



Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

ОСНОВИ ГІБЕРГІЄНИ

Понятійний апарат у сфері кібергієни

ЦІЛІ



ВИВЧИТИ:

- поняття кібергігієни
- правила кібергігієни
- поняття кібербезпеки та інформаційної безпеки

розглянути:

- зміст кібергігієни
- нормативно-правову базу кібербезпеки та інформаційної безпеки

ЩО ТАКЕ «КІБЕРГІЄНА»?



Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

Зміст



Соціальна
інженерія



Безпечне користування
мережею Інтернет



Безпечне користування
електронною поштою

Зміст



Шкідливе програмне
забезпечення



Безпека користування
соціальними мережами



Безпека мобільних
пристроїв

Зміст



Фізична безпека



Убезпечення від
неправдивих повідомлень



Захист персональних
даних

Зміст



Реагування на
інциденти безпеки
інформації

Структура національної безпеки

НАЦІОНАЛЬНА БЕЗПЕКА

Зовнішньополітична
безпека

Державна безпека

Воєнна безпека

Кібербезпека

Інформаційна безпека

Екологічна безпека

Економічна безпека

Інші види безпеки



Закон України «Про основні засади забезпечення кібербезпеки України»

Стратегія кібербезпеки України

Закон України «Про критичну інфраструктуру»

Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури



Що таке КІБЕРБЕЗПЕКА?



Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

Стратегія кібербезпеки

МЕТА — створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави

захист прав, свобод і законних інтересів громадян України у кіберпросторі

убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства

європейська і євроатлантична інтеграція у сфері кібербезпеки

ПРІОРИТЕТИ

формування потенціалу стримування

набуття кіберстійкості

вдосконалення взаємодії

ЦІЛІ



ЗАГРОЗИ КІБЕРБЕЗПЕЦІ

Гібридна агресія Російської Федерації проти України у кіберпросторі

Кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат

Організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності

Використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності

Стратегія кібербезпеки

Потенціал Цілі	Стимування (С)	Кіберстійкість (К)	Удосконалення взаємодії (В)
1	Дієва кібероборона	Національна кіберготовність та надійний кіберзахист	Зміцнення системи координації
2	Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму	Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки	Формування нової моделі відносин у сфері кібербезпеки
3	Ефективна протидія кіберзлочинності	Безпечні цифрові послуги	Прагматичне міжнародне співробітництво
4	Розвиток асиметричних інструментів стимування		

Масована кібератака 13-14 січня 2022 року на державні органи



Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

Автор

Гільдія IT Фахівців

<https://adm.dp.gov.ua/>
<https://www.atom.gov.ua/ua/>
<https://bukoda.gov.ua/>
<https://check.gov.ua/>
<https://court.gov.ua/>
<https://diia.gov.ua/>
<https://dpss.gov.ua/>
<https://dsns.gov.ua/>
<https://e-driver.hsc.gov.ua/>
<https://e-journal.iea.gov.ua/>
<https://forest.gov.ua/>
<https://gov.ua/>
<https://kmu.gov.ua/>
<https://mail.gov.ua/>
<https://mepr.gov.ua/>
<https://mfa.gov.ua/>
<https://minagro.gov.ua/>
<https://minregion.gov.ua/>
<https://mon.gov.ua/>
<https://mova.gov.ua/>
<https://mva.gov.ua/>
<https://nads.gov.ua/>
<https://rp.gov.ua/>
<https://rv.gov.ua/>
<https://sies.gov.ua/>
<https://treasury.gov.ua/>

Нравится · Ответить · 54 мин.

Ст. 8 Закону України
«Про захист інформації в інформаційно-
комунікаційних системах»
доповнено ч. 5
(Резервування)

ГЛОБАЛЬНІ ВИКЛИКИ ТА ЗАГРОЗИ

Збільшення кількості глобальних дезінформаційних кампаній

Соціальні мережі як суб'єкти впливу в інформаційному просторі

Інформаційна політика Російської Федерації - загроза не лише для України, але й для інших демократичних держав

Недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій

НАЦІОНАЛЬНІ ВИКЛИКИ ТА ЗАГРОЗИ

Інформаційний вплив Російської Федерації як держави-агресора на населення України

Обмежені можливості реагувати на дезінформаційні кампанії

Несформованість системи стратегічних комунікацій

Інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України

Недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів

Доступ до інформації на місцевому рівні

Спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України

Недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам

Приклад



Павло Бондаренко

16 січня · 🌐

Друзі, це важливо. Проведіть профілактичні бесіди зі своїми дітьми, онуками, племінниками тощо. Рашисти використовують дітей для спрямовування та коригування ракетних ударів. Так могло статися у Дніпрі.

Усе відбувається через ігрову програму для смартфонів. За її умовами, учасники шукають "коробки" з віртуальними призами, які можна обміняти на електронні гроші. Під час проходження маршруту діти здійснюють фотофіксацію місцевості, у тому числі об'єктів військової та критичної інфраструктури на території різних населених пунктів. Інформацію з геолокацією завантажують до бази ігрового додатку.

За відомостями СБУ, доступ до адміністрування цього застосунку має підконтрольна спецслужбам рф ІТ-компанія, зареєстрована в одній з європейських країн.



Організація з безпеки та співробітництва в Європі

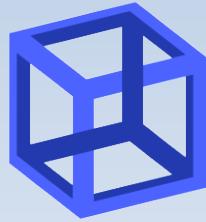


МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

Інформаційна безпека



Інформаційна безпека



МЗС



**Органи
державної влади,
місцевого
самоврядування,
інститути
громадянського
суспільства**



Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

ПРАВИЛА КІБЕРГІГІЄНИ

- ☒ Завжди критично ставтеся до відомостей, одержаних з мережі Інтернет
- ☒ Регулярно здійснюйте резервування важливих даних, не зберігайте все в одному місці
- ☒ Намагайтеся користуватися останніми версіями програмного забезпечення та регулярно робіть оновлення

ПРАВИЛА КІБЕРГІЄНИ

- ☒ Залишайте якомога менше персональних даних в мережі Інтернет
- ☒ Дотримуйтесь вимог парольного захисту та використовуйте за можливості багатофакторну автентифікацію
- ☒ Користуйтеся антивірусним програмним забезпеченням та іншими засобами убезпечення

ПРАВИЛА КІБЕРГІГІЄНИ

- ☒ У випадку компрометації чутливих даних повідомте про це уповноважену особу та вживайте заходів убезпечення решти відомостей
- ☒ Максимально обмежте доступ сторонніх осіб до терміналів, за якими Ви працюєте
- ☒ Використовуйте тільки перевірені носії інформації
- ☒ Регулярно оновлюйте знання у сфері кібергігієни



Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

ПИТАННЯ?