*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА ІТ-БЕЗПЕКИ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика ІТ-безпеки виконавчого комітету Криворізької міської ради (надалі – Політика ІТ-безпеки) є документом, що забезпечує коректне безпечне функціонування інформаційних і комунікаційних технологій щодо здійснення інформаційної діяльності виконкому міської ради в межах області дії системи управління інформаційної безпеки (надалі – СУІБ).

1.2. Політика ІТ-безпеки застосовується до всіх операційних процесів, усіх дій з обробки персональних даних та всіх інформаційних активів, що оброблюються в функціональних підсистемах Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС) «Підсистема документообігу», «Підсистема кадрового забезпечення» та «Webпортал», а також усіх мереж, пристроїв та засобів обробки інформації, якими володіють або користуються посадові особи, підрядники, консультанти, постачальники партнери тощо, які пов’язані з інформаційної діяльністю виконкому міської ради або іншими особами, що використовують чи отримують доступ до ЄІС у межах області дії СУІБ.

1.3. Політика ІТ-безпеки розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу інформаційної безпеки, а саме: Законів України «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-комунікаційних системах», ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки», ДСТУ ISO 31000:2018 (ISO 31000:2018, IDT) «Менеджмент ризиків. Принципи та настанови», ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки», ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) «Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови», рішень виконкому міської ради від 14.05.2014 №141 «Про затвердження порядку обробки персональних даних, володільцем яких є Криворізька міська рада, її виконком», зі змінами, 26.05.2021 №488 «Про впровадження Єдиної інформаційної системи міста Кривого Рогу», 21.07.2021 № 377 «Про затвердження Регламенту виконавчого комітету Криворізької міської ради в новій редакції», зі змінами, 24.11.2021 №933 «Про затвердження Регламенту впровадження та визначення адміністратора Єдиної інформаційної системи міста Кривого Рогу», розпорядження міського голови від 31.05.2011 №122-р «Про захист персональних даних» зі змінами, 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», D1.3-СУІБ «Концептуальні рішення щодо побудови СУІБ», D2-СУІБ «Процедури ідентифікації вимог», D2.2-СУІБ «Політика управління активами», D00ML-СУІБ «Основний перелік документів СУІБ», D10-СУІБ «Методології оцінки та обробки ризиків», D10.1-СУІБ «Таблиця оцінки ризиків та обробки ризиків (реєстр ризиків)», D10.2-СУІБ «План про оцінку та обробку ризику», D10.3-СУІБ «Звіт про оцінку та обробку ризику», D21-СУІБ «Положення щодо організації заходів кібербезпеки», D12-СУІБ «Заява про застосовність (SoA)».

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

2.1. 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)].

2.2. 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.\*

2.3. 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.

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

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

2.6. Chief Security Officer (надалі – CSO) – відповідальний за інформаційну безпеку, 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.

2.7. Chief Information Security Officer (надалі − CISO) − відповідальний за розробку та впровадження політик і процедур інформаційної безпеки, управління ризиками, забезпечення кібербезпеки, реагування на інциденти, підвищення обізнаності працівників та контроль за дотриманням законодавства у сфері захисту інформаційних систем і даних.

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

2.9. Ad1 – адміністратор безпеки.

2.10. Ad2 – адміністратор системи.

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 в межах області дії СУІБ.

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

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

2.14. PII – персональні дані

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

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

2.15.2 органи місцевого самоврядування та територіальні громади;

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

2.15.4 банки, інвестори, рейтингові агентства;

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

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

2.16. 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.

2.17. 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.

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

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

2.20. ПЗ – програмне забезпечення.

2.21. Інтранет – внутрішня локальна мережа, що використовує стандарти, технології і ПЗ мережі «[Інтернет»](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)».

2.22. [Брандмауер](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80%D0%B0%D0%BD) — програма чи пристрій, що здійснює захист комп'ютерних мереж.

