*ЗАТВЕРДЖЕНО*

*Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА КРИПТОГРАФІЇ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика криптографії виконавчого комітету Криворізької міської ради (надалі – Політика криптографії) є документом, що встановлює правила використання засобів криптографічного захисту інформації (надалі – КЗІ), здійснення контролю за їх обігом, а також визначення правил використання криптографічних ключів з метою захисту конфіденційності та цілісності інформаційних активів (надалі – ІА), що оброблюються в інформаційно-комунікаційній системі (надалі – ІКС) виконкому міської ради в межах виконання робочого процесу, побудованого на базі компонентів ІКС в межах області дії системи управління інформаційною безпекою (надалі – СУІБ) для надання послуг:

1.1.1 з розробки та супроводження системи програмного продукту;

1.1.2 технічної та клієнтської підтримки з метою підвищення ефективності роботи виконавчих органів міської ради, комунальних підприємств, установ, організацій, що належать до комунальної власності Криворізької міської територіальної громади.

1.2. Політика криптографії розроблена з метою виконання вимог чинного законодавства в галузі КЗІ, а також впровадження заходів з контролю доступу до засобів КЗІ [(уключаючи засоби кваліфікованого електронного підпису (на-далі – КЕП)] із застосуванням ризикорієнтованого підходу на всіх етапах життєвого циклу СУІБ для захисту конфіденційності та цілісності активів.

1.3. Політика криптографії застосовується до всієї інформаційної діяльності виконкому міської ради, пов’язаної з:

1.3.1 обробкою конфіденційної інформації (включаючи обробку персональних даних) для захисту її конфіденційності;

1.3.2 обробкою відкритої інформації для захисту її цілісності;

1.3.3 використанням засобів КЗІ, криптографічного ключа та засобів КЕП в області дії СУІБ.

1.4. Політика криптографії 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», «Про електронні довірчі послуги», 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», «Правила забезпечення захист інформації в інформаційних, телекомунікаційних

та інформаційно-комунікаційних системах», затверджені Постановою Кабінету Міністрів України від 29 березня 2006 року № 373 (надалі – Постанова КМУ №373), 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: D00DI-СУІБ Порядок оформлення документів та контроль записів, D4.1-СУІБ «Політика інформаційної безпеки», D2.2-СУІБ «Політика управління активами», D8.1-СУІБ «Положення щодо інвентаризації та обробки даних», D10-СУІБ «Методологія оцінки та обробки ризиків», D14.6-СУІБ «Політика класифікації інформації», D14.14-СУІБ «Політика контролю доступу», D14.11-СУІБ «Політика утилізації та знищення».

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

2.1. Власник криптографічного ключа — відповідальна особа, яка працюватиме з криптографічним ключем під час виконання службових обов’язків для забезпечення шифрування/розшифрування інформації, підтвердження її справжності, цілісності, авторства тощо. Якщо криптографічний ключ використовується інформаційною системою, то власником цього ключа є адміністратор цієї системи.

2.2. Відкритий КЕП – це параметр криптографічного алгоритму перевірки кваліфікованого електронного підпису, доступний суб'єктам відносин у сфері використання цифрового підпису.

2.3. Дешифрування – процес перетворення інформації із застосуванням криптографічних алгоритмів у придатну для читання інформацію.

2.4. Засвідчувальний ключ надавача електронних довірчих послуг (надалі – КНЕДП) – таємний ключ, що використовується кваліфікованим надавачем електронних довірчих послуг для накладання електронного цифрового підпису на сертифікат ключа.

2.5. Засоби генерації криптографічних ключів – програмний комплекс, що забезпечує введення персональних даних підписантів, генерацію та збереження ключів на носії, формування і передачу запитів на сертифікацію до КНЕДП.

2.6. Засоби криптографічного захисту інформації – програмні, апаратно-програмні, апаратні або інші засоби, призначені для криптографічного захисту інформації.

2.7. Захищений інформаційний обмін – відправлення, отримання та передача електронного документа (надалі – ЕД), що здійснюється користувачем кваліфікованих електронних довірчих послуг в електронній формі за допомогою

використання технологій шифрування або за умови дотриманням вимог політик СУІБ шляхом відправлення електронних носіїв, на яких записано цей документ.

2.8. Імітозахист – захист системи шифрувального зв’язку від нав’язування хибних даних.

2.9. Інформаційно комунікаційна система (надалі – ІКС) – інформаційно комунікаційна система виконкому міської ради, компоненти якої виконують функції для забезпечення інформаційної діяльності.

2.10. КЕП – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити істинність ЕД, його цілісність, авторство тощо. КЕП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

2.11. Компрометація особистого ключа – будь-яка подія й/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа.

