*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №939*

***МЕТОДОЛОГІЯ ОЦІНКИ ВПЛИВУ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

***(DATA PROTECTION IMPACT ASSESSMENT)***

#### *1. Загальні положення*

1.1. Методологія оцінки впливу на захист персональних даних виконавчого комітету Криворізької міської ради (надалі – DPIA) є документом що визначає підхід, порядок та критерії проведення оцінки впливу на захист персональних даних у діяльності виконавчого комітету міської ради.

1.2. Метою DPIA є:

1.2.1 застосування оцінки впливу на захист персональних даних, що оброблюються в функціональних підсистемах Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС) у межах області дії системи управління інформаційної безпеки (надалі – СУІБ) у функціональних підсистемах ЄІС: «Підсистема документообігу», «Підсистема кадрового забезпечення» та «Webпортал» виконкому міської ради;

1.2.2 визначення особливостей обробки та застосування заходів і засобів для захисту персональних даних (надалі – PII) суб'єкта персональних даних (надалі – Суб'єкт PII), його представника або іншого уповноваженого, що діє від імені Суб'єкта PII;

1.2.3 визначення етапів, відповідних дій і кроків, необхідних для проведення DPIA.

1.3. DPIA дозволить виконкому міської ради:

1.3.1 дотримуватися юридичних зобов'язань;

1.3.2 досягати керованості процесом захисту PII, що циркулюють в інформаційних активах (надалі – ІА), визначати загрози/вразливості та вживати відповідні захисні заходи в залежності від критичності ІА для зниження ризиків, що виникають у процесі роботи з PII;

1.3.3 забезпечити кращий контроль і моніторинг інформаційної діяльності процесорів PII в (моніторинг виконання умов договору щодо обробки PII), з якими укладені цивільно-правові договори;

1.3.4 забезпечити кращий контроль, моніторинг та підтримку актуальності анкетних даних контролера PII та процесора PII відповідно D11.2-СУІБ «Реєстр ризиків» (захист персональних даних, оцінка впливу, DPIA, «Анкета оцінки впливу на захист даних»);

1.3.5 гарантувати Суб’єкту PII, що будь-яка інформація про нього є надійно захищеною внаслідок постійного проведення заходів з оцінки впливу на захист PII з метою поліпшення якості СУІБ та гарантування, що PII є точними протягом усього їх життєвого циклу.

1.4. DPIA застосовується до всіх суб'єктів господарювання або інших організацій, постачальників послуг, Суб'єктів PII та інших осіб, що належать або управляються виконкомом міської ради в межах області дії СУІБ щодо обробки PII.

1.5. Дія DPIA поширюється на опрацювання персональних даних повністю чи частково із застосуванням автоматизованих засобів та до опрацювання PII із застосуванням неавтоматизованих засобів, що формують частину картотеки або призначені для внесення до картотеки, що містить PII.

1.6. DPIA є складовою загального процесу обробки персональних даних та застосовується для всіх ІА, у яких циркулюють PII.

1.7. DPIA 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 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги» (надалі – ДСТУ ISO/IEC 27001), ДСТУ ISO/IEC 27002:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки» (надалі – ДСТУ ISO/IEC 27002), ДСТУ ISO/IEC 27701:2022 «Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови» (надалі – ДСТУ ISO/IEC 27701), ДСТУ ISO/IEC 27005:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT)» (надалі – ДСТУ ISO/IEC 27005); 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 (Загальний регламент про захист даних) (надалі – GDPR); політик, процедур і технічних заходів: «D4.1-СУІБ Політика інформаційної безпеки», «D3-СУІБ Сфера застосування СУІБ, D4.2-СУІБ Політика захисту персональних даних», «D4.3-СУІБ Політика захисту персональних даних працівників», «D4.6-СУІБ Норми поведінки», «D12-СУІБ Заява про застосовність (SoA)», «D14.6-СУІБ Політика класифікації інформації», «D11.2-СУІБ Реєстр ризиків» (захист персональних даних, оцінка впливу, DPIA) (надалі – реєстр DPIA).