#### *3. Прийнятна політика використання ІА*

3.1. Прийнятне використання: активи можуть використовуватися лише для потреб інформаційної діяльності виконкому міської ради з метою виконання завдань у межах області дії СУІБ:

3.1.1 виготовлення якісного актуального інформаційного контенту, який може бути використаний з метою підвищення ефективності роботи виконавчих органів, підприємств та установ міської ради шляхом скорочення часу передачі необхідної інформації;

3.1.2 надання дієвої допомоги при проведенні профілактичної роботи щодо попередження кіберзлочинів. Визначення пріоритетних заходів, що спрямовані на захист інформаційних активів. Основні властивості інформаційних активів, що підлягають захисту — це конфіденційність, цілісність та доступність. Захист інформації ґрунтується на ризикорієнтованому підході шляхом протидії загрозам, що можна очікувати внаслідок подій на всіх технологічних етапах обробки ІА та в усіх режимах функціонування СУІБ.

3.2. Прийнятне використання активів забезпечує виконання таких вимог політики ІБ:

3.2.1 інформація в процесі її обробки засобами ЄІС захищена від несанкціонованого ознайомлення та модифікації неавторизованими та неуповноваженими користувачами;

3.2.2 система розмежування доступу (надалі – система РД) до ресурсів ЄІС передбачає адміністративний принцип з виділенням адміністративних привілеїв на всіх рівнях реалізації ЄІС, за виключенням об’єктів файлової системи на автоматизованому робочому місці (надалі – АРМ) користувачів адміністратора ЄІС, власника ЄІС. Для каталогів та файлів на АРМ адміністраторів і операторів указаних суб’єктів, у яких здійснюється експорт даних з об’єктів системи РД, застосовується довірчий принцип розмежування доступу користувачів операційних систем до об’єктів захисту;

3.2.3 розмежування доступу ґрунтується на основі встановлених груп безпеки та ролей користувачів в підсистемах ЄІС (наданих їм відповідно до їх повноважень);

3.2.4 технологічні дані функціонування ЄІС захищені від несанкціонованого доступу;

3.2.5 облікові дані користувачів ЄІС захищені від несанкціонованого ознайомлення, модифікації та знищення;

3.2.6 система РД забезпечує максимальне розділення технологічних процесів обробки даних та інтерфейсу доступу користувача;

3.2.7 програмно-технічний комплекс компонентів ЄІС та організаційно-технічні заходи захисту забезпечують захист від несанкціонованого доступу до компонентів системи й захист від несанкціонованого експорту інформації на зовнішні носії засобами зовнішніх інтерфейсів (USB, CD/DVD тощо);

3.2.8 проведення безперервного аудиту подій у підсистемах ЄІС;

3.2.9 засоби безпеки забезпечують моніторинг дій користувача і його ідентифікацію та автентифікацію в системі РД з метою верифікації достовірності введених (безпосередньо) даних;

3.2.10 для передачі інформації між компонентами системи РД використовуються довірчі та/або захищені канали зв’язку;

3.2.11 передача інформації здійснюється виключно між ідентифікованими компонентами системи РД, після їх взаємної верифікації (клієнт-сервер);

3.2.12 у системі РД використовується ліцензійне ПЗ тільки згідно із специфікацією, визначеною на етапі формування області дії СУІБ. Тільки відповідний адміністратор або визначена особа (розробник, постачальник ПЗ) має право встановлювати ПЗ. Усім іншим користувачам заборонено встановлення будь-якого ПЗ.

3.3. Засоби мережевого захисту розміщуються на межі логічних зон і забезпечують виконання таких функцій:

3.3.1 фільтрація та аналіз трафіку на рівнях L2-L4 мережевої моделі (рівень обробки кадрів, пакетів та файлів);

3.3.2 розмежування доступу між серверами ЄІС та зовнішніми мережами;

3.3.3 маскування топології і мережевих адрес компонентів ЄІС від публічного перегляду;

3.3.4 виявлення комп’ютерних атак і несанкціонованої мережевої активності;

3.3.5 здійснення фільтрації та аналізу мережевого трафіку за протоколами, портами і IP-адресами відправника й одержувача;

3.3.6 забезпечення завершення з’єднання з вузлом, у разі атаки;

3.3.7 здійснення протоколювання (реєстрації) подій, що мають відношення до безпеки.

