*ЗАТВЕРДЖЕНО*

*Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА БЕЗПЕЧНОЇ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика безпечної розробки програмного забезпечення виконавчого комітету Криворізької міської ради (надалі – Політика безпечної розробки) є документом, що визначає основні правила безпеки з розробки програмного забезпечення (надалі – ПЗ) та систем, модернізації ПЗ Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС), вимог інформаційної безпеки (надалі – ІБ) для взаємовідносин з постачальниками в межах безпеки ланцюга постачання.

1.2. Політика безпечної розробки має мету забезпечити:

1.2.1 процес розробки, придбання та підтримки ПЗ згідно з вимогами чинного законодавства й внутрішніх документів з питань ІБ виконкому міської ради;

1.2.2 дотримання її вимог на всіх етапах життєвого циклу ПЗ у межах області дії системи управління інформаційної безпеки (надалі – СУІБ);

1.2.3 мінімізацію ризиків, пов’язаних з розробкою, придбанням, постачанням і впровадженням ПЗ та інших компонентів у складі ЄІС у межах дії СУІБ.

1.3. Політика безпечної розробки розроблена з метою виконання вимог чинного законодавства в галузі ІБ та кіберзахисту, а також упровадження заходів з розробки/модернізації/упровадження/поліпшення ПЗ із застосуванням ризик-орієнтованого підходу на всіх етапах життєвого циклу СУІБ.

1.4. Політика безпечної розробки застосовується до усієї інформаційної діяльності, уключаючи дії, які можуть вплинути на обробку персональних даних (надалі – PII) виконкому міської ради в області дії СУІБ.

1.5. Політика безпечної розробки 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 ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки», ДСТУ EN 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» (надалі – ДСТУ ISO/IEC 27701), 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», D14.9-СУІБ «Політика управління змінами», D10-СУІБ «Методологія оцінки та обробки ризиків», D14.10-СУІБ «Політика резервного копіювання»; D14.11-СУІБ «Політика утилізації та знищення»; D14.14-СУІБ «Політика контролю доступу», D15.1-СУІБ «Політика безпеки постачальника».

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

2.1. Аналіз ризику – процес розуміння характеру ризику й визначення його рівня.

2.2. Визначення ступеня ризику – процес порівняння результатів аналізу ризику з критеріями ризику для визначення, чи є ризик і/або його величина допустимими чи прийнятними.

2.3. Власник ризику – посадова особа виконкому міської ради, яка несе відповідальність за обробку та управління ризиком у межах області дії СУІБ. Власника ризику визначає CSO або керівник відділу, управління, іншого виконавчого органу міської ради, у володінні/розпорядженні якого перебуває цей актив за погодженням з CSO.

2.4. 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, видачи документів дозвільного характеру, голосування за електронні петиції та подання скарг

2.5. 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.\*

2.6. 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)].

2.7. 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.\*\*

2.8. Інформаційний актив – 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.

2.9. 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.

2.10. 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.

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

2.12. 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.

2.13. 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.

2.14. 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.

2.15. PII – персональні дані.

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

2.17. Security Operations Center (надалі − SOC) − група ІБ виконкому міської ради, що відповідає за моніторинг, виявлення, аналіз та реагування на інциденти кібербезпеки в реальному часі.

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

#### *3.* *Розробка безпечного* *ПЗ*

3.1. У доповнення до оцінки ризиків, що проводиться відповідно до D10-СУІБ «Методологія оцінки та обробки ризиків», SOC періодично виконує такі оцінки:

3.1.1 ризики, пов'язані з несанкціонованим доступом до середовища розробки;

3.1.2 ризики, пов'язані з несанкціонованими змінами в середовищі розробки;

3.1.3 ризики, пов'язані з несанкціонованим доступом до середовища тестування;

3.1.4 ризики, пов'язані з несанкціонованими змінами в середовищі тестування;

3.1.5 ризики, пов'язані з несанкціонованим доступом у процесі прийому/передачі між середовищами розробки, тестування, продуктивної;

3.1.6 ризики, пов'язані зі змінами ролевої моделі без попереднього погодження з відповідальною особою за розробку та реалізацію стратегії цифрової трансформації міста, управління інформаційними системами та ресурсами, кібербезпеку CIO/CISO, та дозволу CSO після ретельної перевірки компетентності доцільності внесення цих змін;

3.1.7 ризик конфлікту інтересів між розробником, тестувальником та особою, що приймає в продуктивне середовище ПЗ (CISO має обов’язок суворо стежити за виконанням правил мінімально наданих повноважень, здійснювати контроль передачі ПЗ між середовищами з виключенням можливості використання одного акаунта в різних середовищах);

3.1.8 ризики, пов'язані з несанкціонованими змінами в продуктивному середовищі;

3.1.9 ризики, пов'язані з використанням конфіденційної інформації в порушення політик СУІБ, що вимагають використання тестової інформації в процесі розробки та тестування ПЗ;

3.1.10 технічні вразливості в компонентах ЄІС, що використовуються в межах області дії СУІБ;

3.1.11 ризики, пов'язані з упровадженням нових технологій у виконкомі міської ради.

