*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА КОНТРОЛЮ ДОСТУПУ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика контролю доступу виконавчого комітету Криворізької міської ради (надалі – Політика контролю доступу) є документом, що визначає напрями, принципи та основні правила контролю доступу в області дії системи управління інформаційною безпекою (надалі – СУІБ) для захисту інформаційних активів, які мають обіг в Єдиній інформаційній системі міста Кривий Ріг (надалі – ЄІС). Мета процесу управління доступом є визначення послідовності необхідних дій для отримання, блокування, припинення, перегляду прав доступу користувачів до активів у межах області дії СУІБ.

1.2. Політика контролю доступу розроблена з метою підтвердження готовності виконкому міської ради виконувати вимоги чинного законодавства в галузі інформаційної безпеки (надалі – ІБ) та кіберзахисту, а також гарантувати впровадження заходів з контролю доступу до активів із застосуванням ризикорієнтованого підходу на всіх етапах життєвого циклу СУІБ.

1.3. Політика контролю доступу застосовується до всієї області дії СУІБ, а саме:

1.3.1 усіх робочих процесів та інформації, що обробляється у ЄІС;

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

1.4. Політика контролю доступу 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 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», Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29 березня 2006 року №373, 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», D8.1-СУІБ «Положення щодо інвентаризації та обробки даних», D2.2-СУІБ «Політика управління активами», D14.6-СУІБ «Політика класифікації інформації».

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

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

2.2. Кваліфікований електронний підпис (надалі – КЕП) – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити істинність електронного документа, його цілісність, авторство тощо. КЕП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

2.3. Криптографічний захист інформації (надалі – КЗІ) – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою захисту конфіденційності ІА шляхом приховання (або відновлення) змісту інформації.

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 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 персональних даних у виконкомі міської ради, відповідає за організацію роботи, пов’язаної із захистом персональних даних у процесі інформаційної діяльності виконкому в межах області дії СУІБ.

2.12. 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 та систем.

2.14. PII – персональні дані.

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

2.16. Ad1 – адміністратор безпеки.

2.17. Ad2 – адміністратор системи.

2.18. Chief Human Resources Officer (надалі – CHRO) – відповідальна особа за кадрову політику.

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

2.20. Рівень конфіденційності – надається інформаційним активам з метою обмеження доступу відповідно до правил розмежування доступу з урахуванням контексту виконкому міської ради та схеми класифікації інформації, визначеної в Політиці класифікації інформації.

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

2.22. Chief Financial Officer (надалі – CFO) – керівник підрозділу, який відповідає за фінансове забезпечення.

2.23. Chief Legal Officer (надалі – CLO) – керівник юридичного підрозділу.

2.24. Privacy Information Management System (надалі – PIMS) – система управління ІБ, що стосується захисту конфіденційності, на яку потенційно може вплинути обробка PII.

#### *3. Управління доступом*

3.1. Існує 2 типи доступів:

3.1.1 стандартний доступ – визначається, як попередньо узгоджений набір доступів, властивих для посадових осіб виконкому міської ради/користувачів ІКС.

3.1.2. нестандартний доступ – всі інші доступи, що не входять до стандартного доступу.

 3.2. Доступ консультантів, розробників, аналітиків та інших спеціалістів до продуктивних систем або систем, що перебувають у дослідно-промисловій експлуатації, обмежується тільки на перегляд, окрім випадків, пов’язаних з обслуговуванням систем або виправленням помилок, які заздалегідь погоджені із CSO.

***Таблиця «Матриця робочого процесу управління доступом користувача»***

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Операції*** | ***Відповідальний за процес*** |
| ***Ініціатор*** | ***Безпосередній керівник СП*** | ***Адміністратор системи (Ad2)*** | ***Власник активу*** | ***CISO*** | ***Адміністратор безпеки (Ad1)*** | ***CSO*** |
| 1 | Створення заявки на надання стандартного доступу | R | R/C | I | I/S | I/C | I | A |
| 2 | Створення заявки на надання нестандартного доступу | R | R/C | C | C/S | C | C | A |
| 3 | Створення заявки на перегляд прав доступу | R | R/C | I | I/S/R | I/C | R | A |
| 4 | Створення заявки на блокування/ розблокування доступу | I | R | I/S/R | R | R/C | R | A |
| 5 | Надання стандартного доступу | I | I | I/S | I | I/C | R | A |
| 6 | Надання нестандартного доступу | I | I | I/S | I | I/C | R | A |
| 7 | Блокування доступу | I | I | I/S | I | I/C | I/R\* | A |
| 8 | Розблокування доступу | I | I | I/S | I | I/C | I/R | A |
| 9 | Інвентаризація наданих прав доступу | I | I | I/S | I | I/C | I/R | A |

Позначення:

«R» - Responsible (виконує);

«A» - Accountable (несе відповідальність, контролює, приймає рішення);

«S» - Supportive (супроводжує виконання);

«C» - Consulted (консультує);

«I» - Informed (інформується після виконання).

3.3. Рівень доступу до ІА, компонентів та сервісів ЄІС, кінцевого й мережевого обладнання ЄІС, приміщень виконкому міської ради визначається, виходячи із цілей, потреб та вимог ІБ на підставі результатів оцінки та обробки ризиків і критичності активів, до яких мають доступ користувачів в рамках ролей у межах області дії СУІБ.

