*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА КЕРУВАННЯ ПАРОЛЯМИ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика керування паролями виконавчого комітету Криворізької міської ради (надалі – Політика керування паролями) є документом, що встановлює порядок формування, збереження паролів та таємної інформації, а також визначає відповідальність користувачів Єдиної інформаційної системи міста Кривий Ріг (надалі – ЄІС) за виконання вимог у процесі здійснення інформаційної діяльності у межах області дії системи управління інформаційної безпеки (надалі – СУІБ).

1.2. Політика керування паролями розроблена з метою підтвердження виконання вимог чинного законодавства в галузі інформаційної безпеки та кіберзахисту, упровадження заходів з контролю доступу до активів із застосуванням ризик орієнтованого підходу на всіх етапах життєвого циклу СУІБ.

1.3. Політика керування паролями розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу інформаційної безпеки (надалі – ІБ), а саме: Законів України «Про інформацію», «Про захист персональних даних», «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», Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄC (Загального регламенту про захист даних) (надалі – GDPR), Наказу Адміністрації ДержСпецзв’язку України від 06 жовтня 2021 року №601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури», зі змінами, Стандарту інформаційної безпеки NIST Special Publication 800-53 Revision 5 «Security and Privacy Controlsfor Information Systems and Organizations», Структури кібербезпеки The NIST Cybersecurity Framework (CSF) 2.0, політик, процедур і технічних заходів: D4.1-СУІБ «Політика інформаційної безпеки», D14.9-СУІБ «Політика управління змінами», D14.11-СУІБ «Політика утилізації та знищення», D14.14-СУІБ «Політика контролю доступу», D14.15-СУІБ «Заява про ознайомлення та прийняття документів системи управління інформаційною безпекою та конфіденційністю».

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

2.1. Автентифікація – процедура встановлення належності користувачеві пред'явленого ним ідентифікатора.

2.2. Авторизація – надання користувачу прав на виконання певних дій, а також процес перевірки (підтвердження) даних прав під час спроб виконання цих дій.

2.3. Ідентифікація – процедура розпізнавання користувача в системі, як правило, за допомогою заздалегідь визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, що сприймається системою.

2.4. Компрометація пароля – несанкціоноване отримання пароля сторонніми особами.

2.5. Пароль – секретна послідовність символів, що відома лише користувачу.

2.6. Початковий пароль – тимчасовий пароль, що призначений для отримання доступу під час першого входу в інформаційну-комунікаційну систему (надалі – ІКС) та надалі має бути зміненим на постійний пароль.

2.7. ІКС – система виконкому міської ради, компоненти якої виконують функції для забезпечення інформаційної діяльності. До її складу 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.

2.8. 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)].

2.9. 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.\*

2.10. 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.

2.11. 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.

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

2.13. 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.

2.14. 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.

2.15. 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.

2.16. 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.

2.17. PII – персональні дані.

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

2.19. Ad1 – адміністратор безпеки.

2.20. Ad2 – адміністратор системи.

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

2.22. Націона́льний інститут стандартів і технології (надалі – NIST) – національний орган зі [стандартизації](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F) у [Сполучених Штатах А](https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%BE%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D1%96_%D0%A8%D1%82%D0%B0%D1%82%D0%B8_%D0%90%D0%BC%D0%B5%D1%80%D0%B8%D0%BA%D0%B8)мерики, керує діяльністю організацій-розробників [стандартів](https://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82) і ухвалює рішення про надання стандарту статусу національного.

2.23. [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.

