*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

 *25.07.2025 №938*

***ПОЛІТИКА АНОНІМІЗАЦІЇ ТА ПСЕВДОАНОНІМІЗАЦІЇ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика анонімізації та псевдоанонімізації виконавчого комітету Криворізької міської ради (надалі – Політика) є документом надання настанов з визначення і забезпечення анонімізації та псевдонімізації ідентифікованих персональних даних (надалі – PII).

1.2. Політика розроблена з метою впровадження заходів з інформаційної безпеки (надалі – ІБ) для захисту PII з метою підвищення їх конфіденційності, цілісності та доступності PII.

1.3. Політика застосовується до всієї області дії системи управління інформаційною безпекою (надалі – СУІБ):

1.3.1 усіх операційних процесів, дій з обробки PII та всіх інформаційних активів (надалі – ІА), що оброблюються в підсистемах Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС), а саме: «Підсистема документообігу», «Підсистема кадрового забезпечення» та «WebПортал»;

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

1.4. Політика розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу ІБ, а саме: Законів України «Про інформацію», «Про захист персональних даних», «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/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», ISO/IEC 29100:2011 «Інформаційні технології – Методи забезпечення безпеки – Структура конфіденційності», 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, NIST Special Publication 800-53 Revision 5 «Security and Privacy Controlsfor Information Systems and Organizations», The NIST Cybersecurity Framework (CSF) 2.0, політик, процедур і технічних заходів: D4.1-СУІБ «Політика інформаційної безпеки», D2.2-СУІБ «Політика управління активами користувачів», D14.6-СУІБ «Політика класифікації інформації», D14.14-СУІБ «Політика контролю доступу», D14.12-СУІБ «Політика криптографії».

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

2.1. Анонімізація – безповоротна деідентифікація PII таким чином, що особа не може бути ідентифікована за допомогою розумного часу, витрат і технологій контролером або будь–якою іншою особою для ідентифікації цієї особи. Принципи обробки РІІ не застосовуються до анонімних даних, оскільки це вже не РІІ.

2.2. Політика конфіденційності – загальні наміри та напрями, правила й зобов’язання, офіційно виражені контролером PII, пов’язані з обробкою PII у певних умовах.

2.3. Принципи приватності – набір спільних цінностей, що регулюють захист PII, коли вони обробляються в ЄІС.

2.4. Псевдонімізація – обробка PII таким чином, що їх більше не можна віднести до конкретного суб’єкта PII без використання додаткової інформації, за умови, що така додаткова інформація зберігається окремо від PII та підлягає технічним і організаційним заходам для забезпечення того, що PII не віднесено до фізичної особи, яку ідентифіковано чи можна ідентифікувати. Псевдонімізація зменшує, але не усуває повністю можливість пов’язувати PII із суб’єктом PII. Оскільки дані під псевдонімом все ще є PII, обробка даних під псевдонімом має відповідати принципам обробки PII.

2.5. Заявник – це суб’єкт PII, який за допомогою сервісів підсистеми «WebПортал» подає запит (електронне звернення) до повноважних органів виконкому міської ради з метою отримання адміністративних, інших публічних послуг, у тому числі з дозвільних питань, видачі документів дозвільного характеру, голосування за електронні петиції та подання скарг.

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

2.7. Суб’єкти ЄІС – Криворізька міська рада, її виконавчі органи, підприємства, установи, організації, заклади комунальної власності міста, районні в місті ради, що користуються підсистемами ЄІС та обробляють інформацію для реалізації наданих повноважень.

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. 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. 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.

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

2.16. PII – персональні дані.

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

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

2.17.2 органи місцевого самоврядування;

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

2.17.4 банки, інвестори, рейтингові агентства;

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

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

2.18. 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, спі-в-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.

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

2.20. Користувачі ЄІС – фізичні особи та юридичні особи, уповноважені посадові особи, уповноважені посадові особи суб’єктів ЄІС, яким у встановленому порядку надано відповідні права доступу до інформації в підсистемах ЄІС.

#### *3. Псевдонімізація та анонімізація персональних даних*

3.1. DPO та CSO повинні вирішити, чи є відповідними методи псевдонімізації та анонімізації для конкретних видів обробки PII, чи мають бути застосовані методи шифрування для захисту властивостей PII. CISO відповідає за вибір найбільш відповідної технології та впровадження цих методів.

