*ЗАТВЕРДЖЕНО*

*Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА КЛАСИФІКАЦІЇ ІНФОРМАЦІЇ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика класифікації інформації виконавчого комітету Криворізької міської ради (надалі – Політика) є документом для впровадження заходів з інформаційної безпеки (надалі – ІБ) та кібербезпеки для захисту інформаційних активів (надалі – ІА) відповідно до рівня їх конфіденційності й критичності.

1.2. Мета Політики полягає:

1.2.1 у наведенні схеми класифікації інформаційних активів включаючи персональні дані (надалі – PII) суб'єктів PII, що оброблюються в межах області дії системи управління інформаційною безпекою (надалі – СУІБ) в функціональних підсистемах Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС): «Підсистема документообігу», «Підсистема кадрового забезпечення» та «Web-портал»;

1.2.2 у визначенні критеріїв і рівнів конфіденційності (надалі – РК) ІА.

1.3. Політика дозволить виконкому міської ради:

1.3.1 дотримуватися юридичних зобов'язань щодо визначення типу та критичності ІА;

1.3.2 забезпечити кращий контроль та моніторинг виконання умов обробки ІА;

1.3.3 забезпечити впровадження принципу надання мінімальних повноважень користувачам інформаційно-комунікаційних систем (надалі – ІКС) стосовно доступу до конкретних PII в залежності від їх критичності. Упровадження цього принципу гарантує суб’єкту PII, що будь-яка інформація, призначена для громадськості або суб’єкта PII, є зрозумілою суб’єктам PII, контролеру PII, процесору PII з точку зору її важливості та застосування відповідних технологій захисту PII, включаючи шифрування, анонімізацію та псевдонімізацію.

1.4. Політика застосовується до всієї області дії СУІБ, а саме:

1.4.1 усіх операційних процесів та інформації, що обробляється в ІКС;

1.4.2 усіх посадових осіб виконкому міської ради, процесорів PII, суб'єктів PII, провайдерів, підрядників, консультантів, постачальників, партнерів та інших сторонніх осіб, які пов’язані з інформаційною діяльністю виконкому міської ради або отримують доступ до сервісів ІКС, активів, у тому числі ІА, у межах області дії СУІБ.

1.5. Політика розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу ІБ, 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 «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки», ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT)

«Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови», Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄC (Загального регламенту про захист даних) (надалі – GDPR), політик, процедур і технічних заходів: D4.1-СУІБ «Політика інформаційної безпеки», D4.2-СУІБ «Політика захисту персональних даних», D11.1-СУІБ «Методологія оцінки впливу на захист персональних даних», D11.2-СУІБ «Реєстр ризиків» (захист PII, оцінка впливу, DPIA), D2-СУІБ «Порядок ідентифікації вимог», D3-СУІБ «Сфера застосування СУІБ», D12-СУІБ «Заява про застосовність (SoA)», D14.20-СУІБ «Процедура управління інцидентами», D8.1-СУІБ «Положення щодо інвентаризації та обробки даних».

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

2.1. 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.

2.2. 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.\*

2.3. 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.

2.4. 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)].

2.5. 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.\*\*

2.6. 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.

2.7. 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.

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

2.9. 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.

2.10. 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.

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

2.12. Інформаційно-комунікаційна система (надалі – ІКС) – до складу якої належить комплекс апаратних, програмних, апаратно–програмних (фізичних та/абовіртуальних) телекомунікаційних засобів, призначених для маршрутизації, комутації, зберігання, приймання, передавання інформації між кінцевим обладнанням ІКС у межах виконання цілей виконкому міської ради.

2.13. PII – персональні дані.

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

2.15. Ad1 – адміністратор безпеки.

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

2.17. 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, співконтролерів 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. ІзОД – інформація з обмеженим доступом.

2.21. Bring your own device (BYOD) – це IT-політика, згідно з якою посадовим особам дозволено або рекомендується використовувати особисті мобільні пристрої (телефони, планшети, ноутбуки) для доступу до даних та систем.

#### *3.* *Класифікація інформації*

3.1. Класифікація та пов’язані з нею заходи безпеки щодо інформації враховують операційні процеси, що стосуються спільного використання чи обмеження інформації, а також вимоги національного та міжнародного законодавства в галузі ІБ.

3.2. Заходи та обов'язки в галузі управління інформацією наведені в таблиці1:

Таблиця 1 Заходи та обов'язки

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Заходи*** | ***Обов'язок*** |

| ***1*** | ***2*** | ***3*** |
| --- | --- | --- |
| 1 | Інвентаризація активів (первинних, підтримки, у тому числі ІА), документування, визначення власників ІА та під-тримка їх актуальності | CEO - відповідальний за своєчасність проведення інвентаризації усіх активів СУІБ, всебічний контроль та забезпечення ресурсами для якісного проведення інвентаризації.  CSO – відповідальний за своєчасність та ефективність проведення заходів з інвентаризації, здійснює контроль за строками проведення інвентаризації усіх активів СУІБ та ефективним застосуванням ресурсів.  CISO – відповідальний за результативність проведення заходів з інвентаризації у межах області дії СУІБ, контролює повноту проведених заходів, актуальність активів та власників активів, відповідність проведених заходів з інвентаризації усіх активів СУІБ до вимогам керівних документів, визначених у D2-СУІБ «Порядок ідентифікації вимог» |
| 2 | Класифікація інформації | Власник активів |
| 3 | Маркування інформації | Власник активів, адміністратор документів |
| 4 | Обробка ІА | Особа, що має певну роль у СУІБ та яка має право доступу до відповідних ІА із застосуванням принципу надання мінімального рівня повноважень у межах правил розмежування доступу, що встановлені Політикою інформаційної безпеки, Політикою контролю доступу, Політикою захисту PII |

3.3. Якщо інформація була отримана від зовнішньої сторони, то відповідальною за класифікацію інформації є посадова особа виконкому міської ради, до компетенції якої належить отримання певного виду інформації. Отримавши інформацію, посадова особа стає власником даного ІА.

3.4. Критерії класифікації: рівень захисту інформаційних ресурсів визначається за допомогою аналізу конфіденційності, цілісності й доступності та будь-яких інших вимог для інформації, що розглядають, а саме:

3.4.1 цінність інформації ґрунтується на рівні впливу, отриманого в процесі оцінки ризиків;

3.4.2 чутливість і критичність інформації ґрунтується на рівні максимального ризику для кожного ІА, отриманого в процесі оцінки ризиків;

3.4.3 законодавчі та договірні вимоги ґрунтується на вимогах D2-СУІБ «Порядок ідентифікації вимог» (додаток – D2.1-СУІБ «Перелік юридичних, нормативних, договірних та інші вимоги»).

3.5. Кожному РК надано ім’я, що має сенс у контексті використання схеми класифікації.

3.6. Уся інформація в межах області дії СУІБ класифікується у відповідності до відомостей, наведених у таблиці 2. Таблиця 2 Схема класифікації інформаційних активів.

