

РОЗДІЛ 8

МАТЕМАТИЧНЕ ОБҐРУНТУВАННЯ ВИМОГ ДО СКЛАДНОСТІ ПАРОЛІВ І ЧАСТОТИ ЇХ ЗМІНИ

Штонда Р.М., начальник науково-дослідного відділу, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ

Ляшенко Г.Т., старший науковий співробітник, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ

Самусь О.Ю., науковий співробітник, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ

У сучасних умовах цифровізації державного управління, розвитку мережових технологій та зростання інтенсивності кіберзагроз проблема забезпечення надійної автентифікації користувачів набуває особливої актуальності. Парольна автентифікація залишається одним із найпоширеніших механізмів контролю доступу до інформаційних систем, попри активне впровадження багатофакторних та безпарольних рішень. Водночас статистика інцидентів свідчить, що компрометація облікових даних (через фішинг, витоки баз даних, перебір паролів, credential stuffing тощо) є однією з основних причин несанкціонованого доступу до інформаційних ресурсів.

Нормативні документи та галузеві стандарти, зокрема рекомендації National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) та European Union Agency for Cybersecurity (ENISA), пропонують сучасні підходи до формування парольної політики, які базуються не лише на формальних вимогах до складності, але й на оцінці ризиків, поведінкових факторах користувачів та економічній доцільності заходів захисту [1]. Водночас у практиці державних установ часто застосовуються шаблонні підходи (фіксована мінімальна довжина,

обов'язкова наявність спеціальних символів, жорстка періодичність зміни), які не завжди мають достатнє математичне обґрунтування.

У поданому розділі здійснюється формалізований аналіз вимог до складності паролів та періодичності їх зміни на основі теорії інформації, ймовірнісних моделей та підходів до мінімізації очікуваних витрат і обмеження ризику. Запропоновані моделі дозволяють перейти від інтуїтивних або традиційних рішень до кількісно обґрунтованої політики управління паролями, що особливо важливо для державних установ, де наслідки компрометації можуть мати критичний характер.

1 Математичне обґрунтування вимог до складності паролів.

Складність пароля визначається його стійкістю до атак, таких як brute-force (перебір усіх можливих комбінацій) або dictionary attacks (перебір словникових слів). Ключовим показником є ентропія пароля, яка вимірює кількість інформації в бітах і вказує на “невизначеність” пароля для атакуючого [2].

Ентропія H для пароля довжиною L з кількістю можливих символів із алфавіту розміром S обчислюється за формулою (8.1),

$$H = L \times \log_2 S, \quad (8.1)$$

Це впливає з того, що загальна кількість можливих паролів дорівнює S^L , а ентропія – це \log_2 від цієї кількості, оскільки кожен біт подвоює кількість варіантів.

Давайте розглянемо детальніше розрахунок формули обчислення ентропії паролів (1):

– визначити складові для стандартного пароля – цифри (кількість 10), малі літери латинського алфавіту (кількість 26), прописні літери латинського алфавіту (кількість 26) та неалфавітні символи (до 33 символів, залежно від

реалізації системи), загалом $S = 94$ для повного набору (цифри, малі літери алфавіту, прописні літери алфавіту та неалфавітні символи);

– наступним кроком є обчислення кількості комбінацій, що вираховується за формулою (8.2):

$$N = S^L, \quad (8.2)$$

де N – загальна кількість можливих комбінацій;

S – кількість можливих символів;

L – довжина пароля;

– наступним кроком є визначення ентропії, що вираховується за формулою (8.3):

$$H = \log_2 N = L \times \log_2 S, \quad (8.3)$$

де H – ентропія пароля (вимірюється у бітах);

N – загальна кількість можливих комбінацій;

L – довжина пароля;

$\log_2 S$ – ентропія на кількість можливих символів.

Примітка. Для пароля довжиною у 8 символів з $S = 94$ буде наступне: $\log_2 94 \approx 6.55$, тоді $H \approx 8 \times 6.55 = 52.4$ біт. Це означає, що противник або зловмисник повинен перевірити в середньому $2^{52.4}/2 \approx 2^{51.4}$ комбінацій для 50 % ймовірного успіху (за моделлю рівномірного розподілу).

Час до злому пароля залежить від швидкості перевірки (комбінацій на секунду), що вираховується за формулою (8.4) для 50 % ймовірності:

$$T = \frac{2^H}{2R}, \quad (8.4)$$

де T – час підбору паролю із 50 % ймовірністю;

R – швидкість перевірки (вимірюється в комбінаціях на секунду);

H – ентропія пароля (вимірюється у бітах).

Примітка. Якщо $R = 10^{12}$ (сучасні GPU-кластери), для $H = 52.4 \div T \approx 2^{52.4} \div (2 \times 10^{12}) \approx 10^3$ секунд (близько 17 хвилин). Це демонструє, чому паролі з низькою ентропією (наприклад, лише цифри $S = 10$, $H \approx 26.6$) є вразливими. За цих умов час злому противником або зловмисником зменшується до секунд.

Вимоги до складності паролів накладаються із розрахунку, щоб час на підбір пароля (T) перевищував десятки років чи століття, враховуючи використання методів паралельних розрахунків при проведенні атак.

Для паролів, створених із застосуванням словникових послідовностей символів (слів), ентропія зменшується і розраховується за формулою (8.5):

$$\frac{D}{H} = \log_2 D, \quad (8.5)$$

де D – кількість унікальних слів у словнику;

H – ентропія пароля (вимірюється у бітах).

$\log_2 D$ – ентропія, яку додає кожне слово.

Чим більша кількість унікальних слів у словнику (D), тим більше ентропії додає кожне слово до парольної фрази, тому вимоги забороняють прості слова і рекомендуються складні парольні фрази (при їх застосуванні) [3].

У випадку парольної фрази, пароль складається з кількох слів, обраних із певного словника.

Примітка. Словник може містити 10000 поширених слів (як у англійській мові за стандартом Diceware або аналогічному україномовному словнику).

Таким чином, ентропія парольної фрази обчислюється за формулою (8.6):

$$H = \log_2(D^W), \quad (8.6)$$

де H – ентропія паролльної фрази;

D – кількість унікальних слів у словнику;

W – кількість слів у фразі.

Формулу (8.6) можливо перетворити у формулу (8.7):

$$H = W \times \log_2 D, \quad (8.7)$$

де H – ентропія паролльної фрази;

W – кількість слів у фразі.

$\log_2 D$ – ентропія, яку додає кожне слово.

Примітка. Якщо словник містить кількість унікальних слів $D = 10000$ слів, тоді $\log_2 10000 \approx 13.29$ біт. Для фрази, що буде складатись із кількості слів $W = 6$ слів, ентропія паролльної фрази буде розрахована так: $H = 6 \times \log_2 10000 \approx 6 \times 13.29 \approx 79.74$ біт. Для досягнення ентропії паролльної фрази $H \geq 80$ біт потрібно 7 символів: $H = 7 \times 13.29 \approx 93.03$ біт.

