ЗАТВЕРДЖЕНО

Наказ Головного управління Держгеокадастру у Рівненській області

18.05.2021 № 51-од

**Основні вимоги у сфері кібербезпеки під час використання**

**відомчої електронної пошти Головного управління Держгеокадастру у Рівненській області**

1. Вимоги до використання паролю

1.1. Не зберігати свій пароль у відкритому вигляді, не лишати його на робочому столі;

пароль не повинен використовуватися в будь-яких інших облікових записах (*для доступу до соціальних мереж, банківських систем, приватної електронної пошти тощо*).

* 1. У випадку підозри щодо компрометації паролю невідкладно звернутися до штатного спеціаліста інформаційних технологій та кіберзахисту для зміни паролю.

Компрометація пароля – викрадення облікових даних користувача (*логіна та пароля доступу*). До ознак компроментації можуть бути віднесені: підозрілі дії в персональних поштових скриньках, зокрема, такі:

відсутність або видалення повідомлень електронної пошти;

отримання іншими користувачами від скомпроментованого облікового запису електронних листів та відсутність таких листів у каталозі «Надіслані» відправника;

наявність налаштувань поштової скриньки, які не здійснювалися користувачем або адміністратором;

каталоги «Надіслані» або «Кошик» містять повідомлення невідомого походження;

невідомо ким внесені зміни до профілю користувача (*номер телефону, посада, прізвище та ін.*).

* 1. Не повідомляти пароль доступу до поштової скриньки третім особам.

1. Правила безпечного входу до персональної електронної скриньки.

Не рекомендується:

здійснювати вхід з персонального комп’ютера, на якому не встановлено та не запущено антивірусне програмне забезпечення;

здійснювати вхід з незнайомих чи незахищених пристроїв (*існує ймовірність, що після завершення роботи не буде здійснено вихід із свого облікового запису або пристрій запам’ятає вказаний при вході логін та пароль. Крім того, існує ймовірність ураження такого пристрою шкідливим програмним забезпеченням, що може здійснювати збір та передачу відомостей щодо паролів та логінів зацікавленим особам*);

використовувати для входу точки публічного доступу до мережі Інтернет.

1. При прийманні електронного повідомлення забороняється:

відкривати повідомлення або вкладення, що містяться у них, якщо авторство цих повідомлень або їх тема викликають сумнів;

здійснювати перехід за посиланнями, що містяться у повідомленнях від незнайомих відправників або виконувати вказівки (пропозиції, рекомендації) в таких повідомленнях;

відкривати підозрілі файли, що отримані від невідомих відправників, а саме архіви (*найчастіше* ZIP *або* RAR), виконувані файли (*файли з такими розширеннями як* «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm». «.scr» *тощо*), що містяться як вкладення у цих повідомленнях.

Про сумнівність прийнятих електронних повідомлень можуть свідчити наступні ознаки:

**Підозрілий домен** – електронне повідомлення може містити офіційні логотипи або інші ознаки авторитетної організації, але реальна адреса відправника викликає сумнів, наприклад, не відповідає зазначеному у листі логотипу чи назві організації або має незначні зміни (*наприклад, одна літера чи один знак*) справжніх адрес реальних відправників.

**Загальні або неофіційні привітання** у листах без персоналізації (*наприклад, «Шановний клієнт»*) та формальностей, має викликати підозри.

**Некоректна граматика** – орфографічні та друкарські помилки, а також незвичайні (*нетипова побудова*) фрази часто можуть означати небезпеку. Відсутність помилок не є доказом легітимності повідомлення.

**Терміновість** – фішингові повідомлення часто намагаються викликати відчуття терміновості дій, залишаючи отримувачам менше часу на роздуми.

**Нетипова (дивна) тематика** поштового повідомлення теж повинна викликати підозру та привід для уважного аналізу отриманого повідомлення.

**Пропозиція, від якої важко відмовитися** – якщо лист занадто хороший, щоб бути правдою, він, напевно, є фішинговим.

Про виявлення таких та інших підозрілих випадків невідкладно повідомити штатних спеціалістів інформаційних технологій та кіберзахисту.

1. Користувачі відомчої електронної пошти не мають права:

використовувати відомчу електронну пошту для цілей, не пов’язаних зі службовою діяльністю (*приватне листування, створення акаунтів у соцмережах та ін.*);

передавати електронні повідомлення, що містять:

а) інформацію з обмеженим доступом, персональні дані громадян у відкритому вигляді (*за відсутності згоди останніх*), матеріали, використання яких порушує права інтелектуальної власності;

б) недостовірну інформацію, а також інформацію, яка ображає честь і гідність інших осіб, ганьбить ділову репутацію, пропагує ненависть та/або дискримінацію людей за расовими, етнічними, статевими, релігійними, соціальними ознаками та закликає до протиправних дій;

в)  матеріали, що містять шкідливий код; файли, програми, призначені для порушення, знищення або обмеження функціональності будь-якого комп’ютерного або телекомунікаційного обладнання; програми для здійснення несанкціонованого доступу;

г) матеріали, виготовлення, зберігання та розповсюдження яких заборонено чинним законодавством України.

5. Під час створення електронного повідомлення, що надсилається засобами відомчої електронної пошти, необхідно:

вказати тему електронного повідомлення, що відповідає його змісту;

у разі додавання до електронного повідомлення вкладених файлів, зазначити про це в тексті електронного повідомлення;

в кінці електронного повідомлення зазначити прізвище та ім’я, назву установи, структурний підрозділ, номери телефонів (службового, за необхідності – мобільного).

1. Не допускається надання звичайним користувачам прав адміністратора системи.
2. У разі виявлення повідомлень з підозрілим вмістом, працівникам Головного управління Держгеокадастру у Рівненській області невідкладно повідомляти підрозділ відповідальний за захист інформації Головного управління Держгеокадастру у Рівненській області.

Начальник відділу інформаційних

технологій та захисту інформації Віктор СВІНЦІЦЬКИЙ