

ЗАТВЕРДЖЕНО
рішенням Національної комісії зі
стандартів державної мови
від «13» вересня 2022 року № 281

Порядок
використання комп'ютерної техніки та програмного забезпечення в
Національній комісії зі стандартів державної мови

1. Загальні положення

1.1. Порядок використання комп'ютерної техніки та програмного забезпечення (далі – Порядок) в Національній комісії зі стандартів державної мови (далі – Комісія) розроблений з урахуванням стандартів ISO 27001/27002, Розпорядження Кабінету Міністрів України від 15.05.2002 N 247-р, Постанови Кабінету Міністрів України від 10.09.2003 N 1433 та визначає правила роботи з комп'ютерною технікою та застосування програмного забезпечення, що перебувають на балансі Комісії, а також встановлює загальні засади, принципи, правила доступу та зобов'язання щодо інформаційної безпеки під час роботи з персональними комп'ютерами, підключеними до локальної обчислювальної мережі, та інформаційними ресурсами корпоративної мережі, технічні аспекти забезпечення конфіденційності даних в корпоративній мережі, порядок надання та погодження дозволу на доступ до корпоративної мережі та інформаційних ресурсів корпоративної мережі, відповідальних осіб за надання та погодження такого доступу, а також відповідальність за порушення вимог цього Порядку.

1.2. Метою цього Порядку є організація надійного функціонування інформаційно-телекомунікаційної системи Комісії та її інформаційних ресурсів, що в свою чергу забезпечить своєчасне та ефективне виконання завдань Комісії відповідно до законодавства.

1.3. Дія Порядку поширюється на організацію в Комісії роботи із комп'ютерною технікою, надання доступу до інформаційно- телекомунікаційної системи Комісії та мережі Інтернет, придбання та використання комп'ютерної техніки та програмного забезпечення.

1.4. Вимоги Порядку є обов'язковими для виконання всіма державними службовцями Комісії, а також фізичними особами та представниками підприємств, установ та організацій у випадку, якщо їм надані права доступу до приміщень Комісії та роботи в корпоративній мережі Комісії.

1.5. Будь-які відхилення від вимог цього Порядку, які зумовлені службовою необхідністю, повинні погоджуватися із Сектором інформаційних технологій та цифрової трансформації (далі – Сектор) та/або Головою Комісії та/або Керівником апарату Комісії.



ДОКУМЕНТ СЕД АСКОД

Сертифікат [58E2D9E7F900307B04000000CC5F3400AEC0A000](#)
Підписант [Мозгунов Володимир Володимирович](#)
Дійсний з [15.02.2022 0:00:00](#) по [14.02.2024 23:59:59](#)

НКСДМ



281 від 13.09.2022

2. Терміни та визначення.

2.1. **Корпоративна мережа Комісії** – це складна інфраструктура, призначена для передачі великого обсягу різномірних інформаційних потоків у межах Комісії, сукупність комп'ютерів, кабельної системи, мережевих адаптерів, активного мережевого устаткування, які працюють під управлінням мережевих операційних систем та прикладного програмного забезпечення.

2.2. **Зовнішній носій інформації** – засіб, що створений для зберігання та перенесення інформації. До зовнішніх носіїв інформації належать оптичні та магнітні накопичувані інформації (CD-диски, DVD-диски, касети, стрічки тощо), переносні жорсткі диски, картки пам'яті (memory cards), флеш-пам'ять та інші носії інформації, на які можливо копіювати (переносити) дані з комп'ютерного обладнання або таких самих цифрових рухомих носіїв інформації через різні апаратні інтерфейси в цифровому вигляді.

2.3. **Інформаційна безпека** – сукупність процесів та заходів, які мають на меті забезпечення цілісності, конфіденційності та доступності інформації.

2.4. **Компрометація паролю** – будь-які дії та/або події, що могли призвести або призвели до того, що особистий пароль став відомим третім особам.

2.5. **Користувач інформаційно-телекомунікаційної системи** – державний службовець Комісії, фізична особа або представник сторонніх підприємств, установ або організацій, який має погоджений дозвіл на доступ до корпоративної мережі та/або інформаційних ресурсів корпоративної мережі Комісії.

