*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА РЕЗЕРВНОГО КОПІЮВАННЯ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика резервного копіювання виконавчого комітету Криворізької міської ради (надалі – Політика резервного копіювання) є документом, що описує дії, пов’язані з діяльністю виконкому міської ради стосовно резервного копіювання активів системи управління інформаційною безпекою (надалі – СУІБ).

1.2. Політика резервного копіювання розроблена з метою підтвердження готовності впровадження заходів з інформаційної безпеки для захисту активів СУІБ з метою підвищення їх конфіденційності, цілісності та доступності.

1.3. Політика резервного копіювання застосовується до всієї області дії СУІБ, а саме:

1.3.1 усіх операційних процесів, програмних продуктів та їх налаштувань, інформації, що обробляється в Єдиній інформаційній системі міста Кривий Ріг (надалі – ЄІС);

1.3.2 усіх користувачів виконкому міської ради або інших дотичних сторін, що мають певні повноваження і отримують доступ до ЄІС у межах області дії СУІБ.

1.4. Політика резервного копіювання спрямована на захист активів виконкому міської ради в області дії СУІБ у разі збою будь-якого системного процесу чи обладнання, пошкодження даних або обставин непереборної сили. Політика резервного копіювання гарантує, що активи СУІБ не будуть втрачені та мають можливість повного відновлення через такі заходи:

1.4.1 резервні копії інформації, програмного забезпечення (надалі – ПЗ) та систем створюються через певний час, обліковуються і їх наявність регулярно перевіряється;

1.4.2 резервні копії інформації, ПЗ та систем підтримуються і регулярно тестуються з метою гарантування їх актуальності, цілісності та можливості розгортання.

1.5. Політика резервного копіювання розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу інформаційної безпеки, а саме: Законів України «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-комунікаційних системах»; ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги»; ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки»; ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) «Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови», Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄC (Загального регламенту про захист даних) (надалі – GDPR), Наказу Адміністрації ДержСпецзв’язку України від 06 жовтня 2021 року №601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (зі змінами), Стандарту інформаційної безпеки NIST Special Publication 800-53 Revision 5 «Security and Privacy Controlsfor Information Systems and Organizations», Структури кібербезпеки The NIST Cybersecurity Framework (CSF) 2.0, політик, процедур і технічних заходів: D4.1-СУІБ «Політика інформаційної безпеки», D2.2-СУІБ «Політика управління активами», D10-СУІБ «Методологія оцінки та обробки ризиків», D14.1-СУІБ «Політика ІТ-безпеки», D14.6-СУІБ «Політика класифікації інформації», D14.14-СУІБ «Політика контролю доступу».

#### *2. Терміни, визначення та скорочення*

2.1. Диференціальне резервне копіювання (Differential backup) – резервне копіювання, за якого кожен файл, що був змінений з моменту останнього повного резервного копіювання, копіюється кожен раз заново.

2.2. Інкрементне резервне копіювання (Incremental backup) – резервне копіювання, за якого відбувається копіювання тільки тих файлів (інформації), що були змінені з тих пір, як в останній раз виконувалося повне або додаткове резервне копіювання. Подальше інкрементне резервне копіювання додає тільки файли (інформацію), що були змінені з моменту попереднього копіювання.

2.3. Критичні операційні процеси – операційні процеси діяльності виконкому міської ради, які визначені критичними щодо інформаційної безпеки за результатом їх оцінювання за такими критеріями: конфіденційність, цілісність, доступність.

2.4. Повне резервне копіювання (Fullbackup) – створення повної копії даних інформаційних систем і всіх файлів (даних), що дозволяє забезпечити максимальну відповідність копії оригіналу.

2.5. Система резервного копіювання – сукупність програмного й апаратного забезпечення, призначеного для створення резервних копій і відновлення даних.

2.6. Актив – активом є все, що має цінність для виконкому міської ради й потребує захисту [інформаційний актив, апаратне забезпечення, ПЗ, інфраструктура, мережа розповсюдження інформації, посадові особи, сервіси, технології та ресурси (фінансові, технічні, адміністративні, організаційні) для забезпечення інформаційної діяльності, нематеріальні активи (імідж, довіра, сертифікати відповідності, ліцензії тощо)].

