, збої сервісів і мережевого обладнання; потребує резервування й автоматичного відновлення.

5. Внутрішні загрози. Дії авторизованих користувачів (навмисні або помилкові), що порушують роботу стендів; важливі аудит і журналювання.

Ключові вразливості системи включають: використання застарілих протоколів доступу (telnet, небезпечний SSH-конфіг); недостатньо захищені API або відкриті порти; некоректно налаштовані політики доступу до обладнання й контейнерів; відсутність моніторингу стану сервісів і журналювання дій користувачів; залежність від одного вузла або сервера без резервування.

Сформована модель загроз є підґрунтям для вибору механізмів захисту й відмовостійкості, які зменшують вплив кожної з визначених груп ризиків і підтримують стабільну роботу платформи.

Забезпечення надійності системи віддаленого доступу є ключовою умовою її ефективного функціонування, оскільки відмова будь-якого критичного компонента може призвести до зупинки навчального процесу або втрати доступу до лабораторного обладнання. Методи підвищення надійності мають охоплювати апаратний, мережевий і програмний рівні, а також механізми оперативного реагування на збої.

Резервування серверів автентифікації, вузлів керування доступом і контейнерних середовищ дає змогу підтримувати роботу платформи навіть у разі відмови одного з елементів. Для цього застосовують такі підходи: Active-Active – одночасна робота двох або більше серверів з балансуванням навантаження між ними; Active-Standby – дублювальний сервер переходить у робочий стан у разі відмови основного; Резервування мережевих шляхів – використання альтернативних каналів зв'язку між вузлами.

Системи, що обслуговують одночасно багато користувачів, потребують рівномірного розподілу запитів між серверними вузлами. Для цього застосовується: балансування на мережевому рівні (L4), балансування HTTP/SSH-трафіку на рівні застосунків (L7), автоматичне додавання нових контейнерів при зростанні навантаження.

Балансування навантаження запобігає перевантаженню окремих компонентів і підвищує стабільність роботи сервісів.

Технології контейнеризації дають можливість автоматично перезапускати сервіси в разі помилки або зависання. До таких механізмів належать періодичні health-check перевірки стану контейнерів; автоматичний перезапуск сервісів при виявленні некоректної роботи; моніторинг стану обладнання лабораторії, що дає змогу вчасно реагувати на перебої.

Для задоволення потреб різних груп користувачів система має підтримувати горизонтальне та вертикальне масштабування: горизонтальне – додавання нових інстансів сервісів при зростанні кількості студентів; вертикальне – збільшення обчислювальних ресурсів для окремих вузлів; ізоляція навантаження – поділ користувачів між різними робочими середовищами для запобігання конфліктам.

Надійність системи неможлива без механізмів спостереження за її роботою. Система моніторингу має фіксувати час відгуку сервісів; оцінювати навантаження на сервери й обладнання; виявляти збої або підозрілу активність; зберігати журнали подій для аналізу й оптимізації.

Оскільки студенти працюють із реальним мережевим обладнанням, важливо регулярно зберігати його конфігурації: автоматичне створення резервних копій; можливість швидкого відновлення після некоректних команд; захищене зберігання історії змін.

Інформаційна безпека є одним із ключових аспектів системи віддаленого доступу до телекомунікаційного обладнання, оскільки користувачі працюють із реальними мережевими пристроями, що можуть впливати на загальну інфраструктуру лабораторії. Забезпечення конфі-

денційності, цілісності й доступності інформації потребує застосування комплексного підходу, який охоплює захист каналів зв'язку, контроль доступу, ізоляцію середовища та аудит дій користувачів.

Для запобігання перехопленню або модифікації даних між користувачем і лабораторним обладнанням необхідно застосовувати шифрування каналів зв'язку. Основними методами є використання захищених протоколів (SSH, HTTPS, TLS 1.3); заборона застарілих протоколів (telnet, HTTP, weak SSH-ciphers); застосування сучасних криптографічних алгоритмів шифрування.

Система повинна гарантувати, що доступ до обладнання отримують лише авторизовані користувачі, а їхні права відповідають навчальним завданням. Для цього використовують такі методи: багатофакторну автентифікацію (MFA); використання ролей доступу (RBAC) для розмежування дозволів; обмеження доступу до конкретних пристроїв або інтерфейсів; установлення політик часу доступу або дозволених типів операцій.