3.2. Для організації безпеки продуктивних систем у виконкомі міської ради розгортається окремий тестовий «майданчик» та середовище розробки без прямого зв’язку з продуктивним середовищем. Тестування проводиться на спеціально виділених блоках серверів, що розташовані в інфраструктурі виконкому міської ради й прямо не пов'язані з продуктивними серверами. Розробникам ПЗ надається доступ до тестового «майданчика» та середовища розробки через систему контролю дій привілейованих користувачів (наприклад «FUDO PAM»). Доступ до середовищ тестування та розробки обмежується засобами міжмережевих екранів та служби каталогів «ActiveDirectory».

3.3. Середовища розробки та тестування ПЗ відокремлюються від виробничого середовища.

3.4. Розподілення обов’язків забезпечується таким чином:

3.4.1 розробники ПЗ не повинні відповідати за його тестування;

3.4.2 розробники й тестувальники не повинні відповідати за виробниче середовище.

3.5. CSO за поданням CIO та CISO затверджує процедури безпечної розробки нових систем і підтримки існуючих, а також визначає мінімальні стандарти безпеки, що мають дотримуватися.

3.6. DPO надає рекомендації, щоб під час розробки та тестування виконували такі настанови:

3.6.1 виконання вказівок щодо захисту PII та впровадження принципів конфіденційності, що втілюються в життєвий цикл розробки ПЗ;

3.6.2 виконання вимог до конфіденційності та захисту PII на етапі проєктування, що ґрунтуються на результатах оцінки ризиків для конфіденційності та/або оцінки впливу на конфіденційність;

3.6.3 створення контрольних точок захисту PII на етапах проєкту;

3.6.4 розробники й тестувальники отримують необхідні знання про конфіденційність та захист PII;

3.6.5 розробники й тестувальники за замовчуванням мінімізують обробку PII.

3.7. Системи, пов'язані з обробкою РІІ, розробляються відповідно до принципів конфіденційності за задумом та конфіденційності за замовчуванням, передбачають та сприяють упровадженню відповідних засобів контролю для контролерів РІІ та процесорів РІІ відповідно таким чином, щоб збір і обробка РІІ у цих системах обмежувалися лише тим, що необхідно для визначених цілей обробки РІІ.\*\*\*

3.8. Ці вимоги застосовуються при аутсорсингу розробки ПЗ, і регулюються в договорах згідно з Політикою інформаційної безпеки при взаємовідносинах з постачальниками та підрядниками.

3.9. При придбанні нових інформаційних систем, розробці або зміні існуючих, відповідальна особа (керівник проекту, якого призначає CEO) забезпечує виконання вимог ІБ, що викладені в технічній документації. CISO відповідальний за розробку та відображення в технічній документації вимог щодо ІБ.

3.10. При розробці вимог щодо ІБ відображається таке:

3.10.1 опис системи автентифікації, що буде використовуватися;

3.10.2 опис забезпечення конфіденційності й цілісності інформації;

3.10.3 опис забезпечення доступності із застосуванням принципу мінімальних повноважень на доступ до модулів/підсистем/середовищ/систем;

3.10.4 опис забезпечення безвідмовної роботи з урахуванням наявних робочих процесів та операційного часу;

3.10.5 опис забезпечення принципів конфіденційності за задумом та конфіденційності за замовчуванням під час розробки системи.

3.11. SOC спільно з підрозділом ІТ відповідають за визначення контролів для онлайн-транзакцій, що включають таке:

3.11.1 запобігання збоям маршруту;

3.11.2 запобігання неповній передачі даних;

3.11.3 запобігання неавторизованій зміні повідомлень;

3.11.4 запобігання неавторизованому дублюванню повідомлень;

3.11.5 запобігання неавторизованому розголошенню даних.

3.12. CSO за поданням CISO визначає методологію, обов'язки й терміни перевірки виконання вимог ІБ, погоджує переведення системи в продуктове середовище (прийняття в промислову експлуатацію). Розробка та тестування проводяться тільки з використання тестових даних. Використання інформації з обмеженим доступом у продуктивному середовищі дозволяється тільки після прийняття ПЗ в експлуатацію, що підтверджується актом прийняття та введення в експлуатацію (форма документа довільна) за рішенням CEO.

