СТАРОКОСТЯНТИНІВСЬКА МІСЬКА РАДА
ХМЕЛЬНИЦЬКОЇ ОБЛАСТІ
ВИКОНАВЧИЙ КОМІТЕТ

РОЗПОРЯДЖЕННЯ

__31 серпня _2026__року м. Старокостянтинів № __320/2026-р____

Про затвердження Політики кіберзахисту та інформаційної безпеки виконавчого комітету Старокостянтинівської міської ради

Відповідно до законів України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України», постанови Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», розпорядження міського голови від 11 серпня 2026 року № 625/2026-рвс «Про надання частин чергових відпусток Миколі МЕЛЬНИЧУКУ», керуючись статтею 42 Закону України «Про місцеве самоврядування в Україні»:

1. Затвердити Політику кіберзахисту та інформаційної безпеки виконавчого комітету Старокостянтинівської міської ради (додається).

2. Керівникам виконавчих органів Старокостянтинівської міської ради та структурних підрозділів виконавчого комітету Старокостянтинівської міської ради забезпечити ознайомлення посадових осіб з Політикою кіберзахисту та інформаційної безпеки засобами системи електронного документообігу АСКОД із фіксацією факту ознайомлення в зазначеній системі, а також забезпечити дотримання її вимог.

3. Відповідальній особі за виконання заходів з технічного захисту інформації та забезпечення захисту інформації в інформаційно-комунікаційних системах виконавчого комітету Старокостянтинівської міської ради забезпечити організацію впровадження, перегляд та оновлення Політики кіберзахисту та інформаційної безпеки.

4. Контроль за виконанням цього розпорядження покласти на заступника

міського голови з питань діяльності виконавчих органів Старокостянтинівської міської ради Миколу КОШИКА.

Заступник міського голови з питань діяльності виконавчих органів Старокостянтинівської міської ради підпис Володимир БОГАЧУК

ЗАТВЕРДЖЕНО

Розпорядження міського голови

31 серпня 2026 року № 320/2026-р

Політика кіберзахисту та інформаційної безпеки виконавчого комітету Старокостянтинівської міської ради Версія 1.0

Зміст

1. Загальні положення

Політика кіберзахисту та інформаційної безпеки виконавчого комітету Старокостянтинівської міської ради (далі - Політика) визначає загальні вимоги до інформаційної безпеки у виконавчому комітеті Старокостянтинівської міської ради (далі - ВКМР), основні принципи, цілі та завдання управління інформаційною безпекою ВКМР.

Метою Політики є: забезпечення захисту інформаційних ресурсів ВКМР від зовнішніх і внутрішніх загроз, включаючи кіберзагрози в умовах воєнного стану.

Ця Політика є обов'язковим документом для ознайомлення при прийомі на роботу, поширюється на всі процеси діяльності ВКМР та є обов'язковою для виконання всіма посадовими особами ВКМР. Порушення вимог Політики тягне за собою дисциплінарну відповідальність та відповідальність згідно з чинним законодавством України.

2. Терміни та визначення

Власник інформаційного активу - посадова особа ВКМР, яка несе відповідальність за забезпечення належної класифікації інформації та активів, визначення обмежень доступу, управління ризиками, пов'язаними з активом.

План забезпечення безперервності діяльності - документ, що описує процедури відновлення критичних функцій та інформаційних активів ВКМР після інциденту інформаційної безпеки.

План відновлення після надзвичайних ситуацій - технічний документ відновлення інформаційно-технологічних систем (далі - ІТ-систем) після інцидентів інформаційної безпеки.

Багатофакторна (MFA)/двофакторна автентифікація (2FA) - підтвердження особи за допомогою двох або більше незалежних факторів.

Управління привілейованим доступом - засоби контролю та аудиту дій адміністративних облікових записів.

Вплив - величина збитку внаслідок несанкціонованого розкриття, зміни, знищення або втрати доступності інформації.

Доступність - властивість інформації бути доступною та використовуватися на вимогу авторизованого користувача і/або процесу.

Загроза - можлива небезпека, яка може використовувати вразливість в інформаційній системі.

Інцидент інформаційної безпеки (далі - ІБ) - подія, що порушує нормальну роботу або безпеку інформаційних систем ВКМР.

Конфіденційність - властивість інформації не бути отриманою неавторизованим суб'єктом.