У багатокористувацьких системах важливо, щоб робота одного студента не впливала на результати інших. Ізоляція досягається через запуск окремих контейнерів або віртуальних середовищ для кожного користувача; сегментацію мережевої інфраструктури на окремі логічні домени; блокування небажаних міжсегментних взаємодій між стендами.

Для запобігання порушенню конфігураційної цілісності обладнання необхідно впроваджувати механізми журналювання команд, уведених користувачами; фіксації часу, джерела доступу й дій адміністратора; збереження архівів конфігурацій і їх автоматичної перевірки; виявлення аномальної активності (наприклад, масової зміни параметрів).

Сервери, що обслуговують систему віддаленого доступу, також є критичними об'єктами. Основні методи їх захисту: регулярне оновлення програмного забезпечення; застосування принципу мінімальних привілеїв для службових процесів; використання міжмережевих екранів і фільтрація портів; обмеження доступу до серверів на рівні мережевих ACL; контроль ресурсів контейнерів (CPU, пам'ять, мережеві ліміти).

Забезпечення інформаційної безпеки системи віддаленого доступу ґрунтується на комплексному підході: захищені канали, надійна автентифікація, ізольоване середовище, активний аудит і захист серверної інфраструктури. Поєднання цих методів створює безпечні умови роботи з телекомунікаційним обладнанням і запобігає більшості типових кіберзагроз.

Інтеграція методів підвищення надійності й інформаційної безпеки потребує узгодження архітектурних рішень, механізмів захисту й процедур адміністрування. Для системи віддаленого доступу до телекомунікаційного обладнання важливо, щоб усі технологічні компоненти працювали як єдиний комплекс, де кожен елемент доповнює інші та забезпечує безперервність і захищеність роботи.

Запропонована схема реалізації передбачає поєднання таких ключових елементів:

1. Багаторівнева архітектура з контейнеризацією. У центрі системи знаходиться сервер керування доступом, функціональні модулі якого виконуються у вигляді контейнерів. Це дає змогу ізолювати сервіси один від одного; швидко оновлювати окремі компоненти без зупинки всієї системи; застосовувати механізми самовідновлення та контроль працездатності.

2. Резервована серверна інфраструктура й балансування навантаження. Основні сервери продубльовано в режимах Active-Active або Active-Standby. Над ними працює балансувальник навантаження, який рівномірно розподіляє запити; виключає з пулу вузли, що некоректно відповідають; забезпечує автоматичне переключення в разі збою.

3. Захищені канали між користувачами, сервером та обладнанням. Передача даних між усіма компонентами здійснюється шифрованими каналами. Сегментація мережі дає змогу відокремити користувацький доступ; серверну інфраструктуру; мережеве лабораторне обладнання.

4. Ізоляція користувацьких сесій і середовищ. Кожен користувач або група отримують окремий робочий простір: контейнер або віртуальне середовище з відповідним набором інструментів; ізоляцію команд, щоб запобігти конфліктам; можливість відновлення середовища до початкового стану.

5. Централізований аудит і моніторинг. Усі дії користувачів і сервісів реєструються в централізованому журналі: команди, уведені на обладнанні; зміни конфігурацій; події автентифікації; збої та аномалії сервісів.

6. Автоматизоване відновлення конфігурацій обладнання. Система регулярно створює резервні копії стану лабораторних пристроїв, що дає змогу оперативно повернути зміни до попереднього стану; відновити лабораторію після некоректного експерименту; зберігати історію конфігурацій для викладацького контролю.

У результаті формується комплексна система, здатна забезпечувати стабільний і безпечний доступ до телекомунікаційного обладнання навіть у випадках збоїв чи високого навантаження. Така інтеграція відповідає вимогам сучасних освітніх платформ і дає можливість підтримувати безперервність навчального процесу.

Представлено результати впровадження методів підвищення надійності й інформаційної безпеки в систему віддаленого доступу до телекомунікаційного обладнання. Результати отримані на основі моделювання роботи системи в умовах багатокористувацького доступу, змінного навантаження та відмов окремих компонентів. Окрему увагу приділено реальним сценаріям використання, які дають змогу оцінити ефективність запропонованих рішень у практичному освітньому середовищі.