2.12. Користувач сертифіката ключа – фізична особа, яка використовує сертифікат ключа КЕП.

2.13. Криптографічний алгоритм – алгоритм, що визначає правила перетворення інформації з метою її криптографічного захисту.

2.14. КЗІ – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою захисту конфіденційності ІА шляхом приховання (або відновлення) змісту інформації.

2.15. Криптографічні ключі – таємні та відкриті ключі призначені для накладання/перевірки КЕП, шифрування/дешифрування ЕД.

2.16. Кваліфіковані електронні довірчі послуги – електронні довірчі послуги, що надаються кваліфікованим надавачом електронних довірчих послуг відповідно до [Закону України](https://zakon.rada.gov.ua/laws/show/2155-19) «Про електронні довірчі послуги».

2.17. КНЕДП – кваліфікований надавач електронних довірчих послуг.

2.18. Особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписанту ЕД.

2.19. Підписант – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає КЕП на ЕД.

2.20. Симетричні криптографічні ключі — криптографічні ключі, що використовуються в симетричних криптографічних алгоритмах (шифрування, створення кодів автентифікації повідомлень тощо). Головна властивість симетричних ключів: для виконання як прямого, так и зворотного криптографічного перетворення (шифрування та розшифрування даних, обчислення і перевірки MAC-підпису) необхідно використовувати той самий ключ.

2.21. Система криптографічного захисту інформації (надалі – СКЗІ) – сукупність робочої інфраструктури, організаційно-технічних заходів та засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи

безпеки), використання якої забезпечує належний рівень захищеності інформації, що обробляється, зберігається і (або) передається.

2.22. Сертифікат відкритого ключа КЕП – документ, виданий КНЕДП, який засвідчує чинність і належність відкритого ключа підписувачу ЕД.

2.23. Сертифікація ключа КЕП – формування сертифіката відкритого ключа, заснованого на перевірці реєстрації даних та накладанні на сертифікат ключа КЕП.

2.24. Таємні ключі – ключові дані, призначені для накладання КЕП та шифрування ЕД.

2.25. Шифрування – перетворення електронного документа (даних) із застосуванням криптографічних алгоритмів з метою захисту його (їх) змісту.

2.26. Хешування — криптографічне перетворення даних довільного об’єму у рядок фіксованої довжини. Використовується переважно для створення кодів автентифікації повідомлення, контрольних сум, а також на одному з етапів створення КЕП.

2.27. [MAC-підпис](https://uk.wikipedia.org/wiki/MAC-%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81) — маленький шматок інформації, використовний для [автентифікації](https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F) повідомлення.

2.28. Актив – активом є все, що має цінність для виконкому міської ради й потребує захисту [інформаційний актив, апаратне забезпечення, програмне забезпечення, 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)].

2.29. 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.\*

2.30. 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.

2.31. Єдина інформаційна система міста Кривий Ріг (надалі – 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.

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

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

2.34. 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.

2.35. 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.

2.36. Інформаційно-комунікаційна система (надалі – ІКС) – до складу якої належить комплекс апаратних, програмних, апаратно–програмних (фізичних та/або віртуальних) телекомунікаційних засобів, призначених для маршрутизації, комутації, зберігання, приймання, передавання інформації між кінцевим обладнанням ІКС у межах виконання цілей виконкому міської ради.

2.37. PII – персональні дані.

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

2.39. 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.

2.40. Рівень конфіденційності (надалі – РК) – надається інформаційним активам з метою обмеження доступу відповідно до правил розмежування доступу з урахуванням контексту виконкому міської ради та схеми класифікації інформації, що визначена в Політиці класифікації інформації.

2.41. Комунікаційний протокол – це обумовлені наперед правила передачі [інформації](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) між двома пристроями [комунікаційної системи](https://uk.wikipedia.org/w/index.php?title=%D0%9A%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0&action=edit&redlink=1). Протокол визначає правила, [синтаксис](https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BD%D1%82%D0%B0%D0%BA%D1%81%D0%B8%D1%81), [семантику](https://uk.wikipedia.org/wiki/%D0%A1%D0%B5%D0%BC%D0%B0%D0%BD%D1%82%D0%B8%D0%BA%D0%B0_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), [синхронізацію](https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BD%D1%85%D1%80%D0%BE%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F) [комунікації](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F) і можливі методи [виявлення та виправлення помилок](https://uk.wikipedia.org/wiki/%D0%92%D0%B8%D1%8F%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F_%D1%82%D0%B0_%D0%B2%D0%B8%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F_%D0%BF%D0%BE%D0%BC%D0%B8%D0%BB%D0%BE%D0%BA).

