*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*22.08.2025 №1047*

***ПРОЦЕДУРА КОРИГУЮЧИХ ДІЙ***

***У СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Процедура коригуючих дій у системі управління інформаційною безпекою виконавчого комітету Криворізької міської ради (надалі – Процедура коригуючих дій) є документом, що описує дії, пов’язані з проведенням коригувальних та корекційних дій, а саме: ідентифікація, документування, аналіз та впровадження дій, необхідних для усунення невідповідностей/аномалій та/або проведення корекції для покращення системи управління інформаційною безпекою (надалі – СУІБ).

1.2. Результат Процедури коригуючих дій:

1.2.1 коригувальні дії виконано при чіткому розумінні невідповідності/ей або аномалій у сфері інформаційної безпеки (надалі – ІБ);

1.2.2 корекційні дії виконано при чіткому розумінні кінцевої мети здійснення покращення СУІБ.

1.3. Вимоги Процедури коригуючих дій розповсюджуються на інформаційну діяльність виконкому міської ради, уключаючи дії та процеси з обробки персональних даних (надалі – РІІ) у межах області дії СУІБ.

1.4. Процедура коригуючи дій стосується власників активів, власників ризиків, користувачів Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС), третіх та зацікавлених сторін, що мають відношення до інформаційної діяльності виконкому міської ради, зокрема до обробки РІІ.

1.5. Процедура коригуючих дій 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 27005:2023 (ISO/IEC 27005:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки», ДСТУ ISO 31000:2018 «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), 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», D14.10-СУІБ «Політика резервного копіювання», D14.14-СУІБ «Політика контролю доступу», D14.18-СУІБ «План безперервності бізнесу та аварійного відновлення», D14.9-СУІБ «Політика управління змінами», D15.1-СУІБ «Політика безпеки постачальника».

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

2.1. Аномалія – незначна невідповідність, що характеризується невиконанням вимог внутрішньої документації, але без порушень вимог стандартів, правил, договірних та інших зобов'язань у межах області дії СУІБ. Аномалії можуть бути виявлені в ході внутрішньої чи зовнішньої перевірки, після подій, у ході звичайної господарської діяльності тощо.

2.2. Виправлення – процедура проведення коригувальних або корекційних дій у межах області дії СУІБ.

2.3. Ініціатор – особа (фізична чи юридична), яка виявила невідповідність/аномалію або пропонує шляхи вдосконалення СУІБ щодо, обробки інформаційних активів (включаючи обробку PII) та захисту активів, які можуть вплинути на функціонування СУІБ.

2.4. Корекція – дія, що зосереджується на заходах, пов’язаних з поліпшенням СУІБ виконкому міської ради, і на контролі виявленої невідповідності та усуненні її прямих наслідків.

2.5. Коригувальна дія – це дія для усунення причини виявленої невідповідності/аномалії і запобігання її повторному прояву.

2.6. Корекційна дія – це дія, що передбачає проведення корекції в залежності від ситуації контексту та контенту ініціатора.

2.7. Невідповідність – будь-яка невідповідність вимогам стандартів, внутрішньої документації, нормативних документів, правил, договірних та інших зобов'язань у межах області дії СУІБ. Невідповідності можна виявити під час внутрішнього або зовнішнього аудиту, на основі результатів перевірки керівництва, після інцидентів, під час звичайних операцій або будь-якої іншої події.

2.8. 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)].

2.9. 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 ІБ та кібербезпеку.\*

2.10. 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.

2.11. 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, що забезпечують логічне поєднання визначених інформаційних ресурсів, обробку й захист інформації, внутрішню та зовнішню інформаційну взаємодію.

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

2.13. 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.

2.14. Incident Response Team (надалі – IRT) – група реагування на інциденти.

2.15. 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 в межах області дії СУІБ.

2.16. 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.

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

2.18. PII – персональні дані

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

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

2.19.2 органи місцевого самоврядування та територіальні громади;

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

2.19.4 банки, інвестори, рейтингові агентства;

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

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

2.20. Третя сторона – це фізична або юридична особа, що може вплинути на ІБ та безперервність процесів. У контексті СУІБ третя сторона може не мати створений та зареєстрований акаунт у межах області дії СУІБ. Це можуть бути члени сімей посадових осіб, суб’єктів PII, процесорів PII, підпроцесорів PII, спів-контролерів PII, екстрені служби, консультанти (включаючи юристів, податкових консультантів, консультантів з питань праці тощо), які можуть мати вплив на ІБ в межах області дії СУІБ.