2 Математичне обґрунтування періодичності зміни пароля

Математичне обґрунтування періодичності зміни пароля (тобто як вибрати оптимальний інтервал t між змінами), розглянувши кілька простих моделей загрози і математично вивівши оптимум там, де це можливо. Пояснення – крок за кроком, з інтерпретацією результатів.

2.1 Модель А – атаки перебором/постійний ризик зламу.

Нехай пароль має “стійкість” (ентропію) H біт і противник (зловмисник) робить спроби зламу зі швидкістю, що дає ефективну інтенсивність успішних компрометацій β (тобто hazard rate) для пароля. Тоді ймовірність, що пароль буде зламаний протягом часу t , дорівнює:

$$P_{\text{comp}}(t) = 1 - e^{-\beta t}. \quad (8.8)$$

Припустимо, що в разі компрометації установа несе одноразовий збиток C . Вартість однієї зміни (операційні/адміністративні витрати) – K .

Зміну проводять кожні t одиниць часу. Тоді очікувані витрати за інтервал між змінами:

$$\text{Loss}_{\text{interval}} = C(1 - e^{-\beta t}) + K. \quad (8.9)$$

Середні витрати на одиницю часу:

$$f(t) = \frac{C(1 - e^{-\beta t}) + K}{t}. \quad (8.10)$$

Щоб знайти оптимальний t , мінімізуємо $f(t)$. Диференціювання дає (після перетворень) вираз:

$$C\beta t e^{-\beta t} = C(1 - e^{-\beta t}) + K. \quad (8.11)$$

Після спрощення отримаємо:

$$e^{-\beta t} (1 + \beta t) = 1 + \frac{K}{C}. \quad (8.12)$$

Однак ліва частина $e^{-\beta t}(1 + \beta t)$ при $t \geq 0$ набуває максимального значення 1 (при $t = 0$) і зменшується далі, отже права частина $1 + \frac{K}{C} > 1$. Тобто рівняння не має розв'язання при позитивних K, C . Інтерпретація: у цій простій моделі, де ризик компромісу зростає плавно з часом і збиток C – одноразовий, середні витрати $f(t)$ монотонно зменшуються при збільшенні t . Тобто математично модель пропонує не змінювати ($t \rightarrow \infty$), якщо є лише постійний ризик перебору, але існують витрати на зміну пароля. Це інтуїтивно важко сприймається, але має логічне пояснення: якщо

компрометація дає одноразовий збиток, який не росте з експозицією, то часті зміни лише додають K/t .

Висновок із моделі А: сама по собі боротьба з перебором не дає аргументу “чому зміни потрібні” – краще провадження в збільшення ентропії пароля/багатофакторну аутентифікацію/зниження β (частоти компрометації).

2.2 Модель В – витік (leak) як подія Poisson + експозиційне вікно до зміни.

Ця модель реалістичніша: компрометація пароля (через фішинг, брехню співробітника, витік бази паролів тощо) відбувається випадково з інтенсивністю μ (кількість витоків на одиницю часу). Коли відбувся витік, пароль стає скомпрометованим і нападник може його використати до наступної зміни. Якщо зміни відбуваються регулярно кожні t , то середній час, протягом якого скомпрометований пароль дає доступ, становить $t/2$ (середній залишок інтервалу до наступної зміни). При цьому вважаємо, що в разі витоку збиток накопичується пропорційно часу зламу, тобто існує щогодинний/щоденний збиток S (втрата в ресурсах або ризик) за одиницю часу, поки пароль скомпрометований.

Тоді:

- очікувана кількість витоків за одиницю часу: μ ;
- середній час доступу (експозиції) на один витік: $t/2$;
- очікувані витрати від витоків за одиницю часу: $\mu \times (t/2) \times S$;
- операційні витрати на зміну: K за кожну зміну, тобто K/t за одиницю часу.

Отже загальні середні витрати на одиницю часу [4]:

$$g(t) = \underbrace{\frac{\mu S}{2} t}_{\text{витік/експозиція}} + \underbrace{\frac{K}{t}}_{\text{витрати на ротацію}} \quad (8.13)$$

Це стандартна форма “лінійно-зростаюча + обернено-пропорційна” і має внутрішній мінімум. Знайдемо його.

Диференціюємо:

$$g'(t) = \frac{\mu S}{2} - \frac{K}{t^2}. \quad (8.14)$$

Розв’язання при $g'(t)=0$ дає:

$$\frac{\mu S}{2} = \frac{K}{t^2} \Rightarrow t^2 = \frac{2K}{\mu S}. \quad (8.15)$$

Отже, раціональним буде інтервал зміни пароля:

$$t^* = \sqrt{\frac{2K}{\mu S}}. \quad (8.16)$$

Це означає, що:

- якщо витоків багато (μ великий) або збиток від доступу великий (S великий) – t^* зменшується (потрібні частіші зміни);
- якщо зміна дорога (K велике) – t^* збільшується (зміни рідше).

Приклад розрахунку.

Припустимо:

- $K = 100$ UAH (вартість однієї зміни – робота адміністратора, розсилка повідомлень користувачам тощо);
- $\mu = 0.01$ компрометації/місяць (1 витік на 100 місяців в середньому);
- $S = 1000$ UAH/місяць (вартість того, що зловмисник робить за 1 місяць доступу).

Тоді:

$$t^* = \sqrt{\frac{2 \cdot 100}{0.01 \cdot 1000}} = \sqrt{\frac{200}{10}} = \sqrt{20} \approx 4.47 \text{ місяців.} \quad (8.17)$$

Отже, приблизно 4,5 місяці між змінами пароля (за цими умовами).

2.3 Фактори, які впливають на періодичність зміни пароля.

1. Вплив людського фактору. Часті примусові зміни стимулюють користувачів обирати слабші шаблони створення нових паролів (*password1* → *password2* → *password3* або внесення невеликих змін). Це знижує “ефективну ентропію” H_{eff} . Модель може включати негативний вплив $D(t)$ – приріст імовірності компрометації при зниженні t . Практичний висновок: надто часті зміни можуть знизити рівень безпеки.

2. Виявлення витоку. Якщо в установі реалізовано достатні механізми виявлення (інструменти моніторингу, SIEM тощо) і виявлення відбувається швидко після компрометації (час виявлення τ малий), ефект зміни пароля знижується – витік закінчиться виявленням, а не зміною.

3. Використання багатофакторності. Якщо багатофакторну автентифікацію увімкнено, вартість доступу S або ймовірність успішного використання витоку зменшується, отже t^* зростає – зміни паролів стають менш критичними.

4. Використання комбінованих моделей автентифікації. Можна об’єднати моделі А і В (і додати виявлення): загальні витрати міститимуть складову від безперервного *hazard* β (атак на підбір пароля) і складову від витоків μ , плюс збитки від отримання доступу зловмисниками (K/t). Рациональне значення можливо знаходити в числовому вираженні.