Таблиця 2 Схема класифікації ІА

|  |  |  |  |
| --- | --- | --- | --- |
| ***№ п/п*** | ***Класифікація інформації по категоріям*** | ***Критерій класифікації інформації*** | ***Маркування РК*** |

| ***1*** | ***2*** | ***3*** | ***4*** |
| --- | --- | --- | --- |
| 1 | ПУБЛІЧНА  (РК0) | | |
| 1.1 | «ПУБЛІЧНА» | Будь-яка інформація, за якою було ухвалено рішення про те, що вона може бути оприлюднена й розголошення якої не завдає шкоди інтересам виконкому міської ради.  Вимоги до захисту властивостей: вимоги щодо захисту не висовуються, інформація є відкритою | Інформація може бути доступна громадськості.  При маркуванні документів з РК «ПУБЛІЧНА» не обов’язково наводити маркування РК0 відповідно до пункту 4.3.1 цього документа |
| 2 | ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ  (РК1) | | |
| 2.1 | «ДЛЯ  ВНУТРІШНЬО-ГО ВИКОРИСТАННЯ» | Будь-яка інформація несанкціонований доступ, виток, розголошення якої з порушеною цілісністю призведе до мінімальної шкоди або мінімальних операційних незручностей виконкому міської ради.  Вимоги до захисту властивостей:  захист стосовно конфіденційності не висовуються, захист стосовно цілісності та доступності висовуються, є відкритою, але цю інформацію дозволено розповсю-джувати між користувачами, що мають певну роль у межах області дії СУІБ | РК «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ» або РК1.  Інформація доступна всім користувачам ІКС та зацікавленим сторонам, які дотичні до інформаційної діяльності виконкому міської ради в межах області дії СУІБ (постачаль-ники послуг/програмного забезпечення/компонентів ІКС, провайдери, хостинг компанії, процесори PII, суб’єкти PII, інші сторони, що здійснюють обслуговування систем у цілях виконкому міської ради) |
| 3 | Ідентифіковані PII  («ЧУТЛИВА» та «PII КОНФІДЕНЦІЙНО»)  (РК21, РК22, РК23, РК24, РК25) | | |
| 3.1 | «ЧУТЛИВА» | «ЧУТЛИВА» – це будь-яка інформація, що в складі має PII, несанкціонований доступ, виток або розголошення якої може завдати значної шкоди суб’єкту PII.  Розкриття має значний короткочасний вплив на тактичні цілі виконкому міської ради, може призвести до величезних штрафних санкцій та значно погіршити довіру суб’єктів PII і регуляторних органів.  «ЧУТЛИВА» поділяється на такі види інформації: РК21, РК22  Вимоги до захисту властивостей «ЧУТЛИВА»: захист стосовно конфіденційності цілісності та доступності висовуються, є конфіденційною та належить до ІзОД | РК «ЧУТЛИВА» (РК21, РК22)  PII доступна тільки обмеженому колу осіб за мінімальних потреб для доступу до PII з відповідним ступенем обмеження доступу в межах визначених повноважень в області дії СУІБ |
| 3.2 | «PII  КОНФІДЕНЦІЙНО» | «PII КОНФІДЕНЦІЙНО» – це будь-яка інформація, що у своєму складі має PII, несанкціонований доступ, виток або розголошення якої може завдати шкоди суб’єкту PII.  Розкриття має значний короткочасний вплив на тактичні цілі виконкому міської ради, може призвести до величезних штрафних санкцій та значно погіршити  довіру суб’єктів PII і регуляторних органів.  «PII КОНФІДЕНЦІЙНО» поділяється на такі види інформації: РК23, РК24, РК25;  Вимоги до захисту властивостей «PII КОНФІДЕНЦІЙНО»: захист стосовно конфіденційності, цілісності та доступності висовуються, є конфіденційною та належить до інформації ІзОД | РК «PII КОНФІДЕНЦІЙНО» » (РК23, РК24, РК25)  PII доступна тільки обмеженому колу осіб за мінімальних потреб для доступу до PII з відповідним ступенем обмеження доступу в межах визначених повноважень в області дії СУІБ |
| 4 | ДІЛОВА ІНФОРМАЦІЯ | | |
|  | «ДІЛОВА ІН-ФОРМАЦІЯ» | Будь-яка інформація несанкціонований доступ, виток або розголошення якої може завдати суттєвої шкоди інтересам виконкому міської ради та мати великий вплив на довгострокові стратегічні цілі.  Поділяється на такі види інформації: РК31, РК32, РК33.  Вимоги до захисту властивостей «ДІЛОВА ІНФОРМАЦІЯ»: захист конфіденційності, цілісності та доступності висовуються, є приватною інформацією виконкому міської ради | РК «ДІЛОВА ІНФОРМАЦІЯ» (РК31, РК32, РК33).  Інформація доступна тільки конкретному колу посадових осіб виконкому міської ради в межах визначених повноважень |
| 5 | ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ | | |
|  | «ТЕХНО-  ЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ» | Технологічна інформація захисту (надалі – ТІЗ), виток або розголошення якої може загрожувати припиненням працездатності ІКС та діяльності виконкому міської ради.  Вимоги до захисту властивостей ТІЗ: захист конфіденційності, цілісності та доступності висовую-ться, ТІЗ є ІзОД | РК «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ» (РК4).  Інформація доступна тільки конкретному користувачу ІКС з адміністративною роллю, як виняток за рішенням СЕО може бути доступна конкретному привілейованому користувачу Us1 |

3.7. До категорії «ПУБЛІЧНА» (РК0) належить уся інформація, що створюється в діяльності виконкому міської ради, якщо інше не було визначено СЕО, вона є відкритою та публічною.

3.8. До категорії «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ» (РК1) належить інформація, що утворюється в діяльності виконкому міської ради й є відкритою для посадових осіб. Інформація «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ» не є публічною, доступна всім користувачам ІКС та зацікавленим сторонам у межах області дії СУІБ. Уся документація СУІБ має категорію «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ», якщо Власником СУІБ не визначена інша категорія (РК) на конкретну інформацію, що оброблюється в ІКС. До інформації «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ» застосовується довірче розмежування доступу (власник ІА самостійно може надавати права доступу до конкретного свого ІА користувачу ІКС у межах області дії СУІБ з дотриманням вимог Політики інформаційної безпеки). Інформація з РК «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ» протягом усього життєвого циклу в ІКС зберігає цілісність та доступність.

3.9. Інформація з РК «ЧУТЛИВА» та «PII КОНФІДЕНЦІЙНО» належить до PII і дозволяє ідентифікувати суб’єкта PII та є інформацією особистого характеру, що стосується, у тому числі, недоторканності приватного життя суб’єкта PII.

3.10. PII є ІзОД.

3.11. Інформація з РК «ЧУТЛИВА» у діяльності виконкому міської ради поділяється на такі види інформації:

3.11.1 РК21 (спеціальна інформація, перелік якої визначено в пункті 3.35.1 Політики);

3.11.2 захищена медична інформація, перелік якої визначено в пункті 3.35.2 Політики (надалі – protected health information або РК22).

3.12. Інформація з РК «PII КОНФІДЕНЦІЙНО» у діяльності виконкому міської ради поділяється на такі види:

3.12.1 PII робочого характеру, перелік яких визначено в пункті 3.35.3 Політики (РК23);

3.12.2 особиста інформація [дані про освіту, трудова діяльність та фінансові відомості, інтелектуальна власність (intellectual property, IP)], перелік якої визначено в пункті 3.35.5 Політики (РК24),

3.12.3 PII, що стосуються фізичної особи, яку ідентифіковано чи можна ідентифікувати, перелік яких визначено в пункті 3.35.6 Політики (РК25).