2.7. Власник активу – відповідальна посадова особа або відділи, управління інші виконавчі органи міської ради, у розпорядженні та/або користуванні, та/або розробці, та/або підтримці яких перебуває актив, що може впливати на інформаційну безпеку (надалі − ІБ) та кібербезпеку.\*

2.8. Інформаційний актив (надалі − ІА) – це сукупність відомостей (інформації у фізичній або електронній формі), що представляє цінність для виконкому міської ради, а також будь-яка інформаційна система обробки, обміну чи фізичного місця зберігання інформації.

2.9. ЄІС – багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб’єктів, інформаційну підтримку та супроводження їх діяльності й становить сукупність взаємопов’язаних функціональних підсистем, програмно-інформаційних комплексів, комп’ютерних програм, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку й захист інформації, внутрішню та зовнішню інформаційну взаємодію.

2.10. Chief Executive Officer ( надалі – CEO) – власник і розпорядник СУІБ.

2.11. Chief Security Officer (надалі – CSO) – відповідальний за ІБ, який відповідає за керування процесом організації безпеки у виконкомі міської ради, включаючи фізичну безпеку, ІБ, кібербезпеку та інші види безпеки в межах сфери застосування СУІБ.

2.12. Chief Information Security Officer (надалі − CISO) − відповідальний за розробку та впровадження політик і процедур ІБ, управління ризиками, забезпечення кібербезпеки, реагування на інциденти, підвищення обізнаності працівників та контроль за дотриманням законодавства у сфері захисту інформаційних систем і даних.

2.13. Data Protection Officer (надалі − DPO) − відповідальний за захист персональних даних у виконкомі міської ради, відповідає за організацію роботи, пов’язаної із захистом персональних даних у процесі інформаційної діяльності виконкому в межах області дії СУІБ.

2.14. Chief Information Officer (надалі − CIO) − відповідальний за розробку та реалізацію стратегії цифрової трансформації міста, управління інформаційними системами та ресурсами, кібербезпеку.

2.15. Ad1 – адміністратор безпеки.

2.16. Ad2 – адміністратор системи.

2.17. Security Operations Center (надалі − SOC) − група інформаційної безпеки виконкому міської ради, що відповідає за моніторинг, виявлення, аналіз та реагування на інциденти кібербезпеки в реальному часі.

#### *3.* *Резервне копіювання та відповідальність*

3.1. Резервні копії створюються для всіх компонентів підсистем ЄІС з періодичністю, указаній у цій Політиці.

3.2. Резервному копіюванню підлягають усі продуктивні сервери та бази даних виконкому міської ради:

3.2.1 сервери прикладного ПЗ;

3.2.2 бази даних прикладного ПЗ;

3.2.3 бази даних електронної пошти;

3.2.4 файлові сервери;

3.2.5 системні образи (налаштування) функціонального та спеціального (комплекс засобів захисту) ПЗ;

3.2.6 інформаційні активи.

3.3. У разі необхідності інформація з комп’ютерів користувачів підлягає резервному копіюванню, але користувачі ЄІС зобов’язані зберігати свої файли у власній мережевій папці на файловому сервері (крім кваліфікованого електронного підпису, що зберігається в спеціальній захищеній папці).

3.4. CIO та Ad2 безпосередньо відповідають за резервне копіювання інформації, ПЗ та системних образів (операційних систем і прикладного ПЗ) усіх функціональних компонентів ЄІС, а також за належне усунення збоїв ЄІС. CIO та Ad2  відповідають за актуальність цих резервних копій та їх тестування з метою гарантування відновлення інформації та налаштувань компонентів ЄІС у разі порушення її безперервної роботи в межах області дії СУІБ. CIO контролює результативність заходів з резервного копіювання, що проведені повноважними особами виконкому міської ради у відповідності до вимог Політики резервного копіювання. CIO відповідає за своєчасне формування звіту до CSO стосовно проведених заходів резервного копіювання у виконкомі міської ради з урахуванням ризикорієнтовного підходу.