2.24. Embedded OpenType – компактний формат шрифтів, що впроваджуються на вебсторінки, розроблений компанією «Microsoft». Файли таких шрифтів мають розширення «.eot»

#### *3.* *Обов'язки користувача, правила створення паролів та відповідальність*

3.1. Усі користувачі повинні дотримуватися таких заходів захисту при виборі й використанні паролів:

3.1.1. паролі не можуть будь-кому передаватися (включаючи керівників відділів, управлінь, інших виконавчих органів міської ради, привілейованих користувачів та адміністраторів) будь-яким способами (усно, письмово, з використанням засобів зв'язку та ін.);

3.1.2. паролі не можуть записуватися на необліковані електронні або друковані носії інформації. Електронний або друкований носій інформації має дорівнювати/відповідати рівню конфіденційності інформації, що захищається за допогою використання пароля. CSO визначає безпечний спосіб запису та

зберігання паролів з урахуванням рівня конфіденційності інформації, до якої має доступ користувач за допомогою використання цього пароля;

3.1.3 паролі мають бути негайно змінені, якщо є ознаки, що паролі або компоненти ЄІС були скомпрометовані. У всіх таких випадках має бути створено повідомлення про інцидент інформаційної безпеки.

3.2. Паролі звичайних користувачів мають відповідати таким вимогам:

3.2.1 мінімальна довжина пароля – 8 символів;

3.2.2 пароль має містити такі набори символів:

3.2.2.1 цифри;

3.2.2.2 великі літери;

3.2.2.3 малі літери;

3.2.2.4 спеціальні символи;

3.2.3 пароль не може містити PII (дати народження, номера телефонів, адреси, ПІБ власні або членів сім'ї);

3.2.4 заборонено повторно використовувати паролі протягом одного року;

3.2.5 пароль має змінюватися не рідше кожних шести місяців у разі наявності технічної можливості;

3.2.6 усі початкові паролі змінюються при авторизації;

3.2.7 паролі не можуть перебувати в скриптах автоматизації, програмному забезпеченні (браузери, та ін.);

3.2.8 паролі, що використовуються для особистих цілей, не можуть використовуватися для робочих цілей.

3.3. Паролі привілейованих користувачів (у тому числі користувачі з особовим статусом якщо такі є) мають відповідати таким вимогам:

3.3.1 мінімальна довжина пароля – 10 символів;

3.3.2 пароль має містити наступні набори символів:

3.3.2.1 цифри;

3.3.2.2 великі літери;

3.3.2.3 малі літери;

3.3.2.4 спеціальні символи;

3.3.3 пароль не може містити PII (дати народження, номера телефонів, адреси, ПІБ власні або членів сім'ї);

3.3.4 заборонено повторно використовувати паролі протягом двох років;

3.3.5 пароль змінюється не рідше кожних трьох місяців;

3.3.6 усі початкові паролі змінюються при авторизації;

3.3.7 паролі не можуть перебувати в скриптах автоматизації, програмному забезпеченні (браузери, та ін.);

3.3.8 паролі, що використовуються для особистих цілей, не можуть використовуватися для робочих цілей.

3.4. Паролі користувачів з адміністративною роллю мають відповідати таким вимогам:

3.4.1 мінімальна довжина пароля – 12 символів;

3.4.2 пароль має містити такі набори символів:

3.4.2.1 цифри;

3.4.2.2 великі літери;

3.4.2.3 малі літери;

3.4.2.4 спеціальні символи;

3.4.3 пароль не може містити PII (дати народження, номера телефонів, адреси, ПІБ власні або членів сім'ї);

3.4.4 заборонено повторно використовувати паролі протягом трьох років;

3.4.5 пароль змінюється не рідше ніж кожні 30 діб;

3.4.6 усі початкові паролі змінюються при авторизації;

3.4.7 паролі не можуть перебувати в скриптах автоматизації, програмному забезпеченні (браузери, та ін.);

3.4.8 паролі, що використовуються для особистих цілей, не можуть використовуватися для робочих цілей.

