

The background features a light blue field with various geometric shapes in blue and orange. These include squares, triangles, circles, and semi-circles, some of which are partially cut off by the edges of the frame. The shapes are arranged in a non-repeating, abstract pattern.

ЗУСТРІЧ З ПРЕДСТАВНИКАМИ КІБЕРПОЛІЦІЇ

30.10.2024



**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ



Конфіденційність

Захист інформації від доступу сторонніх осіб.
Використання надійних паролів для обмеження доступу до облікових записів.



Цілісність

Забезпечення захисту даних від змін або фальсифікації.
Впровадження перевірок для виявлення несанкціонованих змін, наприклад, цифрових підписів або хешів.



Доступність

Забезпечення своєчасного доступу до інформації для авторизованих користувачів.
Захист серверів від атак типу DDoS, які можуть призвести до недоступності даних.



Аутентифікація

Перевірка особи користувача, що входить у систему.
Використовуйте двофакторну автентифікацію (2FA) для підвищення рівня безпеки.



Контроль доступу

Обмеження доступу до інформації відповідно до рівня прав користувачів.
Надання доступу лише тим, хто його потребує для виконання своїх обов'язків.



Як уникнути загроз у цифровому середовищі?

Остерігайтесь фішингових атак

Не відкривайте підозрілі електронні листи чи повідомлення і не переходьте за невідомими посиланнями.
Завжди перевіряйте відправника та автентичність сайтів, на які вводите особисті дані.

Регулярно оновлюйте програмне забезпечення

Регулярні оновлення допомагають усунути вразливості, які можуть використовуватися зловмисниками.

Захист від соціальної інженерії

Усвідомлюйте маніпуляції, які спрямовані на виманювання конфіденційної інформації.

Використовуйте антивірусні програми

Завжди майте активний антивірус і брандмауер для захисту вашого пристрою від шкідливого програмного забезпечення.

Будьте обережними з публічними мережами Wi-Fi

Уникайте введення паролів або фінансових даних під час підключення до публічних мереж. Використовуйте VPN для шифрування свого трафіку.



Як забезпечити безпеку під час проведення онлайн-уроків?



Паролі та обмеження доступу

Встановлюйте унікальні паролі для кожного заняття і контролюйте доступ через віртуальні "очікувальні кімнати".



Контроль екрану та чату

Обмежте можливість учасників (студентів) ділитися екраном, вмикати мікрофони та камери без дозволу.
Увімкніть режим очікування, щоб контролювати, хто приєднується до уроку.



Захист персональних даних

Зберігайте записи уроків лише в безпечному середовищі та надавайте доступ тільки авторизованим користувачам.

**Критичне ставлення до
джерел**

Викладачі повинні перевіряти джерела інформації, звертати увагу на їх надійність, а також бути обізнаними щодо сайтів, які можуть поширювати фейки.

01

Фактчекінг

Використання інструментів для перевірки фактів, таких як спеціалізовані сервіси та сайти, щоб підтверджувати або спростовувати сумнівні твердження.

02

Регулярне навчання

Освітняни мають постійно вдосконалювати свої навички медіаграмотності, проходити тренінги з виявлення дезінформації та маніпуляцій.

03

Фільтрація контенту

Викладачі можуть використовувати фільтри контенту та інструменти для блокування небажаної інформації у соцмережах або новинних сайтах.

04

Важливість уміння перевіряти достовірність інформації, розпізнавання фейків та маніпуляцій.

Забезпечення безпеки в соціальних мережах

01

Налаштуйте приватність акаунту

Встановіть обмеження на доступ до вашого профілю, щоб інформація була видимою лише для друзів або певного кола осіб.

02

Використовуйте надійні паролі та двофакторну автентифікацію

Це допоможе захистити ваш обліковий запис від зламу.

03

Не публікуйте особисту інформацію:

Уникайте розміщення приватних даних, таких як адреса, номери телефонів, або інформація про фінанси.

04

Будьте обережні з незнайомцями

Не приймайте запити на дружбу або повідомлення від підозрілих або незнайомих акаунтів.

05

Фільтрація контенту та кібербезпека:

Будьте уважні до інформації, яку поширюєте або лайкаєте, щоб уникнути участі у фейкових новинах або шахрайствах.

Дотримуйтесь етики спілкування

Не поширюйте неперевірену або конфіденційну інформацію про колег, студентів чи заклад освіти.

Контролюйте інформацію про заклад

Використовуйте лише офіційні канали для поширення інформації про навчальний процес, заходи чи успіхи.



Розділяйте професійне та особисте спілкування

Створюйте окремі акаунти для роботи і особистого життя, щоб уникнути змішування контенту.

Встановіть політику публікацій

Створіть внутрішні правила для комунікації в соцмережах, які включатимуть контроль за тим, що публікується від імені університета або викладача.

Обмежуйте час використання соцмереж

Регулюйте час, проведений у соцмережах під час робочого дня, щоб не відволікатися від основних завдань.

БРАМА ОНЛАЙН
ВАРТА
УКРАЇНИ

**Донатъ свій час
на захист
інфопростору**



БРАМА - це синергія громадян, приватного та державного секторів у протидії дезінформації та незаконному контенту в інформаційному просторі.

Запрошуємо долучитись до соціального проєкту
"БРАМА" https://t.me/+3VRwQDd_zdthZDUy

Напрямки діяльності кіберполіції. Реалізація проєкту «БРАМА»

Наші цілі:

- Знищення російських осередків в Інтернеті
- Зменшення рівня булінгу та цькування в мережі
- Протидія наркотикам та шахрайству
- Навчання та тренінги з кібергігієни
- Просвіта населення щодо інформаційної гігієни
- Залучення та мотивація громадян до активної громадянської позиції.