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

2.1. Заявники – 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

2.2. Суб’єкт PII – фізична особа, персональні дані якої обробляються в межах згоди Суб’єкта PII 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.\*

2.3. Суб’єкти ЄІС – Криворізька міська рада, її виконавчі органи, підприємства, установи, організації, заклади комунальної власності міста, відділи, управління, інші виконавчі органи районних у місті рад, що користуються підсистемами ЄІС та обробляють інформацію для реалізації наданих повноважень.

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

2.5. 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)].

2.6. 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.

2.7. 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.

2.8. 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.

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

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

2.11. 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.

2.12. 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.

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

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

2.13.2 органи місцевого самоврядування;

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

2.13.4 банки, інвестори, рейтингові агентства;

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

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

2.14. Третя сторона – це фізична або юридична особа, яка може вплинути на інформаційну безпеку та безперервність процесів. У контексті СУІБ третя сторона може не мати створений та зареєстрований акаунт у межах області дії СУІБ. Це можуть бути сім’ї посадових осіб, суб’єктів PII, процесорів PII, підпроцесорів PII, співконтролерів PII, екстрені служби, консультанти (включаючи юристів, податкових консультантів, консультантів з питань праці тощо), які можуть мати вплив на інформаційну безпеку в межах області дії СУІБ.

2.15. 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.

2.16. Спільний контролер PII – контролер РІІ, який визначає цілі та засоби обробки РІІ спільно з одним або кількома іншими Контролерами PII.

2.17. Суб’єкт PII – фізична особа, персональні дані якої обробляються в межах згоди Суб’єкта PII 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.

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

2.19. Процесор PII – фізична або юридична особа, державний орган, агентство або будь-який інший орган, який обробляє персональні дані від імені контролера PII.

#### *3. Призначення DPIA*

3.1. Безпосереднє призначення DPIA полягає в деталізації заходів, що досягається виконанням таких основних заходів:

3.1.1 визначення необхідності проведення DPIA;

3.1.2 проведення DPIA (за допомогою анкетування);

3.1.3 ідентифікація та визначення критичності ІА;

3.1.4 заповнення всіх дій для ІА, у яких циркулюють PII;

3.1.5 визначення переліку дій для контролера PII та процесора PII.

3.1.6 наведення допоміжних ключових кроків (з поясненнями), за допомогою яких заповнюються дії для контролерів PII і процесорів PII.

3.2. Перелічені заходи для кожного з ІА консолідовані в реєстрі DPIA, що надає можливість спрощено керувати та мати цілеспрямований процес управління ризиками DPIA для відповідальних осіб (власників активів, власників ризиків, DPO).

#### *4. Відповідальність та повноваження*

4.1. Контролер РІІ несе відповідальність за організацію проведення DPIA (пункт 84 GDPR). Контролер РІІ звертається за рекомендаціями до DPO у ході проведення DPIA. (ст. 35(2) GDPR)

4.2. DPO своєчасно переглядає і актуалізує DPIA в разі необхідності (зміна робочих процесів в ІКС, рівнів критичності ІА тощо), але не рідше одного разу на півроку.

#### *5. Заходи щодо управління ризиками DPIA*

5.1. Відповідальним за якість та повноту виконання всіх етапів є DPO, якщо інше не визначене окремим рішенням СЕО.

5.2. DPIA є обов’язковою процедурою для Контролерів PII. У разі наявності процесора PII, контролер PII повинен зробити запит до процесора PII у формі анкети, яка наведена в D1.1-СУІБ «Готовність Системи до ISO/IEC 27701/GDPR». Після отримання відповіді від процесора PII, контролер PII заповнює аркуш «Процесор PII Активи Перелік Дій» у реєстрі DPIA. DPIA необхідно виконати до обробки PII.

5.3. DPO відповідає за загальний процес оцінки впливу на захист даних. DPO вирішує, чи проводитимуться консультації із Суб’єктами PII (особи, які беруть участь у обробці PII) під час виконання DPIA. Функції DPO полягають у такому:

5.3.1 на запит контролера РІІ надавати рекомендації щодо проведення DPIA та здійснювати моніторинг його проведення згідно з вимогами керівних документів (ст. 39(с) GDPR);

5.3.2 організація проведення анкетування зацікавлених сторін, проведення оцінки впливу на захист даних відповідно до DPIA;

5.3.3 заповнення реєстру DPIA з наведенням даних, оцінки ризиків, визначених заходів пом’якшення ризиків до прийнятних;

5.3.4 звітування до CEO про результати DPIA;

5.3.5 моніторинг, своєчасний перегляд DPIA та реєстру DPIA з метою поліпшення стану СУІБ.