2.6. **Локальна обчислювальна мережа (ЛОМ)** – локальна обчислювальна мережа Комісії, що об'єднує в собі такі елементи ІТ-інфраструктури: робочі станції, сервери, мережеве та телекомунікаційне обладнання.

2.7. **Маршрутизатор** – спеціалізований мережевий пристрій, який має два або більше мережевих інтерфейси та пересилає пакети даних між різними сегментами мережі. Маршрутизатор може пов'язувати різномірні мережі різних архітектур. Для прийняття рішень про пересилання пакетів маршрутизатором використовується інформація про топологію мережі, а також певні правила, задані адміністратором мережі.

2.8. **Мобільні пристрої** – портативні персональні комп'ютери (laptop, notebook), кишенькові персональні комп'ютери (PDA), комунікатори (communicator, PDA phone), смартфони (smartphone), digital-media (фотоапарати, mp3-плеєри, мобільні телефони тощо) та інші пристрої, на які можна копіювати інформацію у цифровому вигляді, проте їх основна функція полягає не в зберіганні, а в обробленні інформації.

2.9. **Обліковий запис користувача (обліковий запис)** – це відомості, що використовуються для однозначної ідентифікації та автентифікації користувача в інформаційній системі. Кожен користувач отримує доступ до свого облікового запису за допомогою імені користувача та паролю (та/або іншого засобу

автентифікації). Обліковий запис містить додаткову інформацію (адреса електронної пошти, телефон тощо).

2.10. **Особистий ключ** – унікальна послідовність символів, що доступна тільки користувачеві та призначена для створення електронного цифрового підпису користувача в електронних документах.

2.11. **Пароль** – таємний набір символів (букв, цифр, спеціальних символів), призначений для підтвердження особи користувача та його прав використовувати відповідний обліковий запис для одержання доступу до корпоративної мережі та/або інформаційних ресурсів Комісії. Пароль є засобом для захисту інформації від несанкціонованого доступу та автентифікації користувача в інформаційних системах Комісії.

2.12. **Персональний комп'ютер (ПК)** – електронно-обчислювальна машина (стаціонарна або портативна), яка призначена, як правило, для індивідуального використання.

2.13. **Комп'ютерна техніка (КТ)** – пристрої та системи пристроїв, що є компонентами комп'ютера, а також самі комп'ютери та обладнання, яке працює спільно з комп'ютерами (периферійні пристрої) і забезпечує деяку додаткову функціональність (друк або сканування документів, доступ до мережі, захист від збоїв живлення тощо).

2.14. **Спам** – повідомлення електронної пошти, не пов'язані з виконанням службових обов'язків, що надходять без запиту користувача.

2.15. **Фішинг** – вид шахрайства, один із різновидів соціальної інженерії, що здійснюється за допомогою електронної пошти, спливні вікна на вебсайтах або фішингових сайтів (шахрайських вебсайтів). Інформація, що надається користувачу, є помилковою або замаскованою (наприклад, видаючи себе за системного адміністратора, легітимний вебсайт тощо) так, щоб переконати одержувача передати конфіденційну інформацію (наприклад, авторизаційні повноваження, конфіденційні коди тощо), яка потім може бути використана для незаконних дій.

2.16. **Шпигунське програмне забезпечення** – тип програмного забезпечення, що збирає інформацію про активність користувача без його згоди, передає ці дані через мережу Інтернет в організацію, яка використовує їх.

2.17. **Програмне забезпечення (ПЗ)** – сукупність комп'ютерних програм, що взаємодіють, та відповідної документації, яка дозволяє технічно реалізовувати процеси виконання функціональних завдань комплексних інформаційних рішень у цілому та інформаційно-аналітичних систем зокрема.

2.18. **Сектор інформаційних технологій та цифрової трансформації** – штатний підрозділ Комісії, до основних завдань якого належить впровадження заходів захисту інформації (кіберзахисту) в інформаційно-телекомунікаційній системі Комісії, організація функціонування комп'ютерної техніки та програмного забезпечення.

2.19. Інші терміни вживаються у значенні, відповідно до законодавства.

3. Забезпечення комп'ютерною технікою та її технічне обслуговування.

