Conference name - XXIV International Scientific and Practical Conference "Integration of new technologies into science to improve research", June 17-20, 2025, Paris, France

Section name – TECHNICAL SCIENCES

ІНТЕГРАЦІЯ РІШЕНЬ МОНІТОРИНГУ ТА РЕЗЕРВНОГО КОПІЮВАННЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ IT-ІНФРАСТРУКТУРИ МАЛИХ ПІДПРИЄМСТВ

Dolgova Natalya
Ph.D., Associate Professor
Department Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics
Nauki ave., 9-A, Kharkov, Ukraine, 61166
natalya.dolgova@hneu.net

Інформаційна безпека поступово переходить з розряду допоміжних завдань у категорію ключових функцій IT-інфраструктури, зокрема й у малому бізнесі. Сучасні малі підприємства дедалі частіше стикаються з IT-загрозами, характерними для великих організацій: збої у роботі систем, втрати критичних даних, зовнішні та внутрішні атаки. В умовах обмежених ресурсів це вимагає впровадження простих, але надійних рішень, які дозволяють своєчасно виявляти інциденти, реагувати на них і забезпечувати збереження даних. Інтеграція систем моніторингу та резервного копіювання розглядається як ефективний підхід до побудови базового рівня інформаційної безпеки. У роботі проаналізовано теоретичні засади, сучасні рішення у сфері моніторингу (Zabbix) та резервного копіювання (Veeam), і запропоновано модель інтеграції, адаптовану до потреб малого підприємства.

Ключеви слова: інформаційна безпека; моніторинг; резервне копіювання; малий бізнес; Zabbix; Veeam; інтегровані IT-рішення

Забезпечення інформаційної безпеки поступово переходить з розряду допоміжних завдань у категорію ключових функцій IT-інфраструктури навіть у малому бізнесі. IT-середовище таких підприємств усе частіше стикається з викликами, які раніше були типовими переважно для великих організацій: втрати критичних даних, збої у роботі систем, атаки ззовні та внутрішні порушення. У поєднанні з обмеженими ресурсами це формує потребу в простих, але надійних рішеннях, здатних виявляти проблеми ще на ранньому етапі й гарантувати збереження інформації у випадку збоїв. Інтеграція систем моніторингу та резервного копіювання розглядається як базовий інструмент формування мінімального, але ефективного рівня цифрового захисту, адаптованого до можливостей малого підприємства.

Незважаючи на це, значна частина малих підприємств досі не впровадила повноцінні механізми інформаційної безпеки. Відсутність централізованого моніторингу, ручне або нерегулярне резервне копіювання, слабка система оповіщення — все це створює численні вразливості. Аналітичні дослідження компаній Veeam та IDC підтверджують: малі бізнеси найбільше страждають від інцидентів, яких можна було б уникнути завдяки базовим заходам кіберзахисту.

Інтеграція систем моніторингу та резервного копіювання є ефективним рішенням, що дозволяє не лише забезпечити технічний контроль за станом IT-ресурсів, а й реалізувати елементи багаторівневого захисту — раннє виявлення загроз, фіксацію інцидентів, миттєве сповіщення та можливість швидкого відновлення після збоїв або атак. Поєднання моніторингової платформи, системи резервного копіювання, API-шлюзу для обміну даними між компонентами та каналів сповіщення (через електронну пошту або месенджер) створює основу для побудови захищеної, адаптивної та доступної системи інформаційної безпеки, орієнтованої на потреби малих організацій.

Метою даного дослідження є аналіз теоретичних засад використання систем моніторингу та резервного копіювання у контексті забезпечення інформаційної безпеки, порівняння актуальних технологічних рішень і розробка практично орієнтованої моделі інтеграції, адаптованої до потреб малих підприємств. У межах роботи розглядається інформаційна безпека IT-інфраструктури малого бізнесу як об’єкт дослідження, а предметом виступає інтеграція систем моніторингу (Zabbix) і резервного копіювання (Veeam) із застосуванням механізмів автоматичного обміну даними та сповіщення.

Дослідження передбачає кілька взаємопов’язаних завдань, серед яких: аналіз ролі моніторингу та резервного копіювання в архітектурі IT-безпеки; порівняння найпоширеніших open-source і комерційних рішень у цій сфері; обґрунтування вибору оптимальних інструментів для побудови інтегрованої системи; розробка функціональної архітектури з урахуванням вимог безпеки, а також тестування запропонованого рішення в умовах, наближених до реальних, з метою оцінки його ефективності.

