



ВИКОНАВЧИЙ КОМІТЕТ ШЕПЕТІВСЬКОЇ МІСЬКОЇ РАДИ

РОЗПОРЯДЖЕННЯ

14 березня 2025 року

м. Шепетівка

№ 03-05/38-2025

Про затвердження Порядку використання комп'ютерної техніки, програмного забезпечення та забезпечення інформаційної безпеки виконавчого комітету Шепетівської міської ради

Відповідно до статті 42 Закону України «Про місцеве самоврядування», Закону України «Про основні засади забезпечення кібербезпеки України», з метою виконання вимог нормативно-правових актів, які регулюють питання кібербезпеки та інформаційної безпеки:

1. Затвердити Порядок використання комп'ютерної техніки, програмного забезпечення та забезпечення інформаційної безпеки виконавчого комітету Шепетівської міської ради (додається).
2. Керівникам структурних підрозділів виконавчого комітету Шепетівської міської ради забезпечити дотримання працівниками Порядку використання комп'ютерної техніки, програмного забезпечення та забезпечення інформаційної безпеки виконавчого комітету Шепетівської міської ради.
3. Контроль за виконанням цього розпорядження покласти на заступника міського голови з питань діяльності виконавчих органів ради згідно розподілу обов'язків.

Міський голова

Віталій БУЗИЛЬ

ЗАТВЕРДЖЕНО

розпорядження міського голови

від 14.03.2025 № 03-05/38-2025

**Порядок
використання комп'ютерної техніки, програмного забезпечення
та забезпечення інформаційної безпеки
виконавчого комітету Шепетівської міської ради**

1. Загальні положення

1.1. Порядок використання комп'ютерної техніки, програмного забезпечення та забезпечення інформаційної безпеки виконавчого комітету Шепетівської міської ради (далі Порядок) - це внутрішній документ, який визначає стратегії, правила та процедури для забезпечення безпеки інформаційних систем і даних, які обробляються, зберігаються та передаються в рамках діяльності виконавчого комітету міської ради. Ця політика покликана захищати від несанкціонованого доступу, пошкодження, втрати чи викрадення інформації, а також забезпечити дотримання відповідних законодавчих та нормативних вимог.

1.2. Даний Порядок розроблено на основі нормативно-правових актів, які регулюють кібербезпеку та інформаційну безпеку в роботі органів місцевого самоврядування в Україні: Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Про інформацію», Закон України «Про доступ до публічної інформації», Закон України «Про електронні документи та електронний документообіг», постанова Кабінету Міністрів України «Про затвердження Порядку захисту персональних даних під час їх обробки в базах персональних даних», нормативно-правові акти Державної служби спеціального зв'язку та захисту інформації України.

2. Цілі та завдання

2.1. Порядок має на меті забезпечити захист інформаційних ресурсів та підтримку безперебійної роботи виконавчого комітету Шепетівської міської ради.

2.1.1. Захист конфіденційності інформації. Забезпечення того, щоб чутлива інформація була доступна лише тим, хто має відповідні права доступу.

2.1.2. Забезпечення цілісності даних. Захист даних від несанкціонованих змін або видалення, щоб підтримувати їх точність і достовірність.

2.1.3. Гарантування доступності інформації. Підтримка доступності інформаційних систем і даних для авторизованих користувачів тоді, коли це необхідно, без збоїв або затримок.

2.1.4. Управління ризиками. Виявлення, оцінка та мінімізація ризиків, пов'язаних із кіберзагрозами, через впровадження відповідних заходів безпеки.

2.1.5. Захист від кіберзагроз. Впровадження та підтримка захисних технологій та процесів для запобігання несанкціонованого доступу, атак та зловмисного програмного забезпечення.

2.1.6. Інформаційна обізнаність і навчання. Підвищення обізнаності співробітників щодо загроз кібербезпеки та надання регулярного навчання для забезпечення їхньої готовності реагувати на потенційні інциденти.

2.1.7. Реагування на інциденти. Встановлення чітких процедур для швидкого реагування і відновлення у випадку інцидентів безпеки, таких як витік даних або кібернапад.