3.4. Загальні правила доступу до ресурсів ЄІС базуються на нормативно-правових документах, Політиці ІБ (затверджено рішенням виконкому міської ради від 23.05.2025 №680), Політики ІТ-безпеки і установлюють порядок доступу до інформаційних ресурсів ЄІС.

3.5. Дозвіл користувачам надається лише на доступ до інформації, що стосується їх посадових та функціональних обов'язків і на термін не більший, ніж той, що цими обов’язками передбачений.

3.6. Розробникам ПЗ, фахівцям, які здійснюють монтаж і обслуговування технічних засобів ЄІС надається доступ до програмних та апаратних засобів ЄІС лише під час робіт з тестування та інсталяції ПЗ, установлення і регламентного обслуговування обладнання.

3.7. Кожен актив зобов’язаний мати власника активу. Власник активу несе відповідальність за конфіденційність, цілісність та доступність інформації про відповідний актив.

3.8. Коли актив більше не потрібен, його власник зобов’язаний видалити інформацію з обмеженим доступом, що зберігається на його/її робочій станції (комп’ютер стаціонарний чи мобільний пристрій) чи з’ємному носії інформації.

3.9. Установлення ПЗ та заборонені дії: виконком міської ради встановлює та застосовує суворі правила стосовно видів ПЗ, які посадові особи можуть установлювати (детальна інформація приведена у D14.14-CУІБ «Політика контролю доступу»). Для безпечного керування змінами та інсталяцією ПЗ слід дотримуватися таких правил:

3.9.1 виконання оновлень ПЗ лише навченими адміністраторами з підтвердженою компетентністю після його відповідної авторизації в ЄІС;

3.9.2 гарантування того, що на компонентах ЄІС установлений лише схвалений виконуваний код, а не код розробки чи компілятори;

3.9.3 установлення та оновлення ПЗ лише після ретельного й успішного тестування;

3.9.4 оновлення всіх відповідних вихідних бібліотек ПЗ;

3.9.5 використання системи контролю конфігурації для контролю всього робочого ПЗ, а також системної документації;

3.9.6 визначення та документування стратегії відкату до впровадження змін;

3.9.7 архівування попередньої версії всіх необхідних параметрів конфігурації.

3.10. Будь-яке рішення щодо оновлення до нової версії ПЗ зобов’язане враховувати вимоги СУІБ до зміни (наприклад, упровадження нової функції інформаційної безпеки або кількість і ступінь серйозності вразливостей інформаційної безпеки, що впливають на поточну версію ПЗ). До встановлення ПЗ в ЄІС застосовуватиметься принцип найменших привілеїв. Робочі станції, що використовуються звичайними користувачами (розробник ПЗ, тестувальник ПЗ), не можуть мати прав адміністратора.

3.11. Програмні виправлення слід застосовувати, якщо вони можуть допомогти усунути або зменшити вразливість інформаційної безпеки.

3.12. ПЗ зі складу ЄІС слід відстежувати та контролювати, щоб уникнути несанкціонованих змін, оскільки вони можуть створити вразливість інформаційної безпеки.

3.13. ПЗ, що використовується в ЄІС, підтримується його постачальником на відповідному рівні під контролем відповідального за ПЗ у виконкомі міської ради. У разі закінчення підтримки старих версій ПЗ проводиться оцінка ризиків з метою визначення можливості їх подальшого використання.

3.14. ПЗ з відкритим вихідним кодом, що використовується в ЄІС, зобов’язане підтримуватися до своєї останньої відповідної версії. Виконком міської ради враховує ризики ПЗ з відкритим кодом та проводить їх оцінку з метою визначення можливості його використання в разі його необхідності в ЄІС.

3.15. Коли постачальники ПЗ беруть участь у встановленні або оновленні ПЗ, фізичний або логічний доступ надається лише за необхідності та з відповідного дозволу CEO під контролем CSO та CISO.