Інформаційна безпека (ІБ) як галузь охоплює сукупність організаційних, технічних і програмних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних (CIA-тріада) [1]. Для малого бізнесу, на відміну від великих корпорацій, забезпечення ІБ часто обмежується мінімально необхідними засобами захисту — через дефіцит ресурсів, відсутність профільних фахівців або недооцінку ризиків [2]. У таких умовах особливої актуальності набувають прості в реалізації, проте функціонально повноцінні рішення, які забезпечують ключові аспекти кіберзахисту.

Моніторинг стану IT-інфраструктури є однією з базових функцій систем управління інформаційною безпекою. Він дозволяє виявляти аномалії, збої, перевантаження, а в деяких випадках — ознаки потенційних атак або шкідливої активності [3]. Ефективний моніторинг дає змогу фіксувати події, аналізувати їх у режимі реального часу й оперативно інформувати відповідальних осіб. За сучасними підходами, такі системи є елементом превентивного захисту в рамках моделі багаторівневої оборони (defense in depth) [4].

Резервне копіювання — ще один фундаментальний компонент стратегії інформаційної безпеки, який забезпечує можливість швидкого відновлення після збоїв, втрат даних або атак на системи. Відповідно до рекомендацій NIST, ефективна політика резервного копіювання має включати регулярність, географічну розподіленість копій та контроль доступу до архівів [5]. У малому бізнесі автоматизація цього процесу часто є критичним фактором надійності, оскільки ручне копіювання призводить до ризиків втрати актуальності або повноти даних [6].

Інтеграція систем моніторингу з платформами резервного копіювання — це сучасний підхід до побудови IT-безпеки, який базується на взаємодії кількох ключових модулів: засобів виявлення, реакції, збереження даних та сповіщення. Такий підхід відповідає концепції SIEM (Security Information and Event Management), але в адаптованому для малого бізнесу вигляді [7]. Хоча повноцінні SIEM-рішення залишаються ресурсоємними, навіть базова взаємодія між системами спостереження, резервування та комунікації дозволяє реалізувати частину їхніх функцій — включно з виявленням інцидентів, централізованим логуванням та автоматичним інформуванням.

Поєднання моніторингу, резервного копіювання та механізмів оперативного сповіщення формує концептуальну основу сучасної системи IT-безпеки для малого підприємства. Саме така інтеграція дозволяє реалізувати багаторівневий, адаптивний та масштабований захист із відносно невеликим навантаженням на ресурси.

Враховуючи основні концепції багаторівневого захисту та роль моніторингу й резервного копіювання у формуванні IT-безпеки, доцільно звернути увагу на конкретні інструменти, які можуть бути застосовані на практиці. Вибір рішень значною мірою залежить від їхньої функціональності, сумісності, вартості впровадження та здатності до інтеграції. Для обґрунтування подальшого підходу до реалізації системи цифрової безпеки необхідним етапом є аналіз сучасних доступних технологій, орієнтованих на потреби малих організацій.

Для малого бізнесу ключовими критеріями вибору є надійність, простота впровадження, підтримка автоматизації та доступність. У цьому контексті доцільно порівняти найбільш поширені open-source і комерційні платформи, які можуть бути інтегровані в єдину систему забезпечення IT-безпеки.

Серед систем моніторингу особливої популярності набули Zabbix, Nagios, Prometheus і PRTG Network Monitor.

Zabbix є одним із найбільш функціонально повних безплатних рішень, що підтримує гнучке налаштування тригерів, візуалізацію метрик, масштабування, а також можливість надсилання сповіщень через зовнішні канали. Система має широке ком’юніті, офіційну документацію та підтримує агентський і безагентський збір даних [8].

Nagios — класична платформа з мінімалістичною архітектурою, орієнтована на перевірку доступності та основних сервісів. Хоча вона широко застосовується, її функціональність без сторонніх плагінів обмежена [9].

Prometheus — високопродуктивне рішення з підтримкою time-series аналізу, яке активно використовується в DevOps-середовищі. Однак, для звичних IT-

інфраструктур малого бізнесу воно може виявитися надлишковим за складністю [10].

