Асоціація малих міст УКРАЇНИ

СУПЕРМАРКЕТ РІШЕНЬ для громад

ICWR INSTITUTE OF CYBER WARFARE RESEARCH

CyberLab Комп'ютерна криміналістика

Державне регулювання кібербезпеки на місцях

Держава діє через чотири основні механізми:

Нормативно-правовий	Інституційний	Контрольно-наглядовий	Операційний
Встановлення законів (Закон «Про основні засади забезпечення кібербезпеки»).	Створення спеціальних органів (НКЦК, Держспецзв’язку, СБУ, Кіберполіція).	Проведення державних аудитів, перевірка систем захисту інформації (КСЗІ) та сертифікація засобів захисту.	Реагування на інциденти через центри CERT-UA та обмін даними про загрози.

Законодавчий рівень

- Закон України **«Про основні засади забезпечення кібербезпеки України»** Визначає понятійний апарат (що таке кіберінцидент, кібератака, об'єкт критичної інфраструктури), повноваження державних органів та обов’язки приватного сектору.
- Закон України **«Про захист інформації в інформаційно-комунікаційних системах»** регулює питання технічного захисту інформації (ТЗІ) та створення комплексних систем захисту інформації (КСЗІ).
- Закон України **«Про критичну інфраструктуру»** — визначає критерії віднесення підприємств до критично важливих та встановлює особливі вимоги до їхньої безпеки.
- **Стратегія кібербезпеки України** (2021–2025 та оновлена версія до 2026 року) — затверджується Указом Президента. Вона визначає пріоритети: від розбудови національної системи кібербезпеки до активної протидії кіберагресії.
- **Кримінальний кодекс України** (Розділ XVI) — передбачає відповідальність за кіберзлочини (ст. 361–363-1), такі як несанкціоноване втручання в роботу комп'ютерних мереж або розповсюдження шкідливого ПЗ.

Чому ОМС у зоні підвищеного ризику?

Органи місцевого самоврядування обробляють критичні дані, управляють інфраструктурою та інфраструктурою та забезпечують життєдіяльність громад.
Кожен комп'ютер та смартфон службовця — це потенційна точка входу для ворога.

Кібергігієна та кібербезпека — це не просто "справа IT-відділу", це базова складова національної безпеки.

Фішинг та соціальна інженерія

Спрямовані атаки на працівників через емоційні повідомлення для отримання доступу.

Зупинка критичних послуг

Блокування роботи ЦНАПів, місцевих реєстрів та систем управління життєзабезпеченням.

Витік даних

Крадіжка конфіденційної та службової інформації громади.

Правовий фундамент кіберзахисту

Закон 4336-IX (2025)

- Переформатування системи кіберзахисту.
- Вимога призначення Керівників з кіберзахисту (CISO).
- Адміністративна відповідальність за неповідомлення про інциденти.

Закон про кібербезпеку

- Визначає об'єкти кіберзахисту.
- Формує кібербезпеку.
- Формує національну систему національну реагування (CERT-UA).
- Встановлює вимоги до аудиту безпеки систем.

Закон про критичну інфраструктуру (KI)

- Категоризація об'єктів.
- Створення Реєстру KI.
- Державно-приватна взаємодія на регіональному регіональному та місцевому рівнях.

Ухвалення Закону № 4336-IX переформатувало підходи до кадрового забезпечення та встановило жорстку відповідальність на місцях.

Нові вимоги до кадрової архітектури (CISO)

Розмежування обов’язків відповідно до Закону 4336-IX та Постанови КМУ №1516

Держоргани (Жорсткі вимоги)

- Обов’язкове створення окремого штатного підрозділу.
- Призначення CISO погоджується з Держспецзв’язком після спецперевірки СБУ.
- CISO не може бути керівником IT-відділу (CDTO) — суворе розділення функцій.

ОМС та Об'єкти критичної інфраструктури (Гнучкість)

- Обов’язково: призначення відповідальної особи, яка виконує функції CISO.
- Окремий підрозділ створюється лише за потреби (аутсорс дозволено).
- Внутрішнє призначення (погодження з Держспецзв’язком не вимагається).

Рекомендація: Навіть без прямої заборони, **функціонально розділяйте IT-розвиток та кібербезпеку.**

Керівник з цифрової трансформації

Керівник з кіберзахисту

Суміщення заборонено (Постанова № 1516)

Фокус: Впровадження нових технологий, доступність сервісів, швидкість цифровізації.

Фокус: Жорсткий аудит ризиків, захист інфраструктури, гальмування небезпечних впроваджень.

Розділення усуває внутрішний конфлікт інтересів між швидкістю цифрового розвитку та безпекою громади.

2026 році головний акцент робиться на превентивності.