3.16. Заборонено використовувати активи в спосіб, що без потреби може витрачати ресурси (потужності) засобів обробки інформації, послаблює продуктивність ЄІС або створює загрозу безпеці. Також заборонено:

3.16.1 завантажувати файли зображень або відео, що не належать до інформаційної діяльності в межах діяльності виконкому міської ради, надсилати приватні листи електронною поштою, грати в ігри, використовувати активи не за призначенням тощо;

3.16.2 інсталювати ПЗ на локальний комп’ютер без явного дозволу Ad2;

3.16.3 використовувати програми «Java», елементи керування «ActiveX» та інший мобільний код, за винятком випадків, коли це дозволено Ad2;

3.16.4 використовувати криптографічні засоби (шифрування) на локальному комп’ютері, крім випадків, визначених D14.12-СУІБ «Політика використання шифрування»;

3.16.5 установлювати або використовувати периферійні пристрої, такі як: модеми, карти пам’яті чи інші пристрої для зберігання та читання даних (наприклад, флеш-накопичувачі USB) без явного дозволу Ad2 і без явної ідентифікації та реєстрації цих активів відповідно до D8.1-СУІБ «Положення щодо інвентаризації та обробки даних».

3.17. Обладнання, інформацію чи ПЗ, незалежно від їх форми представлення або носія, не можна виносити за межі контрольованої зони виконкому міської ради без попереднього дозволу CEO або CSO, який отримав такі повноваження від CEO (у паперовій чи електронній формі з використанням технології «DocuSign» або технології кваліфікованого електронного підпису). Такий дозвіл може поширюватися на одноразовій та/або на довгостроковій основі з установленням строку його дійсності.

3.18. Поки зазначені активи перебувають за межами виконкому міської ради, вони контролюються особою, яка отримала дозвіл на їх винос.

3.19. Передача інформаційних активів за допомогою компонентів ЄІС (включаючи користувачів власника ЄІС) здійснюється в межах Регламенту ЄІС та затвердженого власником СУІБ «робочого процесу».

3.20. Після припинення трудового договору або іншого договору, на під-ставі якого використовується різне обладнання, ПЗ або інформація в електронній

чи паперовій формі користувач ЄІС (власник активу) зобов’язаний повернути всі такі інформаційні активи до виконкому міської ради.

3.21. Користувач ЄІС (власник активу) зобов’язаний застосовувати процедури резервного копіювання відповідно до D14.10-CУІБ «Політика резервного копіювання».

3.22. Резервні копії активів зберігаються на власному ресурсі виконкому міської ради (мережа «Інтранет» або з’ємних носіях інформації) у папці, що відповідає рівню конфіденційності резервних копій активів з правами доступу відповідно до D14.14-CУІБ «Політика контролю доступу» з врахуванням рівня критичності активу D14.6-CУІБ «Політика класифікації інформації».

3.23. На кожній робочій станції має бути встановлено антивірусне ПЗ з активованим автоматичним оновленням.

3.24. Посадові особи виконкому міської ради можуть отримувати доступ лише до тих активів, для яких вони були явно авторизовані власником активів відповідно до встановлених правил розмежування доступу та D14.14-CУІБ «Політика контролю доступу».

3.25. Користувачі ЄІС можуть використовувати активи лише для цілей, для яких вони авторизовані, у межах виконання посадових і функціональних обов’язків.

3.26. Посадовим особам виконкому міської ради заборонено здійснювати дії, які можуть бути використані для обходу контролю інформаційної безпеки.

3.27. Користувач ЄІС не зобов’язаний, прямо чи опосередковано, дозволяти іншій особі використовувати його/її права доступу до активів виконкому міської ради (включаючи привілейованих користувачів, користувачів з особливим статусом, користувачів з адміністративною роллю за винятком випадків, які визначає CEO або CSO, дії якого попередньо схвалені рішенням CEO). Користувачу заборонено розкривати іншим особам свої реєстраційні дані: ім’я (логін) та/або пароль та/або інші дані стосовно його ідентифікації у ЄІС. Використання групових імен посадових осіб у виконкомі міської ради заборонено.

3.28. Власник облікового запису користувача є його користувачем, який несе персональну відповідальність за його використання та всі операції, що здійснюються через цей обліковий запис користувача.