PRTG — комерційна система з простим інтерфейсом і широким спектром датчиків, але з обмеженням у безплатній версії (до 100 сенсорів), що може бути критичним для зростаючих компаній [11].

У сегменті систем резервного копіювання основними гравцями є Veeam, Bacula, Acronis, UrBackup та Duplicati.

Veeam Backup & Replication — одне з найпотужніших комерційних рішень, що підтримує резервне копіювання віртуальних, фізичних і хмарних середовищ, має зручний інтерфейс і розвинену політику відновлення [13]. Існує безплатна версія з обмеженим функціоналом, яка підходить для малого бізнесу.

Bacula — модульна open-source система, яка дозволяє створювати гнучкі політики збереження даних. Водночас її конфігурація потребує досвіду адміністрування, що обмежує її застосування в малих організаціях без IT-фахівців [12].

UrBackup — рішення з простою архітектурою, підтримкою інкрементальних копій та веб-інтерфейсом, яке не потребує ліцензійних витрат і швидко впроваджується [14].

Duplicati — орієнтоване на резервне копіювання у хмарні сервіси (Dropbox, Google Drive, Amazon S3), що робить його привабливим для компаній без власних серверів [15].

Таблиця 1.

Порівняльний аналіз існуючих рішень моніторингу та резервного копіювання

Рішення	Тип	Переваги	Обмеження
Zabbix	Моніторинг	Open-source, масштабованість, автоматизація	Вимагає початкового налаштування
Nagios	Моніторинг	Легкий, стабільний	Обмежена функціональність без плагінів
Prometheus	Моніторинг	Висока продуктивність, time-series аналіз	Складність інтеграції, DevOps-орієнтація
Veeam	Резервне копіювання	Потужна платформа, широкий функціонал	Ліцензія на повну версію
Bacula	Резервне копіювання	Гнучкість, скриптованість	Складність конфігурації
UrBackup	Резервне копіювання	Простота, web-інтерфейс	Менш розвинені політики безпеки

Порівняльний аналіз свідчить, що для малого бізнесу найбільш збалансованим за критеріями функціональності, вартості та простоти впровадження є комбінація Zabbix для моніторингу та Veeam (Free Edition) для резервного копіювання. Їх інтеграція із засобами сповіщення та API дозволяє реалізувати ефективну та масштабовану систему захисту інформаційної інфраструктури.

Для реалізації практичного рішення було обрано модульний підхід, що передбачає інтеграцію кількох інструментів із чітким розподілом функціональних ролей: моніторинг, резервне копіювання, логіка взаємодії та система сповіщення. Така архітектура дозволяє забезпечити автономність кожного компонента, спрощує масштабування та полегшує адміністрування в умовах обмежених ресурсів (рис. 1).

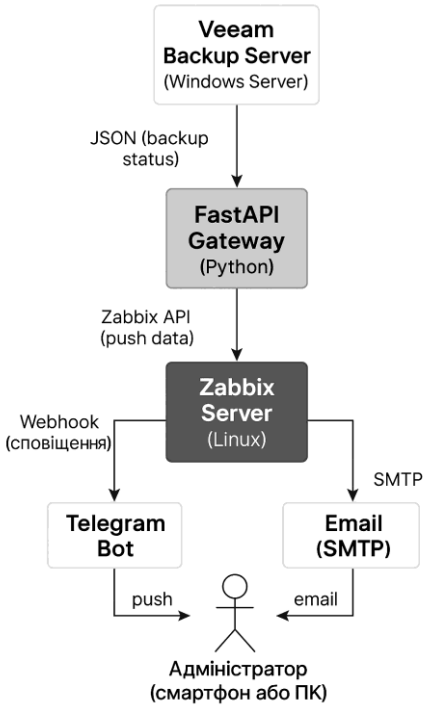

Рисунок 1. Фізична архітектура системи

У якості основи для моніторингу використано систему, яка здійснює безперервний контроль за станом серверів, служб і мережевої інфраструктури. Вона збирає метрики, відслідковує спрацьовування тригерів і може формувати події при досягненні критичних значень. Завдяки API або скриптовим механізмам вона передає інформацію про інциденти до логіки сповіщення або виводить її в загальнодоступний канал, наприклад, в лог-сервер або SIEM-платформу.

Модуль резервного копіювання відповідає за створення актуальних резервів критичних даних та їхнє збереження у безпечному сховищі. Платформа підтримує інкрементальні копії, розклад виконання задач, контроль успішності завершення процесів, а також журналювання. У разі помилки або збою система може передати повідомлення до сповіщувального модуля.