Цілісність - властивість інформації не бути модифікованою неавторизованим суб'єктом.

Уразливість - недолік в інформаційній системі, що може бути використаний для несанкціонованих дій.

Шкідливе програмне забезпечення (ШПЗ) - програмне забезпечення, призначене для порушення конфіденційності, цілісності та/або доступності систем.

Соціальна інженерія - маніпулятивні техніки психологічного впливу з метою отримання несанкціонованого доступу до інформації або систем.

Фішинг - вид кібератаки з використанням підроблених повідомлень або сайтів для викрадення облікових даних чи конфіденційної інформації.

Системний адміністратор (сисадмін) - це ІТ-фахівець, який забезпечує безперебійну роботу комп'ютерної техніки, мереж та програмного забезпечення ВКМР.

3. Класифікація інформації

Вся інформація ВКМР класифікується за чотирма рівнями відповідно до ступеня чутливості та вимог законодавства України:

Рівень	Опис
Публічна	Інформація відкритого доступу, що підлягає оприлюдненню або надається на запит без обмежень, якщо інше не встановлено законом
Конфіденційна	Інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, і яка може поширюватися лише за згодою або на визначених умовах
Для службового користування (ДСК)	Інформація, що міститься в службовій переписці, доповідних записках та інших службових документах, маркуються як «Для службового користування»
Таємна	Інформація, доступ до якої обмежено законом і розголошення якої може завдати шкоди особі, суспільству або державі

4. Управління інформаційною безпекою

4.1. Розподіл обов'язків

Загальна відповідальність за ІБ ВКМР покладається на керівництво виконавчих органів Старокостянтинівської міської ради та структурних підрозділів виконавчого комітету Старокостянтинівської міської ради (далі - Керівництво).

Відповідальна особа за виконання заходів з технічного захисту інформації відповідає за:

впровадження, підтримку та перегляд цієї Політики;

координацію реагування на інциденти ІБ згідно з Планом реагування на кіберінциденти;

організацію навчань та перевірок обізнаності посадових осіб виконавчого комітету Старокостянтинівської міської ради;

взаємодію з CERT-UA та ДССЗЗІ в разі значних кіберінцидентів;

ведення реєстру ризиків та інформаційних активів.

4.2. Перегляд та оновлення Політики

Ця Політика переглядається відповідальною особою за виконання заходів з технічного захисту інформації щонайменше раз на рік, а також при:

суттєвих змінах в процесах або ІТ-інфраструктурі ВКМР;

змінах законодавства України або вимог регуляторів;

виявленні значних кіберінцидентів або нових загроз;

зміні організаційної структури.

Оновлена Політика подається до Керівництва ВКМР для затвердження та розповсюджується з оновленим номером версії.

5. Безпека людських ресурсів

5.1. Прийом на роботу та звільнення

Перевірка кандидатів перед працевлаштуванням повинна враховувати чутливість інформації, до якої вони можуть отримати доступ. Перед звільненням або переведенням посадової особи відділ з кадрової служби виконавчого комітету Старокостянтинівської міської ради зобов’язаний подати заявку адміністратору систем на виконання таких заходів:

відкликання всіх облікових записів (корпоративна пошта, внутрішні системи, мережеві ресурси ВКМР);

відкликання доступу до державних інформаційних реєстрів та електронних сервісів, до яких посадова особа мала доступ у зв’язку з виконанням службових обов’язків;

повернення всіх службових пристроїв (комп’ютерів, ноутбуків, мобільних телефонів, планшетів) та носіїв інформації (токенів, флеш-накопичувачів, зовнішніх дисків), що перебували в користуванні посадової особи та є власністю виконавчого комітету Старокостянтинівської міської ради, з обов’язковим інформуванням відділу бухгалтерського обліку виконавчого комітету Старокостянтинівської міської ради про перелік фактично повернутого майна для внесення відповідних відомостей до бухгалтерського обліку;

передачу доступів до корпоративних ресурсів, якими посадова особа користувалась одноосібно (спільні поштові скриньки, службові акаунти систем), уповноваженому правонаступнику або керівнику підрозділу.

У разі неможливості отримати доступи або пристрої від посадової особи (відмова, відсутність, конфліктне звільнення) керівник підрозділу негайно повідомляє відповідальну особу за виконання заходів з технічного захисту інформації для вжиття технічних заходів із блокування доступів в односторонньому порядку.