Практичні висновки оцінки факторів впливу:

– якщо головна загроза – витоки автентифікаційних даних (фішинг, компрометація бази), модель В показує, що є сенс у періодичній зміні пароля – і раціональний інтервал $t^* = \sqrt{2K/(\mu S)}$;

– якщо головна загроза – перебір паролів і використовуються паролі довгі/унікальні, часті зміни не додають користі; краще впроваджувати багатофакторну автентифікацію та підвищувати ентропію;

– не варто робити заміну дуже часто: це може знизити реальну ентропію паролів через людський фактор (спрощення шаблонів вибору паролів);

– найкраща практика: контекстно-чутлива політика – заміна за умови спрацювання тригера (після виявлення витоку, підозрілої активності) + примусова заміна для неактивованих/давніх паролів + багатофакторна автентифікація.

2.4 Обґрунтування періодичності зміни паролю для державних установ.

Тепер давайте розглянемо державні установи, в яких обробляються державні інформаційні ресурси. Коли збитки від компрометації “непомірно великі/неоціненні”, класична модель мінімізації очікуваних витрат перестає працювати в звичному вигляді: функція витрат ніби “вибухає” (неконтрольовано збільшується) при будь-якій ненульовій ймовірності компрометації, і необхідно переходити до іншої математичної постановки задачі. Далі розглянемо повний розбір наслідків і практичні (математично обґрунтовані) альтернативи.

1) Що означає “неоціненні” втрати математично.

Математично це можна зрозуміти двома шляхами:

А. Асимптотичне уявлення: $S \rightarrow \infty$ або $C \rightarrow \infty$. У нашій цільовій функції (з попередньої моделі):

$$G(t) = \mu S E_{\text{exp}}(t) + \frac{C(1 - e^{-\beta t})}{t} + \frac{K}{t}, \quad (8.18)$$

якщо S або $C \rightarrow \infty$, відповідні члени домінують і $G(t) \rightarrow \infty$ для будь-якого $t > 0$, поки існує ненульова ймовірність або експозиція (доступ злочинця до системи). Отже, мінімум функції досягається лише при границі $t \rightarrow 0^+$, тобто математично – прагнення до миттєвої (безперервної) зміни пароля (абсолютне зменшення експозиції до нуля). Це непрактичне рішення – воно ілюструє лише те, що витрати роблять компрометацію категорично непринятною.

В. Мінімакний показник/жорсткий обмежувальний підхід: замість мінімізації очікуваних витрат ставимо жорстке обмеження на допустимий ризик/експозицію (constraint, обмеження). Це практичніша модель при “неоціненних” втратах.

2) Жорстка умова на ризик (констрейнт-підхід).

Якщо компрометація неприпустима, ставимо порогову умову: допустима ймовірність компрометації за інтервал t не повинна перевищувати ε (дуже мала, наприклад 10^{-3} або 10^{-6}).

Використаємо стандартну пуассонівську формулу розподілу для імовірності ≥ 1 події при інтенсивності λ (тут λ – інтенсивність витоків/компрометацій): $P(\geq 1 \text{ компрометація за } t) = 1 - e^{-\lambda t} \leq \varepsilon$ [5].

Звідси:

$$e^{-\lambda t} \geq 1 - \varepsilon \Rightarrow t \leq -\frac{1}{\lambda} \ln(1 - \varepsilon). \quad (8.19)$$

Для невеликого ε приближено:

$$t \approx \frac{\ln(1/\varepsilon)}{\lambda}. \quad (8.20)$$

Інтерпретація: при “неоцінених” втратах ми не міняємо t за допомогою мінімізації очікуваних витрат – ми встановлюємо максимально допустимий інтервал t так, щоб імовірність компрометації була надзвичайно малою.

Числовий приклад. Якщо $\lambda = 0.02$ (0.02 витоку/місяць) і $\varepsilon = 0.01$ (1 % ймовірності), то:

$$t \leq -\frac{\ln 0.99}{0.02} \approx 0.5025 \text{ місяця} \approx 15 \text{ днів.} \quad (8.21)$$

Для $\varepsilon = 10^{-4}$ це дасть $t \approx \ln(10^4)/\lambda \approx 9.21/0.02 \approx 460$ місяців – але тут видно, що дуже малий ε може дати надто довгий інтервал залежно від λ ; тому треба уважно розглядати вхідні параметри.

3) Замість “нескінченних” втрат – перетворення задачі в жорсткі обмеження.

Практичні варіанти, коли втрати “неоціненні”:

– обмеження по ймовірності компрометації: як вище – вибрати t так, щоб $1 - e^{-\lambda t} \leq \varepsilon$;

– обмеження по очікуваній експозиції: вимагати $\mu E_{exp}(t) \leq \eta$, де η – допустимий середній час ймовірного перебування зловмисника в системі на одиницю часу (абсолютно невелике число);

– мінімакс (robust) підхід: мінімізувати максимальні можливі втрати в гіршому випадку – наприклад, мінімізувати вплив деградації якості паролів при змінах. Якщо в гіршому випадку втрати будуть великими при будь-якому $t > 0$, це призводить до вибору мінімально можливого t згідно з технічними/операційними обмеженнями.

4) Практичні обмеження роблять задачу осмисленою.

Оскільки $t \rightarrow 0$ неможливе операційно, вводимо технічні/людські/нормативні обмеження:

– мінімальний реальний інтервал: $t \geq t_{min} > 0$ (технічно можлива найменша періодичність, наприклад 1 день або 1 година для автоматизованого управління секретами);

– функція деградації безпеки через людський фактор: якщо змін пароля забагато, користувачі придумують слабкі варіанти – моделюємо це як підвищення β при зниженні t : $\beta = \beta_0 + \phi(t)$ з $\phi(t)$ зростаючою при зменшенні t . Це дає компроміс і часто дає інтернальний мінімум $t^* > 0$.

Приклад (конкретна модифікація):

Поставимо обмеження “ймовірність компрометації $\leq \varepsilon$ ” та врахуємо людський фактор через підвищення інтенсивності перебору пароля грубою силою або використання слабших паролів при умові:

$$1 - e^{-(\lambda + \beta(t))t} \leq \varepsilon, \quad (8.22)$$

де $\beta(t) = \beta_0 + \alpha/tp$ (приблизна модель: при малій t користувачі використовують шаблони \rightarrow ефективна β росте). Потрібно знайти найменше $t \geq t_{min}$ що задовольняє цю умову. Це дасть практичне раціональне t .

5) Альтернативні та більш ефективні рішення (коли збитки критичні).

Коли втрати неприпустимі, оптимальні дії – не обов’язково тільки частіша ротація паролів. Математично це виражається тим, що зменшення ймовірності компрометації λ та/або зменшення ефективності використання компрометації ε набагато ефективнішими, ніж звуження t до неможливих значень.

Практичні кроки, які входять в модель як зменшення λ , β або S (ефективно роблять проблему скінченною):

1. Багатофакторна аутентифікація – зменшує ймовірність успішного використання скомпрометованого пароля (ефективно зменшує S чи β).