#### *3. Політика використання шифрування*

3.1. CSO оцінює ризики, пов’язані з обробкою та зберіганням даних, і запроваджує криптографічний контроль для пом’якшення цих ризиків, де це буде вважатися доцільним. Там, де використовується шифрування, упроваджується та задокументовується надійна криптографічна робота з відповідними процесами й процедурами керування ключами. Все шифрування має виконуватися відповідно до галузевих стандартів.

3.2. Для всіх PII CSO та DPO ураховують сучасний рівень, витрати на впровадження, характер та обсяг здійснених заходів, контекст і цілі обробки інформації, особливу увагу приділяють захисту PII тощо відповідно до D14.6-СУІБ «Політика класифікації інформації».

3.3. DPO оцінює ризик різної ймовірності та тяжкості для прав і свобод фізичних осіб, а також контролює повноту й ефективність упроваджених

відповідних технічних та організаційних заходів щодо псевдонімізації та шиф-рування даних, щоб створити рівень безпеки, відповідний ризику.

3.4. Для всього трафіку, що надсилається через загальнодоступну мережу «Інтернет» і містить інформацію з рівнем конфіденційності:

3.4.1 РК1 та PK3 використовують лише безпечні комунікаційні протоколи, такі як «IPsec», «SSL/TLS», «SSH» (стандарт для зашифрованого мережевого зв’язку) і лише надійні криптографічні алгоритми для зберігання та обробки інформації;

3.4.2 PK2, PK4 використовують лише безпечні комунікаційні протоколи, такі як «IPsec», «SSL/TLS», «SSH» (стандарт для зашифрованого мережевого зв’язку) і лише надійні криптографічні алгоритми для зберігання та обробки інформації з обов’язковим виконанням таких додаткових засобів захисту: усі ІА з PK2, PK4, що передаються з однієї системи до іншої через незахищене середовище (каналами мережі «Інтернет»), мають бути захищені (вимога пункту 13 Постанови КМУ №373) з використанням засобів КЗІ, що забезпечують шифрування інформації з обмеженим доступом (надалі – ІзОД) та мають експертний висновок від Адміністрації Держспецзв’язку України. Політика криптографії, що реалізується комплексом захисту засобів (надалі – КЗЗ) СУІБ, дозволяє автоматизовану передачу ІзОД через незахищене середовище лише з використанням технології шифрування. Обмін ІзОД за межі КЗ також можливо здійснювати з використанням з'ємних носіїв інформації з дотриманням вимог політик СУІБ;

3.4.3 Під час передачі ІА з PK1, PK2, PK3, PK4 в межах контрольованої зони шифрування ІзОД здійснюється.

3.5. Процес використання шифрування: відповідно до D14.6-СУІБ «Політика класифікації інформації», а також юридичних та договірних зобов'язань, виконком міської ради має захищати критичні інформаційні системи/активи та інформацію за допомогою таких криптографічних засобів:

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Сервіс/система*** | ***Метод захисту*** |
| 1 | Робочі станції користувачів інформаційно-комунікаційних систем | Шифрування жорсткого диску |
| 2 | Віддалений доступ | VPN |
| 3 | ЗНІ з рівнем конфіденційності РК1, РК3 | Шифрування ІА |
| 4 | Матеріальні носії інформації із рівнем конфіденційності РК2, РК4 | Застосування засобів КЗІ, які мають чинний експертний висновок від Адміністрації Держспецзв’язку України, що дозволяє захищати ІА за допомогою використання технології шифрування саме цього виду ІА |
| 5 | Дані міжсистемної взаємодії (інформаційний обмін) | TLS від v.1.1 і вище |
| 6 | WEBресурси (сайти, портали) | SSL сертифікати |

3.6. При цьому використовуються такі криптографічні алгоритми:

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Алгоритм шифрування*** | ***Розмір ключа*** |
| 1 | AES 256 | 256 біт |
| 2 | AES 128 GCM | 2048 біт (RSA) |
| 3 | SHA-2 | 256 та вище |
| 4 | SHA-3 | 256 та вище |
| 5 | ECDSA | 224 |
| 6 | RSA | 2048 |
| 7 | DSS | 2048 |

3.7. Керівник групи КЗІ несе відповідальність за наявність детальних інструкцій з використання криптографічних засобів, облік та застосування засобів КЗІ у відповідності до вимог політик СУІБ.