2.21. Контролер PII – фізична або юридична особа, державний орган, агентство або будь–який інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки PII.

2.22. Суб’єкт PII – фізична особа, персональні дані якої обробляються в межах її згоди та якої стосується ідентифікаційна інформація в межах визначеної мети обробки персональних даних, що встановлює склад цих персональних даних та процедури їх обробки, якщо інше не визначено законом.

2.23. Ризик – вплив невизначеності на досягнення цілей.\*\*

#### *3. Коригувальні та корекційні дії*

3.1. Критерії, що можуть сприяти проведенню коригувальних або корекційних дії:

3.1.1 результати аналізу внутрішніх та зовнішніх факторів у межах СУІБ;

3.1.2 зміна відповідності осіб, дотичних до процесу виправлень СУІБ;

3.1.3 зміна контролів СУІБ, які визначаються в положенні про застосовність;

3.1.4 результати обробки ризиків відповідно до критеріїв їх ризиків;

3.1.5 результати перевірок проведених виправлень;

3.1.6 результати перевірок керівництва, внутрішнього аудиту, зовнішнього аудиту, Уповноваженого Верховної Ради України з прав людини, власника ЄІС.

3.2. Визначені критерії можуть призвести до виявлення невідповідності/аномалії або знаходження можливостей покращення СУІБ, що будуть використані для сприяння постійному:

3.2.1 перегляду та усуненню невідповідностей (значні – «major» та незначні – «minor»), аномалій, виявлених під час аудитів третьої сторони (наприклад, сертифікаційних аудитів, наглядових);

3.2.2 перегляду та усуненню невідповідностей (значні – «major» та незначні – «minor»), аномалій, виявлених під час аудитів першої та/або другої сторони (наприклад, внутрішній аудит, перегляд ефективності СУІБ керівництвом у межах області дії СУІБ);

3.2.3 удосконаленню СУІБ.

3.3. Розподіл обов’язків: опис ролевої моделі наведено в таблиці 1.

*Таблиця 1*

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Учасник робочого процесу*** | ***Визначення та склад учасників робочого процесу*** |
| 1 | Ініціатор | Особа, яка в межах повноважень ініціює процес проведення коригувальних або корекційних дій  |
| 2 | Відповідальна особа | Власник активу, власник ризику або користувач ЄІС, у межах повноважень якого було виявлено невідповідність/аномалію або виявлено можливість удосконалення СУІБ |
| 3 | Виконавець | Особа (юридична, фізична, посадова), яка буде залучена до проведення виправлень |
| 4 | CSO | Відповідальний за ІБ, який контролює та бере участь у процесі виправлень у межах області дії СУІБ та перевірки результатів проведених дій |
| 5 | CISO | Керівник групи ІБ є відповідальним за формування та реалізацію стратегій і програм виконкому міської ради із забезпечення та захисту інформаційних активів і технологій у межах області дії СУІБ. Керує діями посадових осіб при виявленні невідповідностей/аномалій, розробці, упровадженні та підтримці процесів, направлених на зниження інформаційних ризиків і ризиків інформаційних технологій, та за розпорядженням CSO перевіряє результативність проведених виправлень |
| 6 | CIO | Керівник підрозділу ІТ є відповідальним за безперервність робочих процесів, функціонування IT-інфраструктури з дотриманням вимог СУІБ |
| 7 | DPO | Уповноважена особа, яка є відповідальною за виконання та контроль за процесами, пов’язаними з обробкою і зберіганням PII |

3.4. Детальна інформація щодо відповідальності за етапами виконання виправлень викладена в додатку 1.