3.13. PII супроводжуються списком уповноважених осіб, у якому власник ІА вказує прізвище, ім’я, по батькові (надалі – ПІБ) або посаду осіб, які мають право доступу до цих PII.

3.14. До PII застосовується адміністративне розмежування доступу (тільки Ad1 може налаштувати права доступу до конкретного ІА користувачу ІКС у межах області дії СУІБ з дотриманням вимог Політики інформаційної безпеки, Політики контролю доступу, Політики захисту персональних даних).

3.15. Власники ІА регулярно переглядають РК не рідше разу на рік і, якщо це допустимо, знижують РК в межах виконання правила «Використання найнижчого РК, забезпечує відповідний рівень захисту для уникнення зайвих захисних заходів».

3.16. До категорії «ДІЛОВА ІНФОРМАЦІЯ» належить інформація, що є конфіденційною відповідно до рішення виконкому міської ради на виконання законодавства України (ведення військового обліку), а також робоча та ділова інформація, доступна тільки конкретній посадовій особі чи колу осіб.

3.17. «ДІЛОВА ІНФОРМАЦІЯ» протягом усього життєвого циклу в ІКС зберігає конфіденційність, цілісність та доступність.

3.18. Інформація, класифікована як «ДІЛОВА ІНФОРМАЦІЯ», супроводжується списком уповноважених осіб, у якому власник ІА вказує ПІБ або посаду осіб, які мають право доступу до цієї інформації.

3.19. До інформації з РК «ДІЛОВА ІНФОРМАЦІЯ» застосовується адміністративне розмежування доступу (тільки Ad1 може налаштувати права доступу до конкретного ІА користувачу ІКС у межах області дії СУІБ з дотриманням вимог Політики інформаційної безпеки, Політики контролю доступу, Політики захисту персональних даних).

3.20. Власники ІА регулярно переглядають РК не рідше разу на рік і, якщо це допустимо, знижують РК в межах виконання правила «Використання найнижчого РК, забезпечує відповідний рівень захисту для уникнення зайвих захисних заходів».

3.21. До категорії ТІЗ належить інформація стосовно адміністрування та управління компонентами комплексу засобів захисту ІКС і налаштування правил розмежування доступу.

3.22. ТІЗ протягом усього життєвого циклу в ІКС зберігає конфіденційність, цілісність та доступність.

3.23. Інформація, класифікована як ТІЗ, супроводжується списком уповноважених осіб, у якому Ad1 вказує ПІБ або посаду осіб, які мають право доступу до цієї інформації.

3.24. До ТІЗ застосовується адміністративне розмежування доступу. ТІЗ доступна тільки конкретному користувачу ІКС з адміністративною роллю, як виняток за рішенням СЕО може бути доступна конкретному привілейованому користувачу Us1 у межах області дії СУІБ з дотриманням вимог Політики інформаційної безпеки, Політики контролю доступу, Політики захисту персональних даних.

3.25. Ad1 регулярно переглядає РК ІА не рідше разу на рік і, якщо це допустимо, знижує РК в в межах виконання правила «Використання найнижчого РК, забезпечує відповідний рівень захисту для уникнення зайвих захисних заходів».

3.26. ІзОД в ІКС – є PII, «ДІЛОВА ІНФОРМАЦІЯ», «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ», що захищена від несанкціонованого доступу та періодично оцінюється відповідно до критеріїв контролю ІБ згідно з вимогами ДСТУ ISO/IEC 27001, ДСТУ ISO/IEC 27701, D11.1-СУІБ «Методологія оцінки впливу на захист персональних даних».

3.27. Перелік інформації «ПУБЛІЧНА», що належить виконкому міської ради підлягає оприлюдненню в мережі «Інтернет» на офіційному вебсайті Криворізької міської ради та її виконавчого комітету (надалі – вебсайт):

3.27.1 загальнодоступна інформація – публічно оголошувана інформація, користуватися якою можуть будь-які фізичні або юридичні особи, що мають доступ до мережі «Інтернет»;

3.27.2 інформація про організаційну структуру виконкому міської ради, функції, повноваження, основні завдання, напрями діяльності;

3.27.3 нормативно-правові акти (крім внутрішньо-організаційних);

3.27.4 проєкти рішень міської ради та її виконавчого комітету, що підлягають обговоренню;

3.27.5 інформація про нормативно-правові засади діяльності виконкому міської ради;

3.27.6 форми й зразки документів, правила їх заповнення;

3.27.7 порядок складання, подання запиту на інформацію, оскарження рішень, дій чи бездіяльності посадових осіб;

3.27.8 інформація про механізми чи процедури, за допомогою яких громадськість може представляти свої інтереси;

3.27.9 загальні правила роботи виконкому міської ради, правила внутрішнього трудового розпорядку;

3.27.10 інформація про діяльність виконкому міської ради, а саме:

3.27.10.1 місцезнаходження, поштову адресу, номери засобів зв'язку, адреси вебсайта та електронної пошти;

3.27.10.2 прізвище, ім'я та по батькові, службові номери засобів зв'язку, адресу електронної пошти відділів, управлінь, інших виконавчих органів міської ради, їх основні функції, крім випадків, коли ці відомості належать до ІзОД;

3.27.10.3 розклад роботи та графік прийому громадян;

3.27.10.4 вакансії, порядок і умови проходження на заміщення вакантних посад;

3.27.10.5 перелік та умови надання послуг, форми й зразки документів, необхідних для надання послуг, правила їх оформлення;

3.27.10.6 перелік і службові номери засобів зв'язку комунальних підприємств, установ та організацій, що належать до сфери управління виконкому міської ради;

3.27.10.7 інша інформація про діяльність виконкому міської ради, порядок обов'язкового оприлюднення якої встановлено законом;

3.27.10.8 тендерна документація, розроблена відповідно до вимог Закону України «Про публічні закупівлі»;

3.27.10.9 відомості про посадових осіб виконкому міської ради, уповноважених здійснювати зв’язок з учасниками тендерної процедури;

3.27.10.10 назва предмета закупівлі, інформація про технічні, якісні та кількісні характеристики предмета закупівлі;

3.27.10.11 місце, кількість, обсяг поставки товарів (надання послуг, виконання робіт);

3.27.10.12 строк поставки товарів (надання послуг, виконання робіт);

3.27.10.13 відомості щодо умов, правил, обмежень, кваліфікаційні та технічні критерії, технічні вимоги до предмету закупівлі та надання роз’яснень стосовно тендерної документації;

3.27.10.14 відомості про результати торгів та зміст договорів про закупівлю.

3.28. Негайному оприлюдненню підлягає будь-яка інформація про факти, що загрожують життю, здоров'ю або/та майну громадян, та про заходи, які застосовуються у зв'язку з цим.

3.29. Державні інформаційні ресурси (надалі – ДІР) – це відкрита інформація «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ», що відображена та задокументована в електронному вигляді.\*\*\*

3.30. ДІР – це інформація, необхідність захисту якої визначено Постановою Кабінету Міністрів України від 07 вересня 2011 року №938 «Про внесення змін до деяких постанов Кабінету Міністрів України з питань доступу до інформації». ДІР – це інформаційні ресурси, що внесені та/або плануються до внесення до реєстру інформаційних, телекомунікаційних та інформаційно-комунікаційних систем органів виконавчої влади. Для однозначної ідентифікації ДІР слід ураховувати правило, яке визначає, що ДІР створюється за державні кошти. До ДІР відповідно до вимог додатка «Перелік відомостей про інформаційну, електронну комунікаційну та інформаційно-комунікаційну систему органу виконавчої влади, а також підприємства, установи і організації, що належать до сфери його управління» до Положення про Реєстр інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належить до сфери їх управління, затвердженого Постановою Кабінету Міністрів України від 03 серпня 2005 року №688, належать відомості про склад, структуру, розміщення, умови функціонування, призначення ІКС державних органів та/або державних підприємств (надалі – ІКС ДІР), стан захисту інформації, якщо ця інформація не віднесена до конфіденційної, службової інформації та/або державної таємниці.