5.4. Етапи DPIA (п. 5.45. DPIA Крок 1, п. 5.47. DPIA Крок 2, п.5.48. DPIA Крок 3, п. 5.49. DPIA Крок 4) деталізують послідовність проведення оцінки та мають відповідні посилання на Реєстр DPIA, що містить форми, анкети, переліки дій, кроки, тобто сутності, за допомогою яких цей процес набуває більшої прозорості.

5.5. Етапи та Реєстр DPIA містять відповідальних за заповнення даних сутностей осіб.

5.6. Реєстр DPIA містить оцінку ризиків і захисних заходів, які спрямовані на компенсацію ризиків.

5.7. Для ухвалення на наступному етапі рішення про необхідність проведення DPIA DPO повинен:

5.7.1 переглянути всі види інформаційної діяльності та послуг виконкому міської ради з обробки даних (на аркуші «DPIA так чи ні» у межах області дії СУІБ, опитування для визначення необхідності проведення DPIA), узяти до уваги будь-які нові види діяльності або послуг;

5.7.2 указати всі дії з обробки даних у визначених видах діяльності, відповідаючи на питання:

5.7.2.1. Чи ваша діяльність пов'язана зі збиранням, використанням, зберіганням або передачею будь-яких персональних даних громадян України чи Європейського Союзу?

5.7.2.2. Чи ваша діяльність пов'язана із широкомасштабним опрацюванням спеціальних категорій даних (персональних даних, що розкривають расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, чи членство в професійних спілках, і опрацювання генетичних даних, біометричних даних для цілі єдиної ідентифікації фізичної особи, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації), та персональних даних про судимості й кримінальні злочини?

5.7.2.3. Чи використовує ваша діяльність або послуга особисті дані для прогнозування будь-яких особистих уподобань, місцезнаходження, пересування осіб, фінансового стану, стану здоров’я або трудової діяльності громадян України чи Європейського Союзу?

5.7.2.4. Чи допомагає ваша діяльність ухвалювати рішення, що можуть суттєво негативно вплинути на людей, як приклад: відмова в послугах?

5.7.2.5. Чи передбачає ваша діяльність або послуга систематичний моніторинг громадських місць у великому масштабі?

5.7.2.6. Чи існують інші ризики, пов’язані з використанням вашої діяльності або послуг для прав і свобод громадян України чи Європейського Союзу, про які ви можете згадати?

5.8. Одна оцінка може бути виконана для кількох дій з обробки даних одночасно, якщо ці дії з обробки представляють однаково високі ризики. Спеціаліст із захисту даних вирішує, які види діяльності з обробки даних будуть оцінюватися разом (угруповувати обробку).\*\*

5.9. Після проведення перегляду всіх видів діяльності та заповнення всіх дій з обробки персональних даних у визначених видах діяльності DPO ідентифікує та детально аналізує кожен вид діяльності з обробки PII за допомогою власників активів і керівників відділів, управлінь, інших виконавчих органів міської ради. Цей аналіз необхідний для визначення того, чи може діяльність з обробки PII призвести до високого ризику для прав і свобод фізичних осіб, з якими пов’язані певні операції щодо обробки їх персональних даних.

5.10. DPO визначає в полі «Потрібен DPIA» чи потрібно відповідні види діяльності з обробки даних аналізувати через DPIA. Якщо на будь-яке запитання з анкети отримано відповідь «Так», для цього конкретного виду діяльності з обробки даних необхідно провести DPIA. Навіть якщо відповідь на всі запитання в анкеті: «Ні», DPO може ухвалити рішення про проведення DPIA, якщо потрібно отримати більш чітке уявлення про пов’язані з цим видом діяльності ризиками.

5.11. Аналіз проводиться в Реєстрі DPIA шляхом заповнення на аркуші «DPIA так чи ні», «Опитувальник для визначення необхідності проведення DPIA», поле «Потрібен DPIA? (Так/Ні)». У результаті для кожного виду діяльності є статус, який визначає необхідність проведення DPIA.