5.2. Навчання та обізнаність

Усі посадові особи зобов’язані проходити вступний інструктаж з ІБ при

прийомі на роботу, а також щорічні навчання з оновленнями щодо актуальних загроз.

Програма навчань охоплює: базові принципи ІБ, розпізнавання фішингових атак та соціальної інженерії, правила роботи з паролями та MFA, порядок повідомлення про інциденти, правила використання месенджерів і хмарних сервісів.

Відповідальна особа за виконання заходів з технічного захисту інформації проводить симульовані фішингові атаки не рідше одного разу на рік для оцінки реального рівня обізнаності персоналу. Результати фіксуються та використовуються для коригування програми навчань.

6. Вимоги до підрядників та зовнішніх виконавців

До надання доступу до систем або інформації ВКМР будь-яка третя сторона зобов’язана:

1) підписати угоду про нерозголошення (NDA);
2) ознайомитися з цією Політикою під підпис;
3) отримати доступ виключно до ресурсів, необхідних для виконання конкретного завдання (принцип мінімальних привілеїв).

Роботи підрядника в системах ВКМР проводяться виключно в присутності або під наглядом адміністратора систем. Підряднику забороняється:

1) копіювати дані ВКМР на особисті носії;
2) встановлювати програмне забезпечення без погодження;
3) залишати несанкціонований віддалений доступ після завершення робіт.

Одразу після завершення договірних відносин адміністратор систем зобов’язаний: відкликати всі облікові записи підрядника; видалити або заблокувати VPN-доступ; перевірити журнали подій на наявність підозрілої активності.

7. Управління привілейованим доступом

Управління привілейованим доступом є критично важливим елементом захисту інформаційних систем ВКМР. Компрометація адміністративного облікового запису є одним із найнебезпечніших типів інцидентів ІБ.

Обов’язкові вимоги:

1. Адміністративні облікові записи повністю відокремлені від звичайних робочих. Для повсякденної роботи (пошта, браузер, документи) адміністратори використовують звичайні непривілейовані облікові записи.
2. Привілейовані облікові записи використовуються виключно для виконання адміністративних задач.
3. Для привілейованих облікових записів обов’язкова MFA без винятків.
4. Застосовується принцип «just-in-time access» - привілейований доступ надається тимчасово, на конкретний час і задачу, після чого відкликається.
5. Паролі сервісних та технічних облікових записів підлягають обов’язковій ротації щонайменше раз на 180 днів або негайно при підозрі на компрометацію.

6. Всі дії привілейованих облікових записів фіксуються в захищених журналах аудиту, які не можуть бути змінені або видалені тими самими обліковими записами.

7. Перелік осіб з привілейованим доступом переглядається адміністратором систем щоквартально та після кожного кадрового переміщення.

8. Забороняється передача привілейованих облікових даних третім особам або зберігання їх у незахищеному вигляді.

8. Парольна політика

Ця Парольна політика розроблена відповідно до сучасних стандартів NIST SP 800-63B та рекомендацій CERT-UA.

8.1. Вимоги до паролів

Параметр	Вимога
Мінімальна довжина (звичайні облікові записи)	12 символів
Мінімальна довжина (привілейовані облікові записи)	16 символів
Склад пароля	Щонайменше три з чотирьох категорій: великі літери, малі літери, цифри, спеціальні символи (! @ # $ % тощо)
Заборонено	Ім’я, дата народження, назва підрозділу, послідовності «123456», «qwerty», «password», загальновживані слова
Зміна пароля	Лише при підозрі на компрометацію або витік. Регулярна примусова зміна НЕ застосовується (відповідно до NIST SP 800-63B)
Блокування облікового запису	Після 3 невдалих спроб входу - тимчасове блокування на 1 хвилину або до розблокування адміністратором
Зберігання паролів	Лише в корпоративно затвердженому менеджері паролів або захищеному сховищі. Заборонено зберігати у відкритому вигляді, у браузері, у текстових файлах
Передача паролів	Заборонено будь-якими каналами зв’язку, включаючи електронну пошту та месенджери

8.2. Багатофакторна автентифікація (MFA)

Двофакторна або багатофакторна автентифікація є обов’язковою для:

всіх зовнішніх сервісів (система електронного документообігу, VPN,

вебпошта, хмарні сервіси);

всіх адміністративних облікових записів без винятку;

систем, що містять конфіденційну або обмежену інформацію;

корпоративної електронної пошти.