3.31. ДІР – це систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, державним підприємствам, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб’єктами владних повноважень (представлені у вигляді – файлів різних форматів, електронних листів, записів таблиць баз даних).

3.32. До ДІР, що оброблюється в ІКС виконкому міської ради в межах інформаційної взаємодії з державними органами та/або державними підприємствами, належить така інформація:

3.32.1 повна назва ІКС ДІР;

3.32.2 повне найменування власника СУІБ ДІР;

3.32.3 відомості щодо технічного завдання та заходів зі створення СУІБ у ІКС ДІР;

3.32.4 відомості про віднесення інформації до ДІР, що обробляється або планується до обробки в ІКС;

3.32.5 режим доступу до ДІР, що обробляються в ІКС;

3.32.6 місцезнаходження елементів ІКС ДІР, якщо ця інформація не віднесена до конфіденційної та/або службової інформації та/або державної таємниці відповідно до чинного законодавства;

3.32.7 зведені дані за видами та кількістю одиниць комп'ютерної техніки, комутаційного та телекомунікаційного обладнання, що використовуються в ІКС ДІР, спосіб їх об'єднання в ІКС ДІР (окремі автоматизовані робочі місця, сервер, локальні та/або розподілені телекомунікаційні мережі тощо) без оголошення/розповсюдження відомостей щодо налаштування комплексу засобів захисту;

3.32.8 відомості про підключення ІКС ДІР до мережі «Інтернет», інших глобальних мереж передачі даних та систем, що не входять до її складу, із зазначенням типу зв'язку (постійний, комутований тощо), типу і швидкості каналів зв'язку, їх належності, телекомунікаційних операторів та провайдерів;

3.32.9 відомості про наявність кластерів і їх призначення у ІКС ДІР із зазначенням кількості кластерів та кількості одиниць комп'ютерної техніки і зовнішніх систем зберігання даних у кожному кластері;

3.32.10 назва та версія операційних систем, що використовуються в ІКС ДІР, з відображенням кількості одиниць комп'ютерної техніки, де вони встановлені;

3.32.11 назва та версія програмного забезпечення, що використовується в ІКС ДІР, з відображенням кількості одиниць комп'ютерної техніки, де воно встановлено;

3.32.12 відомості щодо серверів (склад, місце розташування), що входять до складу ІКС ДІР;

3.32.13 відомості про правила розмежування доступу (наявність документального визначення) відповідно до обов'язків користувачів ІКС ДІР та/або персоналу щодо їх функцій у ІКС ДІР (системні адміністратори, Ad1 та баз даних, звичайні користувачі ІКС ДІР);

3.32.14 види оброблення (створення, зберігання, накопичення, передавання, видалення тощо) ДІР, способи й методи його здійснення в ІКС ДІР;

3.32.15 види електронних носіїв інформації (накопичувачі на твердих та/або гнучких магнітних дисках, оптичні диски тощо), що використовуються для зберігання (у тому числі тимчасового) ДІР ;

3.32.16 відомості про наявність відповідальної особи та/або підрозділу за стан технічного та/або криптографічного захисту ДІР у ІКС ДІР, у тому числі на які покладено функції служби захисту інформації відповідно до вимог нормативних документів з технічного захисту інформації;

3.32.17 відомості про назву, зміст та вміст документів СУІБ (назва, реєстраційний номер, зміст), якщо ця інформація не віднесена до конфіденційної та/або службової інформації та/або державної таємниці;

3.32.18 види та типи засобів криптографічного захисту інформації, що використовуються в ІКС ДІР, без розкриття їх характеристик. Відомості про наявність для зазначених засобів сертифікатів відповідності, експертних висновків та/або документів щодо допуску до експлуатації згідно з вимогами нормативних документів з криптографічного захисту інформації;

3.32.19 види та типи засобів технічного захисту інформації, у тому числі антивірусного, що використовуються у системі, з відображенням назв і версій цих засобів та кількості одиниць комп'ютерної техніки, де вони встановлені. Відомості про наявність для зазначених засобів сертифікатів, експертних висновків, дозволів згідно з вимогами нормативних документів з технічного захисту інформації;

3.32.20 відомості про проведення та результати сертифікаційних випробувань СУІБ ІКС ДІР;

3.32.21 відомості про спроби вчинення та (або) вчинені несанкціоновані дії стосовно ІКС ДІР.

3.33. До категорії «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ» належить інформація, що створюється в діяльності виконкому міської ради, а саме:

3.33.1 відомості «Wiki-системи» (єдина база знань виконкому міської ради) для внутрішнього використання посадовими особами;

3.33.2 інтелектуальна власність виконкому міської ради;

3.33.3 відомості щодо наявності програмних засобів (прикладне програмне забезпечення, системне програмне забезпечення, інструментальні засоби розробників і утиліти, комплекс засобів захисту без розкриття правил налаштувань і ролевої моделі);

3.33.4 узагальнені відомості щодо наявності апаратних, апаратно-програмних, фізичних активів та послуг (тип, кількість, вартість, назва виробника, відповідальний за актив), що є на фінансовому балансі виконкому міської ради;

3.33.5 відомості про підключення інформаційних систем до мережі «Інтер-нет», інших глобальних мереж передачі даних та систем, із зазначенням типу зв'язку (постійний, комутований тощо), типу та швидкості каналів зв'язку, їх належності, телекомунікаційних провайдерів;

3.33.6 програмні продукти (модулі, сегменти, програмні коди тощо), створені для внутрішніх потреб та/або розроблені на замовлення зовнішніх сторін, технічна, проєктна, робоча, конструкторська, експлуатаційна, звітна та супровідна документація щодо виготовлених активів;

3.33.7 відомості, що мають знеособлені PII (тобто ті що не є PII) та отримані в процесі інформаційної діяльності в межах області дії СУІБ з підсистем ЄІС.

3.34. Транзитна інформація – це інформація «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ», до якої належать мережеві інформаційні потоки абонентів, що користуються послугами доступу до мережі «Інтернет», у вигляді ІР-пакетів.

3.35. PII – це ІзОД, до якої належить:

3.35.1 РК21 – це «ЧУТЛИВА» ІзОД, що за своєю специфікою є особливо чутливою щодо фундаментальних прав і свобод, потребує особливого захисту, оскільки контекст її опрацювання може створити істотні ризики для фундаментальних прав і свобод Суб’єкта РІІ. Відповідно до пункту 7.2.5 ДСТУ ISO/IEC 27701 вона належить до спеціальних категорій PII, до якої належать особисті дані, що розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, членство в профспілці, генетичні дані, біометричні дані, оброблені виключно для ідентифікації людини, дані про статеве життя людини або сексуальну орієнтацію (стаття 4 (13), (14) та (15), стаття 9 та твердження (51)-(56) GDPR).