3.8. Керівник групи КЗІ відповідає за контроль наступних процесів, що стосуються управління ключами:

3.8.1 генерація приватних та публічних криптографічних ключів;

3.8.2 активація та розподіл криптографічних ключів;

3.8.3 визначення терміну використання ключів та їх регулярне оновлення (згідно з оцінкою ризику);

3.8.4 архівування неактивних ключів, необхідних для зашифрованих електронних архівів;

3.8.5 знищення ключів;

3.8.6 дійсність КЕП та виконання заходів захисту щодо Політики криптографії.

3.9. Ключі керуються їх власниками відповідно до вимог, що зазначені для кожної системи, де використовуються ключі. Власники активів, до яких застосовуються окремі криптографічні засоби захисту, несуть відповідальність за їх належне використання.

3.10 CSO відповідає за постійний контроль щодо використання засобів криптографічного захисту.

3.11. CIO відповідає за працездатність та безперервність функціонування засобів криптографічного захисту.

3.12. Керівник SOC несе відповідальність за застосування засобів КЗЗ та виконання правил розмежування доступу до активів.

3.13. Визначаються властивості, атрибути й процедури, що можуть використовуватися для однозначного підтвердження належності об'єкта захисту незалежною стороною – КНЕДП. Установлення належності виконується на підставі протоколу автентифікації. Політика автентифікації відправника, що реалізується КЗЗ здійснюється шляхом використання технології шифрування та сервісів кваліфікованих електронних довірчих послуг, що дозволяє виконати політику безпеки в частині забезпечення неспростовності авторства відправника електронних даних та документів, що циркулюють у ІКС з використанням цифрового підпису.

#### *4. Призначення й принципи побудови системи криптографічного захисту інформації*

4.1. При укладанні договорів з юридичними та фізичними особами, що використовують/постачають засоби КЗІ, одним з пунктів зазначається, що сторони визнають КЕП, що є аналогом власноручному підпису в документі на паперовому носії.

4.2. Під час проведення заходів з побудови СУІБ, у межах якої передбачається передача/прийом відкритими каналами зв’язку PII, мають бути передбачені заходи та засоби із захисту конфіденційності PII, що базуються на використанні технологій та засобів КЗІ, що мають сертифікат відповідності або позитивний експертний висновок від Адміністрації ДержСпецзв’язку України за результатами експертизи у сфері КЗІ.

4.3. Застосування КЕП дозволяє захистити цілісність та неспростовність ІА, що підлягає захисту у ІКС виконкому міської ради у межах області дії СУІБ.

4.4. КНЕДП забезпечує виконання таких функцій:

4.4.1 генерація криптографічних ключів КНЕДП та підписантів;

4.4.2 сертифікація відкритих ключів КЕП;

4.4.3 ведення електронного переліку діючих, відкликаних і блокованих сертифікатів ключів;

4.4.4 забезпечення доступу користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів;

4.4.5 забезпечення зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

4.4.6 управління сертифікатами ключів КЕП.

4.5. Центр реєстрації КНЕДП забезпечує виконання таких функцій:

4.5.1 генерація криптографічних ключів підписантів;

4.5.2 формування запитів на сертифікацію відкритих ключів підписантів;

4.5.3 накладання КЕП на запити на сертифікацію відкритих ключів засвідчувальним ключем КНЕДП;

4.5.4 управління сертифікатами ключів КЕП підписантів.

4.6. Для вирішення завдань КЗІ в межах області дії СУІБ створюється СКЗІ.

4.7. СКЗІ є універсальним механізмом організації безпеки ІА. Наявність СКЗІ в складі СУІБ розглядається як необхідна умова в межах області дії СУІБ. У рамках керування засобами КЗІ вирішуються завдання:

4.7.1 захист від нав'язування хибної інформації;

4.7.2 захист інформації від навмисних і ненавмисних викривлень;

4.7.3 автентифікація джерел і приймачів інформації;

4.7.4 шифрування змісту інформації при передачі відкритими каналами зв'язку;

4.7.5 забезпечення персональної відповідальності виконавців за формування та обробку інформації.

4.8. Принципи створення СКЗІ:

4.8.1 СКЗІ будується на основі використання технологій КЗІ та засобів КЗІ, що мають сертифікат відповідності або позитивний експертний висновок за результатами експертизи в сфері КЗІ;

4.8.2 порядок побудови й функціонування СКЗІ враховує технологічні й архітектурні особливості в ІКС й не повинен суперечити стратегічним напрямам розвитку виконкому міської ради;

4.8.3 архітектура СКЗІ, порядок її функціонування в складі в ІКС мають відповідати вимогам захисту ІА;

4.8.4 СКЗІ має універсальну масштабовану й гнучку підсистему керування криптографічними ключами, що не залежить від технологічних, архітектурних і функціональних особливостей в ІКС;

4.8.5 СКЗІ забезпечує весь спектр криптографічних функцій (шифрування, КЕП):

4.8.6 порядок функціонування СКЗІ, обов'язки користувачів та персоналу служби захисту інформації, що забезпечує роботу засобів КЗІ, правила роботи виконавців із засобами КЗІ регламентуються внутрішніми організаційно-технічними документами.