3.1. Сектор забезпечує встановлення та налаштування комп'ютерної техніки на робочих місцях працівників Комісії. Конфігурація комп'ютерної техніки визначається залежно від:

3.1.1 завдання за посадою;

3.1.2 програмного забезпечення, яке має використовуватися у процесі виконання службових обов'язків;

3.1.3 наявності відповідної комп'ютерної техніки.

3.2. Отримання комп'ютерної техніки підтверджує працівник власноручним підписом в інвентарній картці обліку об'єкта основних засобів (далі – Картка).

3.3. Напередодні звільнення працівник передає комп'ютерну техніку відповідальній особі до Сектору в комплектності, зазначеній у Картці.

3.4. Технічне обслуговування та ремонт комп'ютерної техніки організовують працівники Сектору (за можливості – самостійний ремонт або обслуговування, в іншому випадку – укладання Договору з підрядною організацією на здійснення цих послуг).

4. Облік програмного забезпечення та комп'ютерної техніки

4.1. Сектор фінансів, бухгалтерського обліку та звітності веде інвентарний облік комп'ютерної техніки (далі – КТ) та програмного забезпечення (далі – ПЗ).

4.2. Облік КТ та ПЗ здійснюється згідно з вимогами бухгалтерського обліку Комісії.

5. Встановлення програмного забезпечення

5.1. Вся КТ, що підключена до інформаційно-телекомунікаційної системи Комісії, є частиною цієї інформаційно-телекомунікаційної системи, відповідно її функціонування повинно відповідати вимогам політики безпеки інформації стосовно програмного забезпечення та вимогам розділу 3 цього Порядку.

5.2. Роботи зі встановлення, налаштування, видалення та оновлення програмного забезпечення користувачів мають право виконувати лише спеціалісти Сектору.

6. Тимчасове використання власної комп'ютерної техніки в Комісії.

6.1. Працівники Комісії мають право тимчасово використовувати власну комп'ютерну техніку (через службової необхідності) за наступних умов:

6.1.1 Керівник структурного підрозділу Комісії (в якому встановлюється власна комп'ютерна техніка) зобов'язаний написати службову записку на ім'я Голови Комісії про дозвіл на використання власної комп'ютерної техніки із зазначенням виробника та моделі комп'ютерної техніки, а також

структурного підрозділу та номеру кабінету.

6.1.2 У разі отримання дозволу на використання власної комп'ютерної техніки працівник Комісії (власник комп'ютерної техніки) має написати службову записку на ім'я головного бухгалтера Комісії для внесення зазначеної комп'ютерної техніки до позабалансового обліку. Подальше переміщення комп'ютерної техніки в межах або за межі Комісії заборонено.

6.1.3 У разі службової необхідності використання на робочому місці власного персонального комп'ютера, ноутбука або моноблока власник зазначеної комп'ютерної техніки передає її для налаштувань до Сектору. Під час налаштування видаляється все встановлене програмне забезпечення, окрім необхідного для виконання працівником Комісії своїх посадових обов'язків (за потреби встановлюється додаткове програмне забезпечення). Працівник Комісії отримує обліковий запис користувача операційної системи без адміністративних прав.

6.1.4 Після забезпечення комп'ютерною технікою, що знаходиться на балансі Комісії, працівник Комісії зобов'язаний власноруч написати службову записку в довільній формі на ім'я головного бухгалтера Комісії для зняття власної комп'ютерної техніки з позабалансового обліку із зазначенням виробника, моделі комп'ютерного обладнання та оціночної вартості, структурного підрозділу та номеру кабінету. Працівники Сектора знімають обмеження з облікового запису користувача та видаляються: обліковий запис локального адміністратора системи та програмне забезпечення Комісії.

7. Придбання програмного забезпечення (комп'ютерних програм) та комп'ютерної техніки.

7.1. Придбання ПЗ та КТ здійснюється з урахуванням потреби. При цьому Комісії здійснює придбання і використання виключно ліцензійного ПЗ, яке повинно мати відповідну ліцензію в паперовій та/або електронній формі та, у разі наявності, іншу документацію в паперовій та/або електронній формі, яку надає правовласник (за його наявності).