3.35.2 РК22 – це «ЧУТЛИВА» ІзОД, до якої належить захищена медична інформація (protected health information), що відповідно до пункту 7.2.5 ДСТУ ISO/IEC 27701 належить до спеціальних категорій PII (інформація, що стосується стану здоров'я). Записи лікаря, що призводять до створення/додавання

інформації до електронної медичної картки (electronic health record) фізичної особи. Ця картка має зберігатися в ІКС виконкому міської ради (підрозділ кадрів, бухгалтерії тощо) з наведенням даних про:

3.35.2.1 фізичне здоров'я;

3.35.2.2 психічне здоров'я та іншу особисту інформацію;

3.35.2.3 історії хвороби, РК22 може також включати інформацію про членів сім'ї цієї людини. PII стосовно стану здоров'я містять всі дані, що пов'язані зі станом здоров'я суб'єкта PII та розкривають інформацію про минулий, поточний або майбутній стан фізичного чи психічного здоров'я суб'єкта PII.\*\*\*\*

3.35.3 РК23 – конфіденційна інформація «PII КОНФІДЕНЦІЙНО», що дозволяє ідентифікувати особу, яка є посадовою особою виконкому міської ради. До складу РК23 належить така інформація про суб’єкта PII, що є посадовою особою:

3.35.3.1 номер робочого телефону;

3.35.3.2 IP робочої станції;

3.35.3.3 робочий email;

3.35.3.4 ПІБ;

3.35.3.5 місце розташування;

3.35.3.6 дані щодо маскування, анонімізації та псевдонімізації, зміст яких дозволяє зв’язати із знеособленими даними та однозначно ідентифікувати суб’єкт PII;

3.35.3.7 будь-яка інформація, що використовується для ухвалення рішень про працевлаштування, відомості стосовно соціального страхування;

3.35.3.8 відомості з адміністрування посадових осіб виконкому міської ради та формування звітності з кадрового адміністрування;

3.35.3.9 відомості документів про відрядження;

3.35.3.10 дані про пенсіонерів/третіх осіб;

3.35.3.11 відомості щодо ведення, оцінки та коригування часових даних посадових осіб виконкому міської ради, звітність, табель робочого часу;

3.35.3.12 відомості щодо даних із соціальних виплат, у т.ч. пенсіонерам та третім сторонам, премії, розрахунок заробітної плати, платіжні документи та проводки за результатами розрахунку заробітної плати, розрахунковий листок.

3.35.4 До РК23 належать відомості стосовно посадових осіб виконкому міської ради, які забезпечують ІБ:

3.35.4.1 відомості про наявність фахівців та підрозділів виконкому міської ради, які забезпечують ІБ, їх чисельний склад, посада, прізвище, ім’я по батькові, контактні дані, зобов’язання;

3.35.4.2 відомості про фахівців, які залучаються до комісій з питань контролю за станом СУІБ, керування інцидентами ІБ, їх чисельний склад, посада, прізвище, ім’я та по батькові, контактні дані, зобов’язання;

3.35.4.3 результати проведення розслідувань за фактами порушень Політики інформаційної безпеки й виявленим інцидентам щодо конфіденційної та чутливої інформації.

3.35.5 РК24 – конфіденційна інформація «PII КОНФІДЕНЦІЙНО», до якої належать відомості про:

3.35.5.1 освіту суб’єкта PII, містять інформацію про оцінки, результати тестів, відвідуваність, проходження курсів, нагород, присуджених ступенів та дисциплінарні звіти. Цей запис може також включати контактну інформацію, PII, записи про спеціальну освіту, включаючи індивідуальні освітні програми (individualized education programs);

3.35.5.2 відомості щодо трудової діяльності: інформація про зайнятість, що включає минулу зайнятість, результати роботи, контактну інформацію та PII. Трудові книжки, страхування та PII.

3.35.5.3 фінансові відомості: фінансові записи, що містять інформацію про доходи, витрати та PII, податкові записи, виписки з кредитних карток, кредитний рейтинг, банківську інформацію та PII.

3.35.5.4 інтелектуальна власність (intellectual property) суб’єкта PII.

3.35.6 РК25 – конфіденційна інформація «PII КОНФІДЕНЦІЙНО», до якої належить будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ПІБ, індивідуальний податковий номер, номер телефону або контактні дані соціальної мережі, дані про місцеперебування та/або шляхи пересування особи, громадянство, адреса проживання, номер власного автомобіля, онлайн-ідентифікатор робочої станції (використання власного пристрою), приватний email, банківські реквізити-IBAN, за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.

3.36. РК25 може становити (пункт (18) GDPR) відомості про особисту або побутову діяльність суб’єкта PII, які контролер PII або процесор PII може отримати в процесі надання суб’єкту PII засобів для опрацювання PII для такої особистої або побутової діяльності. Особисту чи побутову діяльність може становити ведення кореспонденції та зберігання адрес, або ведення соціальних мереж і онлайн-діяльності, розпочатої в контексті такої діяльності.

3.37. «ДІЛОВА ІНФОРМАЦІЯ» – це інформація, до якої належить робоча (РК31) і ділова (РК32) інформація виконкому міської ради та інформація щодо захисту комерційної таємниці (РК33), втрата якої може створити небажаний ризик несанкціонованого витоку в громадськість або стороннім організаціям та нанести суттєвої шкоди інтересам виконкому міської ради й мати великий вплив на довгострокові стратегічні цілі.

3.38. Втрата РК3 може призвести до:

3.38.1 погіршення ділового стану виконкому міської ради або третіх сторін, з якими встановлені робочі стосунки;

3.38.2 втрата цінності робочих операційних процесів у межах області дії СУІБ;

3.38.3 порушення планів і кінцевих термінів виконання контрактів, невідкладних завдань тощо;

3.38.4 порушення законодавчих, регулюючих або договірних вимог.

3.39. До РК31 належать:

3.39.1 узагальнені відомості про посадових осіб виконкому міської ради, що не належать до PII та включають знеособлені дані про фізичну особу з наведенням розміру заробітної плати, фінансових винагород, листи з пропозиціями, угоди посадових осіб;

3.39.2 зведені фінансові дані за виконкомом міської ради (звіти про доходи, баланси та звіти про рух грошових коштів, що дають змогу визначити дійсний фінансовий стан);

3.39.3 узагальнені відомості щодо наявності програмних засобів (прикладне програмне забезпечення, системне програмне забезпечення, інструментальні засоби розробників і утиліти, комплекс засобів захисту (надалі – КЗЗ) з наведенням їх вартості та шляхів походження;

3.39.4 узагальнені відомості щодо наявності активів і застосованих заходів захисту (бази даних і файли даних, системна документація, дослідницька інформація, навчальні матеріали, процедури: експлуатаційні або підтримки, плани безперервності операційних процесів, аудиторські акти та архівована інформація);

3.39.5 відомості щодо ведення обліку юридичних (податкових) організацій.