Для MFA рекомендується використовувати апаратні токени або застосунки-автентифікатори (наприклад: Google Authenticator, Microsoft Authenticator). SMS-коди допускаються лише як резервний метод через їх вразливість до SIM-swapping атак.

Адміністратор систем веде актуальний реєстр облікових записів з увімкненою MFA та перевіряє його щоквартально.

9. Безпека мережі та сегментація

9.1. Загальні положення

Мережа ВКМР повинна бути організована з урахуванням вимог захисту інформації, забезпечення безперервності роботи та запобігання несанкціонованому доступу.

Побудова складної багаторівневої сегментації мережі не є обов’язковою. Захист мережі забезпечується шляхом належного налаштування, обмеження доступу та контролю використання серверного і мережевого обладнання.

9.2. Вимоги до безпеки мережі

1. Налаштування мережевого обладнання повинні відповідати встановленим вимогам безпеки та періодично перевірятися адміністратором систем або відповідальною особою за виконання заходів з технічного захисту інформації.

2. Усі зміни в мережевій інфраструктурі здійснюються виключно відповідальною особою за виконання заходів технічного захисту інформації або системним адміністратором із обов’язковою фіксацією таких змін.

3. Повинно забезпечуватися регулярне резервне копіювання налаштувань мережевого обладнання.

4. Забороняється підключення до мережі установи виконавчого комітету Старокостянтинівської міської ради неавторизованих або невідомих пристроїв.

5. Доступ до налаштувань мережевого обладнання надається лише спеціалістам відділу інформаційного забезпечення виконавчого комітету Старокостянтинівської міської ради, які мають відповідний дозвіл Керівництва.

6. Усі точки підключення до мережі «Інтернет» від провайдерів варто підключати через маршрутизатори з використанням Національної системи доменних імен (DNS) відповідно до рекомендацій CERT-UA та Держспецзв’язку.

9.3. Вимоги до Wi-Fi мереж

1. Паролі за замовчуванням на мережевому обладнанні повинні бути змінені на складні.

2. Функція швидкого підключення (WPS) повинна бути вимкнена.

3. Повинно забезпечуватися своєчасне оновлення програмного

забезпечення мережевого обладнання.

4. Службова та гостьова Wi-Fi мережі повинні бути розділені та ізольовані одна від одної.

10. Електронна пошта, месенджери та хмарні сервіси

10.1. Використання електронної пошти

Корпоративна електронна пошта надається посадовим особам ВКМР виключно для виконання службових обов'язків.

Заборонено:

1. Надсилати паролі, ключі доступу або конфіденційні дані у відкритому вигляді.
2. Використовувати корпоративну пошту для особистих цілей.
3. Підписуватися на маркетингові розсилки без погодження з Керівництвом.
4. Відкривати вкладення або переходити за посиланнями від невідомих або підозрілих відправників. При виявленні підозрілих листів обов'язково повідомити відповідальну особу за виконання заходів з технічного захисту інформації та керівника структурного підрозділу.
5. Надсилати масові розсилки (понад 50 адрес) на зовнішні адреси без дозволу Керівництва.
6. Надсилати матеріали, що містять ШПЗ, забороненим законодавством контент або матеріали, захищені авторським правом.

Доступ колишньої посадової особи до облікового запису корпоративної пошти повинен бути заблокований не пізніше ніж у день припинення трудових відносин.

10.2. Використання месенджерів

Для службового листування дозволяється використовувати месенджери в такому порядку пріоритетності:

1. 1-й пріоритет - захищені корпоративні канали зв'язку або корпоративна електронна пошта;
2. 2-й пріоритет - Signal або інші e2e-шифровані месенджери за погодженням з відповідальною особою за виконання заходів з технічного захисту інформації;
3. Telegram - не рекомендується для передачі службової інформації, оскільки за замовчуванням не забезпечує наскрізного шифрування (відповідно до рекомендацій CERT-UA та ДССЗЗІ). Якщо використання Telegram неминуче - лише в режимі «Таємного чату» (Secret Chat) для конфіденційних повідомлень.