#### *5. Об'єкти й методи криптографічного захисту інформації*

5.1. Об'єктами СКЗІ є функціонуючі в ІКС засоби КЗІ та КЕП, за допомогою яких обробляється інформація, що належить до таких категорій:

5.1.1. ІзОД чутлива (PII з РК2 та технічний захист інформації з РК4);

5.1.2 відкрита інформація, що потребує захисту щодо цілісності (з РК1);

5.1.3 інша інформація, що потребує захисту конфіденційності (з РК3).

5.2. У СКЗІ використовуються такі методи:

5.2.1 автентифікація виконавців при підключенні до СКЗІ;

5.2.2 автентифікація джерел і приймачів інформації;

5.2.3 накладання КЕП підписантами ЕД та контроль автентичності ЕД шляхом перевірки КЕП при кожному звернені до них;

5.2.4 шифрування інформації з обмеженим доступом при передачі відкритими каналами зв'язку, дешифрування та контроль цілісності даних (файлів) при прийомі.

#### *6. Структура системи криптографічного захисту інформації*

6.1. СКЗІ складається з таких підсистем:

6.1.1 підсистеми керування криптографічними ключами й сертифікатами ключів;

6.1.2 підсистема шифрування;

6.1.3 підсистеми організаційно-технічного захисту.

6.2. Підсистема керування криптографічними ключами й сертифікатами:

6.2.1 підсистема керування криптографічними ключами й сертифікатами призначена для генерації криптографічних ключів, формування сертифікатів і забезпечення гарантованої своєчасної та безпечної доставки й обробки ключових повідомлень;

6.2.2 підсистема керування криптографічними ключами й сертифікатами забезпечує єдність технологій і засобів генерації, розподіл і застосування сертифікатів відкритих ключів в автоматизованих системах різного призначення;

6.2.3 заходи з використання КЕП та технології підпису ЕД здійснюються відповідно до Постанови Кабінету Міністрів України від 01 серпня 2023 року №798 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності».

6.3. Елементами підсистеми керування криптографічними ключами й сертифікатами є:

6.3.1 КНЕДП;

6.3.2 засоби генерації криптографічних ключів.

6.4 КНЕДП є основним елементом підсистеми керування криптографічними ключами та сертифікатами і призначений для організації, забезпечення функціонування й розвитку СКЗІ в цілому. КНЕДП призначений для ідентифікації виконавців, генерації для них криптографічних ключів, сертифікації ключів, керування сертифікатами. Функціонування КНЕДП організується відповідно до вимог Положення про КНЕДП, при цьому до складу ІКС не належить.

6.5. Підсистема шифрування призначена для автентифікації джерел і приймачів інформації, криптографічного перетворення даних з метою приховання їх змісту, забезпечення перевірки дійсності, цілісності та неспростовності інформації. Основними функціями підсистема шифрування є:

6.5.1 автентифікація (установлення дійсності) підписантів, технічних засобів і повідомлень, що беруть участь в обміні даними;

6.5.2 криптографічне перетворення інформації (шифрування), що передається каналами зв'язку або збереженої на носіях інформації;

6.5.3 авторизація даних (формування КЕП з метою забезпечення неспростовності, запобігання модифікації та підробки даних).

6.6. Елементами підсистеми шифрування є:

6.6.1 програмні засоби КЕП, шифрування та імітозахисту даних, що працюють під керуванням програмних засобів ІКС;

6.6.2 автономні програмні (програмно-апаратні) засоби, що реалізують функції автентифікації та шифрування даних;

6.6.3 таємні ключі, захищені носії інформації із ЗНКД і діючі таблиці сертифікатів відкритих ключів.