3.40. До РК32 належить (якщо ця інформація не віднесена за рішенням власника ІА до конфіденційної інформації ТІЗ):

3.40.1 облікова та звітна документація виконкому міської ради стосовно його діяльності (контракти, договори, угоди, протоколи, акти, дозволи та інші документи, що складають цінні активи для виконкому міської ради);

3.40.2 відомості з ведення військового обліку;

3.40.3 інформація, що розкриває концепцію, плани розвитку та стратегію виконкому міської ради в інтересах забезпечення робочих процесів;

3.40.4 програмна документація (структури вхідних та вихідних даних, алгоритми розв'язання завдань, форми представлення вхідних і вихідних даних, відомості щодо визначення семантики й синтаксису мови, структура та опис програми, відомості щодо конфігурації програмного продукту, технічне завдання, технічні вимоги, програма та методики випробувань створеного програмного забезпечення, акт та протоколи випробувань);

3.40.5 контракти, угоди з вендорами на придбання складових ІКС;

3.40.6 угоди («Service Level Agreement», «Non-disclosure agreement») на придбання послуг, сервісів тощо з метою впровадження в ІКС сучасних технологій та обмеження доступу третіх сторін до комерційної таємниці;

3.40.7 зведені відомості стосовно фізичних або юридичних осіб, з якими виконком міської ради має стосунки з метою забезпечення власної інформаційної діяльності;

3.40.8 відомості щодо оперативних даних проєктів та репозиторії зберігання конфігураційних, структурних і критичних даних виконкому міської ради.

3.41. До РК33 належать:

3.41.1 відомості щодо здійснення конкретних заходів із розкриттям планів, строків та задіяних ресурсів (обсяг фінансування тощо) з ІБ з метою захисту активів, що складають цінність для виконкому міської ради;

3.41.2 відомості, що встановлюють порядок ідентифікації та автентифікації користувачів у ІКС з наведенням заходів, засобів та способів захисту;

3.41.3 відомості, що встановлюють порядок проведення контрольних заходів (плани раптових перевірок, поточні та перспективні плани перевірок), пов’язаних з обробкою ІзОД з метою дотримання вимог міжнародних стандартів з питань ІБ. Результати контрольних перевірок (протоколи, акти та висновки стосовно обробки ІА;

3.41.4 відомості про спроби вчинення та (або) вчинені несанкціоновані дії щодо доступу до ІА;

3.41.5 відомості, що встановлюють порядок проведення службових розслідувань (програма, методики) та результати їх проведення щодо конкретних фактів порушення вимог СУІБ з питань ІБ (втрата матеріальних носіїв ІА, несанкціонований доступ та розповсюдження ІА, результати, протоколи та висновки проведення розслідувань за виявленими інцидентами щодо обробки ІА);

3.41.6 відомості стосовно технології обробки інформаційних ресурсів у ІКС та застосування засобів шифрування (логін, пароль, токен/card/захищений носій ключової інформації, ключ шифрування, алгоритм, матеріальний носій з ІзОД, тощо);

3.41.7 відомості щодо правил розмежування доступу відповідно до обов'язків користувачів в ІКС;

3.41.8 види та типи засобів криптографічного захисту інформації, що використовуються в ІКС, без розкриття їх характеристик. Відомості про наявність для зазначених засобів сертифікатів, експертних висновків та/або документів щодо допуску до експлуатації згідно з вимогами нормативних документів з криптографічного захисту інформації;

3.41.9 вміст журналів, які входять до складу супровідної документації СУІБ виконкому міської ради та мають у складі ІзОД;

3.41.10 склад комплексу засобів захисту СУІБ: EDR (Endpoint Detection and Response), DLP (Data Loss Prevention Software), SIEM (Security Information and Event Management), WAF (Web Application Firewall), IAM (Identity and Access Management), IDS (Intrusion detection system), IPS (Intrusion prevention system), система антивірусного захисту, що використовуються в ІКС, з відображенням назв і версій цих засобів, вартості, вендору та комп'ютерної техніки, де вони вбудовані/установлені. Відомості про наявність для зазначених засобів сертифікатів, експертних висновків, дозволів на використання;

3.41.11 узагальнені дані складових ІКС та зведені відомості у формулярі/паспорті на ІКС щодо:

3.41.11.1 типу, кількості одиниць комп'ютерної техніки, комутаційного та телекомунікаційного обладнання з розкриттям IP-адреси, що використовуються у ІКС та оброблюють інформацію, яка підлягає захисту;

3.41.11.2 засобів та способів їх об'єднання у ІКС (окремі автоматизовані робочі місця, сервер, локальні та/або розподілені телекомунікаційні мережі тощо) з наведенням конкретних відомостей щодо налаштування комплексу засобів захисту й відповідного мережевого та серверного обладнання;

3.41.11.3 назв та версій операційних систем, прикладного та спеціального програмного забезпечення, що використовується в складових ІКС, з відображенням кількості та місця розташування комп'ютерної техніки, де вона встановлена.

3.42. До РК33, також, належать відомості у сфері забезпечення заходів з охорони та виконання протипожежних заходів на об’єктах захисту (надалі – ОЗ) виконкому міської ради:

3.42.1 відомості щодо охорони та режиму доступу до важливих об’єктів інфраструктури виконкому міської ради (плани, схеми розташування ОЗ, схеми евакуації ОЗ та ІзОД, графік чергування служби охорони, договірні документи стосовно охорони);

3.42.2 відомості щодо пропускного режиму, списки доступу до ОЗ;

3.42.3 схема побудови охоронної, пожежної сигналізації з наведенням характеристик устаткування та обладнання, порядку проведення регламентного й технічного обслуговування комплексу засобів захисту та засобів КЗІ;

3.42.4 структура та чисельний склад підрозділів охорони виконкому міської ради.

3.43 «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ» – це конфіденційна інформація з РК4.

3.44. Технологічна інформація призначена для адміністрування та управління обчислювальною системою компонентів ІКС, яку дозволено використовувати лише повноваженим користувачам з числа посадових осіб SOC та осіб, які забезпечують функціонування ІКС виконкому міської ради.

3.45. До ТІЗ належить така інформація:

3.45.1 відомості щодо адміністрування та управління компонентами комплексу засобів захисту ІКС, налаштування сервісів безпеки програмного забезпечення та засобів криптографічного захисту інформації (надалі – КЗІ);

3.45.2 списки зареєстрованих користувачів, імена користувачів, облікові записи зареєстрованих користувачів, атрибути доступу захищених інформаційних об’єктів;

3.45.3 повноваження та права доступу користувачів до об’єктів захисту, інформація журналів реєстрації дій користувачів, інформація КЗЗ щодо журналу аудиту, інформація КЗЗ щодо реєстру захищених носіїв інформації інша інформація КЗЗ та баз даних захисту;

3.45.4 інформація про функціональні профілі захисту з відповідними налаштуваннями КЗЗ, режими функціонування та встановлені робочі параметри прикладного програмного забезпечення зі складу ІКС;

3.45.5 файли налаштування програмного забезпечення складових ІКС, атрибути доступу захищених інформаційних об’єктів, дані структури ІКС з наведенням мережевих адрес;

3.45.6 відомості щодо впроваджених/запланованих рішень з налаштувань складових КЗЗ: EDR (Endpoint Detection and Response), DLP (Data Loss Prevention Software), SIEM (Security Information and Event Management), WAF (Web Application Firewall), IAM (Identity and Access Management), IDS (Intrusion

detection system), IPS (Intrusion prevention system), системи антивірусного захисту тощо.