Незалежно від месенджера, забороняється передавати: паролі, ключі доступу, PIN-коди; персональні дані громадян; документи ДСК та вище; фінансову або бюджетну інформацію; будь-яку непублічну інформацію ВКМР.

10.3. Хмарні сервіси

Зберігання документів у хмарних сервісах (Google Drive, OneDrive,

Dropbox тощо) допускається виключно за таких умов:

Якщо доступ надається конкретним особам (через запрошення на електронну пошту):

1. На обліковому записі увімкнена MFA.
2. Доступ до файлів надається виключно конкретним особам за їхньою електронною адресою - посилання типу «для всіх, хто має посилання» не використовується.
3. Зберігання персональних даних та інформації з обмеженим доступом у хмарних сервісах заборонено.

10. Управління пристроями

11.1. Робочі пристрої

Блокування екрану

На всіх комп'ютерах та ноутбуках має бути налаштоване автоматичне блокування екрану - якщо ви нічого не робите 5 хвилин, екран блокується автоматично. Залишати комп'ютер увімкненим і розблокованим без нагляду - заборонено. Якщо відходите від робочого місця - заблокуйте екран вручну (Win + L).

Пароль на вхід до Windows

Ваш обліковий запис на робочому комп'ютері обов'язково має бути захищений паролем. Пароль повинен відповідати вимогам парольної політики, описаної в цьому документі.

Ведеться актуальний реєстр дозволеного та забороненого ПЗ (whitelist/blacklist). Адміністратор систем перевіряє наявність шифрування та відповідність реєстру ПЗ щоквартально.

Шифрування накопичувача є обов'язковим для: усіх ноутбуків та мобільних робочих станцій ВКМР; знімних носіїв (USB, зовнішніх дисків) для зберігання або передачі службових даних. Рекомендовані засоби: BitLocker (Windows), FileVault (macOS).

Встановлення програм

Встановлювати будь-яке програмне забезпечення на робочий комп'ютер самостійно - заборонено. Якщо вам потрібна певна програма, зверніться до відповідальної особи за виконання заходів з технічного захисту інформації або системного адміністратора. Вони встановлять її або нададуть дозвіл. Адміністратор систем разом з відповідальною особою за виконання заходів з технічного захисту інформації ведуть список дозволених і заборонених програм та раз на квартал перевіряють, що на комп'ютерах встановлено лише дозволене ПЗ.

Шифрування даних

Щоб захистити службові дані в разі втрати або крадіжки пристрою, рекомендовано увімкнути шифрування:

на всіх ноутбуках - засобами BitLocker (Windows) або FileVault (macOS);

на USB-флешках та зовнішніх дисках, якщо на них зберігаються або передаються службові файли.

Налаштування шифрування на вимогу користувача виконує системний адміністратор або відповідальна особа за виконання заходів з технічного захисту інформації під час видачі пристрою. Користувачу нічого додатково робити не потрібно - достатньо не вимикати цю функцію самостійно.

11.2. Особисті пристрої

ВКМР може дозволяти використання особистих пристроїв для виконання посадових обов’язків. На таких пристроях обов’язкові:

встановлення антивірусного програмного забезпечення;

активоване шифрування диска;

блокування екрану з паролем або біометрією;

актуальна версія операційної системи та програм.

Зберігати службові документи та чутливі дані на особистих пристроях забороняється. У разі крадіжки або втрати особистого пристрою, з якого здійснювався доступ до систем ВКМР, необхідно негайно повідомити відповідальну особу за виконання заходів з технічного захисту інформації для блокування доступу до інформаційних ресурсів ВКМР.

11.3. Оновлення програмного забезпечення

Режим автоматичного оновлення має бути активований на всіх пристроях та серверах. Критичні оновлення безпеки встановлюються протягом 72 годин після їх виходу. Антивірусне ПЗ та компоненти безпеки оновлюються в автоматичному режимі.

11.4. Захист від шкідливого ПЗ

Антивірусне програмне забезпечення налаштовується на: постійний захист у реальному часі; сканування під час завантаження файлів; сканування поштових серверів щодня, інших серверів - щотижня; сканування вкладень вхідної та вихідної пошти. Комп’ютери з виявленим ШПЗ або без антивірусного захисту негайно ізолюються від мережі ВКМР з обов’язковим оповіщенням відповідальної особи за виконання заходів з технічного захисту інформації.