3.5. Усі користувачі повинні дотримуватися таких правил:

3.5.1 користувач приймає зобов'язання забезпечити конфіденційність усіх паролів, як це встановлено Політикою керування паролями;

3.5.2 кожен користувач має використовувати тільки свій акаунт, створений Ad2 для нього із використанням його унікального ідентифікатора (login, ім'я користувача);

3.5.3 кожен користувач має право вибору власного пароля там, де це може бути застосовано;

3.5.4 тимчасові або початкові паролі, використовувані для першого входу в систему, для активних облікових записів мають відповідати всім вимогам, описаним вище;

3.5.5 тимчасові або початкові паролі передаються користувачеві безпечним способом, і користувач повинен бути однозначно ідентифікований;

3.5.6 інформаційні системи мають вимагати зміни первинних паролів при першому вході в систему;

3.5.7 строк дії первинного/початкового пароля не має перевищувати одного робочого дня;

3.5.8 інформаційні системи забезпечують складність паролів відповідно до вимог, наведених вище, за наявності технічної можливості;

3.5.9 інформаційні системи забезпечують зміну паролів користувачів кожні три місяці в разі наявності технічної можливості;

3.5.10 скидання пароля користувача на тимчасовий (у разі, якщо користувач забув пароль) виконується тільки після ідентифікації користувача та заявки;

3.5.11 паролі, що вводяться, не мають відображатися на екрані;

3.5.12 якщо користувач увів неправильний пароль п’ять разів поспіль, його обліковий запис має бути заблокованим автоматично в разі наявності технічної можливості;

3.5.13 усі початкові паролі, установлені виробниками обладнання та розробниками програмного забезпечення, змінюються перед уведенням в експлуатацію обладнання або відразу після розгортання програмного забезпечення.

3.6. Підрозділ ІТ послуг під керівництвом CIO відповідають за автоматизацію процесу управління паролями, якщо цю технологію погоджено CSO та ухвалено CEO.

3.7. CSO відповідає за постійний контроль за виконанням вимог Політики керування паролями.

3.8. CISO відповідає за консультування, підвищення обізнаності користувачів, упровадження захищених технологій у цілях Політики керування паролями, контроль за дотриманням усіма користувачами ЄІС вимог щодо порядку отримання, зберігання, складності та періодичності зміни паролю.

#### *4. Настанова щодо встановлення паролів та забезпечення їх збереження*

4.1. Нижче наведені сучасні міжнародні практики щодо створення та зберігання паролів для звичайних користувачів (уключаючи користувачів власних пристроїв BYOD), користувачів з адміністративними правами та користувачами привілейованих облікових записів щодо дотримання правил інформаційної безпеки:

4.1.1 не використовувати один і той же пароль для кількох акаунтів, процесів, рахунків тощо (особливо ця вимога розповсюджується для найбільш конфіденційних, таких як банківські рахунки, кредитні картки, юридичні чи податкові записи та файли, що містять критичну інформацію). Інакше доступ до одного з облікових записів, може відкрити доступ до багатьох інших;

4.1.2 увести заборону веббраузеру запам’ятовувати паролі (якщо неавторизована особа отримає доступ до вашого комп’ютера або смартфона, вона може отримати доступ до будь-якого облікового запису, у який ваш браузер автоматично входить. Найбільший ризик для користувачів BYOD);

4.1.3 не використовувати паролі, які можна легко відтворити, наприклад загальні слова та дні народження членів сім’ї. Замість цього використовувати комбінацію літер, цифр та символів. Чим довший і надійніший пароль, тим більше захищена інформація;

4.1.4 використовувати лише унікальні паролі для кожного облікового запису.

4.2. Невикористання надійних та унікальних паролів робить дані вразливими для кіберзлочинців. Одним зі способів уникнути повторного використання паролів або використання слабких паролів є використання менеджера паролів. Менеджер паролів зберігає та шифрує всі різні й складні паролі. Менеджер паролів може допомогти автоматично входити у свої онлайн-акаунти/рахунки тощо, при цьому потрібно лише пам’ятати свій головний пароль, щоб отримати доступ до диспетчера паролів та керувати всіма своїми обліковими записами й паролями.