*Таблиця «Матриця доступу»*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***№ п/п*** | ***Найменування активу у межах області дії СУІБ*** | ***Посада*** | ***Роль*** | ***Рівень доступу*** |

| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** |
| --- | --- | --- | --- | --- |
| 1 | Службові приміщення | Посадові особи виконкому міської ради | Власник активу, користувачі ЄІС | Доступ надано відповідно до правил розмежування доступу |
| 2 | Робочі станції (корпоративні та BYOD) | Посадові особи виконкому міської ради | Користувачі ЄІС, власник активу | Доступ дозволений відповідно до правил розмежування доступу |
| 3 | Серверне приміщення та обладнання, си-стеми підтримки функціональ-ності та доступності | Посадові особи виконкому міської ради | Користувачі з адміністративною роллю ЄІС, власник активу | Адміністративні привілеї в межах повноважень відповідно до правил розмежування доступу та згідно з процедурами роботи в безпечних зонах |
| 4 | Комплекс засобів захисту (надалі – КЗЗ) та захисне обладнання в серверному приміщенні | Посадові особи виконкому міської ради | Обмежене коло користувачів з адміністративною роллю, власник активу, CSO, CISO | Адміністративні привілеї в межах повноважень відповідно до правил розмежування доступу |
| 5 | Обладнання криптографічного захисту інформації (КЗІ) у режимному приміщенні | Посадові особи виконкому міської ради | Адміністратор КЗІ, спеціалісти групи КЗІ | Адміністративні при- вілеї в межах повноважень відповідно до правил розмежування доступу та згідно з процедурами роботи в безпечних зонах |
| 6 | Активне мережеве обладнання функціональне (АМО) | Посадові особи підрозділу ІТ та SOC | Адміністратор системи, доступ до функціонального програмного забезпечення, інсталяція, налаштування, обслуговування, резервне копіювання | Адміністративні при- вілеї в межах повноважень відповідно до правил розмежування доступу |
| 7 | Активне мережеве обладнання з функціями КЗЗ (АМО) | Посадові особи SOC | Адміністратор безпеки, повний доступ до КЗЗ | Адміністративні при-вілеї стосовно КЗЗ відповідно до правил розмежування доступу |

3.4. Стандартний доступ надається посадовій особі виконкому міської ради за фактом прийому її на роботу, чи переведення між різними відділами, управліннями, іншими виконавчими органами міської ради. Стандартний доступ надається на підставі електронної заявки в системі «Сервіс-Деск». Заявка на надання стандартного доступу може бути сформована як ініціатором, так і автоматично, на основі даних про прийом/переведення посадових осіб з одної посади на іншу.

3.5. Після створення заявка візується відповідальним за розробку та впровадження політик і процедур ІБ CISO та CIO в системі «Сервіс-Деск».

3.6. Після погодження CISO, CIO за ухвалою CSO заявка маршрутизується на:

3.6.1 Ad2, який створює акаунт;

3.6.2 Ad1, який здійснює налаштування правил розмежування доступу з урахуванням цієї заявки та відповідно до реєстру стандартних доступів у межах визначених повноважень.

3.7. Відповідальним за надання доступу користувачу до активів та контроль усього робочого процесу надання доступу є CSO, що остаточно ухвалює рішення про надання відповідного доступу та візує цю заявку в Сервіс-Деск.

3.8. Загальний контроль за виконанням вимог політик СУІБ здійснює CEO.

3.9. Нестандартний доступ надається в разі виробничої необхідності розширення існуючого набору стандартного доступу. Нестандартний доступ надається на підставі електронної заявки в системі «Сервіс-Деск». Ініціатором створення заявки на надання нестандартного доступу може виступати користувач, для якого необхідно розширити стандартний доступ, або безпосередній керівник відділу, управління, іншого виконавчого органу міської ради або адміністратор чи власник активу, або інша посадова особа виконкому міської ради, яка має певну роль у СУІБ та відповідні повноваження (привілейовані користувачі). При створенні заявки на надання нестандартного доступу необхідно обрати , які права на доступ до активу надаються. У заявці мають бути присутні такі реквізити:

3.9.1 ПІБ посадової особи, для якого запитується доступ;

3.9.2 назва відділу, управління, іншого виконавчого органу міської ради та посада;

3.9.3 ID комп’ютера (опціонально, не обов’язковий параметр);

3.9.4 перелік доступів із зазначенням активу;

3.9.5 підстава/обґрунтування необхідності.

3.10. Безпосередній керівник відділу, управління, іншого виконавчого органу міської ради (якщо ініціатором заявки є посадова особа виконкому міської ради), власник активу, CISO, CIO візують заявку в системі «Сервіс-Деск». Після створення заявка візується CISO та CIO в системі «Сервіс-Деск».

3.11. Після погодження CISO, CIO за ухвалою CSO заявка маршрутизується на:

3.11.1 Ad2, який створює (або змінює за необхідності) аккаунт;

3.11.2 Ad1, який здійснює налаштування правил розмежування доступу з урахуванням цієї заявки та відповідно до реєстру нестандартних доступів.

3.12. Відповідальним за надання доступу користувачу до активів та контроль усього робочого процесу надання доступу є CSO, який за розпорядженням CEO надає дозвіл щодо надання відповідного нестандартного доступу та візує цю заявку в Сервіс-Деск. За фактом виконання проводиться інформування ініціатора/користувача або доручається CISO провести інформування ініціатора/користувача.

3.13. При переміщенні посадової особи в межах відділу, управління, іншого виконавчого органу міської ради зміна доступів може:

3.13.1 не відбуватися за рішенням безпосереднього керівника відділу, управління, іншого виконавчого органу міської ради;

3.13.2 відбуватися за ініціативи безпосереднього керівника відділу, управління, іншого виконавчого органу міської ради, в разі необхідності.

3.13.3 може бути заблоковано існуючий доступ та надано набір стандартних доступів.

3.14. При переведенні посадової особи між відділами, управліннями, іншими виконавчими органами міської ради – існуючий набір доступу блокується та надається стандартний доступ.