2. Короткоживучі (short-lived) автентифікаційні дані та токени – автоматична, машинна зміна секретів із малим часом життя; для машинних облікових записів t може бути у хвилинах/годинах.

3. Secrets manager / автоматична зміна – зміна без участі людини, з низькими операційними K .

4. Тригерні зміни – зміна при інциденті/підозрі замість частих примусових змін.

5. Зниження λ через превентивні заходи – навчання персоналу, фільтри фішингу, контроль доступу.

6. Швидке виявлення (зменшення $1/\delta$) – зменшення експозиції $E_{exp}(t)$.

Математично: ці заходи або дають змогу підвищити допустиме t при фіксованому ε , або роблять ситуацію такою, що звичайна мінімізація очікуваних витрат знову має сенс (бо S, C стають скінченними).

б) Підсумок – практична інструкція при “неоцінених” втратах.

1. Не варто мінімізувати $G(t)$ прямолінійно, якщо S або $C \approx \infty$.

Замість цього.

2. Варто встановити жорстку політику ризику: вибрати допустиму ймовірність компрометації ε і вирахувати максимально допустимий інтервал:

$$t \leq -\frac{1}{\lambda} \ln(1 - \varepsilon). \quad (8.23)$$

3. Або встановити допустиму очікувану експозицію η і знайти t із $\mu E_{exp}(t) \leq \eta$.

4. Врахувати операційні обмеження: технічно мінімальний t_{min} та людський фактор (модель $\beta(t)$).

5. Варто переорієнтувати заходи на зменшення λ, β і покращення δ : багатофакторна автентифікація, автоматична заміна секретних даних для привілейованих користувачів, швидке виявлення, політики тригерної заміни пароля.

2.5 Приклад розрахунку необхідного періоду зміни пароля для реальних параметрів.

Проведемо розрахунок, **підставивши конкретні числа** (наприклад, $\lambda = 0.02/\text{місяць}$, $\varepsilon = 10^{-3}$) і покажемо обчислення t , а також порівняємо його з моделлю з людським фактором.

Вхідні параметри розрахунку:

- інтенсивність витоків $\lambda = 0.02 / \text{місяць}$;
- допустима ймовірність компрометації $\varepsilon = 10^{-3}$;
- для демонстрації витрати й інші параметри:
 - 1) $\mu = 0.02/\text{місяць}$;
 - 2) $S = 2000 \text{ UAH}/\text{місяць}$;
 - 3) $\delta = 0.5/\text{місяць}$ (середній час виявлення $\approx 2 \text{ місяці}$);
 - 4) $\beta_0 = 0.0005/\text{міс}$, $C = 50000 \text{ UAH}$, $K = 100 \text{ UAH}$;
 - 5) людський фактор: $\beta(t) = \beta_0 + \alpha / t$, $\alpha = 0.02$.

Результати розрахунків:

- максимально допустимий інтервал за констрейнтом $1 - e^{-\lambda t} \leq \varepsilon$:

$$t_{\text{constraint}} = -\frac{\ln(1 - \varepsilon)}{\lambda} \approx 0.0500 \text{ місяця} \approx 1.5 \text{ дня}; \quad (8.24)$$

- мінімум функції витрат без людського фактора (чисельно, локально):

$$t^*_{\text{basic}} \approx 4.24 \text{ місяці}, G(t^*) \approx 95.35 \text{ (UAH/міс. умовно)}; \quad (8.25)$$

- мінімум при включенні людського фактора (модель $\beta(t) = \beta_0 + \alpha/t$):

$$t^*_{\text{human}} \approx 90.67 \text{ місяців}, G(t^*) \approx 115.59. \quad (8.26)$$

Порівняння загальної цільової функції для базової моделі та моделі із впливом людського фактору представлено на рисунку 8.1.

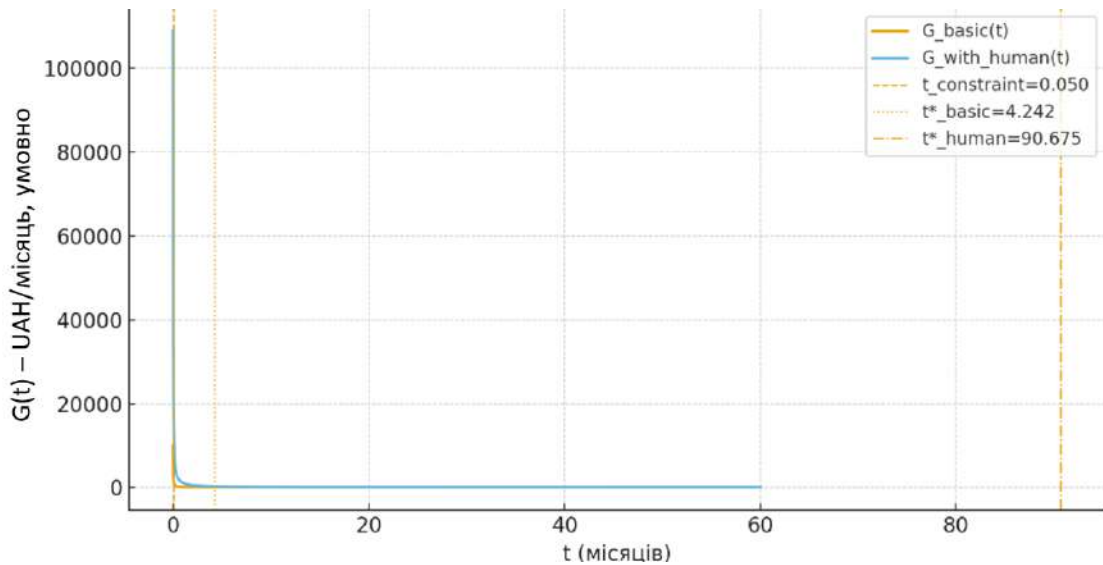


Рисунок 8.1. Порівняння загальної цільової функції для базової моделі та моделі із впливом людського фактора

Інтерпретація результатів:

– **обмеження ($\epsilon = 10^{-3}$)** дає надзвичайно малий період на оновлення пароля (~ 1.5 дня). Це типовий результат: коли вимагається дуже мала ймовірність компрометації, то регулярний інтервал ротації повинен бути надзвичайно коротким – часто технічно нереально. Саме тому при «неоціненних» втратах установи переходять до жорстких політик і автоматизованих механізмів (багатофакторна автентифікація, короткожвучих токенів, автоматизація зміни секретів), а не до ручної ротації кожні кілька днів;

– **раціональне значення базової моделі (~ 4.24 місяці)** відображає баланс між:

- 1) витратами на зміни (K);
- 2) ризиком витоків (μ, S, δ);
- 3) ризиком підбору грубою силою (β_0, C).