4.3. Доцільно використовувати парольну фразу замість паролю. Створити довгу парольну фразу простіше, ніж пароль, оскільки вона, як правило, має форму речення, а не слова. Більша довжина робить парольні фрази менш вразливими до атак (brute force), але слід уникати поширених або відомих висловлювань, наприклад, текстів популярних пісень тощо. Нижче викладено більш

детальну інформацію щодо формування паролів з використанням кращих практик від NIST:

4.3.1 не використовувати один і той же пароль, захисне запитання та відповідь для декількох важливих облікових записів;

4.3.2 використовувати пароль, який має щонайменше 8 – 12 символів (більш детальна інформація наведена у пункті 3.2. Політики керування паролями), використовувати принаймні одну цифру, одну велику літеру, одну малу літеру та один спеціальний символ;

4.3.3 не використовувати в паролях імена членів сімей, друзів чи домашніх тварин;

4.3.4 не використовувати в паролях поштові індекси, номери будинків, номери телефонів, дати народження, номери ID-карток, номери соціального страхування тощо;

4.3.5 не використовувати жодного словникового слова в паролях:

4.3.5.1 приклади надійних паролів: [9hY5Y\*J2N3n, u0Bc[J|dA%GEfP@, m{fjDh464k$(t8zh$C;

4.3.5.2 приклади слабких паролів: qwerty12345; Tbt3fC79ZmxEFUFJ; 1234567890; 987654321; nordpassword.

4.3.6 не використовувати два або більше схожих паролів, у яких більшість символів однакові, наприклад, myloveflowersMac, myloveflowersDropBox;

4.3.7 не використовувати як паролі те, що можна клонувати (але не можна змінити), наприклад, відбитки пальців;

4.3.8 не надавати веббраузерам погодження («FireFox», «Chrome», «Safari», «Opera», «IE», «Microsoft Edge» та ін.) на зберігання паролей, оскільки всі паролі, збережені у веббраузерах, можна легко розкрити;

4.3.9 не входити у важливі облікові записи на комп’ютерах інших людей або під’єднаних до загальнодоступної точки доступу «Wi-Fi», «Tor», безкоштовного «VPN» чи вебпроксі;

4.3.10 не надсилати конфіденційну інформацію в мережі «Інтернет» через незашифровані (наприклад, HTTP або FTP) з'єднання, оскільки повідомлення в цих з'єднаннях можна розкрити без великих зусиль; слід використовувати зашифровані з'єднання, такі як HTTPS, SFTP, FTPS, SMTPS, IPSec, коли це можливо;

4.3.11 під час подорожі (відрядження) слід шифрувати з’єднання з мережею «Інтернет» за допомогою VPN; можливо налаштувати зашифрований тунель SSH між комп’ютером та власним сервером і налаштувати «Chrome» або «FireFox» для використання проксі-сервера. Тоді навіть, якщо хтось захопить дані під час їх передачі між власним пристроєм (наприклад, ноутбуком, iPhone, iPad) та власним сервером за допомогою засобу зчитування пакетів, він не зможе викрасти дані та паролі із зашифрованих потокових даних;

4.3.12 використовувати тільки надійні паролі, сформовані відповідно до Політики керування паролями. Не використовувати прості паролі навіть з використанням механізму перетворення паролю в хеші MD5 на генераторі хеш-файлів MD5. Наприклад, пароль «0123456789A» у хеші MD5 (C8E7279CD035B23BB9-

9C0F1F954DFF5B3) на вебсайті дешифрування MD5 зловмиснику буде дуже легко розпізнати;

4.3.13 змінювати паролі відповідно до вимог, наведених у пункті 3.2. (для адміністраторів слід розглядати більш жорсткі умови за можливості);

4.3.14 рекомендується (у разі великої кількості паролів та за умови якщо це погоджено CSO) запам’ятати кілька головних паролів, зберегти інші паролі в текстовому файлі та зашифрувати цей файл за допомогою програмного забезпечення для управління паролями;

4.3.15 зашифровувати та створювати резервні копії паролів у різних місцях, тоді, якщо втрачено доступ до власного комп’ютера чи облікового запису, можна швидко повернути паролі;

4.3.16 необхідно вмикати двохетапну або багатофакторну автентифікації, коли це можливо;

4.3.17 не зберігати критичні паролі в хмарі;