2.1.8. Відповідність законодавству. Забезпечення відповідності всім застосованим законодавчим і нормативним вимогам щодо захисту інформації.

2.1.9. Неперервність діяльності. Розробка стратегій для забезпечення безперервності роботи виконавчого комітету міської ради в разі надзвичайних ситуацій, які можуть вплинути на інформаційні системи.

3. Оцінка ризиків

3.1. У працівників виконавчого комітету міської ради можуть виникати такі основні ризики кібербезпеки та інформаційної безпеки на робочому місці чи під час виконання робочих задач:

3.1.1. Фішингові атаки. Спроби отримати конфіденційну інформацію, таку як паролі або фінансові дані, шляхом обману, наприклад, через електронні листи або фальшиві веб-сайти.

3.1.2. Несанкціонований доступ. Ризик отримання доступу до чутливих даних або інформаційних систем сторонніми особами або зловмисниками.

3.1.3. Витік даних. Втрата або несанкціоноване розголошення конфіденційної інформації, що може статися через хакерські атаки або недбалість співробітників.

3.1.4. Зловмисні програми. Інфікування комп'ютерних систем шкідливим програмним забезпеченням, яке може викрасти, знищити або заблокувати інформацію.

3.1.5. Соціальна інженерія. Маніпуляції, що націлені на те, щоб змусити співробітників розкрити конфіденційну інформацію або отримати доступ до систем.

3.1.6. Незахищені мережі. Використання ненадійних або погано захищених мереж, що може призвести до перехоплення даних під час їх передачі.

3.1.7. Недостатня автентифікація. Використання слабких паролів або відсутність двофакторної автентифікації, що полегшує несанкціонований доступ.

3.1.8. Вразливості в програмному забезпеченні. Використання застарілого або неоновленого програмного забезпечення, яке може містити відомі вразливості, що використовуються хакерами.

3.1.9. Відсутність резервного копіювання даних. Ризик повної втрати даних у разі атаки з використанням зловмисного програмного забезпечення або технічної аварії без можливості їх відновлення.

3.1.10. Людський фактор. Недбалість або помилки співробітників, які можуть призвести до випадкового видалення або розголошення даних.

4. Вимоги до працівників

4.1 Кожен працівник виконавчого комітету міської ради зобов'язаний особисто ознайомитися з цим Порядком.

4.2. Комп'ютерна техніка та програмне забезпечення надані виключно для виконання службових і посадових обов'язків.

4.3. Першою лінією захисту в системі управління інформаційною безпекою є працівники виконавчого комітету міської ради або користувачі. Користувачі несуть відповідальність за безпеку всіх даних, які можуть надходити до них у будь-якому форматі.

4.4. Працівник повинен вживати необхідних заходів для забезпечення фізичної та цифрової безпеки даних та інформації.

4.5. Всі робочі станції (ПК), які знаходяться в установі, не повинні залишати приміщення виконавчого комітету міської ради без відповідного дозволу керівника. При використанні робочих станцій за межами, користувач повинен вжити всіх можливих заходів із забезпечення безпечного зберігання та використання ПК, інформації та програмного забезпечення, що на ньому знаходяться.

4.6. Робочі станції, які залишаються без нагляду, повинні бути заблоковані користувачем при виході з робочої зони (робочого місця). На робочих станціях може

застосовуватись налаштування автоматичного блокування екрана за бездіяльності або функція «Динамічне блокування».

5. Заборонена діяльність

5.1. Несанкціонований перегляд інформації. Умисний, несанкціонований доступ або перегляд інформації, до якої не надавалися права на доступ чи перегляд.

5.2. Використання особистого або недозволеного програмного забезпечення на робочих станціях. Все програмне забезпечення, встановлене на робочих станціях, має бути затверджене та дозволене до використання.

5.3. Використовувати дозволене програмне забезпечення неналежним чином.

5.4. Порушувати або намагатися порушити умови використання або ліцензійну угоду будь-якого програмного продукту, що дозволено до використання на робочих станціях.