Тобто при обраних кінцевих числах мінімізуються середні витрати – і раціональне значення виходить у кілька місяців;

– модель із людським фактором дала дивовижний результат: дуже великий раціональний період (~90 місяців). Причина – вибрана модель $\beta(t) = \beta_0 + \alpha/t$: при дуже малих t (часті ротації) $\beta(t)$ значно зростає (α/t великий), що робить часті ротації контрпродуктивними; отже, алгоритм “відсовує” раціональне значення у дуже великі t , де $\beta(t) \approx \beta_0$ і операційні витрати K/t малі. Це ілюстрація важливості правильної форми $\beta(t)$: якщо людський фактор справді сильно погіршує ефективність паролів при частих ротаціях, то примусові часті зміни можуть різко зменшити безпеку;

– **практичний висновок:**

1) якщо вимагається математично "надзвичайно низька" ймовірність компрометації (ϵ дуже мале), ручна зміна паролів – неефективна/непрактична. Потрібні автоматичні рішення (короткоживучі токени, автоматизація зміни секретів) або жорсткий контроль доступу/багатофакторної автентифікації;

2) якщо витрати скінченні, то існує внутрішній раціональний період (кілька місяців у прикладі). Але форма й місце раціонального значення дуже чутливо залежать від припущень (особливо $\beta(t)$ і δ);

3) модель людського фактора має бути обґрунтована даними (як саме змінюється якість паролів при частих ротаціях). Проста модель α/t – лише ілюстрація.

Математичне обґрунтування вимог до складності паролів на основі ентропійного підходу дозволяє кількісно оцінити їх стійкість до атак перебором та словникових атак. Показано, що ключовими параметрами є розмір алфавіту S та довжина L , а також характер формування пароля (випадкова послідовність чи парольна фраза).

Для протидії brute-force атакам доцільніше підвищувати ентропію (збільшення довжини, використання парольних фраз), ніж покладатися лише на часту зміну паролів. Модель А демонструє, що за наявності постійного

ризик перебору та одноразового збитку часта зміна пароля не забезпечує економічно обґрунтованого виграшу в безпеці.

У випадку витоків автентифікаційних даних (фішинг, компрометація баз) модель В показує існування внутрішнього раціонального інтервалу зміни пароля, який визначається співвідношенням між інтенсивністю витоків μ , величиною збитків S та операційними витратами K . Отримана формула для t^* дає можливість адаптувати політику до конкретного середовища.

За умов “неоцінених” втрат класична мінімізація очікуваних витрат стає непридатною. Доцільно переходити до жорсткого обмеження на допустиму ймовірність компрометації (ϵ) або на допустиму експозицію. У таких умовах регулярна ручна ротація паролів повинна доповнюватися або замінюватися автоматизованими механізмами керування секретами, багатofакторною автентифікацією та тригерною зміною паролів.

Людський фактор істотно впливає на ефективність парольної політики. Надмірно часта примусова зміна може зменшувати фактичну ентропію через використання шаблонних модифікацій. Отже, оптимальна політика повинна враховувати поведінкові аспекти та бути контекстно-чутливою.

Загалом проведений аналіз підтверджує, що раціональна політика управління паролями повинна базуватися на формалізованій оцінці ризиків, параметрів загрозового середовища та організаційних обмежень, а не лише на традиційних регламентних вимогах. Поєднання математичних моделей з практичними механізмами зниження λ , β та експозиції дозволяє досягти збалансованого рівня безпеки в інформаційних системах державного сектору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

До розділу 1

1. Semigina T. Navigating Wartime Realities: Adaptation and Resilience in Ukrainian Social Work Education / T. Semigina, O. Stoliaryk // *Socialinė teorija, empirija, politika ir praktika*. 2025. Vol. 31. P. 8–24.
2. Любарець В. Соціальна резильєнтність як стратегічний принцип трансформації системи соціальних послуг в Україні / В. Любарець, А. Гриньків, Є. Панюшкін // *Humanitas*. 2025. № 4. С. 183–193.
3. Життєстійкість для кожного українця: презентовано концепт проєкту // Астарта-Київ. URL: <https://astartaholding.com/zhyttyestijkist-dlya-kozhnogo-ukrayinczya-prezentovano-konczep-t-proyektu/>.
4. Про реалізацію експериментального проєкту із запровадження комплексної соціальної послуги з формування життєстійкості : Постанова Кабінету Міністрів України від 03.10.2023 № 1049 URL: <https://ips.ligazakon.net/document/KP231049>.
5. Про внесення змін до постанови Кабінету Міністрів України від 3 жовтня 2023 р. № 1049 : Постанова Кабінету Міністрів України від 07.06.2024 № 663. Урядовий портал. 2024. URL: <https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-postanovy-kabinetu-ministriv-ukrainy-vid-3-zhovtnia-2023-r-1049-i070624-663>
6. Economics of Better Care: Brief / UNICEF, Maestral International. 2025. URL: <https://knowledge.unicef.org/resource/economics-better-care>
7. У 22 областях України працюють Центри життєстійкості. Неємія. URL: <https://nehemiah.org.ua/novyny/u-22-oblastyakh-ukrajini-pratsyuyut-tsentri-zhittestijkosti.html>
8. Про затвердження плану заходів з реалізації у 2024–2027 роках Стратегії демографічного розвитку України на період до 2040 року :

Розпорядження Кабінету Міністрів України від 01.11.2024 № 1091-р. Урядовий портал. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-z-realizatsii-u-20242027-rokakh-stratehii-demohrafichnoho-rozvytku-ukrainy-na-period-do-2040-roku-i011124-1091>

9. Стратегія демографічного розвитку України на період до 2040 року : схвалено розпорядженням Кабінету Міністрів України від 30.09.2024 № 922-р.

10. Всеукраїнська програма ментального здоров'я «Ти як?» // Офіційний сайт програми. URL: <https://howareu.com/pro-prohamu>.

11. Перший «Центр життєстійкості» у Закарпатській області. ГО Неємія. URL: <https://nehemiah.org.ua/novyny/pershij-tsentr-zhittestijkosti-u-zakarpatskij-oblasti.html>

12. Центри життєстійкості: посібник з облаштування та функціонування // Big City Lab ; Міністерство соціальної політики України. URL: https://decentralization.ua/uploads/library/file/900/BigCityLab_Centers_Of_Sustainability__1_.pdf.