11.5. Виведення носіїв з експлуатації

Жорсткі диски, флеш-накопичувачі та інші носії інформації, що виводяться з експлуатації, підлягають фізичному знищенню або гарантованому видаленню даних за допомогою сертифікованого ПЗ (DoD 5220.22-M або аналог). Факт знищення фіксується актом з підписом відповідальної особи за виконання заходів з технічного захисту інформації.

11. Логування та моніторинг

Системи логування та моніторингу забезпечують спостережливість інформаційного середовища ВКМР та є основою для виявлення інцидентів і розслідувань.

Обов’язковий мінімум подій, що фіксуються:

1. Дата, час та джерело події (із синхронізацією за NTP).
2. Ідентифікатор облікового запису та пристрою.
3. Тип дії та її статус (успішно/невдало).

4. Успішні та невдалі спроби автентифікації.
5. Зміни в привілейованих облікових записах та правах доступу.
6. Запуск та зупинка критичних сервісів.
7. Встановлення, видалення та запуск програмного забезпечення.
8. Вхід/вихід з системи.

Журнали подій зберігаються в централізованій захищеній системі, недоступній для редагування або видалення з боку адміністраторів систем, щодо яких ведеться моніторинг. Термін зберігання журналів - не менше 12 місяців. Регулярний перегляд журналів здійснюється відповідальною особою за виконання заходів з технічного захисту інформації не рідше одного разу на тиждень, а також при кожному підозрілому інциденті.

13. Резервне копіювання та відновлення

Параметр	Вимога
Критичні реєстри та бази даних	Не більше 4 годин
Документообіг	Не більше 24 годин
Відновлення критичних систем	Не більше 4 годин
Відновлення некритичних систем	Не більше 48 годин
Тестове відновлення критичних систем	Не рідше одного разу на квартал
Тестове відновлення некритичних систем	Не рідше одного разу на рік
Зберігання резервних копій	Мінімум два незалежних місця зберігання: одне локальне, одне географічно віддалене або захищена хмара
Доступ до резервних копій	Обмежено переліком визначених посадових осіб; захищено окремими паролями

Резервні копії зберігаються в зашифрованому вигляді. Результати тестового відновлення фіксуються в протоколі та зберігаються не менше 3 років. Відповідальність за резервне копіювання покладається на адміністратора систем та відповідальну особу за виконання заходів з технічного захисту інформації.

14. Фізична безпека

Доступ до серверних кімнат, комутаційних шаф та приміщень, де зберігається обладнання ВКМР, надається виключно визначеному переліку осіб. Перелік затверджується відповідальною особою з питань цифрового розвитку, цифрових трансформацій і цифровізації у виконавчому комітеті Старокостянтинівської міської ради.

Документи, що містять чутливу або персональну інформацію, забороняється залишати без нагляду. Після використання такі документи зберігаються у закритих шафах або знищуються в шредері. Принцип «чистого столу»: покидаючи робоче місце, посадова особа прибирає всі документи та знімні носії зі столу.

При залишенні пристрою без нагляду він повинен бути заблокований. Про крадіжку або втрату пристрою ВКМР необхідно повідомити відповідальну особу за виконання заходів з технічного захисту інформації.

15. Захист від соціальної інженерії та фішингу

Соціальна інженерія та фішингові атаки є одними з найпоширеніших векторів кіберзагроз для органів місцевого самоврядування, особливо в умовах воєнного стану.

15.1. Правила верифікації запитів

1. Будь-який запит на зміну банківських реквізитів, переказ коштів або надання облікових даних підлягає обов’язковій телефонній верифікації за заздалегідь відомим номером (не з підозрілого листа/повідомлення).

2. При отриманні несподіваного запиту нібито від Керівництва через незвичний канал зв’язку - перевірити особисто або зателефонувати.

3. Принцип «перевір перш ніж клікнути»: перед переходом за посиланням перевірити адресу відправника та URL-адресу.

4. Підозрілі листи або повідомлення не видаляти одразу, а переслати в обов’язковому порядку відповідальній особі за виконання заходів з технічного захисту інформації для аналізу.