5.5. Використовувати інформаційні системи незалежним чином. Брати участь у будь-якій діяльності з будь-якою метою, яка є незаконною або суперечить чинній політиці інформаційної безпеки.

6. Користування мережею Інтернет

6.1. Надані працівникам ресурси, такі як робочі станції або ноутбуки, комп'ютерні системи, мережі, електронна пошта, програмне забезпечення, а також доступ до Інтернет, призначені для використання в робочих цілях.

6.2. Доступ до Інтернету надається тільки тим співробітникам, хто його потребує для виконання службових обов'язків.

6.3. Працівник, що має доступ до Інтернету, не повинен використовувати цей доступ для розваг, прослуховування музики чи радіо, прослуховування онлайн аудіо книг, перегляду фільмів та інших медійних файлів тощо.

6.4. Ресурси, які заборонено відвідувати: ігрові інтернет-сайти, торенти, файлообмінники, сайти інтимного змісту, чати та онлайн програми для обміну музикою, тощо.

6.5. За потреби доступу до зовнішньої ІТ-системи (хмари), необхідно зв'язатися зі своїм безпосереднім керівником або відповідальним за інформаційну безпеку. Вони визначають безпечний метод доступу до потрібної зовнішньої системи.

7. Користування електронною поштою

7.1. Єдиною офіційною електронною поштою виконавчого комітету міської ради є 04060789@shepetivka-rada.gov.ua.

7.2. Офіційна електронна скринька, дозволена для робочого листування - це скринька із доменом gov.ua.

7.3. Офіційне цифрове листування виконавчого комітету міської ради відбувається виключно через запроваджену систему електронного документообігу «DeKa Office» та Систему електронної взаємодії органів виконавчої влади (СЕВ ОВВ) через повноважених на це працівників.

7.4. Заборонено використовувати службову електронну пошту в особистих цілях та для особистого листування.

7.5. Особисті електронні скриньки заборонено використовувати на робочому місці та заборонено використовувати для ведення робочого листування.

7.6. Працівники повинні уважно ставитися до електронної кореспонденції, яка містить файли із розширенням *.BAT, *.COM, *.EXE, якщо їх надходження не було чітко погоджено з адресантом. У разі виникнення сумнівів щодо повідомлення, яке надійшло електронною поштою, користувач повинен звернутись до безпосереднього керівника.

7.7. Виконавчий комітет міської ради зберігає за собою право здійснювати моніторинг змісту будь-якого електронного повідомлення та комунікації, що генерується

або передається з використанням інформаційних активів виконавчого комітету міської ради. Це робиться з метою належного обслуговування та захисту інформаційно-телекомунікаційного обладнання, мереж та ефективного використання наявних ресурсів. Моніторинг може здійснюватися постійно або час від часу. Для цього можуть застосовуватися різні методи моніторингу.

8. Соціальні мережі та месенджери

8.1. Заборонено авторизацію сторінок персональних соціальних мереж (Facebook, Instagram та ін.) на робочому ПК. Виключення становлять фахівці, які займаються веденням каналів комунікацій виконавчого комітету міської ради.

8.2. Пересилання службової інформації через месенджери особистого мобільного телефону заборонено.

8.3. Месенджери Telegram, Viber, WhatsApp, Facebook messenger, тощо заборонено до встановлення та використання на робочому ПК.

9. Встановлення паролів

9.1. Паролі потрібні для того, щоб отримати доступ до мереж і робочих ПК. До всіх паролів застосовується встановлена цим документом Парольна політика для забезпечення стійкості паролів. Це означає, що всі паролі повинні відповідати вимогам, які призначені для того, щоб пароль було важко підібрати чи зламати.

9.2. Користувачі зобов'язані створювати та користуватися паролями, щоб отримати доступ до відповідних мереж, IT-ресурсів чи робочої станції.

9.3. При призначенні паролю користувачеві буде автоматично запропоновано вручну призначити пароль, відповідно до вимог.

9.3.1. Довжина пароля - пароль повинен складатися з мінімуму восьми (8) символів.