7.2. Потреба в ПЗ та КТ визначена з необхідністю забезпечення виконання наявних і нових завдань, покладених на підрозділи Комісії, створенням або модернізацією інформаційних чи телекомунікаційних систем, заміною старих версій ПЗ або компонентів КТ, а також виявленням додаткових вимог до ПЗ, що вже використовується.

7.3. Для оброблення, передавання, зберігання інформації з обмеженим доступом використовують комп'ютерні програми (їхнє оновлення), в яких немає недокументованих функцій, що підтверджено результатами державної експертизи у сфері захисту інформації, яка досліджує вихідні коди та відповідні виконувани модулі програм і компонентів, перевіряє достовірність і повноту (цілісність), ідентифікує джерело походження (авторство) з фіксуванням стану комп'ютерних програм чи їхніх оновлень на момент проведення перевірки.

7.4. Інсталяція (встановлення) ПЗ та його оновлення, про які йдеться у

пункті 3.1. цього Порядку, здійснюється після ідентифікації та автентифікації джерела отримання та встановлення відповідності зразкам, у яких відсутність недокументованих функцій підтверджено результатами державної експертизи у сфері захисту інформації.

7.5. Під час вибору комп'ютерних програм, які пройшли державну експертизу у сфері захисту інформації, перевага повинна надаватися (за інших однакових об'єктивних технічних та якісних характеристик) комп'ютерним програмам, у яких реалізовано вищий рівень гарантій коректності надання функціональних послуг безпеки.

8. Права та обов'язки користувача

8.1. Користувач КТ та ПЗ має право звертатися до працівників Сектору:

8.1.1 за консультаціями і поясненнями стосовно питань роботи та підтримки працездатності комп'ютерної техніки, програмного забезпечення, користування та налагодження роботи з інформаційно-телекомунікаційною системою Комісії;

8.1.2 стосовно захисту і захисних механізмів для забезпечення конфіденційності та цілісності інформації;

8.1.3 у разі виникнення ситуацій, які не передбачені цим Порядком.

8.2. КТ та ПЗ надані державним службовцям Комісії виключно для виконання службових і посадових обов'язків.

8.3. Користувач КТ та ПЗ зобов'язаний:

8.3.1 чітко дотримуватись вимог чинного законодавства, цього Порядку та інших нормативних документів Комісії під час роботи з КТ та з інформаційно-телекомунікаційною системою Комісії, правил охорони праці під час роботи з КТ;

8.3.2 дбайливо ставитись до КТ, вживати всіх заходів для запобігання її пошкодженню;

8.3.3 перед початком роботи провести візуальний огляд КТ та елементів електроживлення;

8.3.4 у разі виявлення порушень у цілісності елементів електроживлення повідомити про це відповідальну особу;

8.3.5 використовувати для роботи з КТ та інформаційно-телекомунікаційною системою Комісії лише своє унікальне ім'я (логін) та пароль, зареєстрований у системі єдиного входу (за наявності такої системи) апарату Комісії та виданий працівником Сектору виключно для виконання покладених на нього функціональних обов'язків. Правила вибору паролів визначені у Додатку 1 до цієї Інструкції. Зміну паролю облікового запису необхідно проводити кожні 42 (сорок два) дні, якщо така зміна не була автоматично ініційована корпоративною мережею та/або інформаційними системами Комісії. Якщо користувач забув свій пароль, він повинен звернутися до спеціалістів Сектору і попросити змінити пароль;

8.3.6 використовувати службову поштову скриньку (e-mail –

електронна пошта, що належить Комісії та має домен tova.gov.ua) та ресурси мережі Інтернет виключно в службових цілях;

8.3.7 уважно стежити за електронною кореспонденцією: з метою захисту інформації від пошкодження користувач повинен знищувати файли з кодами програм (*.BAT, *.COM, *.EXE, *.X)IX та інші), які надійшли електронною поштою, якщо їх надходження не було чітко погоджено з адресантом. У разі виникнення сумнівів щодо повідомлення, яке надійшло електронною поштою, чи підозри на вірус, користувач повинен звернутись до Сектору;

8.3.8 після закінчення роботи з КТ виконати процедуру завершення сеансу роботи з операційною системою та відключити комп'ютерну техніку від мережі електроживлення (якщо інше не обумовлене технологічними вимогами). У разі оновлення операційної системи – не вимикати комп'ютер із мережі електроживлення та дочекатися закінчення процедури її оновлення;