5.12. Для кожного виду діяльності з обробки даних, де потрібен аналіз DPIA (було визначено на попередньому кроці), DPO заповнює «Анкету оцінки впливу на захист даних» у Реєстрі DPIA на аркуші «Анкета DPIA».

5.13. Необхідно заповнити всі обов'язкові поля з позначкою «Обов’язково», це:

5.13.1. Надайте коротке пояснення того, як персональні дані використовуються у вашій діяльності/послузі:

5.13.1.1 як ви збираєте РІІ;

5.13.1.2 як ви зберігаєте РІІ;

5.13.1.3 як ви використовуєте РІІ;

5.13.1.4 хто має доступ до РІІ;

5.13.1.5 з ким ви ділитеся РІІ;

5.13.1.6 терміни зберігання РІІ;

5.13.1.7 заходи безпеки;

5.13.1.8 чи використовуєте при обробці РІІ новітні технології (наприклад штучний інтелект).

5.13.2. Надайте коротке пояснення того, що охоплює обробка РІІ:

5.13.2.1 характер РІІ, що обробляються;

5.13.2.2 обсяг і різноманітність РІІ;

5.13.2.3 обсяг і частота обробки РІІ;

5.13.2.4 тривалість обробки;

5.13.2.5 кількість залучених суб’єктів РІІ.

5.13.3 Надайте коротку інформацію щодо контексту обробки РІІ:

5.13.3.1 джерело РІІ;

5.13.3.2 характер відносин із суб’єктами РІІ.

5.13.4. Чи ваша діяльність/послуги передбачає обробку персональних даних дітей віком до 16 років?

5.13.5. Чи можете ви підтвердити, що зібрані персональні дані є актуальними та обмежені мінімальними потребами робочих процесів у межах конкретних цілей?

5.13.6. Чи вжито вами будь-які заходи для того, щоб зібрані персональні дані не використовувалися для нових або інших цілей, ніж ті, для яких вони були зібрані спочатку?

5.13.7. Опишіть, як і коли були надані повідомлення про конфіденційність користувачам вашого виду діяльності чи послуги, і, якщо це можливо, надайте копію (реєстраційний номер) відповідного(их) повідомлення(нь) про конфіденційність.

5.13.8. Якщо ви маєте згоду Суб’єктів PII на обробку PII для вашого виду діяльності чи послуги, чи є у вас механізми, щоб припинити обробку персональних даних, якщо цю згоду було відкликано?

5.13.9. Чи мають будь-які процесори PII/підпроцесори PII доступ до персональних даних, які ви зібрали? Якщо так, чи знаходиться процесор PII/підпроцесор PII за межами Європейської економічної зони та є наявність транскордонної передачі? Якщо так, перелічьте країни.

5.13.10. Опишіть будь-які наявні у вас механізми для аварійного відновлення під час роботи з PII.

5.13.11. Опишіть, які існують механізми для надання особам копій PII, які ви зберігаєте.

5.13.12. Опишіть, які існують механізми для видалення персональних даних, коли особа подає запит на видалення (за умови, що ідентифікація суб'єкта PII відбулася успішно).

5.13.13. Опишіть будь-які наявні механізми для виправлення неточних персональних даних за запитом суб'єкта PII (за умови, що ідентифікація суб'єкта PII відбулася успішно).

5.13.14. Укажіть, які особи мають доступ до персональних даних, якими ви володієте (наприклад, адміністратори серверів, відділи управління, інші виконавчі органи міської ради або окремі посадові особи тощо).

5.13.15. Коротко опишіть будь-які заходи безпеки, які ви застосували для захисту персональних даних (наприклад, сертифікація ДСТУ ISO/IEC 27001або виконання конкретних заходів відповідно до критеріїв, визначних у ДСТУ ISO/IEC 27701).

5.14. Відповіді на запитання, перелічені в підпунктах 5.13.1. – 5.13.15., дозволять провести детальний аналіз DPIA для перелічених видів діяльності з метою визначення ключових ризиків та захисних заходів для їх подальшого зменшення.

5.15. Упровадження захисних заходів – стовпці «Визначені ключові ризики» та «Зменшення ризику» заповнюються DPO (із залученням експертних знань власників активів, ризиків), при цьому враховується оцінка ризиків, проведена в реєстрі ризиків ІБ, що створено у виконкомі міської ради за результатами формування Порядку аналізу ризиків ІБ.