3.15. Блокування доступу здійснюється у випадках:

3.15.1 звільнення, на підставі заявки, де ініціатором виступає посадова особа підрозділу управління персоналом та оплати праці;

3.15.2 службової необхідності, на підставі заявки, де ініціатором виступає безпосередній керівник відділу, управління, іншого виконавчого органу міської ради або власник активу;

3.15.3 службового розслідування/перевірки, на підставі заявки, де ініціатором виступає посадова особа SOC, IRT, DPO;

3.15.4 інциденту ІБ, на підставі заявки, де ініціатором виступає посадова особа підрозділу ІТ, SOC, IRT або DPO.

3.16. Стандартне блокування доступу здійснюється в разі звільнення або переведення посадової особи на іншу посаду. Доступи не відключаються, якщо посадова особа переводиться на іншу посаду в межах підрозділу.

3.17. Блокування здійснюється на підставі заявки в системі «Сервіс-Деск». Відповідальний за формування заявки – CHRO. Заявка може бути сформована як уповноваженою посадовою особою, так і автоматично на основі даних про звільнення/переведення посадових осіб виконкому міської ради.

3.18. Заявка маршрутизується на безпосереднього керівника відділу, управління, іншого виконавчого органу міської ради, CIO, CISO та адміністраторів відповідних ресурсів для виконання. Заявка виконується згідно з процесом управління запитами та узгоджується CSO.

3.19. Розблокування доступу здійснюється:

3.19.1 автоматично, якщо це передбачається СУІБ;

3.19.2 на підставі заявки безпосереднього керівника відділу, управління, іншого виконавчого органу міської ради або власника активу;

3.19.3 на підставі заявки CSO, CISO, CIO, CHRO, DPO та інших привілейованих користувачів.

3.20. Керівники відділу, управління, іншого виконавчого органу міської ради повинні регулярно переглядати існуючі доступи підпорядкованих посадових осіб, а власники активів існуючі доступи до активу, що їм належать, не рідше ніж один раз на 6 (шість) місяців. За результатом перегляду доступу за необхідності проводяться коригуючі заходи, включаючи надання/зміну доступу. Ініціатором коригуючих заходів за результатом перегляду виступає керівник відділу, управління, іншого виконавчого органу міської ради або власник активу.

3.21. Контроль за своєчасним та повним виконанням заходів робочого процесу щодо моніторингу існуючих доступів здійснює CISO.

3.22. CSO – є відповідальним за виконання всіма посадовими особами вимог Політики контролю доступу стосовно доступу користувачів у відповідності до їх повноважень у межах області дії СУІБ.

3.23. Часові обмеження:

3.23.1. Час погодження заявок власниками активів та керівниками відділів, управлінь, інших виконавчих органів міської ради не регламентується.

3.23.2. Час виконання заявок на надання доступу: згідно процесу обробки запитів.\*\*

3.24. При зміні посади, тимчасовій відсутності (відпустка, хвороба), тимчасовому відстороненні від виконання обов’язків або звільненні посадової особи виконкому міської ради, керівник відділу, управління, іншого виконавчого органу міської ради, у якому працює ця особа, зобов'язаний повідомити (або переконатися що це вже відомо) про це CSO та CHRO, якими вживаються всі необхідні дії із зміни, тимчасового припинення або відкликання прав доступу відповідного користувача.

3.25. Доступи переглядаються посистемно (у рамках однієї системи/ресурсу). Ініціатором запиту може виступати керівник відділу, управління, іншого виконавчого органу міської ради, SOC, CIO, DPO та власник активу. Запит формується через систему «Сервіс-Деск».

3.26. Заявка маршрутизується на відповідного адміністратора підсистеми ЄІС. За результатом запиту (заявки) адміністратором формується звіт, що містить інформацію про наявні доступи для посадових осіб вказаного відділу, управління, іншого виконавчого органу міської ради.

3.27. Ініціатор проводить перегляд доступів та визначає необхідні заходи за його результатами. За необхідності проведення коригувань до наявних доступів, ініціатор заповнює додаткові поля звіту (необхідність доступу взагалі та необхідність конкретних повноважень), формує заявку в системі «Сервіс-Деск» – «Перегляд доступів: коригування». До заявки додається заповнений звіт.

3.28. Ініціатором періодичного перегляду виступає CISO згідно з планом перегляду доступів (не рідше разу на 6 місяців). CISO надсилає запит на Ad1. За

результатом запиту Ad1 формує звіт що містить інформацію про наявні доступи для визначених облікових записів користувачів. У звіті окремо вказується інформація про наявні нестандартні доступи та інформація про стандартні доступи для відділів, управлінь, інших виконавчих органів міської ради.

3.29. SOC проводить аналіз необхідності наявних доступів. За результатом аналізу заповнюються додаткові поля звіту (необхідність доступу взагалі та необхідність конкретних повноважень). CISO формує заявку в системі «Сервіс-Деск» та прикладає консолідований заповнений звіт.

3.30. Ad1 на основі заявки та заповненого звіту виконує необхідні дії, а саме: блокування облікового запису в разі, якщо доступ відмічений як такий що не актуальний, або проводить коригування повноважень згідно з даними у звіті. Заявка виконується згідно з процесом управління запитами.

3.31. Ad2 на основі заявки під контролем Ad1 створює/видаляє акаунт.

3.32. Часові обмеження коригування доступів:

3.32.1 час перегляду існуючих доступів «за запитом» не регламентується;

3.32.2 час заповнення звіту щодо існуючих доступів «періодичний»: 2 робочі тижня;

3.32.3 час обробки заявки «Перегляд доступів: коригування» 1 робочий тиждень.

3.33. Профіль користувача «A»: Us1 – привілейовані користувачі (CEO, CSO, CISO, DPO, CIO, СHRO та ін.).

