Затверджено розпорядженням
Президії НАН України
від 19.05.2025 № 257

Парольна політика
Національної академії наук України

І. Загальні положення

1.1. Парольна політика Національної академії наук України (далі – Політика) визначає порядок організаційно-технічних заходів із захисту інформації й усунення можливих каналів витоку інформації, що є власністю держави та циркулює в Національній академії наук України (далі - НАН України).

1.2. Терміни та їх визначення, що вживаються в цій Політиці:

автентифікація – перевірка приналежності суб'єктові доступу пред'явленого їм ідентифікатора; підтвердження справжності. Найчастіше автентифікація виконується шляхом набору користувачем свого пароля на клавіатурі комп'ютера;

ідентифікація – присвоєння суб'єктам доступу (користувачам, процесам) і об'єктам доступу (інформаційним ресурсам, обладнанням) ідентифікатора та (або) порівняння пропонованого ідентифікатора з переліком привласнених ідентифікаторів;

інформаційна система – сукупність програмного забезпечення і технічних засобів, які використовуються для зберігання, обробки й передачі інформації, з метою виконання завдань структурних підрозділів апарату Президії НАН України, наукових установ, організацій та підприємств НАН України. В НАН України використовуються різні типи інформаційних систем для виконання виробничих, управлінських, облікових та інших завдань;

користувач інформаційної системи – працівник НАН України, а також інша особа (підрядник, аудитор тощо), зареєстрований в корпоративній мережі у встановленому порядку;

корпоративна мережа – об'єднання інформаційних систем, комп'ютерного, телекомунікаційного і офісного устаткування всіх підрозділів апарату Президії НАН України, наукових установ, організацій та підприємств НАН України за допомогою їх підключення до єдиної комп'ютерної мережі передачі даних з використанням різних фізичних і логічних каналів зв'язку;

несанкціонований доступ – доступ до інформації, що порушує встановлені правила розмежування доступу;

пароль користувача – відома тільки конкретному користувачеві послідовність символів, використовувана користувачем для підтвердження своєї дійсності (автентифікації) при вході в систему (мережу), а також (у деяких випадках) для одержання доступу до інформаційних ресурсів;

реєстраційний (обліковий) запис користувача - сукупність відомостей про користувача, яка містить ім'я користувача і його унікальний цифровий ідентифікатор, що однозначно ідентифікує цього користувача в операційній системі (мережі, базі даних, додатку тощо). Реєстраційний запис створюється адміністратором під час реєстрації користувача в операційній системі комп'ютера, у системі керування базами даних, у мережних доменах, додатках тощо. Також запис може містити такі відомості про користувача, як П.І.Б., назва структурного підрозділу, телефони, e-mail тощо.

1.3. Вимоги цієї Політики поширюються на всіх користувачів інформаційних систем. Всі користувачі інформаційних систем, яким надаються паролі для доступу до них, зобов'язані виконувати вимоги цієї Політики.

1.4. Чинна Політика встановлює вимоги до порядку вибору, зберігання, використання, періодичності зміни паролів та інші питання, пов'язані із застосуванням механізмів парольної автентифікації в інформаційних системах.

1.5. Для окремих категорій користувачів інформаційних систем можуть існувати особливі вимоги щодо вибору, зберігання й використання паролів, що оформлюються у вигляді змін або доповнень до чинної Політики.

1.6. Паролі для доступу до корпоративної мережі надаються співробітникам адміністратором під час реєстрації цих співробітників як користувачів інформаційних систем. Під час одержання пароля від адміністратора користувач зобов'язаний змінити наданий пароль. Надалі користувач повинен здійснювати зміну своїх паролів самостійно відповідно до вимог цієї Політики.

1.7. Користувачі інформаційних систем зобов’язані змінювати паролі у разі компрометації облікового запису, але не рідше одного разу на рік.

1.8. Користувачам інформаційних систем забороняється вчиняти дії, спрямовані на одержання (розкриття) паролів інших користувачів.

1.9. З метою запобігання несанкціонованого доступу до робочих місць користувачів, а також до ресурсів корпоративної мережі з використанням чужих облікових записів (імен користувачів інформаційних систем), користувачі зобов'язані блокувати екрани своїх комп'ютерів у випадку залишення ними свого робочого місця натисканням на комп'ютерній клавіатурі набору клавіш win+L.