6.7. Підсистема організаційно-технічного захисту призначена для регламентації порядку створення й функціонування СКЗІ в цілому та окремих її елементів. Основу підсистеми організаційно-технічного захисту складають внутрішні нормативні документи з питань КЗІ. Цими документами встановлюються:

6.7.1 загальні вимоги до порядку генерації криптографічних ключів, керування та застосування сертифікатів ключів;

6.7.2 вимоги до організації обліку, зберігання й знищення таємних ключів, носіїв з таємними ключами, звітно-реєстраційних документів щодо керування криптографічними ключами та захисту даних;

6.7.3 порядок організації роботи посадових осіб виконкому міської ради з ключовими носіями та інформацією, що підлягає криптографічному захисту;

6.7.4 порядок дій посадових осіб виконкому міської ради в аварійних ситуаціях і при компрометації таємних ключів;

6.7.5 порядок контролю дотримання технологічної дисципліни генерації та зберігання таємних ключів, розподіл і застосування сертифікатів ключів;

6.7.6 вимоги до організації контролю виконання нормативних і організаційно-технічних вимог з питань КЗІ;

6.7.7 порядок організації безпеки під час експлуатації засобів КЗІ;

6.7.8 Політика використання, захисту й часу життя криптографічних ключів для всього їх життєвого циклу;

6.7.9 порядок генерації ключових документів та поводження з ключовими документами;

6.7.10 Положення про підрозділ КЗІ.

6.7.11 Порядок дій на випадок компрометації таємних ключів.

6.7.12 Порядок використання таємних ключів.

#### *7. Основи організації та забезпечення функціонування системи криптографічного захисту інформації*

7.1. СКЗІ в ІКС створюється на базі засобів КЗІ. Призначення, функції, організація взаємодії засобів КЗІ, порядок їх установки, налагодження та функціонування описуються у відповідних експлуатаційних документах на засоби КЗІ.

7.2. З метою виключення можливості ослаблення криптографічних і інших властивостей СКЗІ доробка засобів КЗІ, адаптація їх до умов застосування в ІКС та сервісне обслуговування здійснюється винятково розробником/постачальником засобів КЗІ. Унесення будь-яких змін у програмні засоби КЗІ іншими особами забороняється.

7.3. РК таємних ключів та ЗНКД із цими ключовими даними визначається не нижче ніж рівень критичності ІА, що шифруються.

7.4. Інформація з питань організації та забезпечення функціонування СКЗІ, що передається відкритими каналами зв'язку, обов'язково шифрується та має позначення рівня конфіденційності.

#### *8. Порядок допуску до СКЗІ та обов'язки користувачів*

8.1. До роботи із засобами підсистеми керування ключами й сертифікатами допускаються тільки керівник (адміністратор) служби КЗІ та адміністратори безпеки (із числа посадових осіб, які входять до складу SOC).

8.2. До роботи із засобами КЗІ підсистеми шифрування [станцій автоматизованих систем із засобами КЗІ, ключові дані (надалі – КД)], допускаються наступні ІКС, які в межах СУІБ визначаються як уповноважені особи що:

8.2.1 за посадовими обов'язками мають право обробки інформації, що належить до відповідних ІзОД;

8.2.2 вивчили правила роботи із засобами КЗІ;

8.2.3 вивчили правила поводження із ключовими даними та ЗНКД;

8.2.4 підписали зобов’язання (додаток 1).

8.3. Уповноважені особи, допущені до роботи із засобами КЗІ, мають затверджені функціональні обов'язки, що визначають персональну відповідальність за дотримання порядку поводження з програмними засобами КЗІ, які перебувають у їх користуванні, КД, ЗНКД, документацією й листуванням з питань КЗІ.

8.4. Уповноважені особи, допущені до роботи із засобами КЗІ, несуть відповідальність за збереження й нерозголошення змісту довірених їм відомостей, документів і даних щодо КЗІ. Уповноважені особи, допущені до роботи із засобами КЗІ, зобов'язані:

8.4.1 виконувати вимоги організаційних і технічних документів щодо забезпечення КЗІ та своїх функціональних обов'язків;

8.4.2 не допускати спроби порушення порядку доступу до інформації, що обробляється в ІКС і потребує захисту;

8.4.3 вчасно повідомляти безпосередньому керівнику відділу, управління, іншого виконавчого органу міської ради, керівнику групи КЗІ та CSO про всі позаштатні ситуації у функціонуванні засобів КЗІ та про виявлені спроби несанкціонованого доступу до інформації, що захищається.

8.5. Уповноваженій особі забороняється:

8.5.1 копіювати інформацію, що перебуває на носіях інформації із ключовими даними на необліковані носії;

8.5.2 самовільно вносити зміни в організаційні й технічні документи засобів КЗІ, алгоритми функціонування засобів КЗІ, а також у схеми, монтаж і розміщення технічних засобів, на яких установлені засоби КЗІ;

8.5.3 використовувати несправні технічні засоби КЗІ;

8.5.4 самовільно передавати виконання функціональних обов'язків іншим особам.