Обмін інформацією між системами моніторингу та резервування забезпечується за допомогою проміжного логічного компонента — API-шлюзу. Він дозволяє запитувати стан копій, перевіряти наявність збоїв, автоматизувати формування сповіщень та запуск певних дій (наприклад, перевірку цілісності копії або повторну спробу).

Для оперативного інформування про події, помилки або загрози використано механізм сповіщення, який підтримує кілька каналів доставки — електронну пошту, месенджери або push-повідомлення. Це дозволяє отримувати дані в

режимі реального часу без потреби постійного доступу до веб-інтерфейсу системи.

Загалом така архітектура формує єдиний інформаційний контур, що охоплює виявлення, фіксацію та реагування на інциденти. При цьому рішення залишається доступним для малого бізнесу за рахунок використання open-source компонентів та мінімальних вимог до технічних ресурсів.

Описана вище фізична структура системи демонструє розподіл її компонентів у середовищі контейнеризації, способи розгортання та базові канали взаємодії. Проте для глибшого розуміння функціональної логіки рішення доцільно розглянути логічну архітектуру, яка відображає послідовність обробки даних, механізми інтеграції та способи реагування на події (рис. 2).

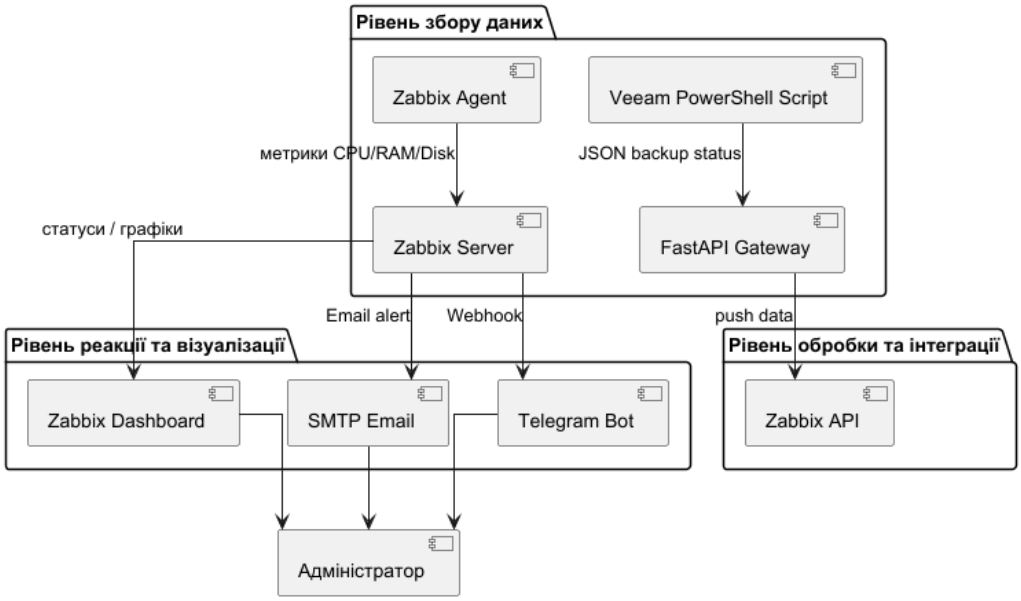

Рисунок 2. Логічна архітектура системи

На схемі представлено логічну архітектуру системи, яка складається з трьох ключових рівнів: збору даних, обробки та інтеграції та реакції й візуалізації. На рівні збору даних працюють агенти моніторингу та скрипти, що відповідають за фіксацію метрик продуктивності серверів (CPU, RAM, Disk), а також за отримання статусів резервного копіювання у форматі JSON. Усі ці дані надсилаються до центрального сервера моніторингу, який є точкою агрегації та аналізу інформації.

Рівень обробки та інтеграції включає проміжну ланку у вигляді API-шлюзу (FastAPI), що забезпечує обмін інформацією між системою резервного копіювання і сервером моніторингу через REST-запити. Для гнучкої обробки подій використовується Zabbix API, який дозволяє генерувати сповіщення або запускати автоматизовані сценарії у відповідь на визначені умови.