5.16. Проведення попередніх етапів дозволяють визначити перелік ІА, що пов’язані з видами діяльності, для яких проводиться детальний аналіз DPIA, та які мають ключові ризики і потребують захисних заходів для PII.

5.17. Для визначення переліку ІА також використовуються їх дані, що є в Порядку аналізу ризиків ІБ, до уваги приймаються активи, у яких наявні ризики, пов’язані із PII.

5.18. Результатом є перелік ІА, у яких циркулюють всі типи PII з наведенням рівня критичності в залежності від властивостей ІА: конфіденційність, цілісність, доступність (надалі – КЦД).

5.19. Проведені попередні етапи, а також інформація з Порядку аналізу ризиків ІБ дозволяють ідентифікувати перелік ІА, у яких циркулює PII.

5.20. З погляду зацікавленості захисту персональних даних є контролер PII та процесор PII.

5.21. Для визначення ключових властивостей ІА, що притаманні контролеру PII та процесору PII, на аркушах «Контролер PII Активи Перелік Дій» і «Процесор PII Активи Перелік дій» заповнюються такі основні спільні поля:

5.21.1 назва ІА (опис ІТ-системи);

5.21.2 назва ІТ-системи;

5.21.3 модуль ІТ-системи;

5.21.4 власник активу (власник модуля, адміністратор);

5.21.5 власник ризику;

5.21.6 реалізація модуля;

5.21.7 відділи, управління, інші виконавчі органи міської ради, посадові особи яких обробляють або контролюють процес обробки персональних даних та забезпечують виконання процесів у модулі;

5.21.8 класифікація PII (відповідно до Політики класифікації інформації);

5.21.9 опис та мета обробки PII;

5.21.10 перелік PII, які циркулюють в ІКС;

5.21.11 джерело PII;

5.21.12 КЦД, рівень критичності активу;

5.21.13 термін зберігання для кожної категорії даних.

5.22. Окремо для контролера PII притаманне таке поле: відмітка про призначення DPO у виконкомі міської ради.

5.23. Процесору PII притаманні такі поля:

5.23.1 відмітка про призначення DPO на боці Контролера PII;

5.23.2 термін зберігання для кожної категорії даних, установлений контролером PII;

5.23.3 наявність у контролера PII Політики конфіденційності та Кодексу поведінки (дата, реєстраційний номер).

5.24. Відмінність даних полів для контролера PII і процесора PII полягає в тому, що для контролера PII важливо контролювати обробку персональних даних на боці процесора PII, а процесору PII – проводити обробку персональних даних за вимогами контролера PII.

5.25. Кінцевою метою заповнення ключових полів є визначення рівнів критичності ІА, що дозволяють скоригувати в розділах «Анкети оцінки впливу на захист даних» «Визначені ключові ризики» відповідні захисні заходи для їх зменшення для видів діяльності, у яких присутні відповідні ІА.

5.26. Для визначення рівня критичності кожного з ІА використовуються рівні критичності активів, у яких наведено допоміжну інформацію.

5.27. Якщо результати DPIA вказують на те, що відповідний вид діяльності з обробки PII призведе до високого ризику, навіть якщо заходи безпеки будуть реалізовані, тоді DPO консультується з органом нагляду до початку обробки PII. У цьому випадку DPO повинен надати органу нагляду таку інформацію:

5.27.1 обов'язки контролера PII, спільного контролера(-ів) PII і процесора (-ів) PII;

5.27.2 призначення та засоби, що будуть використані для обробки даних;

5.27.3 заходи безпеки, призначені для захисту даних;

5.27.4 контактні дані DPO;

5.27.5 результати DPIA.

5.28. DPO переглядає DPIA у будь-якому з таких випадків, якщо:

5.28.1 ризики, пов'язані з діяльністю з обробки PII, змінюються;

5.28.2 є значні зміни в діяльності з обробки даних;

5.28.3 є зміни в правових вимогах;

5.28.4 виконком міської ради виконує функції процесора PII, а контролер PII просить переглянути DPIA.