Органам місцевого самоврядування рекомендується не чекати перевірок, а самостійно впроваджувати стандарти (наприклад, ISO/IEC 27001), оскільки відповідальність за «впавшу» цифрову інфраструктуру міста тепер повністю лежить на місцевому керівництві.

Уніфікований стандарт кіберзахисту (Постанова № 373)

	Відкрита інформація	Обмежений доступ (службова/конфіденційна)
Доступність	Безперешкодний доступ	Лише ідентифікованим та авторизованим особам
Модифікація	Дозволено користувачам з правами	Жорстке розмежування прав, блокування неавторизованих спроб
Логування	Реєстрація при внесенні змін	Реєстрація кожного факту входу та будь-яких дій з файлами
КЕП (Підписи)	Згідно із Законом про довірчі послуги	Спеціальний затверджений порядок

Ризик-орієнтований підхід: постійне оцінювання, мінімізація та моніторинг загроз за методикою Держспецзв'язку.

Захист об'єктів критичної інфраструктури (ОКІ) громади

Крок 1: Ідентифікація

ОМС разом із секторальними органами визначають ОКІ та подають дані до Реєстру.

Крок 2: Планування

Розробка та щорічне оновлення Плану кіберзахисту (за каталогом Держспецзв’язку). Узгодження з паспортом безпеки об’єкта.

Крок 3: Захист

Впровадження базових заходів. Безперервний моніторинг мереж (24/7). Управління ризиками кібербезпеки.

Крок 4: Взаємодія

Негайне інформування Уповноваженого органу про інциденти.

Звітування про зміни режиму функціонування чи форми власності.

Екосистема безпеки: Хто за що відповідає?

Держспецзв'язок (Регулятор)

Формує політику, встановлює стандарти, проводить аудит та здійснює нормативний контроль.

ДЦКЗ / CERT-UA (Реагування)

Моніторинг мереж, реєстрація інцидентів, практична допомога ОМС у відновленні (Не є правоохоронним органом).

Служба безпеки України (Контррозвідка)

Кримінальне розслідування цілеспрямованих атак на державні ресурси та ОКІ, протидія кібершпигунству.

Національна поліція (Кіберполіція)

Боротьба з кіберзлочинністю загального характеру, розслідування фінансового шахрайства.

Обов’язок звітування та відповідальність

Згідно з **Законом 4336-IX**, ненадання або несвоєчасне надання повідомлень про кіберінциденти **тягне за собою адміністративну відповідальність для керівництва.**

Що повідомляти?
Будь-які значні кіберінциденти, аномалії в мережі, спроби втручання в системи ОМС чи ОКІ.

Кому повідомляти?
CERT-UA (Урядова команда реагування на комп'ютерні надзвичайні події).

Розмежування наслідків:
Адміністративна санкція — за приховування інциденту чи запізнення зі звітом.
Кримінальна відповідальність (ст. 361-363[1] ККУ) стосується безпосередньо кіберзлочинців, а не жертв атаки.

Краще своєчасно повідомити про підозру, ніж приховати реальний злам.

Протокол обміну інформацією (TLP)

Як маркувати дані про інциденти, щоб контролювати їх поширення (Стандарт FIRST/ENISA)

TLP:RED (Обмежено)

Лише для визначених осіб. Інформація не може поширюватися поза межами конкретної зустрічі чи вузької групи фахівців.

TLP:AMBER (Внутрішнє користування)

Обмежене поширення. Тільки для учасників вашої організації (ОМС) на основі принципу "необхідно знати".

TLP:GREEN (Для спільноти)

Можна поширювати серед партнерів, інших ОМС та фахівців сектору, але заборонено публікувати у відкритому доступі.

TLP:CLEAR (Публічно)

Без обмежень. Інформація може вільно публікуватися публічно та передаватися ЗМІ.

Алгоритм екстреного реагування

Крок 1: Виявлення та Ізоляція

Фіксація аномалії. Відключення уражених пристроїв від локальної мережі (УВАГА: не вимикайте живлення, щоб зберегти системні логи для розслідування).

Крок 2: Повідомлення

Негайне інформування відповідальної особи (CISO) громади. Подання первинного звіту до CERT-UA (soc@cert.gov.ua).