3.34. Профіль користувача «A» ЄІС має такі права доступу:

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Роль Користувача Us1*** | ***Повноваження щодо доступу до Активів*** |

| ***1*** | ***2*** | ***3*** |
| --- | --- | --- |
| 1 | CEO – власник і розпорядник СУІБ.Послуги та обов'язки: керівництво, забезпечення відповідності та надання належних ресурсів з метою досягнення всіх цілей інформаційної діяльності виконкому міської ради в межах області дії СУІБ , а також задоволення всіх визначених вимог СУІБ з метою повного захисту конфіденційності, цілісності та доступності всієї інформації та організації безпеки активів сторонніх організацій, суб’єктів РІІ та посадових осіб | Повний доступ до активів СУІБ з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно»,«комерційна таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього використання», «чутлива», «конфіденційно», «комерційна таємниця» включають: R (читання), W (запис), Ex (виконання). |
| Права для «технологічна інформація захисту» включають: R (читання) |
| 2 | СSO –– відповідальний за інформаційну безпеку, що організовує процес ке-рування безпекою у виконкомі міської ради, включаючи фізичну безпеку, кібербезпеку та інші види безпеки у межах сфери застосування СУІБ. CSO призначається для моніторингу та забезпечення початкового виконання Політики інформаційної безпеки виконкому міської ради та ІТ-політик. CSO несе відповідальність за впровадження Політики інформаційної безпеки в операційних та технологічних процесах, а також відповідає за щоденні питання ІБ та є першою контактною особою для всіх питань з ІБ й кіберзахисту у виконкомі міської ради. CSO підтримує зв’язок з іншими особами регуляторних органів щодо дотримання, оновлень та реалізації політики, здійснює контроль перегляду ризиків і їх обробку.CSO впроваджує тренінги з ІБ та програми підвищення обізнаності для посадових осіб. Послуги та обов'язки: відповідає за забезпечення виконання Політики ІБ. Він також відповідальний за щоденні питання ІБ і є першою контактною особою для всіх питань, пов'язаних з СУІБ | Повний доступ до активів СУІБ у межах обов'язків з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно», «комерцій-на таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «По-літика класифікації інформації» |
| Права для «для внутрішнього використання», «чутлива», «конфіденційно», «комерційна таємниця», включають: R (читання), W (запис), D (видалення), E (редагування), Ex (виконання) |
| Права для «технологічна інформація захисту» включають: R (читання), W (запис), Ex (виконання) |
| 3 | CFO – керівник підрозділу, який відповідає за фінансове забезпечення виконкому міської ради.Послуги та обов'язки: відповідальний за фінансування/забезпечення ресурсами СУІБ. Надає поради з можливості, ефективності та економічної доцільності придбання ресурсів відповідно до встановленого ризику ІБ та суттєвості активу. Ведення фінансової звітності, розрахункові відомості витрат на заробітну плату, бухгалтерський облік, інвентаризаційні відомості та вартість активів. Аналізує фінансові показники, прогнозує доходи та витрати, проводить оцінку фінансової ефективності. Розробка довгострокових та короткострокових фінансових планів, визначення оптимального розподілу ресурсів та контроль за їх виконанням | Доступ до активів СУІБ у межах обов'язків з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно», «комерційна таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього використання»,«чутлива»,«конфіденційно», «комерційна таємниця», включають: R (читання), W (запис), Ex (виконання) |
| Права для «технологічна інформація захисту» включають: R (читання) |
| 4 | Chief Legal Officer (CLO) – керівник юридичного підрозділу.Послуги та обов'язки: відповідальний за забезпечення виконання найкращих юридичних практик у межах області дії СУІБ. Розглядає існуючі юридичні справи та працює над їх вирішенням. Надає юридичні поради виконкому міської ради | Доступ до активів СУІБ у межах обов'язків з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно», «комерційна таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього викори-стання», «чутлива», «конфіденційно», «комерційна таємниця», включають: R (читання), W (запис), Ex (виконання). |
| Права для «технологічна інформація захисту» включають: R (читання) |
| 5 | DPO – відповідальна особа за захист пер-сональних даних у виконкомі міської ради, що організовує роботу, пов’язану із захистом PII у процесі інформаційної діяльності виконкому міської ради в межах області дії СУІБ. DPO має функцію незалежного органу нагляду, створений відповідно до статті 24 Закону України «Про захист персональних даних», що визначає обов’язковість при-значення відділу, управління, іншого виконавчого органу міської ради або відповідальної особи, яка організовує роботу, пов’язану із захистом PII при їх обробці у володільцях чи розпорядниках PII, що здійснюють обробку PII. Інформація про зазначений відділ, управління, інший виконавчий орган міської ради або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення. DPO несе відповідальність за забезпечення загальної відповідності вимогам ISO 27701 та рекомендаціям GDPR для всіх видів обробки РІІ, а також за координацію та управління СУІБ (PIMS), що стосується захисту конфіденційності виконкому міської ради.Послуги та обов'язки: відповідальна за захист PII і призначена для досягнення відповідності положенням стандарту ISO 27701 та GDPR, а також для забезпечення постійної відповідності видів діяльності щодо PII у межах області дії СУІБ | Доступ до активів СУІБ в межах своїх обов'язків з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно», «комерційна таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього використання», «чутлива», «конфіденційно», «комерційна таємниця»,включають: R (читання), W (запис), D (видалення), E (редагування), Ex (виконання) |
| Права для «технологічна інформація захисту» включають: R (читання) |
| 6 | CIO − відповідальна особа за розробку та реалізацію стратегії цифрової трансформації міста, управління інформаційними системами й ресурсами, кібербезпекуПослуги та обов'язки: відповідає за безперервність операційної діяльності, інформаційної взаємодії та своєчасний доступ користувачів до активів СУІБ, безпечної розробки програмного забезпечення в межах області дії СУІБ | Доступ до активів СУІБ у межах обов'язків з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно», «комерційна таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього використання», «комерційна таємниця» включають: R (читання), W (запис), D (видалення), E (редагування), Ex (виконання) |
| Права для «чутлива», «конфіденційно»включають: R (читання) |
| Права для «технологічна інформація захисту» включають: R (читання), W (запис), D (видалення), E (редагування), I (інсталяція) |
| 7 | CISO − відповідальний за розробку та впровадження політик і процедур ІБ, забезпечення та захист інформаційних активів і технологій виконкому міської ради в межах сфери застосування СУІБ. CISO керує діями посадових осіб виявлення, розробки, упровадження та підтримки процесів для зниження інформаційних ризиків і ризиків інформаційних технологій. CISO відповідає за забезпечення процесів ІБ, перегляд ризиків та їх обробку, упровадження захи-щених технологій для відповідності вимогам стандартів ISO 27001, ISO 27701. CISO відповідає за створення, упро-вадження, підтримку, постійне вдоско-налення СУІБ виконкому міської ради з використанням підходу, що ґрунтується на ризиках. Детальні обов’язки мають бути описані в регламентуючих доку-ментах (положення, інструкції) стосовно діяльності CISO.Послуги та обов'язки: CISO відповідає за забезпечення процесів ІБ й упро-вадження технологій для відповідності вимогам стандартів ISO 27001, ISO 27701 та GDPR. CISO відповідає за створення, упровадження, утримання та постійне вдосконалення СУІБ ор-ганізації, використовуючи ризикорієнтований підхід | Повний доступ до активів СУІБ з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно»,«комерційна таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього використання», «чутлива», «конфіденційно», «комерційна таємниця», включають: R (читання), W (запис), D (видалення), E (редагування), Ex (виконання) |
| Права для «технологічна інформація захисту» включають: R (читання), W (запис), Ex (виконання) |
| 8 | CHRO – відповідальна особа кадрову політику.Послуги та обов'язки: відповідає за управління всіма аспектами процесу працевлаштування, включаючи орієнтацію та навчання нових посадових осіб | Доступ до активів СУІБ з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно»,«комерційна таємниця», «техно-логічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього викори-стання», «чутлива», «конфіденційно», «комерційна таємниця», включають: R (читання), W (запис), Ex (виконання) |
| Права для «технологічна інформація захисту» включають: R (читання) |

