*ЗАТВЕРДЖЕНО*

*Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА УПРАВЛІННЯ ЗМІНАМИ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика управління змінами виконавчого комітету Криворізької міської ради (надалі – Політика управління змінами) є документом для опису всіх заходів, пов'язаних з ініціюванням, упровадженням та збереженням записів про виправлення/корекцію невідповідностей або аномалій, а також виконання коригувальних дій у підсистемах Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС) та здійснення контролю ефективності та результативності проведених змін відповідно до політик системи управління інформаційною безпекою (надалі – СУІБ).

1.2. Політика управління змінами має на меті мінімізувати ризик негативних наслідків, спричинених змінами програмного забезпечення, мережі (складу та топології) або апаратного забезпечення ЄІС, окреслюючи процедури, яких слід дотримуватися під час упровадження змін, таким чином забезпечуючи їх правильне впровадження.

1.3. Політика управління змінами застосовується до всієї області дії СУІБ, а саме:

1.3.1 процесів та інформації, що обробляється в ЄІС;

1.3.2 мереж, пристроїв та засобів обробки інформації, якими володіють або користуються користувачі ЄІС, підрядники, консультанти, постачальники, партнери та інші користувачі, що пов’язані з діяльністю виконкому міської ради або іншими особами, які використовують чи отримують доступ до сервісів ЄІС у межах області дії СУІБ.

1.4. Політика власного пристрою розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу інформаційної безпеки, а саме: ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ EN ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки», ДСТУ ISO 31000:2018 (ISO 31000:2018, IDT) «Менеджмент ризиків. Принципи та настанови», 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», D14.10-СУІБ «Політика резервного копіювання», D14.14-СУІБ «Політика контролю доступу», D14.18-СУІБ «Політика безпечної розробки», D20-СУІБ «Процедура коригуючих дій».

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

2.1. 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)].

2.2. 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.\*

2.3. 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.

2.4. 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.

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

2.6. Chief Security Officer (надалі – CSO) – відповідальний за інформаційну безпеку, 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.

2.7. 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.

2.8. 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.

2.9. 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.

2.10. PII – персональні дані.

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

2.12. Ad1 – адміністратор безпеки.

2.13. Ad2 – адміністратор системи.

2.14. Chief Human Resources Officer (надалі – CHRO) – відповідальна особа за кадрову політику.

2.15. Зацікавлені сторони – це фізичні або юридичні особи, які можуть впливати або на яких може вплинути інформаційна діяльність виконкому міської ради. Зацікавленими сторонами вважаються:

2.15.1 органи державної влади України та за кордоном, у тому числі регуляторний орган, що здійснює державне регулювання у сферах енергетики та комунальних послуг;

2.15.2 органи місцевого самоврядування;

2.15.3 суспільство, громадські організації, міжнародні організації, міжнаро-дні фінансові інституції, медіа, ділові, експертні та галузеві об’єднання, компанії енергетичного чи суміжних секторів економіки, дипломатичні кола тощо;

2.15.4 банки, інвестори, рейтингові агентства;

2.15.5 суб’єкти PII, процесори PII, підпроцесори PII, співконтролери PII, акціонери/власники бізнесу;

2.15.6 інші учасники інформаційного обміну, постачальники послуг/сервісів (у тому числі хмарних), провайдери та партнери, постачальники баз даних.

2.16. Реєстр ризиків – це сховище, у якому зберігають результати процесів управління ризиками. Інформація в реєстрі ризиків може містити дані про особу, відповідальну за управління ризиком, імовірність, вплив, оцінку ризику, заплановані заходи реагування на ризики та іншу інформацію, що використовують для отримання загального розуміння окремих ризиків.

2.17. ПЗ – програмне забезпечення.

#### *3. Завдання, обов’язки, відповідальність*

3.1. Основними завданнями, що вирішуються під час унесення змін/коригувань є уникнення критичних помилок і простоїв, спричинених змінами в

документації СУІБ (опис процесів, планів, правил, обмежень, відповідальності тощо), та основних компонентах підсистем ЄІС, мережевому обладнанні, апаратно-програмному/програмному забезпеченні постачальників (постачальники програмного забезпечення та сервісів), а також проведення постійного моніторингу відповідності СУІБ вимогам керівних документів та проведення певних заходів у разі появи невідповідності або аномалій.