9.3.2. Вимоги до складу - пароль повинен містити комбінацію символів латинського алфавіту верхнього та нижнього регістру, числових символів та спеціальних символів.

9.3.3. Частота зміни - пароль повинен бути змінений кожні 90 днів. Скомпрометований пароль повинен бути змінений негайно.

9.3.4. Повторне використання - попередні три (3) паролі не можуть бути використані повторно.

9.3.5. Обмеження на обмін паролями - паролі не повинні передаватися іншим працівникам, записуватися на папері або зберігатися на робочій станції і повинні зберігатися у таємниці.

9.3.6. Обмеження на відображення та зберігання паролів - паролі маскуються на екрані робочої станції при введенні, не друкуються і не включаються до електронних журналів чи звітів.

9.4. Паролі не зберігаються на паперових носіях.

10. Політика чистого столу/екрану

10.1. Політика чистого столу та чистого екрану знижує ризик несанкціонованого доступу, втрату та пошкодження інформації протягом робочого часу та після його закінчення.

10.2. Політика чистого столу та чистого екрану визначає методи, пов'язані із забезпеченням того, щоб конфіденційна інформація, як у цифровому, так і у паперовому/фізичному форматі, та активи (наприклад, робочі станції, ноутбуки, стаціонарні телефонні апарати, смартфони, цифрове обладнання та інші) не залишаються без захисту, коли вони не використовуються, чи коли працівник залишає свої робочі місця на короткий час або наприкінці дня.

10.3. Дотримання політики чистого столу/екрану дозволить суттєво забезпечити від витоку конфіденційної інформації.

10.4. Метою впровадження політики чистого столу та чистого екрану є:

10.4.1. Запобігання витоку/втраті конфіденційних даних виконавчого комітету міської ради;

10.4.2. Дотримання правил кібергігієни та розвитку кіберкультури, щодо безпечного та належного поводження з конфіденційною інформацією та її носіями;

10.4.3. Створення та підтримання позитивного іміджу.

10.5. Усі працівники повинні дотримуватись наступних правил:

10.5.1. Зберігати власні паролі в таємниці, не розголошувати та нікому не повідомляти їх;

10.5.2. Закривати активні сеанси після завершення роботи, якщо їх не можна захистити відповідним блокуючим механізмом, наприклад блокуванням екрану;

10.5.3. Встановити час автоматичного блокування екрану ПЕС;

10.5.4. Забороняється вести запис паролів (наприклад, на папері, у програмному файлі або в кишеньковому пристрої);

10.5.5. Матеріальні носії конфіденційної інформації повинні замикатися в сейфі або шафі після завершення роботи з ними;

10.5.6. Робочі станції, комп'ютери та засоби зв'язку повинні бути залишені у стані виконаного виходу із системи/вимкнені коли вони перебувають без нагляду;

10.5.7. Документи, які містять конфіденційну інформацію, повинні забиратися виконавцем з принтерів негайно;

10.5.8. Наприкінці робочого дня/зміни працівники повинні упорядкувати своє робоче місце;

10.5.9. Для утилізації конфіденційних документів слід використовувати подрібнювачі паперу;

10.5.10. Після закінчення робочого дня та у разі тривалої відсутності на робочому місці необхідно замикати на замок усі шафи та сейфи де зберігається конфіденційна інформація і робочі документи.

11. Повідомлення про порушення

11.1. Будь-який працівник, якому стало відомо про порушення Порядку, негайно повідомляє про це свого безпосереднього керівника.

11.2. Повідомлення повинно відбуватися негайно після виявлення можливого порушення або до закінчення робочого дня, якщо інші обов'язки заважають зробити це негайно.

11.3. Безпосередній керівник вживає можливі заходи реагування на порушення.

12. Відповідальність

Вимоги цього Порядку поширюються на всіх працівників виконавчого комітету міської ради, які несуть відповідальність за порушення Порядку, згідно чинного законодавства України.

Заступник міського голови

Віталій ЯНУШЕВСЬКИЙ