3.5. CSO є відповідальним за оперативне проведення коригувальних дій та контроль за наявністю необхідних ресурсів, також відповідає за планування корекційних дій з метою вдосконалення СУІБ. CSO організує роботи та контролює ефективність:

3.5.1 проведених заходів і опис ризиків, їх актуальність та документування у реєстрі ризиків;

3.5.2 дій з усунення ризиків та документування виправлень;

3.5.3 заходів, пов’язаних з актуальністю переліку власників активу, власників ризику та доведення до їх відома відповідальності за впровадження заходів захисту з метою усунення невідповідності/аномалії або проведення покращень дій з удосконалення СУІБ;

3.5.4 процесу реєстрації дій, пов’язаних з виправленням [номер(и) заявки на коригувальну/корекційну дію (якщо доречно), дату впровадження заходів)] та визначення відповідального за дію проведення заходів захисту.

3.6. CISO є відповідальним за результативність, своєчасність та якість проведення виправлень власниками активів та власниками ризиків. У разі необхідності CISO звертається до DPO з метою співпраці в галузі обробки PII.

3.7. При проведенні коригувальних/корекційних дій, CISO відповідає за створення та наповнення інформацією документа «Форма проведення процедури виправлень» (надалі – форма) (зразок наведено в додатку 2). Після завершенню коригувальних/корекційних дій CISO надсилає форму до CSO (DPO, якщо дії пов’язані з обробкою PII) з документуванням:\*\*\*

3.7.1 проведеного аналізу внутрішніх та зовнішніх факторів у межах СУІБ;

3.7.2 відповідності СУІБ усім контролям, визначеним у Положенні про застосовність [реєстр застосовності елементів керування (контролів)], політикам та процедурам СУІБ;

3.7.3 проведення оцінки ризиків та внесення відповідних змін до реєстру ризиків ІБ;

3.7.4 результативності проведених виправлень.

3.8. DPO є відповідальним за ефективність (результативність), своєчасність та якість проведення виправлень, якщо проведені виправлення пов’язані з PII.

3.9. Ініціатор (посадова особа виконкому міської ради, власник активу або власник ризику), який помічає невідповідність/аномалію, має негайно вжити заходів, щоб контролювати, локалізувати та виправити, а також усунути їх наслідки. Якщо посадова особа виконкому міської ради, власник активу або власник ризику не несе відповідальності за таку невідповідність/аномалію або має сумнів чи дійсно це є невідповідність/аномалія або невідома подія, вони повинні передати інформацію про цей факт відповідальній особі: CSO, DPO, CISO, власнику активу або власнику ризику, які мають провести виправлення.

3.10. Коригувальні та корекційні дії передбачають організацію роботи з унесення відповідних виправлень (змін) та інформування про вжиті заходи уповноваженим особам у сфері СУІБ.

3.11. Основна відмінність між коригуванням та корекцією полягає в тому, що коригувальні дії усувають причину невідповідності/аномалії, тоді як корекційні дії зосереджуються лише на виправлення наявних заходів/процесів та засобів захисту з метою вдосконалення СУІБ.

3.12. Кінцева мета проведення коригувальних дій – локалізація та/або виправлення виявлених невідповідностей/аномалій, усунення її/їх наслідків. CSO, DPO, CISO, власник активу або власник ризику мають оцінити необхідність усу-нення причини невідповідності та запобігти її повторенню шляхом ужиття коригувальних дій.

3.13. Кінцева мета проведення корекційних дій – проведення покращень СУІБ.

3.14. Процедура виправлень може бути ініційована будь-якою посадовою особою виконкому міської ради, власником активу, власником ризику або (у від-повідних випадках) громадянином, який є суб’єктом PII, постачальником або аутсорсинговим партнером. Виправлення можуть вимагати внесення змін до будь-якого документа, процесу чи домовленості в межах області дії СУІБ.

3.15. Опис виконання коригувальних дій приведено в таблиці 2.

*Таблиця2\*\*\*\**

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Крок*** | ***Відповідальна особа за виконання*** |