3.2. Коригувальна дія може бути ініційована будь-якою посадовою особою або у відповідних випадках зацікавленою стороною (постачальником, партнером), внутрішніми аудиторами відповідно до процедур D20-СУІБ «Процедура коригуючих дій». Коригувальна дія може вимагати внесення змін до будь-якого документа СУІБ, процесу або компоненту ЄІС у межах області дії СУІБ.

3.3. Результат процесу внесення змін – зміни виконано при чіткому розумінні невідповідності або кінцевої мети проведення покращення СУІБ з урахуванням ризикорієнтованого підходу.

3.4. CSO або за його дорученням CISO відповідають за санкціонування запитів на зміни та забезпечення їх виконання відповідно до політик СУІБ.

3.5. CSO відповідає за:

3.5.1 надання консультацій та іншої допомоги для забезпечення придбання інформаційних технологій управління інформаційними ресурсами в спосіб, що відповідає законам, директивам, політикам, положенням та пріоритетам, установленим цілям виконкому міської ради в межах області дії СУІБ;

3.5.2 розробку, підтримку та сприяння впровадженню надійної інтегрованої архітектури інформаційних технологій для ЄІС;

3.5.3 сприяння ефективному дієвому дизайну та експлуатації всіх основних процесів управління інформаційними ресурсами виконкому міської ради, включаючи вдосконалення робочих процесів.

3.6. CSO контролює дотримання заходів інформаційної безпеки в ЄІС у належному стані та веде всебічний систематичний жорсткий контроль на всіх етапах проведення змін (планування, контроль за наявними ресурсами та шляхами їх постачання, формування технічних вимог, проєктування, упровадження, випробування або тематичне тестування, введення в експлуатацію тощо).

3.7. DPO несе відповідальність за оновлення та актуальність усіх документів і процесів стосовно обробки PII у межах області дії СУІБ.

3.8. CISO персонально відповідає за проведення змін у складі комплексу засобів захисту (надалі – КЗЗ), включаючи зміни в налаштуванні модулів КЗЗ.

3.9. CISO несе персональну відповідальність за проведення організаційно-технічних заходів у межах сфери застосування СУІБ:

3.9.1 унесення змін, їх ідентифікацію та реєстрацію значних змін, за яких має переглядатися Політика ІБ (затверджено рішенням виконкому міської ради від 23.05.2025 №680) та реєстр ризиків;

3.9.2 планування та тестування змін з застосуванням ризик-орієнтовного підходу без порушення безперервності робочих процесів у продуктивному середовищі ЄІС;

3.9.3 проведення заходів щодо оцінки потенційних впливів на інформаційну безпеку;

3.9.4 контроль процедур та офіційного оформлення запропонованих змін, відповідно до Політики безпечної розробки ПЗ;

3.9.5 перевірку стану СУІБ для підтвердження факту, що вимоги ІБ виконуються;

3.9.6 доведення до відома всіх відповідальних осіб змісту зміни;

3.9.7 виконання процедур усунення несправностей та аномалій;

3.9.8 відновлення працездатності ЄІС у разі проведення невдалих змін та виникнення непередбачуваних подій;

3.9.9 упровадження та виконання аварійних процедур унесення змін для забезпечення швидкого контрольованого впровадження змін, необхідних для усунення інциденту.

3.10. CISO контролює відділи, управління, інші виконавчі органи міської ради в межах області дії СУІБ з приводу того, що зміни в компонентах ЄІС впроваджено й проведено їх тестування відповідно до вимог політик СУІБ.

3.11. CIO відповідає за проведення змін у функціональних компонентах ЄІС та перевірку впровадження і тестування змін відповідно до вимог політик з дотриманням правил ризик-менеджменту без порушення безперервності робочих процесів у продуктивному середовищі ЄІС.

3.12. Користувачі ЄІС та посадові особи виконкому міської ради, що мають певну роль у СУІБ, у разі виявлення невідповідністі або аномалії, зобов’язані вжити негайних заходів з виправлення і взяття під контроль ситуації з обов’язком дотримання політик безпеки СУІБ, а також виконати дії з оповіщення керівника свого відділу, управління, іншого виконавчого органу міської ради для найскорішого усунення наслідків. Якщо невідповідність або аномалія не входять до зони відповідальності цієї посадової особи, то вона повинна направити інформацію про виявлену невідповідність або аномалію до CSO/CISO/CIO/власника активу або DPO, якщо це стосується обробки PII.

