ОХТИРСЬКА МІСЬКА РАДА

РОЗПОРЯДЖЕННЯ
МІСЬКОГО ГОЛОВИ

11.02.2026 **м. Охтирка** **№ 22 - ОД**

Про заходи з інформаційної безпеки та посилення рівня кіберзахисту в Охтирській міській раді

З метою забезпечення належного рівня захисту службової інформації, недопущення витоку персональних даних, мінімізації ризиків кібератак в умовах воєнного стану, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», постанови Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», керуючись пунктом 20 частини четвертої статті 42 Закону України «Про місцеве самоврядування в Україні»:

1. Затвердити Інструкцію з дотримання вимог інформаційної безпеки та кібербезпеки при роботі з електронною поштою, що додається.

2. Відділу з організаційно-кадрової роботи та контролю апарату міської ради та її виконавчого комітету, керівникам структурних підрозділів зі статусом юридичної особи ознайомити посадових осіб та працівників з інструкцією з дотримання вимог інформаційної безпеки та кібербезпеки при роботі з електронною поштою під особистий підпис та подати підтвердження ознайомлення керуючому справами виконавчого комітету Гуць В.О.

3. Посадовим особам виконавчих органів міської ради пройти навчання з питань кібербезпеки та кібергігієни з обов'язковим отриманням персонального сертифіката:

1) на платформі «Prometheus» https://prometheus.org.ua/ тема навчання : «CS50: Вступ до кібербезпеки»;

2) на платформі «ДіяОсвіта» https://osvita.diia.gov.ua/ тема навчання: «Базові знання з кібергігієни» та «Основи кібергігієни. Як держслужбовцям захиститися від хакерських атак».

Сертифікат про проходження навчання з кібербезпеки долучити до особової справи працівника.

4. Контроль за виконанням цього розпорядження покладаю на керуючого справами виконавчого комітету Гуць В.О.

Міський голова **Павло КУЗЬМЕНКО**

Додаток
до розпорядження міського голови
від 11.02.2026 № 22 - ОД

ІНСТРУКЦІЯ
з дотримання вимог інформаційної та кібербезпеки при роботі з електронною поштою

І. Загальні положення

1. Інструкція визначає порядок забезпечення інформаційної безпеки, кіберзахисту та реагування на інциденти в інформаційно-комунікаційних системах міської ради.
2. Вимоги Інструкції є обов’язковими для всіх посадових осіб та працівників виконавчих органів міської ради.

ІІ. Особливості забезпечення інформаційної безпеки в умовах воєнного стану

1. В умовах воєнного стану інформаційна інфраструктура міської ради розглядається як об’єкт підвищеного ризику кібератак.
2. У період воєнного стану додатково забороняється:
1) використовувати незахищені публічні Wi-Fi мережі для доступу до службових ресурсів;
2) передавати службову інформацію через особисті електронні скриньки;
3) здійснювати дистанційне підключення до робочих станцій без погодження з відповідальною особою.
3. У разі масованих кібератак або підозри на втручання в інформаційні системи може прийматися рішення про тимчасове відключення окремих сервісів.

ІІІ. Використання електронної пошти

1. Забороняється:
1) переходити за підозрілими посиланнями;
2) відкривати вкладення з невідомих джерел;
3) вводити службові паролі за посиланнями з листів;
4) передавати паролі третім особам.
2. У разі виявлення підозрілого листа працівник зобов’язаний:
1) припинити будь-які дії з листом;
2) повідомити відповідальну особу;
3) не здійснювати самостійних технічних втручань.

ІV. Використання месенджерів

1. Месенджери не є офіційними каналами документообігу.

2. Забороняється:

1) передавати через месенджери персональні дані без службової необхідності;

2) надсилати службові документи з грифом обмеження доступу;

3) використовувати особисті акаунти для пересилання службових файлів.

3. У разі використання месенджерів для оперативної координації забороняється:

1) поширювати службову інформацію без визначення кола осіб;

2) пересилати скріншоти внутрішніх систем;

3) зберігати службові файли на особистих пристроях.

4. Вся службова інформація після оперативного обговорення підлягає фіксації в установленому порядку через офіційні канали.