3.13. Необхідно забезпечити централізоване зберігання коду. Доступ до коду, гілок і репозиторіїв налаштовується в рамках команд розробки. Доступ надається в рамках проєкту розробки за принципом «необхідно знати» та «необхідно для роботи».

3.14. Зберігання початкового коду ПЗ організовується з урахуванням таких вимог:

3.14.1 забезпечення захисту від доступу несанкціонованих осіб;

3.14.2 забезпечення можливості виявлення змін у коді;

3.14.3 застосування технічних механізмів, що перевіряють цілісність коду;

3.14.4 створення копії з метою захисту від втрати.

3.15. Усі оновлення ПЗ установлюються на «продуктовий майданчик» лише після їх тестування. Оновлення ПЗ поставляється на «продуктові майданчики»:

3.15.1 згідно з графіком релізів (поставка на «продуктовий майданчик» оновленої версії ПЗ), що складається власником активу (ПЗ/модуль/підсистема/система);

3.15.2 після отримання оновлень від виробника (розробника) ПЗ відповідними фахівцями підрозділу ІТ (для операційних систем та загального ПЗ).

3.16. Перед кожним оновленням ПЗ створюється його резервна копія з документуванням відповідно до D14.10-СУІБ «Політика резервного копіювання». У разі невдалого встановлення оновлень, функціональність інформаційних систем відновлюється із створених резервних копій ПЗ.

3.17. Для ПЗ, що розробляється відповідно до замовлень:

3.17.1 версія ПЗ відповідає гілці у системі контролю версій і створюється розробником;

3.17.2 власник активу не пізніше ніж за 3 дні до дати релізу фіксує відповідну версію ПЗ (забороняє додавати нові задачі) і узгоджує склад версії у вигляді переліку задач;

3.17.3 у випадку необхідності переносу задачі в наступну версію, це робить розробник за поданням власника активу;

3.17.4 згідно зі складом версії формуються Release notes (частина документації, у якій описуються зміни між випуском і попередньою версією ПЗ), за допомогою яких користувачі інформуються про зміни в ПЗ;

3.17.5 у випадку, коли необхідно терміново (поза графіком релізів) поставити оновлення на «продуктові майданчики» (hotfix), власник проєкту розробки ПЗ узгоджує це з підрозділом ІТ;

3.17.6 для термінового релізу розробником створюється окрема версія ПЗ, що є копією версії, розташованій на «продуктовому майданчику», уносяться необхідні зміни згідно із задачею в застосунок «Redmine» (серверний [вебзастосунок](https://uk.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1%D0%B7%D0%B0%D1%81%D1%82%D0%BE%D1%81%D1%83%D0%BD%D0%BE%D0%BA" \o "Вебзастосунок) для [управління проєктами](https://uk.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%BF%D1%80%D0%BE%D1%94%D0%BA%D1%82%D0%B0%D0%BC%D0%B8) та відстежування помилок) і виконується реліз цієї версії.

3.18. Для операційних систем, загального та технологічного ПЗ:

3.18.1 підрозділ ІТ або адміністратор ЄІС після отримання оновлень проводить їх установлення на відповідні системи або пристрої в тестовому середовищі;

3.18.2 підрозділ ІТ або адміністратор інформаційного активу/систем після отримання позитивних результатів тестування інформує свого керівника про це і узгоджує з ним дату встановлення оновлень на продуктові площадки чи обладнання;

3.18.3 підрозділ ІТ або адміністратор ЄІС забезпечує встановлення оновлень на «продуктові майданчики» та обладнання з урахуванням мінімізації часу простою (непрацездатності) критичних інформаційних систем (як правило в неробочий час або святкові та неробочі дні).

3.19. У разі успішного встановлення оновлень ПЗ, створені перед оновленням резервні копії ПЗ знищуються не раніше ніж через 7 днів.

3.20. Конфіденційні дані не можуть бути використані як тестові дані. Слід використовувати фальшиві або синтетичні РІІ. Якщо використання РІІ для тестування неможливо уникнути, для мінімізації ризиків слід ужити технічних та організаційних заходів, еквівалентних тим, що застосовуються у виробничих умовах. Якщо такі еквівалентні заходи є неможливими, слід провести оцінку ризиків і використати її результати для вибору відповідних засобів контролю, що зменшують ризики.

3.21. Винятки можуть бути затверджені тільки CEO, у цьому випадку CSO визначає порядок захисту цих даних та ухвалює його за рішенням CEO.

3.22. SOC визначає рівень навичок і знань з безпеки працівників і бере участь у підготовці тренінгів для посадових осіб, які розробляють ПЗ.

3.23. Особи, які розробляють та підтримують прикладне ПЗ, мають знати й володіти технікою безпечного кодування та навчатися для уникнення, виявлення і усунення вразливостей.