15.2. Ознаки фішингу та соціальної інженерії

1. Термінові або загрозливі вимоги («ваш рахунок буде заблоковано», «негайно виконайте»).

2. Запити облікових даних, паролів, кодів з SMS або банківської інформації.

3. Листи нібито від CERT-UA, ДССЗЗІ, СБУ, банків з вкладеннями або посиланнями.

4. Адреса відправника відрізняється від офіційної або містить підозрілі символи.

5. Посилання, що не відповідає відображеному тексту (перевіряється наведенням курсора).

15.3. OSINT та захист від розвідки

В умовах воєнного стану посадові особи ВКМР зобов’язані:

1) не публікувати у відкритих соціальних мережах інформацію про внутрішню структуру ВКМР, ІТ-інфраструктуру, місця розташування серверів, персонал чи графіки роботи;

2) не розкривати технічні деталі мережевої інфраструктури в публічних документах або листуванні;

3) при виявленні публікацій зі службовою інформацією в інтернеті - негайно повідомити відповідальну особу за виконання заходів з технічного захисту інформації.

16. Безпека ланцюга постачання ПЗ та обладнання

Компрометація через ненадійне програмне забезпечення або обладнання є актуальною загрозою для органів місцевого самоврядування.

1. Дозволено встановлювати виключно ПЗ з офіційних джерел (сайт виробника, верифіковані репозиторії). Забороняється використовувати зламані або неліцензовані версії ПЗ.

2. Цифровий підпис дистрибутивів перевіряється перед встановленням.

3. Заборонено або суттєво обмежено використання ПЗ, розробленого в країні-агресорі або підсанкційними компаніями - відповідно до рішень РНБО та рекомендацій ДССЗЗІ.

4. Адміністратор систем веде актуальний реєстр всього встановленого ПЗ із зазначенням версії та джерела.

5. Оновлення ПЗ здійснюються виключно через офіційні канали виробника.

6. Обладнання постачальників перевіряється на відсутність несанкціонованих модифікацій перед введенням в експлуатацію.

17. Особливі вимоги в умовах воєнного стану

У зв’язку із введенням воєнного стану в Україні та підвищеним рівнем кіберзагроз з боку державних акторів країни-агресора, ВКМР встановлює додаткові вимоги відповідно до рекомендацій CERT-UA та ДССЗЗІ.

1. Підвищена готовність: відповідальна особа за виконання заходів з технічного захисту інформації щотижня переглядає актуальні бюлетені CERT-UA (cert.gov.ua) та вживає відповідних заходів захисту.

2. Обов’язкова звітність: про кіберінциденти рівня P1 (критичний) негайно сповіщається CERT-UA та, за необхідності, СБУ.

3. Заборона ПЗ країни-агресора: використання ПЗ, розробленого в Росії або Білорусі, на пристроях ВКМР заборонено (антивіруси, офісне ПЗ, бухгалтерські системи тощо). Перехід на вітчизняні або міжнародні альтернативи.

4. Підвищена пильність до фішингу: у воєнний час зростає кількість цільових атак на органи місцевого самоврядування.

5. Захист критичних даних: особливий контроль доступу до реєстрів населення, земельного кадастру, фінансових даних та іншої критичної інформації.

6. Резервне копіювання поза межами зони активних бойових дій: резервні копії критичних систем зберігаються на географічно безпечних майданчиках або в хмарних сервісах з серверами поза Україною.

7. Додаткова верифікація: для критичних операцій (зміна реквізитів, видача документів) запроваджена додаткова верифікація особи виконавця.

18. Перелік відповідальних осіб

Роль	ПІБ	Підпис
Відповідальна особа за виконання заходів з технічного захисту інформації та забезпечення захисту інформації в ІКС виконавчого комітету Старокостянтинівської міської ради	АНТОНОВ Владислав Сергійович	підпис
Адміністратор систем виконавчого комітету Старокостянтинівської міської ради	БЛІЩ Сергій Степанович, КАЗМІРЧУК Андрій Васильович	підпис підпис
Керівництво	МЕЛЬНИЧУК Микола Степанович	підпис
	КОШИК Микола Анатолійович	підпис
	ШАБЕЛЬНИК Наталія Іванівна	підпис

Начальник відділу інформаційного забезпечення виконавчого комітету Старокостянтинівської міської ради підпис Сергій БЛІЩ