VI. Реагування на інциденти

1. Будь-який несанкціонований доступ, перехід за фішинговим посиланням або підозра на втручання в систему вважається інцидентом інформаційної безпеки.

2. У разі виявлення ознак інциденту інформаційної безпеки працівник зобов’язаний подати службову записку керівнику структурного підрозділу та повідомити відповідальну особу з інформаційної безпеки.

3. За результатами аналізу може ініціюватися службове розслідування.

VII. Відповідальність

1. Порушення вимог цієї Інструкції є порушенням службової дисципліни.

2. Відповідальність настає відповідно до Кодексу законів про працю України та інших нормативно-правових актів.

Керуючий справами
виконавчого комітету **Володимир ГУЦЬ**

Начальник відділу
з організації діяльності ради **Сергій ЧЕРНОЙВАН**

Пояснювальна записка
до розпорядження міського голови № _____ від _____
«Про заходи з інформаційної безпеки та посилення рівня кіберзахисту в Охтирській міській раді»

1. Глосарій

Електронна пошта - це служба для передавання текстових повідомлень та прикріплених до них файлів у вигляді листів через Інтернет.

Електронний лист - це повідомлення електронної пошти. Електронний лист обов'язково містить такі елементи, як: адреса відправника, адреси отримувачів листа, тему листа, дату та час відправки, та власне текст повідомлення.

SPAM-фільтр - це функціональність електронної пошти, яка допомагає автоматично виявляти листи, які за певними характеристиками вважаються підозрілими. Першочергова мета SPAM-фільтру – це захист користувача від небажаної та несанкціонованої реклами. SPAM-фільтр також допомагає фільтрувати електронні листи з неправдивою інформацією (за допомогою репутаційних рейтингів та інших механізмів).

Месенджер - це програмне забезпечення для обміну текстовими повідомленнями, зображеннями, відео, а також для здійснення аудіо- та відеодзвінків.

2. Електронна пошта та її безпечне використання

В англомовній літературі електронну пошту називають email (від англ. electronic mail). Формат адреси електронної пошти має наступний вигляд:
Ім'я користувача
спеціальний символ @
адреса поштового сервісу (наприклад, gmail.com)
Приклади: ivan.petrenko@meta.ua, ivan.petrenko@ukr.net, info@rada.gov.ua.
Адреса електронної пошти пишеться літерами латинського алфавіту (у переважній більшості випадків). Ім'я користувача може містити знаки пунктуації, такі як крапка та дефіс. Адреса поштового сервісу використовує символ крапки як службовий символ для навігації в адресі (для розмежування назв основного та підлеглого розташування поштової служби).
Електронна пошта дозволяє відправити однаковий електронний лист одразу великому переліку отримувачів.
Окрім зазначених атрибутів електронного листа, також існують: копія та прихована копія для виокремлення деяких адресатів листа, критерій важливості листа (низький, середній, високий).

3. Програмне забезпечення електронної пошти

Існує багато варіацій програмного забезпечення для роботи з електронною поштою.

Існує категорія служб електронної пошти, яка працює на базі інтернет-сайту і не вимагає від користувача навичок зі встановлення та налаштування окремого програмного забезпечення на комп'ютері. Такий вид електронної пошти називається веб-пошта (англ. web-mail).

Варто пам'ятати, що веб-пошта передбачає технічний доступ власника служби веб-пошти до вашої переписки. Деякі з цих програм автоматично аналізують зміст ваших листів з метою надання пропозицій для відповідей на лист. Популярні служби дорожать своєю репутацією. Проте цей аспект не можна ігнорувати повністю при виборі служби електронної пошти. Такі веб-служби, як yandex, mail.ru, rambler мають російське походження.

Переваги сервісів веб-пошти включають у себе також автоматичну перевірку файлів, які вкладено до електронного листа, на наявність шкідливого програмного забезпечення (на наявність комп'ютерних вірусів). Ця функціональність надається не всіма службами і потребує уточнення при виборі служби для майбутнього користування. Наприклад, перевірка файлів виконується в багатьох інших популярних поштових сервісах. Ця функціональність може бути дуже корисною для захисту вашого комп'ютера і особистих даних від можливих загроз.