3.5. CISO та Ad1 безпосередньо відповідають за резервне копіювання інформації, ПЗ та системних образів, пов’язаних з комплексом засобів захисту (надалі – КЗЗ), а також за належне усунення збоїв КЗЗ ЄІС. CISO та Ad1  відповідають за актуальність цих резервних копій та їх тестування з метою гарантування відновлення інформації та налаштувань КЗЗ ЄІС у разі порушення їх безперервної роботи у межах області дії СУІБ. CISO контролює результативність заходів з резервного копіювання, що проведені повноважними особами виконкому міської ради у відповідності до вимог Політики резервного копіювання. CISO своєчасно звітує CSO стосовно проведених заходів резервного копіювання у виконкомі міської ради з урахуванням ризикорієнтовного підходу.

3.6. DPO здійснює контроль та несе відповідальність за проведені заходи резервного копіювання, тестування, відновлення PII згідно з вимогами Політики резервного копіювання. DPO своєчасно CEO та інформує CSO стосовно проведених заходів резервного копіювання у виконкомі міської ради з урахуванням ризикорієнтовного підходу.

3.7. CSO здійснює контроль ефективності проведених заходів резервного копіювання та своєчасності проведених заходів з резервного копіювання, тестування, відновлення усіх активів у відповідності з вимогами Політики резервного копіювання у межах області дії СУІБ. CSO контролює виконання заходів відповідно до правил з періодичністю, визначених документацією СУІБ.

3.8. Електронний журнал обліку резервного копіювання створюється автоматично в компонентах ЄІС. Цей журнал зберігає цілісність даних, а доступ до внесення змін у журналі мають тільки Ad1 (журнали КЗЗ) та Ad2 (системні журнали) під керівництвом CISO та контролем CSO.

3.9. Форма друкованої версії журналу реєстрації резервного копіювання приведена в пункті 3.10. (Таблиця 1) Відповідальність за повноту, якість та своєчасність записів до журналу покладено на Ad2.

3.10. Журнал реєстрації резервного копіювання (зразок):

**Таблиця 1 Відомості резервного копіювання Активів СУІБ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***№ п/п*** | ***Назва активу******(тип)*** | ***Дата******резервного копіювання, результат успішності операцій (місце зберігання)*** | ***Дата проведення тестування з відновлення*** | ***Опис успішності операції відновлення даних з резервної копії*** | ***Посада, ПІБ особи, яка******виконувала роботи (адміністратор системи, адміністратор безпеки або інша уповноважена особа)*** | ***Підпис особи, яка******виконувала роботи*** |
|  |  |  |  |  |  |  |

3.11. Будь-яке ПЗ, що копіюється до його початкового використання, має зберігатися в безпечному місці. Основні копії не можна використовувати для звичайної інформаційної діяльності, їх слід зберігати для відновлення після зараження комп’ютерними вірусами, збоїв жорсткого диска та інших технічних проблем.

3.12. Технології, що використовуються для створення резервних копій, захисту резервних копій, шифрування та паролів, зазначені в Політиці інформаційної безпеки.

3.13. РІІ, включаючи їх резервні копії, зберігаються:

3.13.1 засобами ЄІС у мережі «Інтранет» виконкому міської ради;

3.13.2 у мережі адміністратора ЄІС/процесорів PII, перелік яких визначений у документі: D3-СУІБ «Сфера застосування». Виконком міської ради зберігає PII протягом тривалості відносин із суб’єктом PII протягом певного періоду часу, який визначеного у згоді суб’єкта PII. Виконком міської ради зберігає PII суб’єкта PII до тих пір, поки вони не матимуть цінності та не будуть видалені посадовими особами відповідно до політик СУІБ. Усі PII, включаючи їх резервні копії, якими керує виконком міської ради, будуть видалені за підтвердженим запитом від суб’єктів PII або їх уповноважених агентів. Конкретні обов’язки щодо ідентифікаційної інформації в цьому відношенні можуть залежати від суб’єктів PII. Виконком міської ради переконується, що суб’єкт PII був проінформований про обмеження послуги щодо резервного копіювання.

3.14. У випадах несправності системи, атаки або катастрофи, ідентифікаційна інформація потребує відновлення. Під час відновлення ідентифікаційної інформації (як правило з резервних носіїв) запускаються процеси, для впевненості, що ідентифікаційна інформація буде відновлена в стані, у якому гарантується її цілісність.

3.15. Для чіткого розмежування файлів, які використовуються для роботи, і файлів, що використовуються для тестування чи навчання, слід застосовувати правила іменування файлів.