3.13. Відповідальна посадова особа оцінює необхідність усунення причин невідповідності для подальшого запобігання її повторенню, уживаючи коригувальні дії.

3.14. Постачальники ПЗ відповідають за надання виправлень і оновлень програмного забезпечення в межах договірних умов.

#### *4. Процедура внесення змін в підсистеми ЄІС*

4.1. Зміною вважається встановлення нового програмного забезпечення або нової версії існуючого програмного забезпечення, оновлення драйверів, установлення патчів, зміна конфігурації програмного та апаратного забезпечення (зміна локації, складу основних та допоміжних технічних засобів, ЄІС, технологій щодо обробки інформації), зміна складу КЗЗ.

4.2. Кожну зміну в операційному середовищі ЄІС необхідно вносити таким чином:

4.2.1 зміни можуть бути запропоновані: користувачем ЄІС, CEO, CSO та іншими відділами, управліннями, іншими виконавчими органами міської ради в межах області дії СУІБ;

4.2.2 зміна має бути дозволена CSO, який оцінює її виправданість для цілей інформаційної діяльності та потенційний негативний вплив на активи СУІБ;

4.2.3 зміну має внести Ad1 або Ad2 відповідно до визначених повноважень під контролем CISO чи інша уповноважена посадова особа SOC із залученням відповідального за актив СУІБ, що підлягає зміні;

4.2.4 CISO відповідає за перевірку того, що зміни впроваджено відповідно до вимог політик СУІБ;

4.2.5 CISO сумісно з Ad1 або Ad2 (у межах сфери відповідальності) відповідає за тестування та перевірку цілісності компонентів ЄІС. Компонент, що підлягає зміні, не можна вводити в експлуатацію до проведення ретельного тестування;

4.2.6 про впроваджені зміни CSO повинен доповідати CEO;

4.2.7 CSO відповідає за оновлення та затвердження рішенням CEO всіх документів СУІБ (політики, процедур, планів тощо), на які вплинули зміни;

4.2.8 DPO несе відповідальність за оновлення і затвердження рішенням CEO всіх документів PII (політик, процедур, планів тощо), на які вплинули зміни.

4.3. Будь-які зміни програмного забезпечення, обладнання і конфігурації мережі погоджуються з CEO та CSO через звіт. У разі суттєвих змін у ЄІС, запитується початковий письмовий дозвіл від CEO перш ніж зміни перейдуть на стадію планування.

4.4. У разі впровадження змін у тестовому середовищі, SOC сумісно з власником активу СУІБ проведе оцінку ризиків відповідно до ISO 27005, D10-СУІБ «Методологія оцінки та обробки ризиків» і проводить контрольні заходи з метою підтвердження відповідності СУІБ вимогам ISO 27001.\*\*

4.5. Про впроваджені заходи зі змін у робочому середовищі CSO доповідає CEO.

4.6. Записи про зміни наводяться в супровідній документації СУІБ (формуляр на ЄІС або реєстр активів з визначенням відповідальних за цей актив).

4.7. Зміни можуть бути внесені на підставі розпорядження CEO за результатами планових, контрольних перевірок та внутрішнього аудиту.

4.8. Відомості про проведені зміни необхідно зберігати щонайменше три роки. Відомості про зміни підлягають обліку в журналах перевірок та журналах аудиту.

4.9. У разі виявленні потреб у змінах, пропозиція про них надсилається в письмовій формі електронною поштою CISO, який має зареєструвати та визначити пріоритетність запиту (форма довільна, але якщо потрібно проводити коригування, то застосовується відповідно до D20-СУІБ «Процедура коригуючих дій»). Запит передається на розгляд CSO. CSO за результатами аналізу звітує CEO.\*\*\*

4.10. Запити на зміни зазвичай містять таку інформацію:

4.10.1 область, що потребує змін;

4.10.2 визначена проблема та чому є необхідність у запропонованих змінах;

4.10.3 переваги, що будуть отримані від упровадження змін.