5.29. Критичність усіх інформаційних активів визначається власниками ІА відповідно до трьох властивостей інформації КЦД на аркушах «Контролер PII Активи Перелік дій» і «Процесор PII Активи Перелік дій».

5.30. Використовуються 4 рівні критичності для оцінки активів: низький, середній, високий, дуже високий. Рівні критичності та відповідні значення наведені в таблиці та повинні відповідати вимогам Порядку аналізу ризиків ІБ:

Табл. 6.2.6.1 Рівні критичності

|  |  |  |  |
| --- | --- | --- | --- |
| ***№ п/п*** | ***Конфіденційність*** | ***Цілісність*** | ***Доступність*** |
| 1 | Рівень критичності Активів | Умовне позначення рівня критичності | Рівень критичності | Умовне позначення рівня цілісності | Рівень критичності | Час | Умовне позначено рівня доступності |
| 2 | Низький | К1 | Низький | Ц1 | Низький | Більше 3 діб | Д1 |
| 3 | Середній | К2 | Середній | Ц2 | Середній | 3 доби | Д2 |
| 4 | Високий | КЗ | Високий | ЦЗ | Високий | 1 доба | Д3 |
| 5 | Дуже високий | К4 | Дужевисокий | Ц4 | Дужевисокий | 4 години | Д4 |

Табл. 6.2.6.2 Класифікація Інформаційних Активів та відповідність до рівнів критичності

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***№ п/п*** | ***Класифікація Інформаційних Активів******(п. 4.2. Політики класифікації інформації)*** | ***Конфіденційність*** | ***Цілісність*** | ***Доступність*** |
| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** |
| 1 | ПУБЛІЧНА | Вимоги не висовуються | Вимоги не висовуються | Вимоги невисовуються |
| 2 | ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ | Вимоги не висовуються | Низький | Ц1 | Низький | Д1 |
| 3 | ЧУТЛИВА PII\_К21 | Дуже високий | К4 | Дуже високий | Ц4 | Дуже високий | Д4 |
| 4 | ЧУТЛИВА PII\_К22 | Дуже високий | К4 | Дуже високий | Ц4 | Дуже високий | Д4 |
| 5 | КОНФІДЕНЦІЙНО PII\_К23 | Середній | К2 | Середній | Ц2 | Середній | Д2 |
| 6 | КОНФІДЕНЦІЙНО PII\_К24 | Високий | КЗ | Високий | ЦЗ | Високий | Д3 |
| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** |
| 7 | КОНФІДЕНЦІЙНО PII\_К25 | Високий | КЗ | Високий | ЦЗ | Високий | Д3 |
| 8 | КОМЕРЦІЙНА ТАЄМНИЦЯ | Високий | КЗ | Високий | ЦЗ | Високий | Д3 |
| 9 | ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ | Дуже високий | К4 | Дуже високий | Ц4 | Дуже високий | Д4 |

5.31. Критичність активу визначається на підставі оцінки впливу на роботу в разі:

5.31.1 незапланованого або несанкціонованого розкриття інформації (конфіденційність);

5.31.2 помилок (збоїв) інформації або навмисного маніпулювання інформацією для вчинення або приховування шахрайства (цілісність);

5.31.3 тривалого простою застосування ресурсів (доступність).

5.32. Для кожної властивості ІА (КЦД) проводиться оцінка впливу на обробку персональних даних.

5.33. Оцінка критичності ІА проводиться власниками ІА за підтримки DPO, CSO та SOC.

5.34. Після отримання від власників ІА оцінок критичності ІА та узагальнення інформації DPO подає повний перелік ІА із зазначеним рівнем критичності на розгляд CEO (або дорадчого органу з інформаційної безпеки, якщо такий буде визначений рішенням CEO).

5.35. СSO має право змінювати критичність ІА, визначену власником ІА, при цьому DPO затверджує визначений рівень критичності ІА.

5.36. Перегляд критичності ІА власниками ІА здійснюється за необхідності, але як мінімум щорічно в рамках актуалізації реєстру DPIA. Процес перегляду оцінки критичності ІА застосовується і контролюється за ініціативою DPO.

5.37. Оцінки критичності ІА не є фіксованими і можуть бути змінені на основі змін вимог інформаційної безпеки, сфери діяльності, робочих пріоритетів, а також у разі визначення нових вразливостей.