8.3.9 здійснювати своєчасне резервне копіювання найважливішої інформації. Якщо є підозри, що будь-які документи знищені або пошкоджені, необхідно припинити роботу та негайно звернутись до співробітників Сектору;

8.3.10 у разі незвичайної, нестандартної поведінки КТ або неочікуваних дій ПЗ (явищ, повідомлень, перевірок), апаратного збою (підвищений шум у роботі обладнання та устаткування, запах гару та інше) вимкнути комп'ютерну техніку та повідомити співробітників Сектору та/або керівника підрозділу для визначення подальших дій;

8.3.11 повідомляти працівників Сектору про всі факти несанкціонованого доступу, зміни і знищення інформації, випадкового (ненавмисного) одержання інформації, не передбаченої правами доступу, несанкціонованої зміни програмної конфігурації, характеристик функціонування, появи програмного вірусного ураження;

8.3.12 надавати безперешкодний доступ до комп'ютерної техніки працівникам Сектору для встановлення/видалення (налаштування), перевірки стану програмного забезпечення, проведення профілактичних робіт, інвентаризації (планової щорічної або позапланової) КТ та ПЗ;

8.3.13 Негайно повідомити сектор у випадку компрометації паролю;

8.3.14. здійснювати регулярний антивірусний контроль за допомогою ліцензійних антивірусних програм, які встановлені на комп'ютерну техніку та супроводжуються працівниками Сектору.

8.4. Користувачу КТ та ПЗ заборонено:

8.5.1 використовувати ПЗ, яке не призначене для використання в Комісії та/або не має відповідної ліцензії, не спрямоване на виконання прямих посадових обов'язків користувача та не зазначене в картці обліку комп'ютерної техніки;

8.5.2 призупиняти роботу апаратно-програмних засобів захисту інформації (у т.ч. антивірусного програмного забезпечення). Змінювати налаштування антивірусного та додаткового захисного програмного

забезпечення, яке функціонує на КТ;

8.5.3 змінювати специфікацію, підключення, розташування КТ, конфігурацію встановленого ПЗ без узгодження із Сектором, відкривати електронну кореспонденцію та запускати прикладні програми, отримані засобами електронної пошти з невідомих адрес та/або з підозрілою назвою;

8.5.4 здійснювати доступ до інформаційних ресурсів та КТ з правами іншого користувача (логін, пароль);

8.5.5 передавати свої права користувача (логін, пароль) іншій особі; самостійно створювати на робочому місці інформаційні ресурси (точки доступу WI-FI, Bluetooth);

8.5.6 відключати і роз'єднувати лінії комунікаційних мереж; використовувати КТ, закріплену за іншими працівниками та/або допускати безконтрольну роботу інших працівників на своєму робочому місці;

8.5.7 Самостійно змінювати конфігурацію мережевого оточення (у тому числі змінювати IP та MAC адреси);

8.5.8 Передавати та розголошувати будь-яким іншим особам власні імена облікового запису, пароль або носії ключової інформації, а також передавати на час тимчасової відсутності (відрадження, хвороби тощо);

8.5.9 Використовувати, зберігати на комп'ютерах та розповсюджувати у корпоративній мережі Комісії програми та файли неслужбового характеру (ігри, зображення, музичні файли, інсталяційні файли, файли розважального характеру та інші програми, які не стосуються виконання службових обов'язків);

8.5.10 підключати до КТ:

8.5.10.1 технічні засоби з модулями передачі даних (Bluetooth, GSM, мобільних телефонів тощо), призначених для створення каналів зв'язку з мережами загального користування та іншими електронними пристроями;

8.5.10.2 зовнішні носії інформації, які не були перевірені антивірусним ПЗ;

8.5.11 використовувати та передавати іншим особам документи та носії, на яких знаходиться конфіденційна інформація, без відповідного запису в журналах обліку та/або дозволу відповідних посадових осіб;

8.5.12 використовувати неякісний папір для друку на принтерах та копіювальних апаратах;

8.5.13 самостійно виконувати будь-які ремонтні, профілактичні роботи КТ;

8.5.14 підключати потужні електроприлади (електрочайники, нагрівачі, електроінструмент, освітлювальні прилади, холодильники та іншу побутову техніку) в один мережевий фільтр із комп'ютерною технікою;

8.5.15 піддавати КТ фізичним, термічним і хімічним впливам, наприклад, не можна загороджувати вентиляційні отвори, проливати рідину, протирати монітори засобами, не призначеними для цього, ставити біля батареї або інших нагрівальних приладів.