4.11. Аналіз витрат і користі включає визначення та перелік потенційних витрат на запропоновану діяльність і очікувану користь.

4.12. Проводиться оцінка впливу (оцінка ризику) відповідно до D10-СУІБ «Методологія оцінки та обробки ризиків» з метою виявлення інших змін і виявлення потенційних проблем до їх виникнення.

4.13. Після завершення роботи над пропозицією проводиться тестування готового продукту для перевірки негативного впливу на СУІБ чи ЄІС.

4.14. Незалежно від того, чи була зміна здійснена на програмному обладнанні або мережі, тестування проводиться в тестовому (віртуальному) середовищі. Це віртуальне середовище є копією поточної ЄІС (необхідно попередньо зробити резервну копію системи, до якої вносяться зміни відповідно до D14.10-СУІБ «Політика резервного копіювання»), але для тестування використовуються тестові дані, що не містять інформації з обмеженим доступом. Тестування необхідне для виявлення будь-яких потенційних проблем перед упровадженням.

4.15. Виконується перевірка прийнятності користувача (де це можливо) для впевненості, що зміни відповідають кінцевим потребам і очікуванням користувача, перш ніж вони будуть реалізовані в робочому середовищі. CISO зобов’язаний перевірити зміни на відповідність вимогам СУІБ.

4.16. Тестування завжди документується та схвалюється CSO. Після успішного тестування та схвалення зміни впроваджуються за розпорядженням CEO.

4.17. Після внесення змін CSO заповнює відповідний звіт, при цьому власник ризику погоджує факт зниження ризику відповідно до процедури, що зазначена в D10-СУІБ «Методологія оцінки та обробки ризиків».

4.18. Після впровадження змін проводиться перевірка на їх відповідність очікуванням.

4.19. У разі додавання нових галузей до сфери застосування СУІБ, необхідно отримати схвалення CEO. Нові галузі підлягають незалежному аудиту в галузі ІБ на відповідність вимогам ISO 27001, ISO 27701.

4.20. Екстрені зміни відбуваються за процедурою, передбаченою пунктом 4.19, для яких надається найвищий пріоритет унесення змін в найкоротші терміни. Надзвичайні зміни мають пройти етап затвердження на відповідність політикам СУІБ.

4.21. Модифікації пакетів програмного забезпечення підлягають суворому контролю.

4.22. Пакети програмного забезпечення, поставлені виробником (вендором), потрібно використовувати без доробок. У разі, якщо пакети ПЗ потребують модифікації та доопрацювання, слід розглянути таке:

4.22.1 ризик компрометації вбудованих заходів безпеки та процесів контролю цілісності;

4.22.2 чи потрібно отримати згоду виробника (урахувати дотримання авторських прав та умов ліцензійної угоди);

4.22.3 можливість отримання необхідних змін від виробника (вендора) як стандартних оновлень;

4.22.4 вплив того, що виконком міської ради внаслідок змін стає відповідальним за майбутню підтримку ПЗ;

4.22.5 сумісність з іншим ПЗ, що використовується в ЄІС.

4.23. У разі необхідності внесення змін, оригінальне ПЗ має бути збережене (робиться резервна копія), а зміни застосовуються до чітко визначеної копії. Упроваджується процес керування оновленням програмного забезпечення та маркування версій для гарантій, що нові затверджені виправлення та оновлення прикладного ПЗ обліковані й установлені на всьому санкціонованому ПЗ. Усі зміни повністю тестуються та документуються для потреб у майбутніх модернізаціях ПЗ. Усі зміни тестуються та затверджуються CEO.

\**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.*

*\*\*Недостатній контроль змін у засобах обробки інформації зазвичай призводить до збоїв інформаційної діяльності та порушення ІБ. Зміни операційного середовища, особливо при переході системи від етапу розробки до етапу промислової експлуатації, можуть вплинути на надійність прикладних програм і спеціального програмного забезпечення, що використовується для налаштування правил розмежування доступу та комплексу засобів захисту в цілому.*

*\*\*\*Коригувальні дії усувають причину невідповідності, у той час як мета процесу управління змінами – це моніторинг СУІБ на наявність невідповідностей з метою усунення прямих наслідків та виключення їх появи в майбутньому.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***