3.29. Під час вибору та використання паролів користувачі ЄІС повинні застосовувати такі правила безпеки:

3.29.1 паролі не можна повідомляти іншим особам, включаючи CEO, CSO, адміністраторів та інших привілейованих користувачів ЄІС;

3.29.2 паролі не можна записувати, якщо тільки CSO не схвалить безпечний метод;

3.29.3 створені користувачами паролі (з метою захисту конфіденційної інформації) не можна розповсюджувати будь-якими відкритими каналами (усним, письмовим, електронним розповсюдженням тощо);

3.29.4 паролі необхідно змінити, якщо є ознаки того, що їх або систему могли зламати. У такому випадку необхідно оперативно повідомити про інцидент безпеки на адресу адміністратора IRT, CSO/CISO/Ad1.

3.30. «Політика чистого столу та чистого екрана» (D14.2-СУІБ): уся інформація, класифікована як «ЧУТЛИВА», «КОНФІДЕНЦІЙНО», «КОМЕРЦІЙНА ТАЄМНИЦЯ» та «ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ ЗАХИСТУ», як зазначено в D14.6-СУІБ «Політика класифікації інформації» вважається інформацією з обмеженим доступом (надалі – ІзОД).

3.31. Політика чистого столу:

3.31.1. Якщо власника активу немає на робочому місці, усі паперові документи, мобільні (кінцеві) пристрої та носії ІзОД необхідно прибрати зі столу чи інших місць (принтерів, факсів, копіювальних апаратів тощо) для запобігання несанкціонованому доступу до змісту ІА.

3.31.2. Документи, мобільні пристрої та медіафайли зберігаються в безпечний спосіб відповідно до рівня конфіденційності визначеного у D14.06-СУІБ «Політика класифікації інформації». Коли документи та носії інформації більше не потрібні, їх необхідно утилізувати відповідно до D14.11-СУІБ «Політика утилізації та знищення».

3.31.3. Сейфи та інші види засобів безпечного зберігання можуть також захищати ІзОД, яку в них зберігають, від таких обставин непереборної сили: пожежа, землетрус, повінь чи вибух.

3.32. Політика чистого екрану:

3.32.1. Якщо користувач ЄІС відсутній на робочому місці (біля робочої станції), усю ІзОД необхідно прибрати з екрана робочої станції, а також заборонити доступ до всіх систем/служб/сервісів з цього робочого місця користувача.

3.32.2. У разі короткої відсутності (до 30 хвилин) реалізується політика чистого екрану шляхом виходу з усіх систем або блокування екрана паролем. Якщо користувач ЄІС відсутній протягом тривалого періоду часу (понад 30 хвилин), реалізується політика чистого екрану шляхом виходу з усіх систем і вимкнення робочої станції. Комп’ютери й термінали мають перебувати в стані завершення сеансу чи бути захищені механізмом блокування екрана та клавіатури, який контролюється паролем, токеном чи подібним механізмом автентифікації користувача, якщо їх залишають без нагляду, і мають бути захищені блокуванням клавіатури, паролями або іншими заходами безпеки, якщо їх не використовують.

3.32.3. Інформацію на білих дошках (наприклад, тих, що доступні в кімнатах для нарад) необхідно видалити, коли вона більше не потрібна.

3.32.4. Необхідно запобігати несанкціонованому використанню фотокопіювальної та іншої розмножувальної техніки (наприклад, сканерів, цифрових камер). Документи, що містять ІзОД, повинні видаляти з принтерів негайно. Рекомендовано розглянути використання принтерів з функцією PINкоду, тоді лише ініціатори друку зможуть отримати віддруковані матеріали й лише перебуваючи поруч із принтером.

3.33. Захист спільних приміщень та обладнання.

3.33.1. Приміщення для відправлення та приймання кореспонденції охороняються шляхом їх замикання.

3.33.2. Несанкціоноване використання принтерів, копіювальних апаратів, сканерів та іншого загального обладнання для копіювання запобігається шляхом блокування об’єкта, використання PINкоду.

3.33.3. Перед тим, як залишити об’єкти на тривалий період або назавжди (наприклад під час зміни локації), слід провести детальну перевірку кімнат, кабінетів і меблів у них, щоб переконатися, що активи виконкому міської ради не залишилися.