13. Життєстійкість. // Міністерство соціальної політики, сім'ї та єдності України. URL: <https://www.msp.gov.ua/about/klyuchovi-napryamy/zhyttestiykist>

14. Рибальська А. На Київщині допомагатимуть формувати життєстійкість: відкрили перший Центр.// Суспільне. Київ. 2024, 16 квітня. URL: <https://suspilne.media/kyiv/722840-na-kiivsini-dopomagatimut-formuvati-zittestijkist-vidkrili-persij-centr/>

15. У Ніжині відкрили Центр життєстійкості. Ніжин.City. 2024. 26 черв. URL: <https://nizhyn.city/articles/367148/u-nizhini-vidkrili-centr-zhitytestijkosti>

16. У Менській громаді запрацював Центр життєстійкості. Менська міська рада. URL: <https://mena.cg.gov.ua/index.php?id=524977&tp=page>

17. Бедна А., Приступа К. Заняття для дітей та тренінги для батьків: у Чернігові відкрили перший в місті Центр життєстійкості. //Суспільне. Чернігів. 2024, 12 серпня. URL: <https://suspilne.media/chernihiv/812049-zanatta-dla-ditej-ta-treningi-dla-batkiv-u-cernigovi-vidkrili-persij-v-misti-centr-zittestijkosti/>
18. Ізотов І., Іванова О. На Полтавщині відкрили перший в області центр життєстійкості. //Суспільне. Полтава. 2024, 3 квітня. URL: <https://suspilne.media/poltava/720278-na-poltavsini-vidkrili-persij-v-oblasti-centr-zittestijkosti/>
19. У Черкаській області діють 10 центрів життєстійкості: адреси та послуги. 18000.com.ua. URL: <https://18000.com.ua/strichka-novin/u-cherkaskij-oblasti-diyut-10-centriv-zhittjestijkosti-adresi-ta-poslugi/>
20. Аналітична довідка: Центр життєстійкості Миколаїв за жовтень 2025 року. Департамент праці та соціального захисту населення Миколаївської міської ради. URL: https://sotsdepart.mk.ua/index.php?option=com_content&view=article&id=4319&Itemid=216
21. European Social Network (ESN). Integrated Social Services in Europe. Brighton: ESN, 2019. 124 p.
22. Council of Europe. Recommendation CM/Rec(2011)5 of the Committee of Ministers to member states on reducing the risk of vulnerability of children and young people. URL: <https://search.coe.int>.
23. Про схвалення Стратегії цифрової трансформації соціальної сфери. Розпорядження Кабінету Міністрів України від 28 жовт. 2020 р. № 1353-р. URL: <https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80>.
24. World Health Organization. Problem Management Plus (PM+): Individual psychological help for adults impaired by distress in communities exposed to adversity. Geneva: WHO, 2016.

25. World Health Organization. Self-Help Plus (SH+): A group-based stress management course for adults. Geneva: WHO, 2021.
26. World Health Organization. mhGAP Humanitarian Intervention Guide (mhGAP-HIG): Clinical management of mental, neurological and substance use conditions in humanitarian emergencies. Geneva: WHO, 2015.
27. European Social Network (ESN). Integrated Social Services in Europe. Brighton: ESN, 2019. 124 p.
28. Про затвердження Порядку та умов надання субвенції з державного бюджету місцевим бюджетам на створення мережі спеціалізованих служб підтримки осіб, які постраждали від домашнього насильства : Постанова Кабінету Міністрів України від 21 квіт. 2021 р. № 398. URL:<https://zakon.rada.gov.ua/laws/card/398-2021-%D0%BF>
29. Деякі питання Єдиної інформаційної системи соціальної сфери : Постанова Кабінету Міністрів України від 14 квіт. 2021 р. № 404

To chapter 2

1. Гришко С.В., Прохорова Л.А., Левада О.М., Непша О.В., Іванова В.М., Зав'ялова Т.В. Екологічне виховання студентів-географів під час вивчення курсу «Геологія з навчальною практикою» в закладі вищої освіти. Перспективи та інновації науки: журнал. 2022. № 1(6) 2022. С.141-150. [https://doi.org/10.52058/2786-4952-2022-1\(6\)-141-150](https://doi.org/10.52058/2786-4952-2022-1(6)-141-150)
2. Гришко С.В., Прохорова Л.А., Непша О.В., Зав'ялова Т.В. Педагогічні умови формування екологічної культури майбутніх учителів географії під час вивчення дисциплін професійного циклу. Інноваційна педагогіка. 2021. Вип. 34. Т.2. С. 9-13. <https://doi.org/10.32843/2663-6085/2021/34-2.36>
3. Гришко С.В., Прохорова Л.А., Непша О.В., Зав'ялова Т.В. Формування екологічної культури майбутніх учителів географії під час вивчення курсів «Географія материків і океанів» та «Фізична географія

- України» в закладі вищої освіти. Вісник науки та освіти: журнал. 2023. № 4(10). 2023. С. 424-436. [https://doi.org/10.52058/2786-6165-2023-4\(10\)-424-436](https://doi.org/10.52058/2786-6165-2023-4(10)-424-436)
4. Данильченко О., Корнус О, Корнус А, Сюткін С, Нешатаєв Б. Практична підготовка студентів: стан і проблеми. Проблеми безперервної географічної освіти і картографії. 2018. Вип. 27. С. 28-34.
 5. Донченко Л.М., Зав'ялова Т.В., Іванова В.М., Непша О.В. Формування екологічних знань і вмінь майбутніх вчителів географії під час вивчення курсу «Загальне землезнавство». Педагогіка формування творчої особистості у вищій і загальноосвітній школах: зб. наук. пр. Вип. 63. Т. 2. С. 59-64.
 6. Дудка І.Г., Носаченко В.М. Особливості практичної підготовки майбутнього вчителя географії до екологічної діяльності. Вісник ХДУ. Серія: Географічні науки. 2019. № 11. С. 130-136.
 7. Зав'ялова Т.В., Непша О.В. Екологічне виховання при вивченні дисципліни «Географія ґрунтів з основами ґрунтознавства». Гуманітарний простір науки: досвід та перспективи: зб. Матеріалів VI Міжнарод. наук. практ. інтернет-конф., 25 жовтня 2016 р. Переяслав-Хмельницький, 2016. Вип. 6. С.13-15.
 8. Непша О.В., Гришко С.В. Роль навчальних практик у формуванні професійних компетенцій майбутніх вчителів географії. Збірник тез за матеріалами Міжнародної науково-практичної конференції «Філософські обрії сьогодення» 19 листопада 2020 р. Херсон: ХДАЕУ, 2020. С.91-93.
 9. Прохорова Л. Основні положення проведення навчальної практики з геоморфології зі студентами-географами. Збірник тез II Міжнародної науково-практичної інтернет-конференції «II Шкловські читання «Проблеми сучасних природничо-математичних наук та методик їх викладання». Глухів, 2020. С.127.

10. Прохорова Л.А., Зав'ялова Т.В., Непша О.В. Готовність майбутніх вчителів географії до екологічного виховання учнівської молоді у сучасній загальноосвітній школі. Екологія – філософія існування людства: зб. наук. праць. Мелітополь: ТОВ «Колор Принт», 2018. С.96-100.

To chapter 3

1. Вихляєв Ю.М. Теорія і технології оздоровчо-рекреаційної рухової активності: навч. посіб. Вінниця: ТОВ «ТВОРИ», 2020. 648 с.

2. Круцевич Т.Ю., Безверхня Г.В. Рекреація у фізичній культурі різних груп населення: навч. посіб. Київ: Олімпійська література, 2010. 248 с.