3.16. Для кожного активу/ІА адміністратором системи/підсистеми розробляється інструкція резервного копіювання.

3.17. Для проведення резервного копіювання власники активів/власники ІА розробляють та затверджують вимоги до активу/ІА виконкому міської ради, на підставі яких складається та впроваджується план резервного копіювання. План включає (для кожного активу/ІА виконкому міської ради) таку інформацію:

3.17.1 тип резервного копіювання;

3.17.2 частота копіювання, відповідальний;

3.17.3 носій, на якому зберігається резервна копія;

3.17.4 місце зберігання, відповідальний;

3.17.5 термін тестування, відповідальний;

3.17.6 термін зберігання, відповідальний.

3.18. Електронний журнал реєстрації подій створення резервних копій:

3.18.1 у межах системи резервного копіювання автоматично ведеться електронний журнал реєстрації подій створення резервних копій (надалі – журнал реєстрації подій).

3.18.2 журнал реєстрації подій має містити актуальну інформацію щодо процесу виконання резервного копіювання.

3.19. Графік створення резервних копій: резервне копіювання повинно виконуватися у час, коли навантаження на систему мінімальне. Виконання резервного копіювання має відбуватися за межами операційного часу.

3.20. Регулярна перевірка інформації з резервних копій:

3.20.1 перевірка інформації з резервних копій здійснюється відповідним адміністратором системи резервного копіювання щоквартально;

3.20.2 у графіку регулярної перевірки інформації з резервних копій зазначається список інформаційних активів/систем, що підлягають тестовому відновленню, та періодичність виконання тестового відновлення. Графік проведення регулярних перевірок складається й актуалізується адміністратором системи;

3.20.3 проведення регулярних перевірок інформації з резервних копій виконується в мережі, ізольованій від загальної локальної мережі виконкому міської ради. Специфікація серверів, на яких проводиться тестове відновлення інформаційної системи, має відповідати параметрам серверів, з яких виконується резервне копіювання;

3.20.4 після завершення етапу відновлення інформації адміністратор системи резервного копіювання надає доступ до відновленої інформації адміністраторам відновлених інформаційних активів/систем з метою визначення коректності відновлених даних та повідомляє SOC про результати перевірки.

3.21. Безпека носіїв резервних копій:

3.21.1 резервні копії зберігаються у віддаленому місці, на достатній відстані, щоб уникнути будь-якого ушкодження в разі настання надзвичайних обставин в приміщенні, у якому оброблюються ІА та розташовані активи;

3.21.2 носії резервних копій мають бути захищені від несанкціонованого доступу до них та мати рівень конфіденційності не нижче ніж ІА, що зберігаються на цьому носії.

3.22. Процедура резервного копіювання та відновлення інформації:

3.22.1 резервне копіювання проводиться автоматично на основі плану резервного копіювання;

3.22.2 адміністратори ЄІС/адміністратори підсистем ЄІС у межах повноважень несуть відповідальність за налаштування системи резервного копіювання, а також за перегляд журналів реєстрації подій;

3.22.3 кожного робочого дня виконується інкрементне резервне копіювання, щотижневе – диференціальне резервне копіювання;

3.22.4 щотижневе повне резервне копіювання за наявності технічної можливості виконується в неопераційний час;

3.22.5 щоквартальне та щорічне резервне копіювання проводиться у кінці кожного місяця та року відповідно;

3.22.6 позапланове виключне резервне копіювання може виконується за заявкою власника інформаційного активу/системи, підрозділу ІТ або SOC;

3.22.7 після завершення кожного резервного копіювання генерується відповідний запис у журналі реєстрації подій. У разі виявлення будь-яких помилок адміністратор ІА/системи перевіряє та виконує необхідні дії для усунення причини проблеми резервного копіювання і перезапуск невдалого резервного копіювання. Термін зберігання інформації в журналі реєстрації подій має бути не менше одного року.