3.33.4. Заходи безпеки для робочих місць поза приміщеннями виконкому міської ради, таких як роботи вдома, віддаленої роботи й тимчасових місць перебування потрібно визначати за допомогою оцінки ризиків і відповідних заходів безпеки, таких як: шафи для документів, що зачиняються, політика чистого стола, контролі доступу до комп’ютерів і безпечні комунікації з основним місцем роботи.

3.34. Доступ до мережі «Інтернет» можна отримати лише через локальну мережу виконкому міської ради з відповідною інфраструктурою, захищеною брандмауером. Прямий доступ до мережі «Інтернет» через модеми, мобільний інтернет, бездротові мережі або інші пристрої заборонено.

3.35. CSO/CISO/Ad1/Ad2 можуть заблокувати доступ до деяких інтернет-сторінок для окремих користувачів ЄІС, груп користувачів ЄІС або всіх користувачів ЄІС виконкому міської ради, щоб зменшити ризик доступу до вебсайтів зі зловмисним чи незаконним вмістом, або які можуть бути використані для витоку даних. Якщо доступ до деяких вебсторінок заблоковано, користувач ЄІС може подати письмовий запит до CSO для авторизації доступу до таких сторінок. Користувачу ЄІС заборонено намагатися самостійно обійти таке обмеження.

3.36. Користувач ЄІС зобов’язаний вважати інформацію, отриману через неперевірені сайти, недостовірною. Така інформація може бути використана в цілях інформаційної діяльності виконкому міської ради лише після перевірки Ad1/CSO/CISO/DPO її достовірності та правильності.

3.37. Користувач ЄІС несе відповідальність за всі можливі наслідки, що виникають внаслідок несанкціонованого або неналежного використання інтернет-сервісів чи контенту.

3.38. Доступ до мережі «Інтернет» рекомендовано здійснювати за допомогою ІКС провайдера, який має захищений вузол «Інтернет» з підтвердженням відповідності:

3.38.1 до вимог технічного захисту інформації в Україні (мається чинний Атестат відповідності на створену комплексну систему захисту інформації (КСЗІ), наданий Адміністрацією ДержСпецзв’язку України);

3.38.2 до вимог інформаційної безпеки ISO 27001 (мається чинний Сертифікат безпеки на створену СУІБ, наданий повноважним органом сертифікації відповідно до вимог ДСТУ ISO/IEC 17021-1:2017 «Оцінка відповідності. Вимоги до органів, які здійснюють аудит і сертифікацію систем управління. Частина 1. Вимоги» (ISO/IEC 17021-1:2015, IDT).

3.39. Методи обміну повідомленнями, крім електронної пошти, також включають завантаження файлів з мережі «Інтернет», передачу даних через неї, телефони, факсимільні апарати, надсилання телефонних текстових повідомлень, портативні носії, а також форуми та соціальні мережі.

3.40. Відповідно до D14.14-СУІБ «Політика контролю доступу» та D14.6-СУІБ «Політика класифікації інформації» CSO визначає канал зв’язку, який може використовуватися для кожного типу даних. CSO встановлює можливі обмеження: кому дозволено використовувати канали зв’язку, та визначає, які види діяльності заборонені.

3.41. Користувачі ЄІС можуть надсилати лише повідомлення, що містять правдиву інформацію. Заборонено надсилати матеріали тривожного, неприємного, відверто сексуального характеру, грубого, наклепницького чи будь-якого іншого неприйнятного або незаконного змісту. Посадові особи не можуть розсилати спам-повідомлення, повідомлення особам, з якими не встановлені відносини в межах сфери застосування СУІБ, або особам, яким така інформація не потрібна.

3.42. Якщо користувач ЄІС отримує електронний лист зі спамом, він зобов’язаний повідомити про це CSO або CISO.

3.43. Надсилаючи повідомлення з міткою конфіденційності, користувач зобов’язаний захистити його, як зазначено в D14.6-СУІБ «Політика класифікації інформації».

3.44. Користувач ЄІС зобов’язаний зберігати кожне повідомлення, що містить дані, важливі для діяльності виконкому міської ради, використовуючи метод, визначений CSO.