8.6. CSO відповідає за:

8.6.1 організацію та контроль за роботою щодо створення й розвитку СКЗІ;

8.6.2 забезпечення контролю за застосуванням програмних засобів КЗІ відповідно до вимог затвердженої технології обробки інформації;

8.6.3 розробку й узгодження зі службою КЗІ технологій розподілу та застосування сертифікатів відкритих ключів;

8.6.4 розробку організаційних документів, що регламентують порядок функціонування СКЗІ, обов'язків посадових осіб, що забезпечує роботу засобів СКЗІ, правил роботи виконавців із засобами КЗІ, особистими ключами й сертифікатами ключів;

8.6.5 організацію та забезпечення контролю дотримання технологічного розподілу й застосування ключів і сертифікатів ключів;

8.6.6 організацію та забезпечення контролю дотримання виконання організаційно-технічних вимог СКЗІ;

8.6.7 організацію контролю за функціонуванням засобів СКЗІ;

8.6.8 організацію обліку й поводження з носіями інформації з ключовими даними;

8.6.9 навчання і організацію роботи уповноважених осіб відповідальних за виконання робіт щодо впровадження та забезпечення функціонування СКЗІ;

8.6.10 організацію експлуатації програмно-технічних комплексів КНЕДП;

8.6.11 організацію навчання виконавців правилам поводження з особистими ключами й носіями інформації, на які вони записані;

8.6.12 організацію взаємодії з розробником/постачальником засобів КЗІ;

8.6.13 матеріально-технічне забезпечення СКЗІ;

8.6.14 забезпечення функціонування апаратних засобів та системного програмного забезпечення СКЗІ згідно з вимогами експлуатаційних документів;

8.6.15 функціонування засобів КЗІ в складі ІКС у відповідності до затверджених технологій.

8.7. Керівник (адміністратор) КЗІ здійснює такі функції управління КД:

8.7.1 формування КД;

8.7.2 відкликання КД у зв’язку зі змінами повноважень власників, або компрометацією КД;

8.7.3 за запитами уповноважених осіб підтверджує дійсність КД;

8.7.4 бере участь у вирішенні конфліктних ситуацій, пов’язаних з підтвердженням дійсності КД;

8.7.5 здійснює облік, прийом/видачу, КД та ЗНКД;

8.7.6 виконує інші функції, пов’язані з управлінням КД, обумовлені нормативними документами КЗІ.

#### *9. Порядок обліку, зберігання, прийому/видачі, знищення носіїв із ключовими даними*

9.1. ЗНКД мають спеціальне маркування, що включає обліковий номер та дані власника цього активу. Робити запис КД на необліковані носії інформації забороняється. Відповідальними за облік ЗНКД є: керівник (адміністратор) КЗІ, власники активу.

9.2. Контроль за дотримання вимог щодо обігу КД та ЗНКД здійснює CSO та CISO (за дорученням CSO) у межах повноважень. CSO має здійснювати загальний контроль за ресурсами СУІБ.

9.3. Адміністратор КЗІ виконує такі функції щодо обліку ключових носіїв:

9.3.1 веде загальний облік носіїв призначених для зберігання КД у журналі обліку ключових носіїв (додаток 2);

9.3.2 передає (розсилає) ЗНКД уповноваженим особам;

9.3.3 здійснює видачу КД уповноваженим особам виконкому міської ради;

9.3.4 здійснює контроль за дотриманням порядку поводження з КД.

9.4. Знищення носіїв з КД здійснюється за умови неможливості використання їх у подальшому, у порядку, визначеному для документів, що віднесені до категорії «Конфіденційно». Знищення відбувається за участі комісії, яка створюється розпорядженням CEO та особи, відповідальної за їх облік відповідно Політики утилізації та знищення інформації.

9.5. ЗНКД видаються під розпис уповноваженій особі, функціональними обов’язками якої передбачено використання КД для захист у ІА. ЗНКД

повертаються особі, відповідальній за їх облік, за умови, що КД, які записані на цих носіях виведені з дії.

9.6. Усі КД, що використаються в СКЗІ, за винятком засвідчувальних ключів КНЕДП, є особистими. Особисті ключі записуються тільки на попередньо обліковані ЗНКД, що отримуються під розпис власником активу. За збереження носія із записаним на нього особистим ключем власник активу несе персональну відповідальність.

9.7. Власник активу несе відповідальність за усі документи, підписані його особистим ключем у період дії особистого ключа.

9.8. Період дії особистого ключа визначається відповідним сертифікатом ключа. Відповідальність за планову повторну регенерацію особистого ключа несе власник активу.