Крок 3: Локалізація та Аналіз

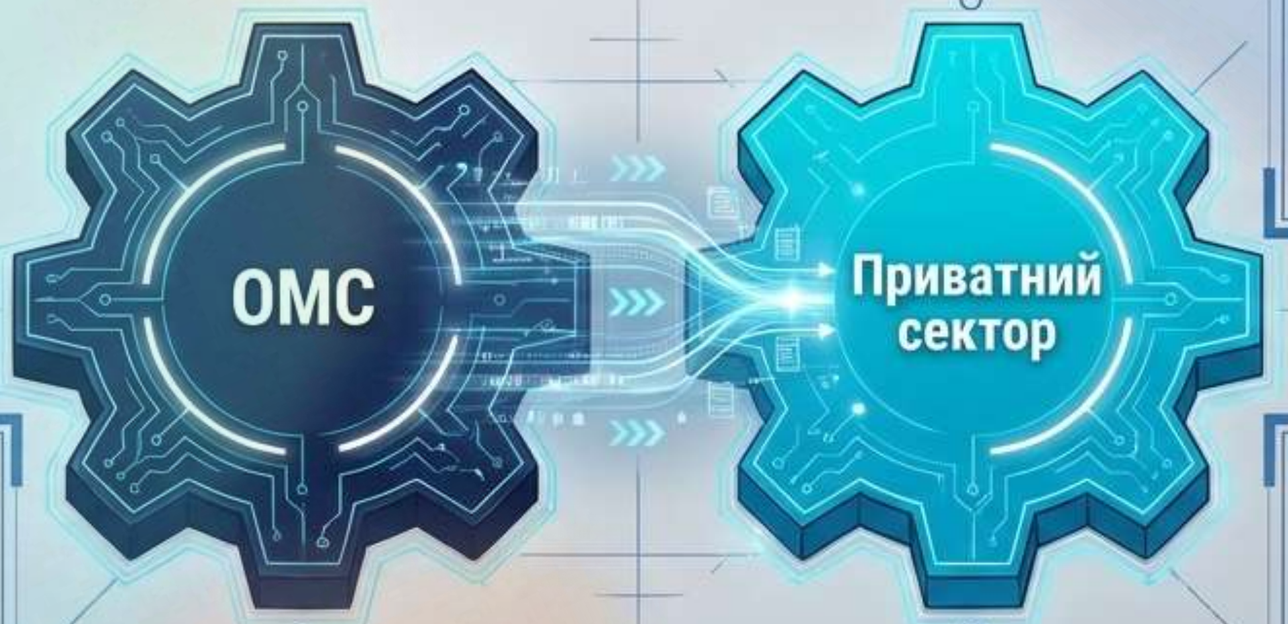
Співпраця з фахівцями CERT-UA або залученими приватними командами для зупинки поширення загрози.

Крок 4: Відновлення

Повернення систем до роботи шляхом розгортання захищених резервних копій. Усунення вразливостей перед повторним підключенням до мережі.

Державно-приватне партнерство у кіберзахисті

Закон 4336-IX стимулює аутсорсинг. ОМС не зобов'язані будувати власні дороговартісні кібер-лабораторії.



Залучення приватних команд реагування

ОМС мають право наймати акредитовані приватні SOC-команди для цілодобового моніторингу та реагування на інциденти.