3.23. Загальна процедура відновлення інформації з резервних копій:

3.23.1 відновлення інформації виконується на підставі поданої заявки на відновлення інформації;

3.23.2 кожна заявка на відновлення інформації реєструється. Кожній заявці присвоюється унікальний ідентифікатор. Обґрунтування подання заявки на відновлення базується на поважних причинах (наприклад: відновлення втрачених даних або відновлення для тестування даних у межах відповідного проєкту);

3.23.3 ініціатором відновлення інформації виступає власник інформаційного активу/системи згідно із реєстром інформаційних активів або адміністратор інформаційного активу/системи в разі необхідності аварійного відновлення;

3.23.4 кожній заявці на відновлення інформації залежно від важливості ІА/системи або відновлюваної інформації користувача присвоюється пріоритет, що є підставою для визначення порядку обробки заявки, виділення ресурсів і часу для реагування на заявку;

3.23.5 заявкам на відновлення інформації присвоюється один з трьох пріоритетів відповідно до Таблиці 2:

 *Таблиця 2*

|  |  |  |  |
| --- | --- | --- | --- |
| ***№ п/п*** | ***Пріоритет*** | ***Критерії*** | ***Час реакції*** |

| ***1*** | ***2*** | ***3*** | ***4*** |
| --- | --- | --- | --- |
| 1 | Критичний | Присвоюється в разі повної відмо-ви важливого інформаційного активу/системи, що викликало пору-шення роботи користувачів. Є підставою для припинення посадовою особою підрозділу ІТ будь-яких інших робіт з виконання заявок з меншим пріоритетом | Роботи починаються протягом 30 хвилин з моменту надхо-дження заявки  |
| 2 | Високий | Присвоюється у таких випадках:звернення CEO, заступника CEO або CSO/DPO/CIO/CISO;втрата інформації стосується більше ніж одного користувача;втрата інформації вплинула на інформаційний актив/систему | Роботи починаються протягом 60 хвилин з моменту надходження заявки  |
| 3 | Стандартний | Призначається за замовчуванням для всіх заявок | Роботи починаються протягом 24 годин з моменту надходже-ння заявки  |

3.23.6 усі заявки на відновлення інформації, у тому числі на середовищах тестування та розробки, погоджуються CSO перед початком виконання робіт;

3.23.7 відновлення інформації відбувається за тісної взаємодії з адміністратором відновлюваного інформаційного активу/системи CIO/CISO.

3.24. Завдання резервного копіювання заплановане згідно з описом, представленим у Таблиці 3:

*Таблиця 3*

|  |  |  |  |
| --- | --- | --- | --- |
| ***№ п/п*** | ***Тип*** | ***Час*** | ***Примітки*** |

| ***1*** | ***2*** | ***3*** | ***4*** |
| --- | --- | --- | --- |
| 1 | Щоденне інкрементне ре-зервне копіювання | Понеділок-четвер | Період резервного копіювання визначається для кожного ІА/системи окремо власником активу.Термін зберігання копій – не менш ніж 1 місяць.Дані, в ЄІС, зберігаються протягом 30 календарних днів, після чого знищуються за допомогою програмно-апаратного комплексу в автоматичному режимі із дотриманням вимог щодо глибини архіву не менше 30 діб |
| 2 | Щотижневе диферен-ціальне резервне копіювання | Кожної п’ятниці,поза межею операційного часу | Завдання резервного копіювання повинно завершитися до початку операційного часу.В іншому випадку завдання повинно бути скасоване.Термін зберігання копій – не менше одного місяця |
| 3 | Щомісячне повне резервне копіювання. | В останню п'ятницю кожного місяця, поза  межею опе-раційного часу | Завдання резервного копіювання повинно завершитись до початку операційного часуВ іншому випадку завдання повинно бути скасоване.Термін зберігання копій – не менше трьох місяців  |
| 4 | Щоквартальне повне ре-зервне копіюваня із пе-ревіркою (виконання процесу вибіркового (усіх критичних резервних копій) відновлення/розгортання) інформації з резервних копій відповідним адмініс-тратором системи/підсисте-ми в ізольованій мережі | В останню п'ятницю кварталу, поза межею операційного часу | Завдання резервного копіювання повинно завершитися до початку операційного часу.В іншому випадку завдання повинно бути скасоване.Термін зберігання копій – не менш ніж 6 (шість) місяців |
| 5 | Щорічне повне резеврне копіювання із перевіркою (виконання процесу повного відновлення або роз-гортання) інформації з ре-зервних копій відповідним адміністратором системи або підсистеми в ізольо-ваній мережі | В останній тиждень останнь-ого місяця року, поза межею операційного часу | Завдання резервного копіювання повинно завершитись до початку операційного часу.В іншому випадку завдання повинно бути скасоване.Термін зберігання копій – не менше одного року |