Додатково існують версії програмного забезпечення електронної пошти для мобільних пристроїв. Варто зауважити, що організації часто не рекомендують використання електронної пошти з мобільних пристроїв для доступу до робочої переписки та конфіденційних службових документів. Це спричинено ризиками втрати або крадіжки мобільного телефону.

Сучасне програмне забезпечення електронної пошти автоматично сортує електронні листи до так званих «папок» та «підпапок» в електронній поштовій скриньці. Стандартними є наступні «папки»: вхідні листи, відправлені листи, чернетки, видалені листи.

4. Поради по безпечному використанню електронної пошти

Хорошою практикою є дотримання наступних підходів та знання наступної допоміжної інформації при використанні месенджерів електронної пошти на робочому місці:

Не використовуйте робочу електронну пошту для особистих потреб та не використовуйте її для реєстрації в Інтернет-сайтах, які не призначені для виконання робочих завдань.

Не повідомляйте адресу своєї робочої електронної пошти без робочої потреби.

Остерігайтеся листів від невідомих відправників.

Остерігайтеся листів, що можуть містити файли зі шкідливим програмним забезпеченням.

Остерігайтеся листів, що містять Інтернет-посилання. Не відкривайте їх, якщо ви не впевнені в легітимності листа.

Остерігайтеся листів відправлених з адрес, які мають підозрілу чи «немилозвучну» адресу поштової служби після символу @ (наприклад, ivan.petrenko@8dd5fas43ff3zdfsgdh343.com). Також варто акцентувати уваги на адреси що схожі на офіційні, але відрізняється одним або кількома символами (наприклад, moz@moz.dov.ua)

Остерігайтеся листів, відправлених з адрес, які мають адресу поштової служби protonmail, це легальна веб-служба, але користується великою популярністю серед різного роду шахраїв та користувачів, які бажають отримати більшу анонімність при роботі з Інтернетом.

Остерігайтеся листів, відправлених з адрес, які належать до іншої країни (див. приклади географічних Інтернет-адрес – англомовне джерело).

Повідомляйте керівництво у випадку отримання листів, які містять особисті погрози чи спроби шантажу.

Будьте уважними під час відправки листів і вводу адреси отримувача. Досить часто програма електронної пошти пропонує можливі адреси по перших літерах. Важливо уважно читати, яку саме адресу пропонує програма, щоб уникнути ситуації, коли лист потрапить до незапланованих отримувачів.

Варто знати, як користуватися функцією прихованої копії (BCC) – а саме відправки листа декільком одержувачам без демонстрації адрес одержувачів один одному.

Варто знати, як працює перевірка факту отримання та читання листа. У певних випадках відправник може отримувати автоматичне сповіщення про те, що ви ознайомилися зі змістом листа.

Варто дізнатися максимальний розмір вашої електронної поштової скриньки, який ви можете використовувати, а також максимальний розмір окремого листа, який може бути оброблений службою.

Деяке програмне забезпечення електронної пошти дозволяє встановити параметр заборони подальшої пересилки вашого листа новим отримувачам. Назва функціональності в англомовному меню – «Do Not Forward».

Ваша організація може використовувати інструменти автоматичного перенесення старих електронних листів до архіву. Постарайтеся дізнатися, чи є подібний механізм автоматичної архівації листів та наскільки довго у вас залишатиметься доступ до вашої старої переписки.

Попросіть співробітників, які мають кращі цифрові навички, навчити вас користуватися SPAM-фільтром.

5. Месенджери та їх безпечне використання

Месенджери (англ. messengers) спроектовані для спілкування через Інтернет у режимі, наближеному до швидкого «живого» спілкування. У той час як електронна пошта розрахована в першу чергу на робочу переписку з поступовою та потенційно відкладеною реакцією на повідомлення.

Першочергове призначення месенджерів – це спілкування.

Важливо зауважити, що месенджери не є сумісними між собою. Неможливо в більшості випадків відправити повідомлення з одного месенджера в інший, на відміну від електронної пошти, де існує відкритий стандарт формату повідомлень та протоколів комп'ютерної мережі.

