

Список використаних джерел

1. Про електронну комерцію : Закон України від 03.09.2015 № 675-VIII. URL: <https://zakon.rada.gov.ua/laws/show/675-19> (дата звернення: 05.05.2026).
2. Про захист прав споживачів : Закон України від 10.06.2023 № 3153-IX. URL: <https://zakon.rada.gov.ua/laws/show/3153-20> (дата звернення: 05.05.2026).
3. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. *Official Journal of the European Union*. 2019. L 136. P. 1–44.
4. Про цифровий контент та цифрові послуги : Закон України від 10.08.2023 № 3321-IX. URL: <https://zakon.rada.gov.ua/laws/show/3321-20> (дата звернення: 05.05.2026).
5. New Consumer Agenda: Strengthening consumer resilience for sustainable recovery. Communication from the Commission to the European Parliament and the Council. COM/2020/696 final. Brussels, 13.11.2020. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0696> (дата звернення: 05.05.2026).
6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. L 2024/1689.
7. Великанова М. М., Атаманчук Н. І., Томкіна О. О. Гармонізація законодавства України про захист прав споживачів з правом Європейського Союзу: аналіз законодавчих ініціатив. *Вісник Національної академії правових наук України*. 2023. Т. 30. №1. С. 190–212.
8. Кочина О.С., Тимченко З.М. Проблеми гармонізації українського законодавства у сфері захисту прав споживачів із законодавством ЄС. *Науковий вісник Ужгородського Національного Університету*, Серія ПРАВО. Вип. 92: Ч. 1, 2025. С. 413 – 418.
9. Starytska, O., & Tarasenko, O. (2025). State of research on the issues of state consumer policy in Ukraine. *Law Journal of the National Academy of Internal Affairs*, 15(4), 9-19. <https://doi.org/10.63341/naia-chasopis/4.2025.09>

Шуляк Богдан Андрійович,
студент I курсу бакалаврату, «Правоохоронна діяльність»
Національна академія внутрішніх справ

Науковий керівник:
Кудінов Вадим Анатолійович,
завідувач кафедри інформаційних технологій
навчально-наукового інституту права та психології
Національна академія внутрішніх справ
кандидат фізико-математичних наук, доцент

РЕАЛІЗАЦІЯ ПРАВА ЩОДО СТВОРЕННЯ ТА ВИКОРИСТАННЯ ПАРОЛЬНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНИХ СИСТЕМ В НАЦІОНАЛЬНІЙ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ

В Національній академії внутрішніх справ (далі – НАВС) протягом останнього часу вживаються заходи щодо створення нових та удосконалення

функціонування вже існуючих інформаційних систем. Одним з важливих напрямів забезпечення ефективного функціонування цих систем є побудова належної інформаційної безпеки їх баз даних, що передбачає створення та використання стійкого (надійного) парольного доступу до злomu [1, 2].

Як відомо, парольний доступ – це набір символів, який користувач повинен ввести через обладнання вводу інформації, перш ніж він почне обробку інформації в інформаційній системі. Парольний доступ призначений для підтвердження особистості або повноважень користувача і в інформаційних системах використовується для захисту інформації від несанкціонованого доступу. Створення стійкого парольного доступу забезпечує лише 50 % успіху в захисті інформації від несанкціонованого доступу, а на реальний рівень безпеки також суттєво впливає «політика використання», яка регламентує правильні дії посадових осіб у цифровому середовищі.

Актуальність розробки політики безпечного використання стійких паролів обумовлена вимогами Стратегії кібербезпеки України, затвердженої Указом Президента України [3], яка передбачає для забезпечення надійності та безпеки цифрових послуг створення необхідних передумов (нормативних, організаційних, технологічних) для автентифікації користувачів сервісів цифрових послуг.

Створення та використання стійкого парольного доступу користувачами інформаційних систем повинно відбуватись з дотриманням законів України «Про інформацію», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про державну таємницю», «Про доступ до публічної інформації», роз'яснень Державної служби спеціального зв'язку та захисту інформації України щодо вимог до захисту інформації в інформаційно-комунікаційних системах у воєнний час [4], нормативно-правових документів МВС, інших нормативно-правових актів у сфері захисту інформації та інформаційної безпеки. Держспецзв'язком [5] та Департаментом кіберполіції Національної поліції України [6] для користувачів інформаційних систем розроблені Правила створення та використання надійних паролів.

З урахуванням зазначених документів в Національній академії внутрішніх справ розроблені «Загальні правила інформаційної безпеки для користувачів НАВС» та «Положення про парольну політику та права доступу в НАВС», які затверджені наказом НАВС від 30.06.2025 № 914. Необхідно відмітити, що в Додатку до «Положення про парольну політику та права доступу в НАВС» наведена таблиця «Основні вимоги до парольної політики НАВС», в якій відображено опис відповідної вимоги та її стислий коментар/пояснення, що дозволяє користувачам правильно створювати та використовувати стійкий парольний доступ до інформаційних систем НАВС.

Таким чином, в роботі розглянута основна правова база щодо створення та використання парольного доступу до інформаційних систем в Національній академії внутрішніх справ.

Список використаних джерел

1. Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). *Сучасна спеціальна техніка*. 2023. № 3 (74). С. 42–49. [https://doi.org/10.36486/mst2411-3816.2023.3\(74\)](https://doi.org/10.36486/mst2411-3816.2023.3(74))
2. Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 2). *Сучасна спеціальна техніка*. 2023. № 4 (75). С. 40–50. [https://doi.org/10.36486/mst2411-3816.2023.4\(75\)](https://doi.org/10.36486/mst2411-3816.2023.4(75))
3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. Урядовий кур'єр від 28 серп. 2021 р. № 165. *Верховна Рада України* : [сайт]. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7> (дата звернення: 07.05.2026).
4. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку. *GOV.UA. Державні сайти України* : [сайт]. URL: <https://cip.gov.ua/ua/news/vimogi-do-zakhistu-informaciyi-v-informaciiikh-sistemakh-u-voyennii-chas-roz-yasnennya-derzhspeczv-yazku> (дата звернення: 07.05.2026).
5. Держспецзв'язку: основні правила використання та зміни паролів. *Урядовий портал* : [сайт]. URL: <https://www.kmu.gov.ua/news/derzhspeczvyazku-osnovni-pravila-vikoristannya-ta-zmini-paroliv> (дата звернення: 07.05.2026).
6. Правила створення та використання надійних паролів – рекомендації кіберполіції. *Кіберполіція України* : [сайт]. URL: <https://cyberpolice.gov.ua/article/pravyla-stvorenniya-ta-vykorystannya-nadijnyx-paroliv--rekomentacziyi-kiberpoli-cziyi-3711/> (дата звернення: 07.05.2026).