Після впровадження резервування та балансування навантаження система продемонструвала значно вищу стійкість до збоїв порівняно з базовою архітектурою. Моделювання відмови одного з вузлів показало, що перемикання між серверними компонентами відбувається автоматично, без переривання активних сесій; час недоступності сервісу скоротився до мінімуму й не вплинув на роботу користувачів; балансувальник навантаження коректно перенаправляє запити на доступні вузли. Окрім цього, упроваджені механізми self-healing забезпечили автоматичний перезапуск контейнерних сервісів при виявленні помилок, що суттєво підвищило стабільність платформи.

Горизонтальне масштабування дало змогу збільшити кількість одночасних користувачів без зниження продуктивності. Тестування в умовах пікового навантаження показало, що система стабільно обслуговує значно більшу кількість паралельних підключень; ізоляція робочих середовищ запобігає взаємному впливу команд різних користувачів; продуктивність серверів залишається на прийнятному рівні навіть при значному навантаженні на мережеву інфраструктуру.

Застосування багатофакторної автентифікації, сегментації мережі та контролю доступу забезпечило значне зменшення ризику несанкціонованого доступу до обладнання. За результатами тестування, усі канали передачі даних працюють через зашифровані протоколи; ризик перехоплення трафіку або модифікації команд практично зведений до нуля; спроби доступу з неавторизованих джерел блокуються на рівні мережевих політик; окремі середовища користувачів унеможливлюють небажаних вплив на роботу інших.

Контейнеризація дала змогу досягти високого рівня передбачуваності й повторюваності лабораторних завдань. Кожен студент отримує власне оточення з початковими конфігураціями, а будь-які зміни не впливають на роботу інших користувачів; можуть бути швидко скинуті до стандартного стану; автоматично фіксуються в журналах для подальшого аналізу.

Централізоване логування, моніторинг стану сервісів та автоматичне резервне копіювання конфігурацій обладнання покращили керованість системи. Адміністратори отримали можливість відстежувати виконувані команди в реальному часі; аналізувати навантаження на обладнання й сер-

вери; оперативно відновлювати конфігурації після некоректних дій користувачів; прогнозувати потенційні проблеми й оптимізувати інфраструктуру. Завдяки цьому зменшилося навантаження на обслуговуючий персонал, а час відновлення після інцидентів скоротився. Для кількісної оцінки ефективності запропонованих рішень виконано порівняльний аналіз ключових показників системи до та після впровадження методів підвищення надійності та інформаційної безпеки (таблиця 1).

Таблиця 1

Оцінка ефективності запропонованих методів

Показник	Базова система (без оптимізації)	Запропонована система
Час відновлення після збою, с	120–180	20–30
Кількість точок відмови	Висока	Знижена
Підтримка резервування	Відсутня	Реалізована
Рівень ізоляції користувачів	Низький	Високий
Захищені канали зв'язку	Частково	Повністю
Контроль доступу	Базовий	Розширений (RBAC, MFA)
Можливість журналювання дій	Обмежена	Централізована
Стійкість до мережевих атак	Середня	Підвищена
Масштабованість	Обмежена	Горизонтальна

Аналіз наведених даних підтверджує, що впровадження запропонованого підходу дає змогу суттєво покращити показники доступності, безпеки та керованості системи.

Висновки. У роботі досліджено методи підвищення надійності й інформаційної безпеки системи віддаленого доступу до телекомунікаційного обладнання. На основі аналізу наявних підходів, виявлених загроз та особливостей архітектури віддалених лабораторій сформовано комплексний підхід, який поєднує сучасні засоби контейнеризації, механізми резервування, захищені канали зв'язку, ізоляцію середовищ і централізований аудит. Розроблена модель дає змогу забезпечити високу доступність системи за рахунок резервування сервісів, балансування навантаження й автоматизованого відновлення працездатності; захищеність даних і керованість доступу, що реалізуються завдяки багатофакторній автентифікації, ізоляції користувацьких середовищ, захищеним протоколам і сегментації мережі; стабільність роботи лабораторних стендів, яка досягається контролем цілісності конфігурацій, регулярним резервним копіюванням і відокремленням робочих середовищ; покращення адміністрування системи, забезпечене завдяки впровадженню моніторингу, журналювання та централізованого управління сервісами.