3. Олексієнко Я.І., Гунько П.М. Теорія, види та технології оздоровчо-рекреаційної рухової діяльності: навч.-метод. посіб. Черкаси: ЧНУ імені Богдана Хмельницького, 2018. 260 с.

4. Пангелова Н.Є., Пангелов Б.П. Сучасні тенденції у розвитку рекреаційної діяльності населення України. Young Scientist. 2019. № 4.1 (68.1). April. С. 161-164.

5. Проценко А.А., Котова О.В., Цибульська В.В., Непша О.В., Суханова Г.П., Кирієнко О.Г. Роль фізичної рекреації у сучасному суспільстві, збереженні та зміцненні здоров'я людини. Actual scientific research in the modern world. Journal. Pereiaslav. 2023. Is. 7(99). С. 137-140.

6. Рибковський А.Г., Канішевський С.М. Системна організація рухової активності людини. Донецьк: ДонНУ, 2003. 436 с.

7. Сопотницька О.В., Сопотницький Р.С. Сучасні оздоровчі технології в процесі фізичного виховання студентської молоді. Інноваційні підходи до фізичного виховання і спорту студентської молоді: матеріали п'ятого регіонального наук.-метод. семінару / за заг. ред. Огнистого А.В., Огнистої К.М. Тернопіль: Видавництво СМТ «ТАЙП», 2020. С. 160-164.

8. Товт В.А., Маріонда І., Сивохоп Е., Сусла В. Теорія і технології

оздоровчо-рекреаційної рухової активності: навч. посіб. для викладачів і студентів. Ужгород: Говерла. 2015. 88 с.

9. Христова Т.Є., Сопотницька О.В., Непша О.В., Суханова Г.П. Організація фізкультурно-оздоровчої і спортивно-масової роботи в літніх дитячих оздоровчих таборах. Гуманітарний діалог у контексті глобальних соціальних змін: кол. моногр. Харків: СГ НТМ «Новий курс», 2025. С. 31-34. <https://doi.org/10.61718/mon2025074>.

10. Ціповяз А.Т., Христова Т.Є., Антонова О.І. Практичні методи фізичного виховання та реабілітації: навч. посіб. Кременчук: Кременчуцький національний університет імені Михайла Остроградського, 2013. 140 с.

11. Юрченко Ю. Рухова активність як чинник, що визначає здоров'я людини. Молода спортивна наука України: зб. наук. праць з галузі фізичної культури та спорту. 2006. Вип. 10. Львів: НВФ «Українські технології». Т. 3. Розділ 3.1. С. 57-62.

12. Khrystova Tetiana. Conceptual approaches to conservation of student health. Education during a pandemic crisis: problems and prospects. Monograph / Eds. Tetyana Nestorenko & Tadeusz Pokusa. Opole: The Academy of Management and Administration in Opole, 2020. P.135-140.

13. Kotova O.V., Sopotnytska O.V., Nepsha O.V. The use of fitness technologies as a motivating factor for physical education classes in institutions of higher education. Development of physical culture and sports amidst martial law: International scientific conference (October 5-6, 2022). Częstochowa: Baltija Publishing, 2022. P. 69-73. <https://doi.org/10.30525/978-9934-26-253-1-16>

14. Protsenko Andrii, Kotova Olena, Tsybulska Viktoriia, Sukhanova Hanna, Sopotnytska Olena. Non-traditional types of physical recreation as a basis for the formation of a healthy lifestyle of student youth. Сучасне суспільство: глобальні трансформації: кол. моногр. Харків: СГ НТМ «Новий курс», 2024. С. 23-26.

До розділу 4

1. Anchondo E.L. The tourism students' awareness of communicative competence in an english as a foreign language context. *European scientific journal*, 2018, №5, 184. URL: <http://dx.doi.org/10.19044/esj.2018.v14n5p184>
2. Bihych O., Okopna Y. E-learning in professionally oriented german communicative competence formation of students majoring in tourism management. *Advanced education*, 2018, №9, 126-131. URL: <https://doi.org/10.20535/2410-8286.132499>
3. Dziubata Z. Labour market trends teaching in tourism industry in the context of eurointegration processes. *Збірник наукових праць ТДАТУ імені Дмитра Моторного (економічні науки)*, 2022, №2(46), 44–51. URL: <https://doi.org/10.31388/2519-884X-2022-46-44-51>
4. Ho Y.-Y. C. Communicative language teaching and English as a foreign language undergraduates' communicative competence in tourism english. *Journal of Hospitality, Leisure, Sport & Tourism Education*, 2020, №27, 100271. URL: <https://doi.org/10.1016/j.jhlste.2020.100271>
5. Lazebna O., Kotvytska V. CLIL in tourism students' multicultural competence development. *Advanced Education*, 2021, №8(19), 4–11. URL: <https://doi.org/10.20535/2410-8286.226588>
6. Zhumbei M., Savchuk N., Apelt H., Kopchak L., Pryimak L. International experience in formation of foreign language communicative competence in tourism students in the context of blended learning. *Khazar journal of humanities and social sciences*, 2023, №1. URL: <https://doi.org/10.5782/.kjhss.2023.21.34>
7. Жумбей М. М. Інноваційні підходи до впровадження інтерактивних моделей навчання іноземних мов у підготовці студентів сфери обслуговування. *Науковий часопис НПУ імені М. П. Драгоманова*, 2024, №97. URL: <https://www.chasopys.ps.npu.kiev.ua/archive/97/13.pdf>

8. Жумбей М. М., Копчак Л. В., Приймак Л. Б. Роль формування іншомовної компетентності майбутніх фахівців сфери туризму та гостинності в умовах війни. Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 5: педагогічні науки: реалії та перспективи, 2023, №93, 53–58. URL: <https://enpuir.udu.edu.ua/entities/publication/5117db6e-6794-42bd-912e-31d6c5ab8c4a>
9. Івасів Н. С. Професійна іншомовна підготовка майбутніх фахівців з туризмознавства як педагогічна проблема. *Science and Education a New Dimension. Pedagogy and Psychology*, 2017, №V(54)(126), 23–27. URL: <https://seanewdim.com/wp-content/uploads/2021/03/Foreign-language-professional-training-of-future-tourism-science-specialists-as-a-pedagogic-problem-N.-S.-Ivasiv.pdf>
10. Кожевнікова В., Шепель М. Іноземна мова професійних комунікацій як елемент підготовки фахівців готельно-ресторанного бізнесу. *Економіка та суспільство*, 2021, №30. URL: <https://doi.org/10.32782/2524-0072/2021-30-6>
11. Мединська С. І. Формування іншомовної компетентності як компонента професійної підготовки фахівців у галузі туризму. *Вісник Дніпропетровського університету імені Альфреда Нобеля. Серія педагогіка і психологія*, 2016, №2(12), 233–237. URL: <https://pedpsy.duan.edu.ua/images/PDF/2016/2/39.pdf>
12. Чорна Л. В. Міжкультурна комунікація в туризмі: професійно-прикладний аспект. *Карпатський край*, 2018, №1–2(10–11), 137–143. URL: <https://journals.pnu.edu.ua/index.php/kk/article/download/3742/4335/7850>
13. Шестель О., Старинець О., Заїка О. Засоби формування іншомовної комунікативної компетентності фахівців сфери обслуговування. *Актуальні питання гуманітарних наук*, 2019, №26(2), 179–184. URL: <https://doi.org/10.24919/2308-4863.2/26.195909>