9. Правила роботи з портативними комп'ютерами

9.1. На використання портативних комп'ютерів поширені правила та вимоги щодо використання стаціонарних персональних комп'ютерів.

9.2. Під час користування службовим портативним комп'ютером, що знаходиться на балансі Комісії, державний службовець Комісії має дотримуватися таких вимог:

9.2.1. Використовувати портативний комп'ютер лише в робочих цілях.

9.2.2. У випадку втрати портативного комп'ютера негайно повідомити свого безпосереднього керівника та Сектор із зазначенням обставин.

9.2.3. Не передавати та не надавати доступ до портативного комп'ютера стороннім особам.

9.2.4. Дотримуватися внутрішніх нормативних документів Комісії під час роботи з портативним комп'ютером як на території Комісії, так і поза її межами.

9.2.5. У випадку, якщо портативний комп'ютер не використовується, він має зберігатися на робочому місці користувача.

9.3. Винесення та внесення портативного комп'ютера здійснюється відповідно до вимог пропускового режиму Комісії (за наявності такого режиму).

10. Відповідальність

10.1. Кожен державний службовець Комісії, який використовує КТ, зобов'язаний особисто ознайомитися з цим Порядком (під підпис).

10.2. Контроль і перевірка стану виконання вимог цього Порядку здійснюють працівники Сектору.

10.3. Якщо користувач порушує вимоги цього Порядку, працівники Сектору мають право від'єднати його КТ від інформаційно-телекомунікаційної системи Комісії або від інформаційних ресурсів до з'ясування причин порушення.

10.4. Питання, які не врегульовані цим Порядком, вирішуються відповідно до нормативно-розпорядчих документів Голови Комісії за участю спеціалістів Сектору із залученням зацікавленого державного службовця Комісії.

11. Доступ до інформації користувачів.

11.1. Спеціалісти Сектору, що відповідають за технічне управління інформаційними системами та безпеку інформаційних технологій, мають право:

11.1.1. Здійснювати доступ до даних користувача, електронної пошти або мережевої навігації, керуючись виключно міркуваннями безпеки чи захисту інформаційних систем (наприклад, для виявлення вірусів, шкідливого коду, хакерських вторгнень, таких явищ, як спам, фішинг, шпигунське програмне забезпечення тощо), технічними причинами та/або підтримкою та/або

проведенням подібних регулярних робіт (наприклад, оновлення/заміна/впровадження програм, підтримка функціонування обладнання тощо).

11.1.2. Здійснювати моніторинг сайтів, що відвідують користувачі, з метою забезпечення належного рівня інформаційної безпеки.

11.1.3. У встановленому законодавством порядку переглядати електронну переписку (e-mail) з метою забезпечення належного рівня інформаційної безпеки. Всі електронні листи, що створені і зберігаються на комп'ютерах і поштових серверах Комісії, є власністю Комісії і не вважаються персональними.

11.2. За погодженням із керівником структурного підрозділу користувача здійснювати доступ до даних користувача, що містяться в інформаційних системах Комісії, які він використовує, у зв'язку з припиненням трудових відносин, заміною обладнання тощо. Відповідальність за передчасне видалення всіх персональних даних несе користувач (в разі виникнення такої ситуації).

12. Заключні положення

12.1. Якщо у кімнаті працює більше ніж один працівник, в приміщенні встановлюється мережевий принтер загального користування, який закріплюється за працівником, визначеним у заявці на отримання КТ.

12.2. У разі виникнення ситуацій, не передбачених цим Порядком, їх розглядають у робочому порядку спільно із Сектором.

12.3. Внесення змін до розділів Порядку дозволено у випадку необхідності надання нових прав та обов'язків, а також у разі вилучення чинних прав та обов'язків і потребує затвердження нової версії Порядку.

**Голова Національної комісії
зі стандартів державної мови**

Володимир МОЗГУНОВ