3.35. Профіль користувача «B»: Адміністратор.

3.36. Профіль користувача «B» має такі права доступу:

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Роль користувача: Адміністратор*** | ***Повноваження щодо доступу до активів*** |

| ***1*** | ***2*** | ***3*** |
| --- | --- | --- |
| 1 | Адміністратор безпеки (Ad1)Послуги та обов'язки: Ad1 установлює, адмініструє та вирішує проблеми з безпеки, організовує безпеку мережі, захищає від несанкціонованого доступу, модифікації або знищення та вирішує будь-які проблеми з доступом. | Доступ до активів СУІБ з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно»,«комерційна таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього використання», «комерційна таємниця» включають: R (читання), W (запис), D (видалення), E (редагування), Ex (виконання) |
| Права для «чутлива», «конфіденційно» включають: R (читання) |
| Права для «технологічна інформація захисту» включають: R (читання), W (запис), D (видалення), E (редагування), S (настройки захисту) |
| 2 | Адміністратор системи Ad2 та адміністратори підсистем у межах повноважень до яких мають відношення як до власника активу.Послуги та обов'язки: організація, установлення та підтримка комп'ютерних систем організації, включаючи ло-кальні мережі «LAN», глобальні мережі «WAN» та інші системи передачі даних у межах СУІБ  | Доступ до активів СУІБ з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно»,«комерційна таємниця», «технологічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього використання», «комерційна таємниця» включають: R (читання), W (запис), D (видалення), E (редагування), Ex (виконання) |
| Права для «чутлива», «конфіденційно» включають: R (читання) |
| Права для «технологічна інформація захисту» включають: R (читання), W (запис), D (видалення), E (редагування), I (інсталяція) |
| 3 | Адміністратор документів.Послуги та обов'язки: адміністратор документів – це особа, призначена CEO для внесення запису в реєстр вхідної кореспонденції, отримання електронної пошти та внесення її в реєстр вхідної кореспонденції. Адміністратор документів класифікує документи згідно з Політикою кла-сифікації інформації та визначає, кому слід направити документ на розг-ляд/погодження/затвердження тощо у визначені строки | Доступ до активів СУІБ з рівнем конфіденційності: «для внутрішнього використа-ння», «чутлива», «конфіденційно»,«коме-рційна таємниця», «технологічна інформа-ція захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього використання», «комерційна таємниця» включають: R (читання), W (запис), D (видалення), E (редагування), Ex (виконання) |
| Права для «чутлива», «конфіденційно», «комерційна таємниця», «технологічна інформація захисту» включають: R (читання) |