3.25. Адміністратор системи здійснює фіксацію та збереження в автоматичному режимі всіх дій щодо роботи з даними в ЄІС. З цією метою в автоматичному режимі зберігається інформація про:

3.25.1 дату, час та джерело зібраних даних;

3.25.2 перегляд даних;

3.25.3 будь-яку передачу (копіювання) даних;

3.25.4 користувача інформації в ЄІС, який здійснив одну з вищевказаних операцій;

3.25.5 дату та час видалення даних ЄІС.

3.26. Адміністратор системи здійснює збереження інформації про операції, пов’язані з обробкою даних в ЄІС та доступом до них.

3.27. Адміністратор забезпечує зберігання цієї інформації впродовж 180 днів з моменту настання події, у якій було здійснено зазначені операції, якщо інше не передбачено законодавством.

3.28. Адміністратор системи/відповідальний за резервне копіювання відповідно до функціональних обов`язків зобов`язаний періодично (наступний робочий день після резервного копіювання за графіком) переглядати журнали реєстрації подій. У разі виявлення будь-якої проблеми в таких журналах, він негайно реєструє її в системах «ServiceDesk», «Jira» тощо та інформує CISO/CSO про неї.

#### *4. Тестування резервних копій*

4.1. Резервні копії та процес їх відновлення тестуються щонайменше раз на три місяці (інтервал визначається, виходячи з оцінки ризиків) шляхом реалізації процесу відновлення даних на сервері виконкому міської ради, на якому здійснюється відновлення даних та перевірка можливості успішного відновлення всіх даних. За рішенням CSO можливе проведення вибіркової перевірки (із застосуванням методу вибірки: випадкова, систематична: вибір з генеральної популяції, потім через рівний інтервал вибір одиниці), але з обов’язковою повною перевіркою всіх критичних резервних копій.

4.2. CIO відповідає за тестування резервних копій функціонального ПЗ.

4.3. CISO відповідає за тестування резервних копій спеціального ПЗ (КЗЗ).

4.4. CSO контролює виконання вимог стосовно періодичності тестування, документування та наявності актуальних, включаючи забезпечення необхідного резервного копіювання даних, конфігураційної інформації і безпечне керування резервними копіями.

4.5. Облік проведення тестування резервних копій ведеться в друкованому вигляді (журнал реєстрації резервного копіювання відповідно до пункту 3.10. Політики резервного копіювання) та в електронному вигляді (журнал реєстрації резервного копіювання).

#### *5. Настанова щодо впровадження заходів захисту*

5.1. Проведення регулярного тестування носіїв резервного копіювання (тестування здатності проводиться у тестовій системі, а не шляхом перезапису оригінального носія, інакше може з’явитися такий інцидент: процес резервного копіювання або відновлення не вдається і спричиняє непоправне пошкодження або втрату даних).

5.2. Захист резервних копій треба здійснювати за допомогою шифрування відповідно до виявлених ризиків (наприклад, у ситуаціях, коли конфіденційність є важливою).

5.3. Слід передбачати, щоб ненавмисна втрата даних була виявлена перед створенням резервної копії.

5.4. Оперативні процедури контролюють виконання резервного копіювання і вирішують помилки запланованих резервних копій, щоб забезпечити повноту резервних копій відповідно до тематичної політики щодо них.

5.5. Заходи резервного копіювання для окремих систем і послуг регулярно перевіряються, щоб переконатися, що вони відповідають цілям планів реагування на інциденти та безперервності роботи.

5.6. У випадку критичних компонентів (ядро системи, серверне обладнання, образи налаштувань ПЗ) та послуг, заходи резервного копіювання мають охоплювати всю системну інформацію, програми та дані, необхідні для відновлення всієї системи в разі аварії.

*\*Термін «Власник» ідентифікує посадових осіб, відділи, управління, інші виконавчі органи міської ради, для яких установлено відповідальність щодо здійснення контролю за створенням, розвитком, підтримкою, використанням*

*безпеки активів та ресурсів СУІБ. Термін «Власник» не означає, що особа дійсно має право власності на активи/ресурс/ризик СУІБ.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***