На рівні реакції система формує сповіщення для адміністратора за допомогою email (SMTP) або месенджера (Telegram Bot). Також передбачено візуалізацію даних у вигляді дашбордів, що дозволяє оперативно оцінювати стан інфраструктури. Така архітектура забезпечує прозорість, контроль і автоматичну взаємодію між усіма компонентами системи.

Розроблена архітектура була реалізована з використанням відкритих технологій та інструментів, доступних за умовами ліцензування для малого

бізнесу. Основна мета практичної частини — забезпечити автоматизований обмін даними між системою резервного копіювання та сервером моніторингу, а також налагодити механізм оперативного інформування адміністратора у випадку інцидентів.

Ключовим функціональним компонентом виступає FastAPI Gateway — легкий REST-сервіс, розгорнутий як проміжна логічна ланка між Veeam Backup та Zabbix. Він отримує статуси завдань резервного копіювання у форматі JSON, обробляє ці дані й передає у Zabbix через його API (рис. 3). Це дозволяє повністю автоматизувати фіксацію успішних або аварійних резервних копій як подій моніторингу.

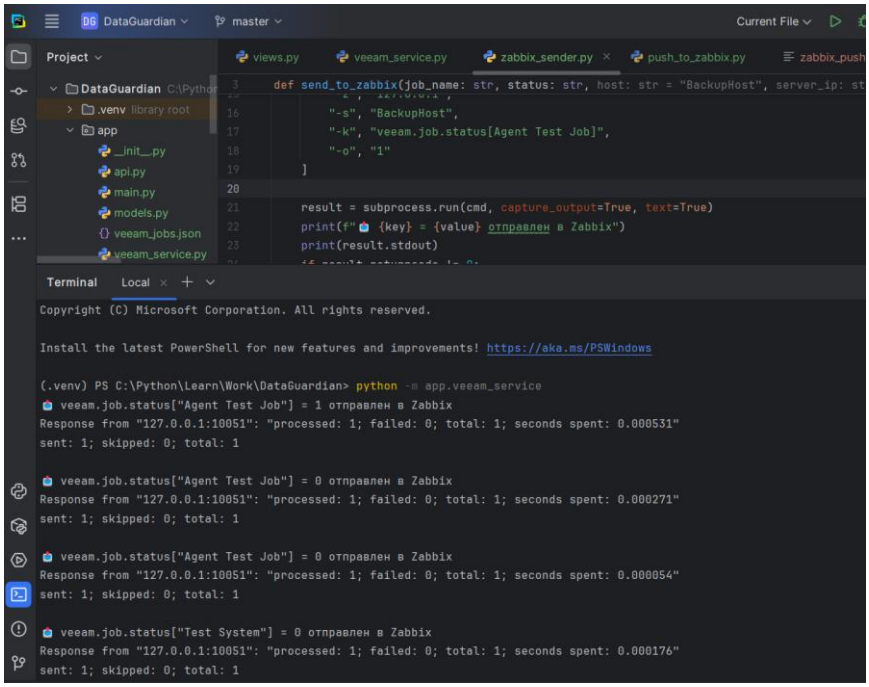

Рисунок 3. Логіка передачі статусів резервного копіювання до системи моніторингу через REST-запит.

Інтерфейс FastAPI додатково надає можливість візуалізувати актуальні статуси завдань у браузері. Це дозволяє проводити ручну перевірку або аудит без необхідності звертання до серверів резервного копіювання (рис. 4).

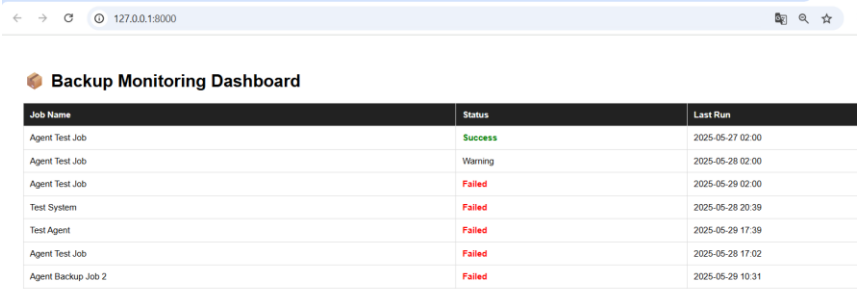

Рисунок 4. Інтерфейс FastAPI для візуалізації статусів завдань резервного копіювання.