3.37. Профіль користувача «С»: звичайні користувачі

3.38. Профіль користувача «С» має такі права доступу:

|  |  |  |
| --- | --- | --- |
| ***№п/п*** | ***Роль користувача: звичайні користувачі*** | ***Повноваження щодо доступу до активів*** |

| ***1*** | ***2*** | ***3*** |
| --- | --- | --- |
| 1 | Us2 – звичайні користувачі, які мають певну роль у центральної підсистемі ЄІС, дані які виконком міської ради за певних умов може обробляти як процесор PII, контролером цих PII є Криворізька міська територіальна громада в особі Криворізької міської ради, що є власником та розпорядником ЄІС. Us3 – звичайні користувачі, які мають певну роль у СУІБ та виконують завдання у функціональній підсистемі ЄІС «Підсистема документообігу». Us31 виконують завдання в межах контрольованої зони. Us32 виконують завдання за межами контрольованої зони (надалі – КЗ). Us4 – звичайні користувачі, які мають певну роль у СУІБ та виконують завдання у функціональній підсистемі ЄІС «Підсистема кадрового забезпечення». Us41 ви-конують завдання в межах контрольованої зони. Us42 виконують завдання за межами КЗ.Us5 – звичайні користувачі, які мають певну роль у СУІБ та виконують завдання у функціональній підсистемі ЄІС «Web Портал». Us51 виконують завдання в межах КЗ. Us52 виконують завдання за межами КЗ  | Доступ до активів СУІБ з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно»,«комерційна таємниця», «техно-логічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього викори-стання», «комерційна таємниця» включають: R (читання), W (запис), D (видалення), E (редагування) |
| Права для «чутлива», «конфіденційно», «комерційна таємниця», «технологічна інформація захисту» включають: R (читання) |
| 2 | Us6 – користувачі, які дотримуються Політики власного пристрою (BYOD) | Доступ до активів СУІБ з рівнем конфіденційності: «для внутрішнього використання», «чутлива», «конфіденційно»,«комерційна таємниця», «техно-логічна інформація захисту» відповідно до D14.6-СУІБ «Політика класифікації інформації» |
| Права для «для внутрішнього викори стання», «комерційна таємниця» включають: R (читання), W (запис), D (видалення), E (редагування) |
| Права для «чутлива», «конфіденційно», «комерційна таємниця», «технологічна інформація захисту» включають: R (читання) |

3.39. Управління привілеями: привілеї щодо вищезазначених профілів користувачів (надання або вилучення прав доступу) розподіляються таким чином:

|  |  |  |
| --- | --- | --- |
| ***Назва системи*** | ***Хто має право надавати або вилучати права доступу до Активів*** | ***Форма процесу авторизації*** |
| Єдина інформаційна система міста Кривий Ріг (ЄІС) | CSO – має право надавати або вилучати права доступу відповідно до ролевої моделі, яку ухвалено відповідними рішенням виконкому міської ради.Налаштування правил розмежування доступу та комплексу засобів захисту здійснює Ad1 під керів-ництвом CISO | Заявка в друкованому вигляді від керівника відділу, управління, іншого виконавчого органу міської ради, власника активів та за допомогою електронної пошти. Дозвіл надається письмовим рішенням з фіксацією факту, хто замовив/погодив/надав доступ до відповідних активів відповідно до робочого процесу, наведеного в пунктах 3.1, 3.2 Політики контролю доступу |

3.40. При розподілі привілеїв та прав доступу мають ураховуватися результати оцінки ризиків, рівень конфіденційності та класифікація інформації (більш детальна інформація про схему класифікації наведена в D14.6-СУІБ «Політика класифікації інформації»), а також повноваження користувача та його належність до відділу, управління, іншого виконавчого органу міської ради, у межах якого відбувається інформаційна діяльність цього користувача.

3.41. CSO за поданням відповідального за програмне забезпечення, CIO, CISO, визначають перелік дозволених програмних продуктів у складі ЄІС. CIO, CISO мають обов’язок суворо контролювати їх цілісність. Унесення змін до складу програмного забезпечення (надалі – ПЗ) можуть робити тільки адміністратори за погодженням CIO, CISO та дозволу CSO. Звичайним користувачам категорично забороняється вносити будь які зміни в склад ПЗ або модулі/сервіси ЄІС. Принцип мінімальних привілеїв має застосовуватися до встановлення програмного забезпечення на робочих системах. Для безпечного управління змінами та встановлення програмного забезпечення на робочих системах слід ураховувати такі вимоги:

3.41.1 виконання оновлень ПЗ на серверному та мережевому обладнанні здійснює лише кваліфікований (з документальним підтвердженням його

компетентності за фахом) авторизований адміністратор, який має відповідні повноваження згідно з правилами розмежування доступу (надалі – ПРД);

3.41.2 виконання оновлень ПЗ на робочих станціях користувачів BYOD здійснює авторизований адміністратор, який має відповідні повноваження згідно ПРД, або власник активу за наявності дозволу від CSO чи CISO;

3.41.3 заборонено встановлювати ПЗ, призначене лише для особистого використання, та ПЗ, чий програмний код щодо можливого шкідливого впливу невідомий чи підозрілий.

3.42. Власники активів (уключаючи власників приміщень) періодично перевіряють на відповідність наданих прав доступу користувачам, актуальним у межах виконання політик СУІБ .

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Назва активів СУІБ*** | ***Інтервали для регулярного огляду*** |