3.2. Зважаючи на сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяги й цілі опрацювання PII, а також ризики різної імовірності та тяжкості для прав і свобод фізичних осіб, що виникають під час опрацювання, контролер PII і процесор PII вживають необхідних технічних та організаційних заходів для організації безпеки відповідно до ризику, а саме:

3.2.1 використання технології анонімізації та/або псевдонімізації;

3.2.2 використання технології шифрування PII;

3.2.3 здатність забезпечувати безперервну конфіденційність, цілісність, наявність та стійкість ЄІС і послуг опрацювання PII;

3.2.4 здатність вчасно відновити наявність і доступ до PII у випадку технічної аварії;

3.2.5 процес для регулярного тестування, оцінювання та аналізу результативності технічних і організаційних заходів для гарантування безпеки опрацювання PII.

3.3. Виконком міської ради забезпечує видалення PII або надання їм форми, що не дозволяє ідентифікувати або повторно ідентифікувати суб’єктів РІІ, як тільки первісні РІІ більше не є необхідними для визначеної мети (цілей).

3.4. Метою анонімізації PII є унеможливлення ідентифікації особи в анонімізованому наборі даних за допомогою оригінальних даних, тобто анонімізовані дані не розглядаються як PII. У межах правових рамок законодавчих актів стосовно захисту PII відсутній чіткий стандарт для анонімізації, тому DPO сумісно з CSO несуть повну відповідальність за вибір та використання відповідних методів анонімізації в процесі інформаційної діяльності у межах області дії СУІБ.

3.5. Виконком міської ради використовує такі методи (узагальнення даних, додавання шуму до даних), ураховуючи ступінь ризику та призначення використання PII:

3.5.1 таблиця замін каталогу (надалі – ТЗК) – заміна імені осіб, включених у дані, з підтриманням узгодженості між такими значеннями: «індекс + місто», «вік + стать»;\*\*\*

3.5.2 перемішування з доданням «шуму» – включає змішування літер з додаванням нових символів;

3.5.3 затемнення – наближення значень даних для того, щоб зробити їх сенс непридатним та/або неможливим для ідентифікації осіб;

3.5.4 диференційна конфіденційність – метод використовується, коли виконком міської ради надає доступ сторонньому суб'єкту PII до анонімізованого набору даних. Копія оригінальних PII залишається у виконкомі міської ради, а зацікавлена або третя сторона отримує лише анонімний набір даних;

3.5.5 агрегація (узагальнення) – суб'єкт PII групується з іншими суб'єктами PII, які діляться деякими або всіма PII;

3.5.6 К-сортування (K-Anonymity) – метод анонімізації, що використовується для захисту конфіденційності РІІ, зменшуючи ризик ідентифікації суб’єкта РІІ з набору даних. Будь-який запис у наборі даних не відрізняється від щонайменше «k – 1» інших записів з точки зору «квазі-ідентифікаторів». Це забезпечує, що суб’єкта РІІ неможна легко ідентифікувати. Дані кластеризуються так, щоб для кожного запису було щонайменше «k» записів з однаковими значеннями квазі-ідентифікаторів. Це досягається шляхом генералізації (узагальнення) або придушення (видалення) даних для зменшення специфічності «квазі-ідентифікаторів».

3.6. Принципи захисту PII застосовуються до будь-якої конфіденційної інформації в контексті робочого процесу та інформації про фізичну особу, яку ідентифіковано чи можна ідентифікувати. PII з використанням псевдоніму, що можна приписати фізичній особі після використання додаткової інформації, необхідно розглядати як інформацію про фізичну особу, яку можна ідентифікувати. Для встановлення можливості ідентифікації фізичної особи беруться до уваги всі способи, що використовуються з високою імовірністю, такі як відокремлення контролером або іншою особою для ідентифікації фізичної особи прямо чи опосередковано.

3.7. Для встановлення достатньої ймовірності використання способів для ідентифікації фізичної особи, беруться до уваги всі об'єктивні фактори, такі як витрати та період часу, необхідні для ідентифікації, з огляду на технології, наявні станом на момент опрацювання, і технологічні розробки. Принципи захисту PII, відповідно, не застосовуються до анонімної інформації, зокрема інформації, що не стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати, або PII, що стали анонімними в такий спосіб, що суб'єкта PII неможливо чи більше неможливо ідентифікувати.