9.9. Дія особистого ключа має тимчасово призупинятися (блокуватися) адміністратором КЗІ в зв’язку з відпусткою, хворобою, чи з інших причин, за яких власник активу тимчасово не може виконувати обов’язки.

9.10. Дія особистого ключа достроково зупиняється (відкликання сертифіката ключа) адміністратором КЗІ у зв’язку з компрометацією особистого ключа, звільненням, чи з інших причин, за яких власник активу не має права використовувати особистий ключ та підписувати ЕД.

9.11. Відкликання сертифіката ключа також може відбуватися за ініціативи власника активу (у випадку неможливості зазначеного – його безпосереднього керівника) на підставі документально підтвердженої заяви про виведення особистого ключа з дії.

9.12. Заява подається у двох примірниках на ім'я керівника (адміністратора) КЗІ. У заяві вказуються:

9.12.1 прізвище й ініціали заявника;

9.12.2 посада;

9.12.3 короткий опис причина виведення особистого ключа з дії;

9.12.4 прохання (за необхідності) про генерацію особистих ключів для заміни особистого ключа, що виводиться з дії;

9.12.5 особистий підпис, дата.

9.13. Адміністратор КЗІ після ознайомлення зі змістом заяви, зобов'язаний:

9.13.1 негайно організувати відкликання відповідного сертифіката відкритого ключа;

9.13.2 зазначити на обох примірниках заяви дату, час, з точністю до хвилини, відкликання сертифіката відкритого ключа;

9.13.3 проставити на обох примірниках заяви своє прізвище, ініціали, особистий підпис;

9.13.4 повернути один примірник заяви заявнику;

9.13.5 другий примірник заяви залишити.

9.14. Адміністратор КЗІ аналізує зміст заяви і ухвалює рішення щодо сертифікації нових ключів.

9.15. Якщо за результатами аналізу отриманої заяви виявляється, що причина виведення з дії особистих ключів містить ознаки компрометації ключових даних, адміністратор КЗІ доповідає письмово службовим листом CSO та CEO.

9.16. CSO організовує службове розслідування за фактом компрометації або підозри в компрометації ключів і вживає заходів до локалізації наслідків можливого несанкціонованого використання ключів в ІКС з негайною доповіддю CEO.

#### *10. Умови використання КД*

10.1. Засоби КЗІ повинні експлуатуватися в захищеному програмно-апаратному середовищі, обладнаному засобами розмежування доступу, у відповідності до вимог нормативних документів виконкому міської ради. Зберігання та використання КД гарантує неможливість несанкціонованого використання.

10.2. Посадова особа виконкому міської ради має право на отримання КД за умов, що вона:

10.2.1 має затверджені встановленим порядком функціональні обов’язки, якими передбачено персональну відповідальність щодо використання КД;

10.2.2 отримала встановленим порядком право доступу до засобів КЗІ;

10.2.3 підписала зобов’язання про дотримання правил поводження із засобами КЗІ, передбачене Політикою криптографії;

10.2.4 призначена розпорядженням CEO у відповідності з наданими повноваженнями про допуск до відповідних засобів КЗІ.

10.3. Права на отримання КД затверджуються в порядку, установленому внутрішніми нормативними документами виконкому міської ради. Створення (генерація) КД для використання в ІКС здійснюється власником активу самостійно.

10.4. Порядок оформлення запиту до КНЕДП на сертифікат відкритого ключа КЕП, що використовує засоби КЗІ, визначається договірними відносинами з КНЕДП. Сертифікація відкритого ключа КЕП здійснюється адміністратором КНЕДП, якщо іншими нормативними документами не визначений інший порядок. КД на ЗНКД повинні зберігати у формі, що дає змогу перевірити їх цілісність та ідентифікувати власника активу. Оригіналом ЕД з КЕП вважається ЕД з обов'язковими реквізитами, у тому числі з КЕП власника активу, який підписав цей ЕД.

10.5. Справжність КЕП, накладеного на ЕД або інші ЕД, та цілісність цього документа (даних) перевіряється з дотриманням таких вимог:

10.5.1 КЕП підтверджується з використанням відповідного сертифіката ключа за допомогою засобів КЗІ;

10.5.2 під час перевірки має використовуватися сертифікат ключа, чинний на момент накладення КЕП;

10.5.3 особистий ключ підписанта має відповідати відкритому ключу, зазначеному у сертифікаті;

10.5.4 на час перевірки повинен бути чинний сертифікат відкритого ключа КНЕДП.

10.6. У випадку виявлення компрометації ключа КЕП, його власник зобов’язаний негайно повідомити про це відповідному адміністратору КЗІ та припинити використання скомпрометованого ключа.

*\*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***