| ***1*** | ***2*** | ***3*** |
| --- | --- | --- |
| ***1. Апаратне забезпечення*** |
| 1.1 | Комп'ютери (наприклад, настільні комп'ютери, ноутбуки, планшети та ін.) | Принаймні один раз на рік або частіше у випадку критичних змін у політиці безпеки (зміна технологій обробки інфор-мації, зміна місцезнаходження основних технічних засобів підсистем ЄІС) |
| 1.2 | Обладнання для мережі (наприклад, брандмауери, комутатори, маршрутизатори, концентратори, точки доступу до бездротового зв'язку, пристрої Bluetooth, VoIP-пристрої, мережеві кабелі, мережеві шафи та ін.) |
| 1.3 | Особистий засіб зв'язку (BYOD, наприклад, телефони, мобільні телефони та ін.) |
| 1.4 | Сервери (наприклад, файлові сервери, системи виявлення/захисту від вторгнень, віртуальні приватні мережі та ін.) |
| ***2. Програмне забезпечення*** |
| 2.1 | Прикладне програмне забезпечення (наприклад, офісні пакети, текстові ре-дактори, електронні таблиці, системи управління базами даних, електронна пошта та ін.) | Принаймні один раз на рік або частіше у випадку критичних змін у політиці безпеки (зміна технологій обробки інфор-мації, зміна місцезнаходження основних технічних засобів підсистем ЄІС) |
| 2.2 | Системне програмне забезпечення (наприклад, операційні системи, робочі середовища, вебсайт, ERP-системи та ін.) |
| 2.3 | Програмне забезпечення для програ-мування (асемблери, компілятори, інтерпретатори та ін.) |
| 2.4 | Інше програмне забезпечення (драйвери принтерів, драйвери маніпулятора типу «миша», мережеві драйвери та ін.) |
| 2.5 | Спеціальне програмне забезпечення (SIEM, WAF, EDR, DLP, IPS, IDS системи виявлення/захисту від вторгнень, віртуальні приватні мережі та ін.) |
| **3. Інформація (в друкованій чи електронній формі)** |
| 3.1 | Документація СУІБ  | Принаймні один раз на рік або частіше у випадку критичних змін у політиці безпеки (зміна технологій обробки інфор-мації, зміна місцезнаходження основних технічних засобів ЄІС) |
| 3.2 | Бази даних (наприклад, бази даних зарплати, контактів суб’єктів PII, замовлень товарів та ін.) |
| 3.3 | Контракти та угоди (наприклад з партнерами, постачальниками та ін.) |
| 3.4 | Вебсторінка та вебсайт |
| 3.5 | Інструкції та стандарти (наприклад, для навчання персоналу або експлуатації та обслуговування обладнання) |
| 3.6 | Внутрішні документи (наприклад, звіти, плани та ін.) |
| 3.7 | Документи посадових осіб |

3.43. Кожен огляд має бути задокументованим: формальний звіт, ручні записи, електронний документ з використанням КЕП тощо.

3.44. Процедури перегляду доступу користувачів мають включати:

3.44.1 отримання авторизації від власника ІА та інших пов'язаних активів для їх використання;

3.44.2 забезпечення видалення прав доступу, коли комусь не потрібно отримувати доступ до інформації та інших пов'язаних активів, зокрема бути переконаними в тому, що права доступу користувачів, які залишили місце роботи, видаляються своєчасно;

3.44.2 видачу тимчасових прав доступу на обмежений період часу та їх анулювання в день закінчення терміну, зокрема для тимчасового персоналу або тимчасового доступу, необхідного для персоналу (наприклад аудитори, контролюючі органи, користувачі в межах виконання завдань за контрактами або конкретних завдань тощо);

3.44.3 перевірку рівня наданого доступу, що відповідає політиці контролю доступу та іншим вимогам ІБ, таким як розподіл обов'язків (правила розмежування доступу);

3.44.4 забезпечення активації прав доступу (наприклад, постачальниками послуг) тільки після успішного завершення процедур авторизації;

3.44.5 ведення централізованого обліку прав доступу (картка обліку користувача) і наданих користувачеві ідентифікатора (ID, логічного або фізичного) для доступу до інформації та інших пов'язаних активів;

3.44.6 зміна прав доступу користувачів, які змінили ролі або роботу;

3.44.7 ведення обліку змін в логічних та фізичних правах доступу користувачів.

3.45. Регулярні огляди фізичних та логічних прав доступу мають ураховувати таке:

3.45.1 права доступу користувачів після будь-якої зміни у виконкомі міської ради (наприклад, зміна обсягу робіт, підвищення або пониження посади) або при припиненні працевлаштування;

3.45.2 авторизації для привілейованих прав доступу.

3.46. Політики безпеки передбачають постійний контроль прав користувачів таким чином:

3.46.1 СHRO має негайно надсилати CSO, CISO, Ad1, Ad2, DPO інформацію про зміни в правах користувача в разі звільнення користувача або зміни посади;

3.46.2 Ad1, Ad2 негайно припиняють діяльність, скасовують, видаляють або налаштовують фізичний та логічний доступ такими способами: видалення, анулювання, заміна ідентифікаційної інформації, ідентифікаційних карток чи підписок.

3.47. CISO відповідає за впровадження цих процедур. СHRO відповідає за своєчасне надання інформації про зміни (розпорядження про звільнення, переведення на іншу посаду, або тимчасове відсторонення тощо) у правах користувача.

3.48. Права доступу користувача до інформації та інших пов'язаних активів переглядаються та налаштовуються або видаляються перед будь-якою зміною чи припиненням трудових відносин на підставі оцінки ризиків, таких як:

3.48.1 зміна чи припинення, ініційовані користувачем чи керівництвом, та причина припинення;

3.48.2 поточні обов'язки користувача;

3.48.3 вартість доступних на даний момент активів.

3.49. Виконком міської ради встановлює ролі доступу користувачів на основі потреб у межах службової необхідності, що узагальнюють ряд прав доступу в типові профілі доступу користувачів.

3.50. Виконком міської ради включає пункти в трудові та службові контракти, що визначають санкції, якщо посадові особи намагаються незаконно отримати доступ. У випадках за ініціативою керівництва припинення трудових відносин з відповідним персоналом, невдоволені або зовнішні користувачі можуть намагатися умисно порушити активи СУІБ чи вивести з ладу засоби обробки та захисту інформації. У цьому випадку виконком міської ради визначає та аналізує такий ризик, ураховує його та визначає компенсаційні заходи. CSO відповідає за впровадження компенсаційних заходів.