3.45. Кожне повідомлення електронної пошти (за винятком повідомлень, надісланих через систему зв’язку виконкому міської ради, які визначені CSO) зобов’язане містить застереження: «Це повідомлення може містити конфіденційну та/або приватну інформацію. Якщо ви не є адресатом, зазначеним у цьому повідомленні (або не несете відповідальності за доставку цього повідомлення цій особі), ви не можете копіювати або доставляти це повідомлення будь-кому. У такому випадку вам слід знищити це повідомлення та повідомити відправника у відповідь електронною поштою». Якщо користувач розміщує повідомлення в системі обміну повідомленнями (соціальні мережі, форуми тощо), він зобов’язаний однозначно вказати, що воно не відображає точку зору виконкому міської ради, що це повідомлення є суто суб’єктивною точкою зору цього користувача ЄІС.

3.46. Посадовим особам заборонено робити несанкціоновані копії ПЗ, що належать виконкому міської ради, за винятком випадків, дозволених законом або CEO/CSO/CISO.

3.47. Посадовим особам заборонено копіювати ПЗ чи інші оригінальні матеріали з інших джерел. Вони несуть відповідальність за всі наслідки, що можуть виникнути відповідно до законодавства про авторське право та інтелектуальну власність.

3.48. Мобільне обчислювальне обладнання включає всі види портативних комп’ютерів (у тому числі BYOD), мобільних телефонів, смартфонів, планшетів, терміналів, карт пам’яті та іншого мобільного обладнання, що використовується

для зберігання, обробки та передачі даних інформаційних активів, незалежно від того, де таке обладнання використовується.

3.49. Вищезазначене обладнання можна використовувати за межами виконкому міської ради лише після отримання дозволу відповідно до пункту 3.17. цієї Політики.

3.50. Посадова особа, яка виносить мобільне комп’ютерне обладнання за межі приміщення, повинна дотримуватися правил, зазначених у D14.3-СУІБ «Політика щодо мобільних пристроїв, дистанційної роботи та роботи з дому».

3.51. CSO відповідає за навчання та підвищення обізнаності осіб, які використовують мобільне комп’ютерне обладнання поза межами виконкому міської ради.

3.52. Дистанційна робота означає, що інформаційне та комунікаційне обладнання використовується для того, щоб посадові особи могли виконувати свою роботу за межами виконкому міської ради, включаючи роботу вдома. Дистанційна робота не включає використання мобільних телефонів поза межами виконкому міської ради.

3.53. Дистанційна робота повинна бути узгоджена за розпорядженням CEO шляхом відправлення електронного листа або підписання документа (дозвіл може бути наданий у письмовій формі: у паперовому або електронному вигляді з використанням технології «DocuSign» або кваліфікованого електронного підпису).

3.54. Усі посадові особи, які виконують дистанційну роботу, повинні дотримуватися правил для мобільних комп’ютерів, визначених у пунктах 3.48. – 3.52. цієї Політики та D14.3-СУІБ «Політика мобільних пристроїв, віддаленої роботи та роботи з дому», D14.4-СУІБ «Політика щодо власного пристрою (BYOD)».

3.55. Усі дані, що створюються, зберігаються, надсилаються чи отримуються через інформаційні або комунікаційні системи інших організацій у межах області дії СУІБ, незалежно від того, є вони особистими чи ні, вважаються власністю виконкому міської ради.

3.56. Посадові особи погоджуються, що уповноважені особи виконкому міської ради можуть отримати доступ до всіх таких даних, і що доступ таких осіб не вважатиметься порушенням конфіденційності посадових осіб виконкому міської ради.

3.57. Виконком міської ради може використовувати та встановлювати на компонентах користувачів (уключаючи BYOD) спеціалізовані інструменти з метою ідентифікації та блокування заборонених методів зв’язку й фільтрації забороненого контенту.

3.58. Кожна посадова особа виконкому міської ради, зацікавлена сторона або третя сторона, які мають контакт з даними виконкому міської ради в процесі інформаційної діяльності, зобов’язані повідомляти про будь-яку слабкість ЄІС, інцидент або подію, що вказує на можливий інцидент, як зазначено в D14.20-СУІБ «Процедура управління інцидентами».

*\*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.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***