3.46. Узагальнені відомості про ТІЗ, що обробляється та зберігається в ІКС, наведені в таблиці 3:\*\*\*\*\*

Таблиця 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***№ п/п*** | ***Вид інформації*** | ***Стисла характеристика інформації*** | ***Ступень обмеження доступу*** | ***Форма представлення інформації*** |

| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** |
| --- | --- | --- | --- | --- |
| 1 | Файли конфігурації програмного та апаратного забезпечення | | | |
| 2 | Списки управління доступом мережевих потоків | Списки управління доступом мережевих потоків (access control lists), що проходять через мережеве обладнання ІКС | Технологічна інформація захисту | У вигляді  файлів |
| 3 | Налаштування виявлення мережевих атак | Конфігураційні налаштування ме- ханізмів виявлення та запобігання мережевим атакам | Технологічна інформація захисту | У вигляді  файлів |
| 4 | Правила політики мережевої безпеки | Правила політики мережевої безпеки щодо дій при виявленні мережевих аномалій | Технологічна інформація захисту | У вигляді  файлів |
| 5 | Мережеві налаштування технічних засобів ІКС | Налаштування тех- нічних засобів ІКС щодо мережевої взаємодії між собою | Технологічна інформація захисту | У вигляді файлів |
| 6 | Інші файли конфігурації програмного та апаратного забезпечення | Інші файли конфігу- рації програмного та апаратного забезпечення, необхідні для коректної роботи ІКС | Технологічна інформація захисту | У вигляді файлів |
| 7 | Журнали реєстрації подій, що ведуться програмними засобами ІКС | Зареєстровані події щодо управління даними облікових записів абонентів | Технологічна інформація захисту | У вигляді файлів |
| Зареєстровані дані щодо надання доступу абонентів до ресурсів ІКС |
| Зареєстровані дані щодо управління конфігураційними налаштуваннями програмного та апаратного забезпечення ІКС |
| Зареєстровані дані щодо проведення  оновлення програмного забезпечення ІКС |
| Зареєстровані дані щодо відновлення працездатності програмного та апаратного забезпечення ІКС |
| Зареєстровані дані щодо помилок, що виникають у процесі функціонування програмного та апаратного забезпечення ІКС |
| Зареєстровані дані щодо виявлених порушень мережевої безпеки |
| 8 | Файли резервних конфігурацій | Резервні копії файлів конфігурації КЗЗ, необхідні для коректної роботи ІКС | Технологічна інформація захисту | У вигляді  файлів |

3.47. Інформація, класифікована як PII, «ДІЛОВА ІНФОРМАЦІЯ», «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ», супроводжується списком уповноважених осіб з наведенням прізвища, ім’я по батькові або посади осіб, які мають право доступу до цієї інформації.

3.48. Інформація з РК «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ» супроводжується списком уповноважених осіб з наведенням прізвищ, імен по батькові або посад осіб, якщо особи зовнішніх сторін – вони повинні мати доступ до такої інформації.

3.49. Власники ІА регулярно переглядають РК не рідше разу на три роки та, якщо це допустимо, знижують РК.

3.50. На будь-яких документах, віднесених до категорії «ПУБЛІЧНА», РК не проставляється.

3.51. РК «ДЛЯ ВНУТРІШНЬОГО ВИКОРИСТАННЯ», PII, «ДІЛОВА ІНФОРМАЦІЯ», «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ» проставляється таким шляхом:

3.51.1 документи на папері – відмітка про РК проставляється в правому верхньому куті кожної сторінки документа; на лицьовій стороні конверта, обкладинці папки / швидкозшивачі, якщо вони містять документи;

3.51.2 електронні документи – відмітка про «РКххх» проставляється в правому верхньому куті кожної сторінки документа;

3.51.3 інформаційні системи – РК в додатках і базах даних відображається у вікні доступу до системи (login screen), а також у правому верхньому кутку області виведення конфіденційної інформації;

3.51.4 електронна пошта – РК вказується в першому рядку тексту повідомлення;

3.51.5 електронні носії інформації (диски, карти пам'яті, та ін.) – відмітка проставляється на поверхні носія;

3.51.6 усно передана інформація – РК (тільки для інформації PII, «ДІЛОВА ІНФОРМАЦІЯ», «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ») при особистих зустрічах повідомляється перед самою інформацією, під час телефонних розмов або при використанні інших засобів зв'язку та ІКС можливе розголошення тільки за умови створеної СУІБ з підтвердженою відповідністю до вимог нормативно-правових документів та міжнародних стандартів у галузі ІБ ДСТУ ISO/IEC 27001, ДСТУ ISO/IEC 27701.

3.52. Усі особи, які отримали інформацію з ІзОД, повинні дотримуватися правил, наведених у таблиці 4.

3.53. Розпорядник ІКС ініціює дисциплінарний процес щодо осіб щоразу, коли правила не були дотримані.

3.54. Кожен інцидент пов'язаний з неприйнятним зверненням з ІзОД, має бути повідомлений відповідно до процедури управління інцидентами, передбаченої Положенням про управління інцидентами ІБ.

3.55. ІзОД не може бути винесена за межі контрольованої зони виконкому міської ради (приміщень, у яких вона оброблюється) за винятком здійснення заходів з діловодства та виконання заходів у межах робочих цілей з обов’язковим дотриманням вимог Політики інформаційної безпеки та тільки після попереднього отримання дозволу Розпорядника ІКС. ІА можуть бути використані тільки для виконання посадових обов'язків з метою досягнення цілей виконкому міської ради.

3.56. Методи безпечного видалення інформації і знищення носіїв інформації визначені в Політиці утилізації та знищення інформації та інструкції «Операційні процедури для ІТ».

Таблиця 4 Правила поводження з ІзОД

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***№ п/п*** | ***Форма інформації*** | ***«Для внутрішнього використання»*** | ***РІІ, «Ділова інформація»*** | ***«Технологічна інформація захисту»*** |

| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** |
| --- | --- | --- | --- | --- |
| 1 | Документи на папері | Коло осіб обмежено відповідно до визначених повноважень.  Документ може бути відправлений за ме-жі виконкому міської ради до адресата з повідомленням про отримання.  Документ зберігаєть-ся в приміщенні без публічного доступу  Документи відразу вилучаються з принтерів і факсів | Документ зберігаєтсья в замкнених шафі, ящику, сейфі.  Документ може бути відправлений за межі виконкому міської ради в закритому та опечатаному конверті тільки за допомогою служби, що заслуговує на довіру.  Відправка за допомогою факсимільного зв'язку не допускається  Документ може бути роздрукований тільки в тому випадку, якщо авторизована особа перебуває біля принтера.  Тільки власник доку-мента або визначена власником СУІБ особа може зробити копію.  Тільки власник доку-мента або визначена вла-сником СУІБ особа (екс-пертна комісія) може його знищити за дозволом власника СУІБ | Тільки обмежене коло користувачів ІКС з адміністра-тивною роллю мають доступ у межах повноважень.  Документ має збе-рігатися в замк-нених шафі, ящику, сейфі.  За погодженням з CSO документ мо-же бути відправлений Ad1 або визначеною власником СУІБ особою за допомогою служби, що заслуговує на довіру у закритому та опечатаному конверті.  Відправка за допомогою факсиміль-ного зв'язку не допускається.  Документ може бу-ти роздрукований тільки в тому ви-падку, якщо авторизована особа перебуває біля принтера, тільки власник документа мо-же зробити копію.  Тільки власник документа або визначена власником  СУІБ особа (екс-пертна комісія) мо-же його знищити за дозволом Власника СУІБ |
| 2 | Електронні документи | Тільки авторизовані особи мають доступ відповідно до визначених повноважень. Перед відправкою документа з викори-станням сервісів миттєвих повідомлень, електронної пошти, FTP та іншого документ має бути захищений паролем або із застосуванням технології хеширування з метою контролю його цілісності.  Передачу через незахищене середовище можливо здійснюва-ти в зашифрованому вигляді із  застосуванням сервісів операційної системи | Коло осіб обмежено, тільки авторизовані користувачі можуть мати доступ до ресурсів PII, «Ділова інформація».  Передачу через незахищене середовище слід здійснювати тільки з використанням апаратно-програмного комплексу криптографічного захисту інформації з викори-станням технології шифрування ІзОД відповідно до вимог законодавства у сфері технічного та криптографічного захисту інформації.  Тільки власник доку-менту може його видалити | Коло осіб обмежено, тільки авторизовані користувачі з адміністративною роллю мо-жуть мати доступ до ТІЗ.  Для роботи з «Пуб-лічна», «для внутрі-шнього використа-ння», РІІ, «ділова інформація» адмі-ністратори мають роль звичайного користувача.  Документ зберігатися тільки в заши-фрованому вигляді.  Перед відправкою документа з використанням сервісів миттєвих  повідомлень, елек-тронної пошти, FTP та іншого документ зашифровується.  Передача через незахищене середови-ще здійснюється ті-льки з використанням апаратно-програмного комплек-су криптографічно-го захисту інфор-мації, технології шифрування ІзОД  відповідно до вимог законодавства у сфері технічного та криптографічного захисту інформації.  Тільки власник документа може йоговидалити |
| 3 | Елетронно-обчислю-вальна техніка (ЕОТ) | Тільки авторизовані користувачі можуть мати доступ.  Доступ до засобів ЕОТ (робоча стан-ція), у яких зберігаються документи, захищяється складним паролем | Тільки авторизовані користувачі мають доступ.  Користувачі блокують систему, якщо вони тим-часово або надовго покинули робоче місце.  Дані видаляються з використанням алгоритмів, що роблять неможливим відновлення інформації.  Доступ до засобів ЕОТ (робоча станція), у яких зберігаються документи захищаються складним паролем.  Екран робочої станції користувача, на якій відображається документ, автоматично блокується пі-сля закінчення 15 хвилин відсутньої активності користувача | Тільки авторизова-ні користувачі з ад-міністративною ро-ллю мають доступ.  Користувачі блокують систему, якщо вони тимчасово або надовго покинули робоче місце.  Дані видаляються з використанням алгоритмів, що робить неможливим відновлення інформації.  Доступ до засобів ЕОТ (робоча стан-ція, активне мережеве обладнання, сервер), у яких збе-рігається технологі-чна інформація захищається складним паролем.  Екран робочої стан-ції адміністратора, на якій відображає-ться документ, автоматично блокує-ться після закінчення 15 хвилин відсутньої активно-сті користувача |
| 4 | Електронна пошта | Тільки авторизовані особи мають доступ.  Відправник уважно перевіряє всіх одержувачів.  Усі правила, викладені в Політиці ІБ та іншій документації СУІБ, повинні дотримуватися | Лист дозволено відправляти авторизованим звичайним користувачам, перед відправкою він зашифровується, якщо від-правляється за межі виконкому міської ради | Лист відправляють авторизовані кори-стувачі з адмініс-тративною роллю, перед відправкою він зашифровуєть-ся, якщо відправ-ляється за межі виконкому міської ради |
| 5 | Електронні носії ін-формації | Тільки авторизовані особи мають доступ.  Файли або носії захищаються паролем.  Носій відправляється за межі виконкому міської ради з по-відомленням про от-римання.  Носії інформації перебувають тільки в приміщеннях з кон-трольованим фізичним доступом | Файли або носії повинні бути зашифровані.  Носії повинні зберігатися в замкнених шафах / ящиках або сейфах.  Облік носіїв з ключовою інформацією ведеться окремо.  Обіг та знищення проводиться окремо створеною службою криптогра-фічного захисту інформації відповідно до Політики криптографії.  Носій відправляється службою, що заслуговує на довіру, у закритому та опечатаному конверті.  Тільки власник носія мо-же його очистити.  Зруйнувати носій можливо лише за рішенням власника СУІБ створеною комісією з наведенням висновка щодо дійс-ного знищення ІзОД | Файли або носії повинні бути зашифровані.  Носії повинні збері-гатися в замкнених шафах / ящиках або сейфах.  Носій має бути відправлений службою, що заслуговує на довіру, у закритому та опечатаному конверті.  Тільки власник но-сія може очистити носій.  Зруйнувати носій можливо лише за рішенням Власника СУІБ на підставі створеної комісіії із наведенням висно-вку щодо дійсного знищення ІзОД |
| 6 | Усно передана інформація | Усі користувачі мають доступ, неавторизовані особи в супроводі авторизованих користувачів теж можуть бути присутніми в приміщен-ні, у якому пере-дається інформація. | Тільки авторизовані користувачі можуть мати доступ.  Вимоги до захисту технічних  каналів  (акустич-ні, віброакустичні, високочастотні наведення та  перетворення тощо) не висовуються, але за фіна-нсової можливості до-цільно проводити захисні заходи щодо звукоізо-ляції приміщення.  Бесіди, переговори з використанням засобів зв'я-зку зашифровуються.  Бесіди, переговори не повинні записуватися / стенографуватися | Тільки авторизова-ні користувачі з адміністративною роллю мають доступ.  Вимоги до захисту технічних каналів (акустичних, віброакустичних, високочастотних наведень та перетворень тощо) не висовуються, але за фінансової можливості проводяться захи-сні заходи щодо звукоізоляції при-міщення.  Бесіди, переговори з використанням засобів зв'язку за-шифровуються.  Бесіди, переговори не повинні записуватися або стенографуватися |

*\*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.*

*\*\*\*ДІР – це інформація, що належить державі. Виконком міської ради в процесі діяльності не формує ДІР, але в межах інформаційної діяльності може використовувати ДІР, тому користувачі ІКС та всі посадові особи виконкому міської ради, які мають певну роль у СУІБ, повинні бути ознайомлені зі змістом ДІР та правилами їх обробки з метою уникнення порушень чинного законодавства стосовно обробки ДІР.*

*\*\*\*\*Відповідно до вимог статті 30 Закону України «Про захист персональних даних» установлено, що в період дії воєнного стану в Україні та протягом шести місяців після його припинення чи скасування, як виняток з положень*[*абзаців першого – третього*](https://zakon.rada.gov.ua/laws/show/2297-17#n216)*частини третьої статті 29 зазначеного Закону, передача PII іноземним суб’єктам відносин, пов’язаних з PII, що необхідні для надання медичної допомоги та/або реабілітаційної допомоги із застосуванням телемедицини, може здійснюватися із забезпеченням захисту PII відповідно до законодавства тієї країни, у якій медичному працівнику, фахівцю з реабілітації чи закладу охорони здоров’я, що надає медичну та/або реабілітаційну допомогу, надано право на провадження медичної практики (крім громадян Російської Федерації та Республіки Білорусь).*

*\*\*\*\*\*Особисті ключі користувачів ІКС повинні бути доступні лише власникам цих ключів (КЕП, ЗНКІ тощо) відповідно до Закону України «Про електронні довірчі послуги»*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***