5.38. DPO організовує процес перегляду оцінки критичності ІА і дає рекомендації власникам ІА щодо необхідності оновлення оцінки критичності ІА.

5.39. Рівні критичності ІА визначаються з урахуванням їх схеми класифікації відповідно до Політики класифікації інформації.

5.40. Визначення властивостей КЦД для кожного ІА дозволяють визначити найбільш критичні, повернутися на аркуш «Анкета DPIA» та скоригувати відповідні захисні заходи для їх зменшення у аркушах «Анкета оцінки впливу на захист даних» «Визначені ключові ризики» для видів діяльності, у яких присутні відповідні ІА.

5.41. Відповідальним за контроль та виконання заходів з оцінки ризиків у виконкомі міської ради – є DPO, за кожним з ІА – є власник ризику та власник ІА із залученням (за необхідності за рішенням власника ІА) інших експертів зі складу SOC, IRT або групи реагування на порушення персональних даних.

5.42. Аркуш «Рівні критичності Активів» містить всю довідкову інформацію з цього пункту DPIA.

5.43. На аркуші «Терміни» Реєстру DPIA наведені всі основні визначення та скорочення, що застосовуються в DPIA та в реєстрі DPIA.

5.44. Аркуш «Перелік PII» реєстру DPIA наводить визначення та деталізує інформацію, що може бути віднесена до PII.

5.45. DPIA Крок 1: інформація на аркуші «DPIA Крок 1» Реєстру DPIA допомагає заповнювати аркуші «DPIA так чи ні» та «Анкета DPIA» шляхом надання необхідних пояснень.

5.46. DPIA: Стаття 35 GDPR вимагає виконання DPIA перед обробкою PII для процесів «Якщо тип обробки, зокрема з використанням нових технологій, і враховуючи характер, обсяг, контексту та цілей обробки, ймовірно, призведе до високого ризику для прав і свобод фізичних осіб, Контролер PII повинен перед обробкою провести оцінку впливу передбачуваних операцій обробки на захист персональних даних».

5.47. DPIA Крок 2: Інформація на аркуші «DPIA Крок 2» Реєстру DPIA допомагає заповнювати аркуші «Контролер PII Активи Перелік дій» та «Процесор PII Активи Перелік дій» шляхом пояснення ідентифікації ІА, класифікації PII та періоду її зберігання. А також пояснює, яким чином можна перевірити поєднання DPIA з іншими процесами, що мають такі ризики.

5.48. DPIA Крок 3: Інформація на аркуші «DPIA Крок 3» Реєстру DPIA розглядає:

5.48.1 кодекси поведінки та фіксацію його наявності;

5.48.2 оцінку ефективності і необхідності обробки PII;

5.48.3 оцінку заходів, що сприяють правам суб’єктів даних.

5.49. DPIA Крок 4: Аркуш «DPIA Крок 4» містить інформацію щодо обробки ризиків і залишкових високих ризиків для заповнення полів на аркушах «Контролер PII Активи Перелік дій» та «Процесор PII Активи Перелік дій», які безпосередньо пов’язані з обробкою ризиків: «Спостереження/ризики», «Деталі обробки ризиків», «Власник ризику» та ін., а також має пояснення щодо попередньої консультації з органом нагляду для більш об’єктивної оцінки ризиків.

5.50. Аркуш «Кодекс поведінки» наводить положення статті 40 GDPR – кодекс поведінки, що деталізує вимоги, які необхідно виконувати для DPIA Крок 3 у межах області дії СУІБ стосовно обробки PII.

5.51.Аркуш «Законність обробки» наводить положення статті 6 GDPR – законність, що деталізує вимоги щодо законності обробки PII для DPIA Крок 3 та DPIA Крок 4 «Обробка ризиків і залишкові високі ризики».

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

*\*\*DPO може проводити єдину оцінку діяльності систем відеоспостереження та контролю фізичного доступу* *– обидві системи є системами безпеки та обидві фіксують присутність людей у певних приміщеннях. З іншого боку, DPO не може провести єдину оцінку для відеоспостереження разом із записами фіксування робочого часу співробітників, оскільки вони призначені для різних цілей: перша система призначена для організації безпеки, друга – для розрахунку заробітної плати.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***