1.10. Усі обрані користувачами інформаційних систем паролі повинні відповідати наведеним нижче вимогам:

1) містити не менш 8 символів;

2) містити символи, набрані в різних регістрах (a-z, A-Z), а також цифри, розділові знаки й/або спеціальні символи (0-9,!@#$%&*()_+I~-=\'{}[]:";'<>?,./);

3) не бути словом зі словника, сленгу, діалекту, жаргону й т.п.

4) не бути персональною інформацією (імена членів родини, адреси, телефони, дати народження й т.п.).

1.11. Користувачі інформаційних систем можуть обирати паролі, що легко запам'ятовуються, однак в той же час важко вгадуються для інших осіб, якщо буде виконано хоча б одна з наступних умов:

1) кілька слів написані разом (такі паролі відомі за назвою "passphrases");

2) слово набране зі зсувом на певну кількість букв нагору або вниз за алфавітом;

3) комбінація цифр і звичайного слова;

4) навмисно неправильне написання слова (незвичайна в даному слові орфографічна помилка).

II. Забезпечення конфіденційності паролів

2.1. Користувачі інформаційних систем зобов'язані дотримуватися необхідних запобіжних заходів для забезпечення конфіденційності своїх паролів.

2.2. Забороняється:

1) повідомляти свій пароль іншим особам, включаючи колег, керівників і фахівців служби технічної підтримки, телефоном, електронною поштою або будь-якими іншими засобами;

2) зберігати паролі в доступній для читання формі в командних файлах, сценаріях автоматичної реєстрації, програмних макросах, функціональних клавішах термінала, на комп'ютерах з неконтрольованим доступом, а також в інших місцях, де неуповноважені особи можуть одержати до них доступ (наприклад, у жодних додатках користувачі не повинні вибирати таку опцію конфігурації, як автоматичне збереження пароля);

3) записувати паролі й залишати ці записи в місцях, де до них можуть одержати доступ сторонні особи;

4) вимовляти свій пароль вголос;

5) використовувати загальні паролі разом з іншими співробітниками.

2.3. Користувач інформаційних систем, у якого вимагають розкриття паролю, зобов'язаний відмовити у розкритті паролю з посиланням на цю Політику та запропонувати звернутися за роз'ясненнями до структурного підрозділу, відповідального за захист інформації.

2.4. Пароль повинен бути негайно змінений, якщо є достатні підстави вважати, що цей пароль став відомий кому-небудь ще, крім самого користувача інформаційних систем.

III. Контроль за виконанням вимог Парольної політики

3.1. Загальний контроль за виконанням вимог Парольної політики здійснюється працівниками Відділу проблем практичної інформатики Інституту програмних систем НАН України.

3.2. З метою перевірки надійності використовуваних паролів за узгодженням із системними адміністраторами періодично можуть здійснюватися тестові "зломи" паролів користувачів. Системні адміністратори мають право брати участь у проведенні подібних перевірок.

3.3. За вказівкою співробітників Відділу проблем практичної інформатики Інституту програмних систем НАН України користувачі інформаційних систем повинні змінити паролі, що не відповідають критеріям надійності, установленим цією Політикою.

3.4. Системні адміністратори там, де це можливо, повинні створювати в операційних системах і додатках такі параметри:

1) мінімальна довжина пароля - 8 символів;

2) пароль повинен відповідати вимогам складності, установленим цією Політикою;

3) максимальний термін дії пароля - 180 днів;

4) не повторюваність паролів (зберігати 10 попередніх);

5) використання шифрування при зберіганні паролів;

6) автоматичне блокування облікових записів користувачів інформаційних систем після 5 невдалих спроб уведення пароля (наступне розблокування пароля користувача може проводитися тільки системним адміністратором).

3.5. Системні адміністратори здійснюють налаштування на робочих місцях користувачів інформаційних систем для блокування комп’ютера через 5 хвилин неактивності.

IV. Відповідальність

4.1. Відповідальність за здійснення загального контролю за виконанням правил цієї Політики, за реалізацію системними адміністраторами вимог цієї Політики, а також за підтримку цього документа в актуальному стані несе керівник Відділу проблем практичної інформатики Інституту програмних систем НАН України.

4.2. Відповідальність за дотримання правил Політики працівниками НАН України покладається на керівників відповідних підрозділів.