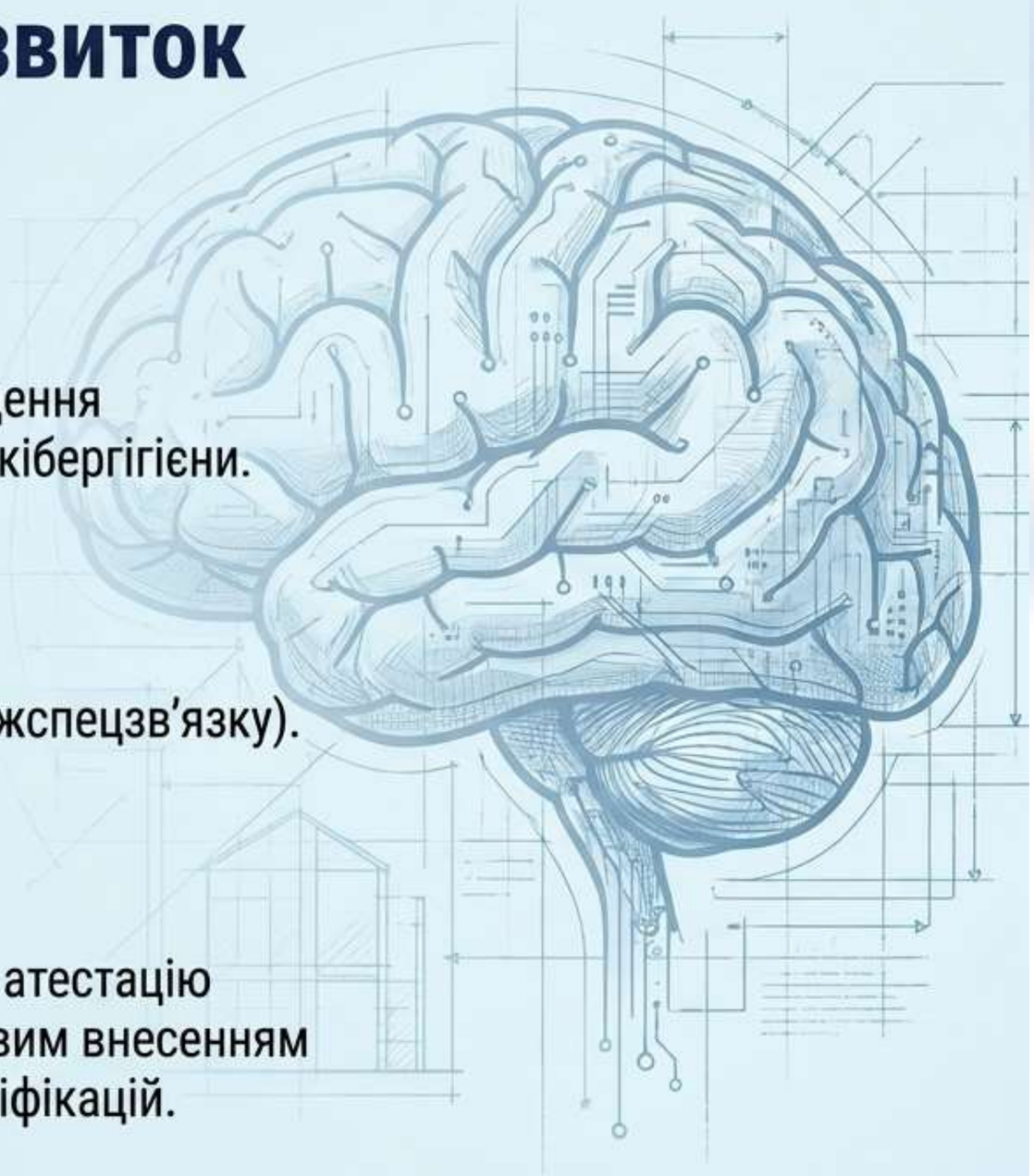
Платформи обміну даними

Спільна участь державних органів та бізнесу в національній системі обміну індикаторами кіберзагроз.

Зовнішній аудит безпеки

Залучення незалежних аудиторів для перевірки стійкості систем та виявлення вразливостей.

Навчання та безперервний розвиток компетенцій



Законодавча вимога

Закон 4336-IX вимагає від ОМС та держорганів проведення регулярних інструктажів та систематичних тренінгів з кібергігієни.

Цільова аудиторія

- Депутати місцевих рад та керівництво ОМС.
- Системні адміністратори (технічні навчання від Держспецзв’язку).
- Рядові службовці (базова кібергігієна).

Обов'язкова сертифікація

Керівники з кіберзахисту (CISO) проходять спеціальну атестацію в акредитованих кваліфікаційних центрах з обов'язковим внесенням до Державного реєстру Національного агентства кваліфікацій.

Синтез: 5 кроків до кіберстійкості громади

1. Лідерство

Призначити відповідального Керівника з кіберзахисту (CISO) та відокремити його функції від IT-відділу.

2. Аудит

Провести інвентаризацію систем, визначити ОКІ громади та внести їх до Реєстру.

3. Гігієна

Впровадити та контролювати суворі правила цифрової безпеки для 100% працівників ОМС.

4. Моніторинг

Забезпечити цілодобовий захист мереж, ізольоване резервне копіювання та суворий контроль віддаленого доступу.

5. Взаємодія

Налагодити постійний канал зв'язку з CERT-UA, інтегрувати приватні SOC-команди та негайно звітувати про інциденти.

Цикл впровадження (5 стадій)

Згідно з постановою КМУ від 2025 року, процес впровадження систем захисту в держсекторі тепер має чіткий цикл

1. **Ініціювання:** Визначення бюджету та потреби.
2. **Проєктування:** Розробка технічного завдання на систему захисту.
3. **Створення та впровадження:** Закупівля обладнання та налаштування ПЗ.
4. **Експлуатація:** Постійний моніторинг (24/7) та реагування на дрібні інциденти.
5. **Аудит та оновлення:** Періодична перевірка відповідності стандартам (наприклад, ISO/IEC 27001).

Дорожня карта керівника ОМС

Як звернутися до служби підтримки кібербезпеки

Служба підтримки - це швидкий доступ до фахової допомоги у сфері кібербезпеки

Заповнити звернення на сайті Супермаркет рішень для громад

через кнопку ‹‹Звернутися до служби підтримки›› на сайті supersolution.net.ua

Отримати зворотній зв’язок

АСОЦІАЦІЯ МАЛИХ МІСТ УКРАЇНИ

СУПЕРМАРКЕТ РІШЕНЬ для громад

ICWR INSTITUTE OF CYBER WARFARE RESEARCH

CyberLab Комп'ютерна криміналістика

Служба підтримки

+38 (096) 380 17 39, +38 (093) 477 50 67