НАЦІОНАЛЬНА АКАДЕМІЯ МЕДИЧНИХ НАУК УКРАЇНИ

вул. Герцена, 12, м. Київ, 04050, тел./факс 489-39-81 тел. 483-68-49
E-mail: amn1@ukr.net, namn_01@ukr.net Код ЄДРПОУ 00061125

07.05.2026 № 5-015/1036 На № _____ від _____

Керівникам державних установ Національної академії медичних наук України
Керівникам структурних підрозділів НАМН України

«Щодо тренінгів з кібергігієни та посилення заходів контролю»

На виконання заходів із забезпечення кібербезпеки національної інфраструктури Міністерством охорони здоров'я України у квітні 2026 року проведено оцінку рівня обізнаності працівників галузі охорони здоров'я щодо загроз у кіберпросторі.

Заходи контролю здійснювались шляхом імітації цілеспрямованої кібератаки з використанням методів соціальної інженерії. На офіційні електронні адреси медичних установ було направлено повідомлення, що імітувало службове сповіщення про необхідність оновлення та верифікації доступу до системи електронного документообігу (СЕД).

Метою заходу контролю було визначення алгоритму дій персоналу при отримати повідомлень, що містять ознаки фішингу (*підміна адреси відправника, наявність неперевірених зовнішніх посилань, спонукання до термінових дій щодо облікових записів*).

Такий захід контролю є актуальним в умовах цілеспрямованих кібератак на заклади охорони здоров'я (зокрема з боку угруповання UAC-0247, що розповсюджує шкідливе програмне забезпечення під виглядом обговорення гуманітарних ініціатив).

Отримані результати засвідчили про необхідність посилення заходів внутрішнього контролю під час роботи працівників з електронною поштою.

Так, під час проведення імітаційної кібератаки, працівники державної установи «Інститут фармакології та токсикології НАМН України» не пройшли безпечну ІТ-перевірку, не продемонстрували високий рівень критичного мислення, чим допустили **компрометацію автентифікаційних даних** *(введення реальних паролів замість введення тестових індикаторів)*.

Ці дії свідчать про неналежну роботу ІТ-спеціалістів медичної установи та не усвідомлення працівниками механізмів соціальної інженерії.

Отримання зловмисниками доступу до службових облікових записів працівників створює передумови для несанкціонованого втручання в роботу внутрішніх систем, витоку службової та фінансової документації, а також використання адрес для поширення шкідливого ПЗ (Ransomware) по всій мережі закладів галузі охорони здоров'я.

Керівництвом НАМН України на постійній основі вживаються організаційні та управлінські заходи щодо функціонування системи внутрішнього контролю та її удосконалення відповідно до вимог постанови Кабінету Міністрів України від 12.12.2018р. № 1062 «Про затвердження Основних засад функціонування внутрішнього контролю у розпорядників бюджетних коштів» та наказу НАМН України від 10.12.2025 № 123 «Про затвердження Порядку та Інструкції щодо організації та функціонування внутрішнього контролю в НАМН України та державних установах, що належать до її сфери управління».

З метою підвищення рівня інформаційної безпеки та кіберзахисту в медичних установах НАМН України, виявлення вразливостей, аналізу поведінкових факторів та оцінки ефективності навчання працівників, доручаю невідкладно вжити таких заходів:

1. Організаційні заходи та навчання працівників установ

Організувати обов'язкове ознайомлення працівників наукових установ НАМН України з Інструкцією про заходи інформаційної безпеки (додаток 1).

Проводити регулярні тренінги з кібергігієни, зокрема щодо правил розпізнавання підозрілих повідомлень, безпечного поводження з посиланнями та файлами, а також захисту облікових записів.

Навчальні матеріали МОЗ: *https://moz.gov.ua/uk/kiberbezpeka;*
https://www.youtube.com/watch?v=54y73kHuI6M.

2. Обмін інформацією про кіберзагрози

Рекомендуємо налагодити взаємодію з мережею вузлів MISP для отримання актуальної інформації про загрози.

Детальніше: *https://cert.gov.ua/article/39962.*

Про результати вжитих заходів внутрішнього контролю поінформувати керівництво НАМН України.

Додаток: 1. Інструкція для ознайомлення на 3 арк. в 1 прим.

Віцепрезидент НАМН України **Сергій ВОЗІАНОВ**

Віхоть З.І.
(044) 486-43-30

Додаток 1 до листа

ІНСТРУКЦІЯ
ПРО ЗАХОДИ КІБЕРГІГІЄНИ ТА БЕЗПЕЧНОЇ РОБОТИ В ПІДПРИЄМСТВАХ, УСТАНОВАХ, ОРГАНІЗАЦІЯХ СФЕРИ ОХОРОНИ ЗДОРОВ'Я

І. Загальні положення

1.1. Ця Інструкція визначає практичні правила кібергігієни та безпечного використання інформаційних активів, інформаційно-комунікаційних систем (ІКС) та електронної пошти працівниками підприємств, установ, організацій сфери охорони здоров'я.

1.2. Метою Інструкції є мінімізація ризиків, пов'язаних із людським фактором (соціальна інженерія, фішинг), та запобігання несанкціонованому доступу до інформації з обмеженим доступом на робочих місцях.