4.3.18 можна перевіряти доменне ім’я вебсайта, щоб переконатися, що це не фішинговий сайт, перш ніж уводити пароль;

4.3.19 необхідно захистити комп'ютер брандмауером та антивірусним програмним забезпеченням, заблокувати всі вхідні з'єднання та всі непотрібні вихідні з'єднання з брандмауером. Завантажувати програмне забезпечення лише з авторитетних сайтів за дозволом CSO і за можливості перевіряти контрольну суму MD5/SHA1/SHA256 або підпис GPG інсталяційного пакета;

4.3.20 зберігати операційні системи (наприклад, «Windows 10», «Windows 11», «MacOS», «iOS», «Linux») та веббраузери (наприклад, «FireFox», «Chrome», «IE», «Microsoft Edge») власних пристроїв (наприклад, Windows PC, Mac PC, iPhone, iPad, Android) оновленими, установлювати останнє оновлення безпеки за умови виконання безпеки оновлення відповідно до політик СУІБ. Після оновлення CSO/CISO/Ad1 повинен перевірити налаштування параметрів безпеки з метою виконання політики безпеки;

4.3.21 перевіряти робочу станцію (особливо це стосується робочих станцій, на яких зберігається важлива для виконкому міської ради інформація) якщо виникає підозра або коли це є необхідним, чи є апаратні кейлогери (наприклад, бездротовий знімок клавіатури), програмні кейлогери та приховані камери. Перевірку здійснює виключно посадова особа SOC за поданням користувача;

4.3.22 якщо в локальній мережі є маршрутизатори Wi-Fi, рекомендовано (за можливості) уводити пароль за допомогою екранної клавіатури. Доцільно (було б більш безпечно) використовувати віртуальну клавіатуру (або м’яку клавіатуру), яка кожен раз змінює розкладки;

4.3.23 заблокувати комп’ютер та мобільний телефон, коли вони залишаються;

4.3.24 перед тим, як розміщувати на Embedded OpenType важливі файли, зашифровується весь жорсткий диск за допомогою функцій «BitLocker», «LUKS» або подібних інструментів;

4.3.25 доступ до важливих вебсайтів виконується в приватному режимі або в режимі анонімного перегляду, чи використовується один веббраузер для доступу до важливих вебсайтів, а другий для доступу до інших;

4.3.26 використовувати (за можливості) 3 різні адреси електронної пошти (із дотриманням правил щодо робочої пошти та погодженням з CSO). Використовувати першу, щоб отримувати електронні листи з важливих сайтів і додатків. Використовувати другу, щоб отримувати електронні листи з неважливих сайтів та програм. Використовувати третю (від постачальника послуг електронної пошти, таких як «Outlook» і «Gmail»), щоб отримувати електронну пошту для скидання пароля, коли перша вийшла з ладу;

4.3.27 використовувати (за можливості) 2 телефонні номери, не повідомляти іншим особам номер телефона, що використовується для отримання текстових повідомлень, кодів підтвердження;

4.3.28 не натискати посилання в електронному листі чи текстовому телефонному повідомленні, не скидати паролі, натискаючи їх, за винятком того, коли відомо, що ці повідомлення не є фальшивими;

4.3.29 не повідомляти паролі нікому в електронній пошті;

4.3.30 бути обережними, використовуючи інструменти онлайн-вставки та інструменти захоплення екрана, не дозволяти їм завантажувати паролі в хмарні сервіси;

4.3.31 вебмайстру/адміністратору сайта заборонено зберігати паролі користувачів, питання безпеки та відповіді як звичайний текст у базі даних, замість цього слід зберігати хеш-значення цих рядків (SHA1, SHA256 або SHA512). Рекомендується створити унікальний випадковий рядок для кожного користувача. Крім того, доцільно реєструвати інформацію про пристрій користувача (наприклад, версію ОС, роздільну здатність екрану тощо) та зберігати їх хеш-значення, а потім, коли користувач намагається увійти з правильним паролем, але його пристрій/інформація не збігається з попередньою збереженою, слід дозволити цьому користувачеві підтвердити свою особу, увівши інший код підтвердження, надісланий через текстове телефонне повідомлення або електронну пошту;

4.3.32 закривати веббраузер, коли користувач залишає комп’ютер, інакше файли «cookie» можна легко перехопити, що дозволяє обійти двоступеневу перевірку та увійти у обліковий запис з украденими файлами «cookie» на інших комп’ютерах;

4.3.33 забороняється використовувати облікові записи та паролі за замовчуванням на активних мережевих пристроях, підключених до мережі.