Результати тестування показали, що запропонований підхід підвищує стійкість системи до збоїв, зменшує кількість інцидентів, пов'язаних із помилками користувачів, і суттєво покращує інформаційну безпеку. Інтеграція розглянутих методів дає змогу створити надійну, масштабовану та безпечну платформу для проведення лабораторних занять у сфері телекомунікацій, здатну підтримувати навчальний процес навіть у умовах зростаючих навантажень.

Перспективи подальших досліджень пов'язані з розробленням методів автоматичного аналізу стану мережевого обладнання, інтеграцією системи з навчальними платформами, а також упровадженням інтелектуальних механізмів прогнозування навантажень і виявлення аномальної активності.

Список використаних джерел

1. Tan H., Peterson A. Safety and Security Considerations for Online Laboratory Management Systems. *Journal of Remote Engineering and Virtual Instrumentation*. 2023. Vol. 5, № 2. P. 45–59.

2. Lopez R., Murray J. Remote Labs in Cybersecurity Education: Analyzing Requirements and Challenges. *Computers & Security*. 2024. Vol. 136. Art. 103081.

3. Aziz M., Rahman S. Survey of Remotely Controlled Laboratories for Research and Education. *International Journal of Online Engineering*. 2022. Vol. 18, № 7. P. 4–22.

4. Silva P., Duarte M. Remote Laboratory for Computer Networks. *Proceedings of the 11th International Conference on e-Learning (ICEL)*. SCITEPRESS, 2014. P. 295–302.

5. Соловйов О. В., Бойко Д. І. Дослідження безпечних методів і засобів віддаленого доступу у корпоративному сегменті. *Наукові праці НТУ «ХПІ»*. 2021. № 2(1288). С. 112–118.

6. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53, Rev. 5. Gaithersburg, MD : NIST, 2020. 492 p.

7. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 : RFC 8446. IETF, 2018. URL: https://www.rfc-editor.org/rfc/rfc8446

8. Docker Documentation. Container isolation principles. Docker Inc., 2023. URL: https://docs.docker.com/

9. OWASP Top 10–2021: The Ten Most Critical Web Application Security Risks. OWASP Foundation, 2021. URL: https://owasp.org/Top10/

10. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO, 2022. URL: https://www.iso.org/standard/27001

Дата першого надходження статті до видання: 10.01.2026
Дата прийняття статті до друку після рецензування: 12.02.2026
Дата публікації (оприлюднення) статті: 28.04.2026

I. Vorobiov, D. Velykodnyi
Sumy State University

METHODS FOR IMPROVING RELIABILITY AND INFORMATION SECURITY OF A REMOTE ACCESS SYSTEM TO TELECOMMUNICATION EQUIPMENT

Summary

The paper substantiates a set of methods aimed at improving the reliability and information security of a remote access system to telecommunication equipment used in educational laboratories. Such platforms combine server components, network infrastructure and real devices, therefore failures of critical services or incorrect user actions may disrupt laboratory sessions, while insufficient isolation and weak access control create risks of unauthorized interference. A threat model for a multi-user environment is outlined and the most significant vulnerability groups are identified, including authentication and authorization weaknesses, network-level attacks, insufficient isolation of user sessions, availability threats, and insider misuse. To ensure fault tolerance, the approach integrates redundancy of key services and network paths, load balancing (L4/L7) and automated recovery of containerized components through health checks and self-healing policies. Centralized monitoring and logging are used to detect failures and anomalies, while configuration backup and rapid rollback mechanisms support the continuity of laboratory operation. To strengthen security, encrypted communication channels (TLS/SSH), role-based access control with multi-factor authentication, network segmentation and auditing of user actions are applied. The proposed integration aligns architectural decisions, protection mechanisms and administration procedures into a single workflow that supports stable operation under peak loads and improves manageability. A comparative evaluation of the baseline and improved systems indicates a reduction of recovery time after failures, higher user isolation level, and improved resistance to common network attacks, confirming the practical applicability of the proposed methods in remote telecommunication laboratories.

Keywords: remote access, telecommunication equipment, reliability, information security, containerization, load balancing, redundancy, RBAC, MFA, network segmentation.