3.8. Псевдонімізація призначена для підвищення конфіденційності через заміну ідентифікаційних полів у записі даних одним чи декількома штучними ідентифікаторами або псевдонімами. Таким чином, псевдонімізація зменшує, але не повністю вилучає можливість пов'язати набір даних з ідентичністю суб'єкта PII.

3.9. DPO разом з CSO установлюють відповідні методи псевдонімізації, такі як:

3.9.1 шифрування з використанням таємного ключа – дані замінюються за допомогою таємного ключа. Власник таємного ключа може легко повторно ідентифікувати суб'єктів PII, розшифровуючи набір шифрованих даних;

3.9.2 хеш-функції – використовуються для відображення даних будь-якого розміру на коди фіксованого розміру;

3.9.3 перемішування – включає звичайне змішування літер. Процес іноді може бути зворотним. Наприклад, Роберт може стати Бетрор;

3.9.4 маскування – дозволяє приховати частину даних випадковими символами або іншими кодами в поєднанні з ключем таким чином, що дані не можуть бути віднесені до фізичної особи без використання ключа;

3.9.5 токенізація – процес заміщення чутливого елемента даних його нечутливим еквівалентом, відомим як токен. Токен є посиланням (тобто ідентифікатором), що відображається на чутливі дані через систему токенізації. Система токенізації надає додаткам обробки даних право та інтерфейси для запиту токенів або детокенізації для отримання чутливих даних;

3.9.6 замінення – дані замінюються на штучні ідентифікатори або «псевдоніми», де замість справжнього імені «Іван Іваненко» використовують псевдонім «Користувач123»;

3.9.7 псевдонімізація на основі індексів – кожному запису присвоюється унікальний код або ідентифікатор, який не несе інформації про оригінальні дані, де замість зберігання даних «Петро Петренко» і його адреси використовують ідентифікатор «ID10001». Інформація про те, що «ID10001» відповідає «Іван Іваненко», зберігається окремо.

3.10. Використання псевдонімів до PII може зменшити ризики для відповідних суб'єктів PII та допомогти контролерам PII та процесорам PII у виконанні обов'язків із захисту PII.

3.11. Для обмеження здатності контролерів та процесорів PII ідентифікувати суб’єкта PII, PII можуть бути замінені псевдонімами. Цю заміну виконує власник/розпорядник/контролер PII перед передачею ідентифікаційної інформації процесору PII.

3.12. Заміна вважається псевдонімізацією за умов:

3.12.1 інших атрибутів, пов’язаних з псевдонімом, недостатніх для ідентифікації суб’єкта PII, до якого вони належать;

3.12.2 призначення псевдоніма є таким, що його неможливо скасувати розумними зусиллями, крім дій тих осіб, які його виконали.

3.13. Псевдонімізація зберігає зв'язок між PII і псевдонімом. З одним псевдонімом можуть бути пов’язані різні дані. Чим більший набір даних, пов’язаних з певним псевдонімом, тим більший ризик того, що властивість порушується. Чим менша група фізичних осіб, до якої належить набір пов’язаних псевдонімних даних, тим більша ймовірність ідентифікації суб’єкта PII.

3.14. Псевдонімізація контрастує з анонімізацією. Процеси анонімізації руйнують можливість зв’язування PII з даними анонімізації. Під час анонімізації інформація про особу або стирається, або змінюється символами, для яких функція призначення або таблиця знищуються. Таким чином, анонімні дані більше не є ідентифікаційною інформацією.

*\*Залежно від юрисдикції та конкретного законодавства про захист персональних даних і конфіденційності фрази: «суб’єкт даних» або «суб’єкт PII» або «власник ідентифікаційної інформації» є синонімом фрази «суб’єкт PII».*

*\*\*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.*

\*\*\* *Якщо виникає необхідність додавання атрибутів заміни у відповідності до контексту виконкому міської ради з урахуванням Регламенту функціонування ЄІС, запиту на ІА від власника ЄІС та/або розпорядника ЄІС та/або компрометації ТЗК, CSO сумісно з DPO проводять роботи щодо відповідних змін/додання/вилучення тощо та ухвалюють ці зміни за рішенням CEO*.

***Керуюча справами виконкому Олена ШОВГЕЛЯ***