1.3. Усі працівники дають зобов'язання виконувати вимоги цієї Інструкції.

ІІ. Вимоги безпеки під час роботи з електронною поштою та мережею Інтернет

2.1. Звертайте увагу на **типові ознаки фішингу в електронних листах (!):** загальні неперсоналізовані вітання, відчуття терміновості чи залякування ("негайне блокування", "термінова верифікація", "термінове оновлення СЕД"), запити на надання облікових даних, орфографічні помилки або підозрілі домени відправника.

2.2. Не відкривайте вкладені файли та не переходьте за посиланнями від невідомих адресатів.

2.3. Відхиляйте будь-які запити (у тому числі телефонні) щодо надання паролів або PIN-кодів від кваліфікованого електронного підпису (КЕП), оскільки працівники ІТ-підрозділів або фахівці з кіберзахисту ніколи їх не запитують.

2.4. Не встановлюйте самостійно на службові комп'ютери невідомі програми, розширення для браузерів або використовувати сервіси обходу мережевого захисту (особисті VPN-сервіси, проксі-сервери, анонімайзери).

2.5. Не зберігайте та не передавайте інформацію з обмеженим доступом або службову інформацію через відкриті публічні файлообмінники чи неперевірені хмарні сервіси.

2.6. Не використовуйте робоче підключення до мережі Інтернет для збирання і/або поширення матеріалів, зміст яких заборонений законодавством України (зокрема таких, що пропагують насильство, наклепницьку чи непристойну інформацію, розпалюють національну ворожнечу, містять заклики до протиправної чи сепаратистської діяльності).

2.7. Не завантажуйте з мережі Інтернет, не поширюйте (у тому числі

електронною поштою), не запускайте зі змінних носіїв матеріали, що містять комп'ютерні віруси чи шкідливий код, файли з розширеннями .exe, .bat, .cmd, .reg, .com, .vbs, .msi та інші подібні програми, призначені для несанкціонованого доступу, а також генератори ключів або паролі.

2.8. Не можна розповсюджувати матеріали, які захищені авторськими правами, комерційною таємницею, патентами чи іншими правами інтелектуальної власності третіх осіб.

III. Парольна політика та управління доступом

3.1. Використовуйте складні паролі: не менше 8 символів, які містять великі та малі літери, цифри і спеціальні символи (! @ # $ % ^ & *). Пароль не повинен ґрунтуватися на персональній інформації (прізвища, дати народження).

3.2. Інструкція зі створення надійного пароля (метод ідентифікаційної фрази): придумайте фразу (наприклад: "Моєму сину Павлу три роки"). Складіть слово з перших літер ("мсптр") та ускладніть комбінацію великими літерами, цифрами і спецсимволами ("M$п3Р!").

3.3. Не рекомендується використовувати один і той самий пароль для робочих інформаційних систем та особистих ресурсів у мережі Інтернет.

3.4. Не потрібно повідомляти свій пароль будь-яким особам (керівнику, колегам, фахівцям ІТ), записувати його на папері або зберігати у відкритому вигляді на робочому місці.

3.5. Не потрібно виконувати усвідомлені багаторазові спроби доступу до будь-яких інформаційних ресурсів та систем установи, права доступу до яких працівнику не надано.

IV. Безпека робочого місця, змінні носії та штучний інтелект

4.1. Дотримуйтесь правила "чистого екрана": екран робочого комп'ютера підлягає обов'язковому блокуванню під час відсутності працівника (комбінація клавіш Win + L).

4.2. Атака через підкинуті носії: у разі знаходження невідомих флеш-накопичувачів чи інших змінних носіїв, суворо забороняється підключати їх до робочих комп'ютерів. Носій необхідно передати відповідальним ІТ-фахівцям.

4.3. Використання штучного інтелекту (ШІ): з метою запобігання компрометації даних, не потрібно передавати (вводити) персональні дані, інформаційні ресурси або інформацію з обмеженим доступом до відкритих систем ШІ (ChatGPT, Google Gemini, Copilot тощо).

4.4. Не можна самостійно вносити зміни в налаштування операційних систем і прикладного програмного забезпечення. Зокрема, не треба зупиняти роботу додатків та засобів захисту від зловмисного коду (антивірусів), змінювати налаштування поштових і веб-клієнтів або несанкціоновано додавати свій обліковий запис до груп із підвищеними привілеями.

V. Порядок дій у разі виявлення кіберзагрози

5.1. Потенційні інциденти кібербезпеки можуть бути виявлені за такими типовими індикаторами: раптове значне уповільнення роботи комп'ютера, спотворення або зникнення файлів, збої в роботі мережі або поява нетипових повідомлень про помилки.

5.2. Порядок дій у разі підозри на кіберінцидент (випадково перейшли за підозрілим посиланням, ввели пароль на сумнівному сайті):

- негайно припинити роботу на скомпрометованому пристрої;
- не вимикати та не перезавантажувати обладнання (для збереження журналів подій);
- локалізувати загрозу: відключити пристрій від мережі Інтернет та локальної мережі (фізично від'єднати кабель);
- невідкладно повідомити ІТ-підрозділ або службу технічної підтримки установи.