3.51. При зміні зайнятості або припиненні працевлаштування особа повинна негайно повідомити відповідальних осіб (CSO, CHRO, CISO, DPO). При зміні трудових відносин із зовнішніми сторонами, які мають доступ до активів СУІБ, або при закінченні строку власник контракту повинен негайно повідомити відповідальних осіб, які схвалили привілеї для зазначених зовнішніх сторін. Права доступу для всіх осіб, які змінили статус зайнятості чи контрактні відносини, негайно скасовуються або змінюються відповідальними особами, як визначено в п.

3.52. Стандартне блокування доступів здійснюється відповідно до п. 3.16. – 3.19. Політики контролю доступу.

3.53. Термінове блокування здійснюється при проведенні службових перевірок/розслідувань або при обробці інцидентів.

3.54. Блокування здійснюється на підставі заявки в системі «Сервіс-Деск». У разі нагальної потреби запит щодо блокування може бути наданий у телефонному або усному режимі. Запит не відміняє створення заявки в системі «Сервіс-Деск».

3.55. Відповідальний за формування заявки:

3.55.1 CISO – у разі проведення службових перевірок/розслідувань або обробки інциденту ІБ;

3.55.2 CIO – у разі обробки ІТ інциденту;

3.56. Заявка маршрутизується на адміністраторів відповідних ресурсів для виконання. Вона виконується згідно з процесом управління запитами.

3.57. Якщо в ЄІС відсутня активність облікового запису працівника протягом 45 календарних днів, такий обліковий запис блокується.

3.58. Блокування здійснюється на підставі заявки в системі «Сервіс-Деск». Ініціатором може виступати CSO, CISO, Ad1, Ad2, аудитор з ІБ. До заявки прикріплюється список облікових записів, отриманий в результаті аудиту відповідної системи.

3.59. Заявка на блокування маршрутизується на власника ІА та адміністраторів відповідних ресурсів для виконання. Вона виконується згідно з процесом управління запитами.

3.60. Для зменшення навантаження на ресурси ЄІС та покращення управління обліковими записами, облікові записи архівуються та видаляються через 180 календарних днів з дати їх блокування. Видалення здійснюється автоматизованими скриптами.

3.61. Технічна реалізація надання чи скасування прав доступу виконується такими особами:

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Назва системи*** | ***Відповідальна особа за виконання*** |

|  |  |  |
| --- | --- | --- |
| 1 | Єдина інформаційна система міста Кривий Ріг | CSO – погоджує ПРД, затверджує ролеву модель та ПРД у CEO, контролює виконання Політики ІБ та Політики контролю доступу.  |
| Ad1 – налаштовує комплекс засобів захисту відповідно до визначених ПРД |
| Ad2 – створює/видаляє (за командою CISO) обліковий запис користувача у ЄІС |

3.62. Особи, перераховані в пункті 3.61. не можуть надавати або скасовувати права доступу вільно, а лише на підставі профілів користувачів, визначених у цій Політиці, та запитів осіб, уповноважених для надання привілеїв.

3.63. CSO, CISO, CIO відповідають за впровадження захищеної процедури входу для всіх пристроїв, систем та сервісів ЄІС у межах області дії СУІБ .

3.64. Ad1 відповідає за забезпечення безперервності функціонування процедури встановлення належності користувачеві інформації в системі відповідно до пред'явленого ним ідентифікатора.

3.65. Ad2 відповідає за забезпечення безперервності функціонування операційних процесів входу для всіх пристроїв, систем та сервісів ЄІС у межах області дії СУІБ.

3.66. При використанні паролів користувачі зобов’язані дотримуватися таких правил:

3.66.1 D14.19-СУІБ «Заява про ознайомлення та прийняття документів системи управління інформаційною безпекою та конфіденційністю»;

3.66.2 кожен користувач може використовувати лише своє унікальне ім'я користувача;

3.66.3 кожен користувач має можливість обирати власний пароль (первинний пароль формує Ad1). Первинний (тимчасовий) пароль, використовуваний для першого входу в систему, має бути унікальним та міцним;

3.66.4 тимчасові паролі передаваються користувачеві безпечним способом (D14.15-СУІБ «Політика керування паролями»), ідентичність користувача перевіряється перед цим;

3.66.5 система управління паролями вимагає від користувача зміни первинного пароля при першому вході в систему;

3.66.6 система управління паролями вимагає від користувача обирати міцні паролі;

3.66.7 система управління паролями вимагає від користувачів зміни паролів згідно з Політикою керування паролями;

3.66.8 якщо користувач запитує новий пароль, система управління паролями визначає ідентичність користувача, наприклад, надсиланням електронної пошти з інструкцією користувачеві тощо;

3.66.9 система управління паролями перешкоджає повторному використанню трьох попередніх паролів;

3.66.10 користувач підтверджує отримання пароля, увійшовши в систему протягом визначеного інтервалу часу, тощо;

3.66.11 пароль не повинен бути видимим на екрані під час входу в систему;

3.66.12 якщо користувач тричі поспіль вводить невірний пароль, система блокує його обліковий запис;

3.66.13 паролі, створені виробником програмного чи апаратного забезпечення, змінюються під час уведення їх в експлуатацію в складі ЄІС;

3.66.14 файли, що містять паролі, зберігаються окремо від ІА.

*\*Термін «Власник» ідентифікує посадових осіб, відділи, управління, інші виконавчі органи міської ради, для яких установлено відповідальність щодо здійснення контролю за створенням, розвитком, підтримкою, використанням безпеки активів та ресурсів СУІБ. Термін «Власник» не означає, що особа дійсно має право власності на активи/ресурс/ризик СУІБ.*

*\*\*Якщо службова необхідність передбачає прискорення надання/скасування доступу – це питання вирішується CSO окремо за кожним випадком.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***