На стороні Zabbix було створено користувацький елемент даних та відповідний тригер, який реагує на невдалі або частково завершені резервні копії. При його спрацюванні формується подія, що активує систему сповіщення.

Для інформування адміністратора реалізовано інтеграцію з Telegram. Повідомлення про інциденти надсилаються через Telegram-бота автоматично, одразу після виявлення події, що дозволяє реагувати на загрози у режимі реального часу без необхідності постійного моніторингу веб-інтерфейсу (рис. 5).

Рисунок 5. Повідомлення про інцидент, отримане у Telegram через інтеграцію з Zabbix API.

Побудована система поєднує моніторинг, резервне копіювання, логіку взаємодії та сповіщення в єдину функціональну структуру. Вона залишається доступною для малого бізнесу, не потребує значних ресурсів і здатна ефективно виконувати ключові завдання цифрової безпеки.

Забезпечення інформаційної безпеки для малого бізнесу потребує практичних, економічно обґрунтованих і технічно ефективних рішень. У межах цієї роботи було продемонстровано, що інтеграція систем моніторингу та резервного копіювання може стати базовим, але надійним інструментом для створення мінімального рівня цифрового захисту в умовах обмежених ресурсів.

На основі аналізу існуючих платформ було обґрунтовано доцільність використання open-source і умовно безоплатних рішень — таких як Zabbix, Veeam Backup, FastAPI та Telegram. Вони забезпечують ключову функціональність: виявлення інцидентів, збереження резервних копій, централізований контроль та оперативне сповіщення.

Практична реалізація підтвердила ефективність обраної архітектури. Система продемонструвала стабільну роботу у тестовому середовищі протягом 14 днів, з автоматичним виявленням та фіксацією 100% тестових збоїв резервного копіювання. Час доставки сповіщення до Telegram-каналу в середньому становив менше 5 секунд, що дозволяє говорити про високий рівень оперативності.

Застосування FastAPI як проміжного логічного шлюзу дозволило реалізувати автоматизовану передачу даних між модулями без складних інтеграцій.

Додаткові переваги забезпечує використання Telegram-бота — як простого і доступного каналу критичних сповіщень.

У перспективі таке рішення може масштабуватись, включаючи додаткові рівні захисту, журнали подій, елементи SIEM-аналітики та візуалізацію KPI. Запропонований підхід є адаптивним і може бути інтегрований в інші середовища малого або середнього бізнесу без значних витрат на впровадження та підтримку.

Література:

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.
2. Cisco. Cybersecurity for Small Business: Protecting Your Digital Assets [Електронний ресурс]. – 2022. – Режим доступу: https://www.cisco.com/
3. Scarfone, K., Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS): NIST Special Publication 800-94. – Gaithersburg: National Institute of Standards and Technology, 2007. – 127 с.
4. SANS Institute. Defense in Depth: Foundations for Secure Systems [Електронний ресурс]. – 2018. – Режим доступу: https://www.sans.org/
5. National Institute of Standards and Technology. Contingency Planning Guide for Federal Information Systems: SP 800-34 Rev. 1. – Gaithersburg: NIST, 2020. – 96 с.
6. Veeam Software. Data Protection Trends Report 2023 [Електронний ресурс]. – 2023. – Режим доступу: https://www.veeam.com/
7. Gartner. SIEM for SMBs: Feasible, Scalable, Effective? [Електронний ресурс]. – 2021. – Режим доступу: https://www.gartner.com/
8. Zabbix Documentation [Електронний ресурс]. – Режим доступу: https://www.zabbix.com/documentation/
9. Nagios. Product Overview [Електронний ресурс]. – Режим доступу: https://www.nagios.org
10. Prometheus. Open-source monitoring system [Електронний ресурс]. – Режим доступу: https://prometheus.io/
11. PRTG Network Monitor. Paessler AG [Електронний ресурс]. – Режим доступу: https://www.paessler.com/prtg
12. Bacula. Enterprise Open Core [Електронний ресурс]. – Режим доступу: https://www.bacula.org
13. Veeam Software. Product Overview [Електронний ресурс]. – Режим доступу: https://www.veeam.com
14. UrBackup. Free Open Source Online Backup Software [Електронний ресурс]. – Режим доступу: https://www.urbackup.org
15. Duplicati. Free backup software to store encrypted backups online [Електронний ресурс]. – Режим доступу: https://www.duplicati.com