| ***1*** | ***2*** | ***3*** |
| --- | --- | --- |
| 1 | Розгляд невідповідності | Усі, хто має певну роль у СУІБ |
| 2 | Визначення причини невідповідності/аномалії | Особа, відповідальна за актив та ризик, у якому виявлено невідповідність |
| 3 | Визначення, чи вже наявна така невідповідність | Особа, відповідальна за актив та ризик, у якому виявлено невідповідність |
| 4 | Оцінка необхідності дій для усунення невідповідності/аномалії | Особа, відповідальна за актив та ризик, у якому виявлено невідповідність |
| 5 | Визначення дій, необхідних для усунення причин невідповідності/аномалії та забезпечення того, щоб вони не повторювалися | Особа, відповідальна за актив та ризик, у якому виявлено невідповідність. CSO у межах планування ресурсів для усунення невідповідності.CISO/DPO у межах корекційних дій реєстру ризиків (надалі – DPIA) |
| 6 | Виконання коригувальних дій | Відповідальний за виконання, призначений CEO |
| 7 | Перевірка того, чи привели вжиті дії до усунення причин невідповідності/аномалії | CSO, DPO |
| 8 | Інформування всіх уповноважених осіб та зацікавлених сторін про вжиття корекційних заходів | Відповідальний за виконання корекційних дій, призначений CEO |
| 9 | Унесення змін до СУІБ, якщо це необхідно | CSO, DPO – особи, які відповідають за ефективність СУІБ.CISO, CIO – особи, які відповідають за результативність СУІБ |

3.16. Схему робочого процесу проведення виправлень наведено в додатку 3.

3.17. Під час ухвалення рішення про проведення виправлень, в їх проведення та після слід провести аналіз здійснених заходів та встановити вплив на інформаційну діяльність виконкому міської ради з метою визначення: чи можуть виправлення призвести до нових ризиків ІБ. Якщо так, має бути проведена ідентифікація, оцінка та обробка ризиків відповідно до D10-СУІБ «Методологія оцінки та обробки ризиків» та врахована ця інформація шляхом унесення змін до:

3.17.1 реєстру ризиків ІБ СУІБ. Відповідальна особа – CSO;

3.17.2 документів, що стосуються DPIA. Відповідальна особа – DPO.

3.18. Визначені дії на підставі проведеного аналізу подій додаються до плану коригувальних/корекційних дій і вдосконалення , а також до реєстру ризиків (захист РІІ, оцінка впливу, DPIA).

3.19. План коригувальних/корекційних дій і вдосконалення має містити таку інформацію:

3.19.1 опис ризику або вразливості;

3.19.2 план проведення виправлень;

3.19.3 власник активу, власник ризику та відповідальний за впровадження заходів захисту з метою усунення визначеної невідповідності/аномалії або виконання заходів з удосконалення СУІБ;

3.19.4 номер(и) заявки на відновлення (якщо доречно).

3.20. CSO і DPO мають підтвердити, що на основі результатів виправлень оновлено наведену супровідну документацію, якщо це необхідно:

3.20.1 внутрішні та зовнішні фактори в межах СУІБ;

3.20.2 контроль, політики та процедури;

3.20.3 оцінка ризиків і реєстр ризиків;

3.20.4 міра ефективності контролю.

3.21. Щорічно CSO разом з DPO повинні контролювати статуси невідповідностей/аномалій, що були або плануються до усунення, та покращень СУІБ у виконкомі міської ради, запланованих до впровадження. Все це відображається в плані проведення виправлень (у якому, у числі іншого, має міститися інформація щодо запланованих дій CSO/DPO на майбутнє).

3.22. CSO та DPO обговорюють/ухвалюють рішення/переглядають дії, необхідні для успішного завершення пунктів плану проведення виправлень.

*\*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.*

*\*\*Вплив – це відхилення від очікуваного (позитивне або негативне).*

*Невизначеність – це стан, навіть частково, браку інформації, пов'язаної з розумінням події або знанням про неї, її наслідки чи ймовірність.*

*Ризик часто характеризується зазначенням можливих подій і наслідків, або їх комбінації.*

*Ризик часто виражається у формі комбінації наслідків події, включаючи зміни в обставинах і пов'язані з ним ймовірності виникнення.*

*У контексті систем менеджменту ризики ІБ можуть бути виражені як вплив невизначеності на досягнення цілей ІБ.*

*Ризик ІБ пов'язаний з імовірністю того, що загрози будуть реалізовуватися використанням уразливості інформаційних активів або груп інформаційних активів і, тим самим, завдавати шкоди організації.*

*\*\*\*На підставі цих даних DPO уносить, у разі необхідності, зміни до документів, що стосуються DPIA.*

*\*\*\*\*Кожен із зазначених кроків має бути зафіксованим у формі корекційних дій [наприклад, програма «Help Desk» або будь-яка інша система («Jira»), що використовується для вирішення певних проблем)].*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***