Поради по безпечному використанню месенджерів
Хорошою практикою є дотримання наступних підходів та знання наступної допоміжної інформації при використанні месенджерів в службових цілях:

Використання месенджерів в службових цілях повинно бути узгоджено з вашим керівництвом та за наявності з ІТ-фахівцем у вашій організації.
Історично месенджери використовувалися для особистої і тільки особистої переписки. Це, своєю чергою, вплинуло на функціональність месенджерів.
Більшість популярних месенджерів сьогодні не пропонують функціональність для централізованого налаштування безпеки в межах організації, а також не підтримують сторонні програмні засоби для аналізу повідомлень тощо. У цьому полягає кардинальна різниця між месенджерами та електронною поштою. Електронну пошту можна централізовано налаштувати для безпеки співробітників, а месенджери – ні.
Більшість популярних месенджерів досить суттєво захищені від несанкціонованого втручання в їх роботу та від крадіжки інформації. Водночас вони пропонують мало механізмів для захисту користувачів від наслідків отримання небажаних повідомлень від незнайомих відправників.
З огляду на зазначені причини ваша організація не може допомогти вам відрізняти надійних та легітимних відправників від злодіїв.
Не вступайте в переписку з невідомими контактами в месенджерах. Будьте пильними при отриманні повідомлень від контактів, які не афішують номер телефону та використовують ім‘я-псевдоніми.
Не розраховуйте на фотографію контакту (аватар) як на достовірну інформацію. Дуже часто зловмисники встановлюють в якості фотографії контакту чуже обличчя, яке викликає менше підозр. Наприклад, обличчя молодої жінки або людини, яку можна легко по фото прийняти за медичного працівника через халат або інші атрибути (стетоскоп у кадрі і т.п. прийоми).
Використання назв та логотипів чужих організацій на власних контактах є також популярною хитрістю злодіїв.
Особливо небезпечно завантажувати файли або відкривати Інтернет-посилання з тексту повідомлення, яке надійшло від сумнівного контакту.
Більшість компаній, які розробляють месенджери, публікують рекомендації користувачам щодо безпечного використання месенджерів саме їхньої платформи. Варто ознайомитися з ними, оскільки вони містять детальну та спеціалізовану інформацію для окремо взятого месенджера.
Більшість компаній, які розробляють месенджери, заявляють що ніколи не порушують таємницю переписки, не дивлячись на той факт, що всі повідомлення потрапляють до їх комп'ютерного середовища, перш ніж досягають кінцевого отримувача. У переважній більшості випадків звіти про

незалежне підтвердження цих гарантій недоторканості таємниці переписки важко отримати.
Умови використання месенджерів та інформації, яку користувач повідомляє та передає з їхньою допомогою регулюється політикою конфіденційності. Політику конфіденційності встановлює та публікує компанія, яка розробляє програму-месенджер. У більшості випадків такі документи опубліковано англійською мовою.
Також варто враховувати, що держава, в якій зареєстровано компанію-розробника або в якій знаходиться комп'ютерне обладнання месенджера, потенційно може отримувати доступ до інформації платформи месенджера відповідно до правових механізмів цієї держави. Це стосується також країни-агресора.
Головна рекомендація щодо використання месенджерів: не передавайте за допомогою месенджерів службову інформацію (наприклад, результати аналізів пацієнтів або рахунки на сплату послуг).

6. Деякі поради по безпечному використанню відеоконференцій у робочих цілях

Для проведення відеоконференцій та відеодзвінків у службових цілях рекомендується використання спеціалізованого програмного забезпечення, а не відеозв’язку через месенджери, які мають особисте, а не корпоративне призначення.
При організації відеодзвінків користуйтеся механізмом парольного захисту та обмежуйте перелік користувачів, які можуть приєднатися, за допомогою критерію приналежності до вашої організації.
Користуйтеся механізмом ручного дозволу адміністратора дзвінка на підключення учасників.
Увімкніть сигнал сповіщення про приєднання нових учасників відеодзвінка.
Не виконуйте запис відеодзвінка без згоди на це учасників дзвінка. Не завантажуйте та не зберігайте файли з записом дзвінка в недовірених Інтернет-ресурсах чи інших сумнівних сховищах даних.