14. Kuzmenko A., Solodiuk N., Petrova Y., Kozinets I. Culture of academic integrity of postgraduate students in Ukraine: peculiarities of development and formation. The Online Journal of Education Policy and Management. Revista on line de Política e Gestão Educacional, Araraquara, 2023, v. 27, n. esp. 2, e023050, DOI: <https://doi.org/10.22633/rpge.v27iesp.2.18782>

До розділу 5

1. Конституція України від 28 червня 1996 р. Відомості Верховної Ради України. 1996. №30. ст. 141

2. Про службу в органах місцевого самоврядування: Закон України від 2 травня 2023 р. Відомості Верховної Ради України. (реєстраційний номер 3077-IX від 02.05.2023).

3. Про заходи щодо впровадження Концепції адміністративної реформи в Україні. Указ Президента України; Концепція від 22.07.1998 № 810/98

4. Стешенко Т.В., Канюк М.Т. Муніципальна служба в Україні: сучасний стан та перспективи розвитку. Державне будівництво та місцеве самоврядування Випуск (43 ' 2022). С.107-115. <https://doi.org/10.31359/1993-0941-2022-43-107> УДК 342.25

5. Мартищенко С.Л. Концептуальні особливості сучасного етапу адміністративно-територальної реформа в Україні. Часопис Київського університету права, (2-4), (2022). С.32-37. <https://doi.org/10.36695/2219-5521.2-4.2022.04>

6. Про державну службу: Закон України від 10 грудня 2015 р. Відомості Верховної Ради України. 2016. №4. ст 43.

До розділу 6

1. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

2. Загальна декларація прав людини : прийнята і проголошена резолюцією Генеральної Асамблеї ООН 217 А (III) від 10 грудня 1948 р.
3. Міжнародний пакт про громадянські і політичні права : Міжнародний документ від 16 грудня 1966 р.
4. Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 04 листопада 1950 р.
5. Про правовий режим воєнного стану : Закон України від 12 травня 2015 р. № 389-VIII.
6. Рішення Європейського суду з прав людини у справі «Verentsov v. Ukraine» від 11 квітня 2013 р.
7. Рішення Європейського суду з прав людини у справі «Shmushkovych v. Ukraine» від 14 листопада 2013 р.

До розділу 7

1. Костицький М. В. Юридична психологія : підручник. — Київ : Атіка, 2004. — 480 с.
2. Васильєв В. Л., Костицький М. В. Юридична психологія : підручник. — Київ : Юрінком Інтер, 2010. — 640 с.
3. Коновалова В. О. Судова психологія : навч. посіб. — Харків : Право, 2012. — 256 с.
4. Сингаївська І. В. Психологічні особливості переживання психотравмуючих подій : монографія. — Київ : КНУ імені Тараса Шевченка, 2018. — 256 с.
5. Чанчиков І. В. Соціально-психологічні чинники спотворення показань свідків // Науковий вісник Херсонського державного університету. Серія: Психологічні науки. — 2019. — Вип. 3. — С. 98–104.
6. Тіщенко В. В. Психологія слідчої діяльності : навч. посіб. — Київ : Нац. акад. внутр. справ, 2013. — 312 с.

7. Шепітько В. Ю. Криміналістика : підручник. — Харків : Право, 2019. — 752 с.
8. Бандурка О. М., Бочарова С. П., Землянська О. В. **Юридична психологія** : навч. посіб. — Харків : Ун-т внутр. справ, 2003. — 352 с.
9. Максименко С. Д. Загальна психологія : підручник. — Київ : Центр учбової літератури, 2017. — 720 с.
10. Коновалова В. О. Психологічні особливості оцінки достовірності показань у кримінальному провадженні // Вісник Національної академії правових наук України. — 2018. — № 2. — С. 145–156.
11. Тіщенко В. В. Психологічні аспекти формування та перевірки показань у слідчій діяльності // Юридична психологія. — 2019. — № 1 (24). — С. 32–41.
12. Сингаївська І. В. Вплив психотравматичного досвіду на процес відтворення подій // Проблеми сучасної психології. — 2020. — Вип. 47. — С. 215–228.

До розділу 8

1. Digital identity guidelines: authentication and lifecycle management (SP 800-63B) [Electronic resource] / National Institute of Standards and Technology. – Gaithersburg, MD : NIST, 2017. – (NIST Special Publication 800-63B). – Mode of access: <https://doi.org/10.6028/NIST.SP.800-63b> (date of access: 20.02.2026).
2. Shannon C. E. A mathematical theory of communication // Bell System Technical Journal. – 1948. – Vol. 27, no. 3. – P. 379–423 ; no. 4. – P. 623–656.
3. Bonneau J. The science of guessing: analyzing an anonymized corpus of 70 million passwords // 2012 IEEE Symposium on Security and Privacy. – Los Alamitos, CA : IEEE Computer Society, 2012. – P. 538–552.
4. Ross S. M. Introduction to probability models. – 11th ed. – Amsterdam : Academic Press, 2014. – 800 p.

5. Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022) [Electronic resource] / International Organization for Standardization. – Geneva : ISO, 2022. – Mode of access: <https://www.iso.org/standard/82875.html> (date of access: 22.02.2026).

До розділу 9

1. Human Development Report 1994. New Dimensions of Human Security. New York : UNDP, 1994. 229 p.

2. Walker B., Salt D. Resilience Thinking: Sustaining Ecosystems and People in a Changing World. Washington : Island Press, 2006. 192 p.

3. Ryzhov I., Yashchuk P. Resilience in the System of National Security: The Concept of the Vital Dimension. Journal of Law and Political Sciences. 2025. Vol. 46, Issue 3. P. 94–121.

4. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР (зі змін.).

5. World Economic Forum. Global Risks Report 2023. Geneva : WEF, 2023. 96 p.

6. Hegel G. W. F. Elements of the Philosophy of Right. Cambridge : Cambridge University Press, 1991. 379 p.

7. Renn O. Risk Governance: Coping with Uncertainty in a Complex World. London : Earthscan, 2008. 368 p.

8. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII // Відомості Верховної Ради України. 2018. № 31. Ст. 241.

Vydavatel:

Publishing house Education and Science s.r.o. IČO : 271 56 877.
Frýdlanská 15/1314 , Praha 8. MS v Praze , oddíl C,vložka 100614

**Cross-Disciplinary Studies in
Science, Innovation and Social
Development**

Volume VI

Signed for printing on February 28, 2026.
Format 60x90/8. Headset Times New Roman.
Mental printing. arc. 6,25. Edition online.