3.24. Підрозділ ІТ, адміністратори ЄІС відповідають за супроводження процесу розробки ПЗ.

3.25. Керівник SOC відповідає за постійний контроль управління ризиками.

3.26. Керівник IRT відповідає за постійний контроль щодо управління інцидентами.

#### *4. Придбання ПЗ*

4.1. При придбанні нових інформаційних систем/підсистем/компонентів, розробці або зміні існуючих відповідальна особа виконкому міської ради (власник активу) документує вимоги безпеки в документі: «Специфікація вимог інформаційної безпеки» (додаток) та узгоджує з CSO.

4.2. Придбання прикладного ПЗ відбувається згідно з установленими правилами з питань закупівель товарів, робіт та послуг. Вимоги щодо безпеки формуються в документації процедур закупівлі та у відповідних договорах. Постачальник повинен надати ПЗ для проведення аудиту відповідності вимогам ІБ та аналізу ризиків.

4.3. Розробник забезпечує підтримку ПЗ.

4.4. Постачальник гарантує виконання галузевих стандартів безпеки в межах своєї системи й забезпечує оновлення системи в разі виявлення вразливостей.

4.5. До загальних вимог ІБ для взаємовідносин з постачальниками слід розглянути ІБ в рамках безпеки ланцюга постачання:

4.5.1 визначення вимог ІБ для застосування до придбання ПЗ;

4.5.2 вимагати, щоб постачальники ПЗ поширювали вимоги безпеки виконкому міської ради по всьому ланцюгу постачання, якщо вони вкладають субпідряд на частину ПЗ, що надається виконкому міської ради;

4.5.3 вимагати, щоб постачальники ПЗ поширювали відповідні методи безпеки по всьому ланцюгу постачання, якщо ці продукти включають компоненти, придбані в інших постачальників або інших організацій (наприклад, субпідрядники розробників ПЗ);

4.5.4 вимагати від постачальників ПЗ надати інформацію з описом програмних компонентів, що використовуються в продуктах;

4.5.5 вимагати від постачальників ПЗ надавати інформацію з описом реалізованих функцій безпеки та конфігурації, необхідної для безпечної роботи ПЗ;

4.5.6 упровадження процесу моніторингу та прийнятних методів перевірки того, що надані ПЗ відповідають заявленим вимогам безпеки. Приклади таких методів перевірки постачальника можуть включати тестування на проникнення та підтвердження або перевірку атестацій третьої сторони для операцій ІБ постачальника;

4.5.7 упровадження процесу ідентифікації та документування компонентів ПЗ, що є критично важливими для підтримки функціональності та, отже, вимагають підвищеної уваги;

4.5.8 наявність упевненості в тому, що критичні компоненти ПЗ та їх походження можна відстежити по всьому ланцюгу постачання;

4.5.9 наявність упевненості в тому, що поставлене ПЗ функціонує належним чином без будь-яких неочікуваних або небажаних функцій;

4.5.10 упровадження процесів для забезпечення того, щоб ПЗ від постачальників було справжнім та не змінювало специфікації. Приклади заходів включають мітки захисту від несанкціонованого доступу, перевірку криптографічного хешу або цифрові підписи. Контроль продуктивності, що не відповідає специфікаціям, може бути показником фальсифікації або підробок. Запобігання та виявлення несанкціонованого втручання має здійснюватися протягом кількох етапів життєвого циклу розробки системи, включаючи проєктування, розробку, інтеграцію, експлуатацію та технічне обслуговування;

4.5.11 наявність упевненості в тому, що ПЗ досягає необхідних рівнів безпеки, наприклад, через формальну сертифікацію або схему оцінювання, таку як домовленість про визнання загальних критеріїв;

4.5.12 визначення правил для обміну інформацією щодо ланцюга постачання та будь-яких потенційних проблем і компромісів між виконкомом міської ради та постачальниками;

4.5.13 упровадження конкретних процесів для управління життєвим циклом і доступністю ПЗ та пов’язаними з ними ризиками безпеки. Це включає управління ризиками недоступності ПЗ через те, що постачальники більше не працюють або більше не постачають це ПЗ через технологічний прогрес. У цьому випадку необхідно розглянути визначення альтернативного постачальника і процес передачі ПЗ та компетенції альтернативному постачальнику.

4.6. Надійність ПЗ є питанням контролю ефективності та результативності СУІБ.

*\*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.*

*\*\*\*Організація, що обробляє* PII*, повинна гарантувати, що згідно з відповідною юрисдикцією вона видаляє РІІ після закінчення певного періоду. Система, що обробляє ці PII, повинна бути спроєктована таким чином, щоб полегшити виконання вимоги щодо видалення.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***