#### *5. Управління таємною інформацією автентифікації користувачів*

5.1. Облік таємної інформації автентифікації користувачів (пароль, login) має контролюватися за допомогою такого процесу управління:

5.1.1 від користувачів треба вимагати підписання положення щодо конфіденційного зберігання персональної таємної інформації автентифікації і зберігання групової (загальної) інформації автентифікації винятково серед членів групи (це підписане положення можливо розмістити в термінах та умовах найму);

5.1.2 якщо від користувачів вимагають підтримки їх власної таємної інформації автентифікації, їм треба спочатку надати безпечну тимчасову таємну інформацію автентифікації, яку їх примушують замінити під час першого використання;

5.1.3 визначено процедури верифікації перевірки ідентичності користувача перед наданням нової, заміненої або тимчасової таємної інформації автентифікації;

5.1.4 тимчасова таємна інформація автентифікації надається користувачам у безпечний спосіб;

5.1.5 уникнення залучення зовнішніх сторін або використання незахищених (відкритий текст) повідомлень електронної пошти;

5.1.6 тимчасова таємна інформація автентифікації має бути унікальною для особи й не повинна бути такою, яку можна відтворити;

5.1.7 користувачі підтверджують отримання таємної інформації автентифікації;

5.1.8 використовувану за замовчуванням таємну інформацію автентифікації постачальника має бути змінено після інсталяції систем або програмного забезпечення.

5.2. Паролі є типом таємної інформації автентифікації, що зазвичай, використовують, і є загальними засобами верифікації особи користувача. Іншими типами таємної інформації автентифікації користувача є криптографічні ключі та інші дані, що зберігаються на апаратних токенах (наприклад, смарткартках), які виробляють коди автентифікації.

#### *6. Керування паролями користувачів*

6. Усі користувачі повинні дотримуватися таких правил:

6.1 з прийняттям документу D14.15-СУІБ «Заява про ознайомлення та прийняття документів системи управління інформаційною безпекою та конфіденційністю», користувач також приймає зобов'язання забезпечити конфіденційність усіх паролів, як це встановлено Політикою керування паролями;

6.2 кожен користувач повинен використовувати тільки свій унікальний ідентифікатор (ім'я користувача), спеціально для нього створений;

6.3 кожен користувач повинен мати право вибору власного пароля там, де це може бути застосовано;

6.4 тимчасові або початкові паролі, використовувані для першого входу в систему, повинні відповідати всім вимогам, описаним вище;

6.5 тимчасові або початкові паролі мають бути передані користувачеві безпечним способом, і користувач повинен бути однозначно ідентифікований;

6.6 інформаційні системи мають вимагати зміни первинних паролів при першому вході в систему;

6.7 інформаційні системи мають забезпечувати складність паролів відповідно до вимог, наведених вище;

6.8 інформаційні системи мають забезпечувати зміну паролів користувачів кожні три місяці;

6.9 скидання пароля користувача на тимчасовий (у разі, якщо користувач забув пароль) повинно виконуватися тільки після ідентифікації користувача;

6.10 паролі, що вводяться, не повинні відображатися на екрані;

6.11 якщо користувач увів неправильний пароль три рази поспіль, то його обліковий запис має бути заблокованим автоматично;

6.12 усі початкові паролі, установлені виробниками обладнання та розробниками програмного забезпечення, мають бути змінені перед уведенням в експлуатацію обладнання або відразу після розгортання програмного забезпечення.

*\*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***