# ДЕПАРТАМЕНТ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

## КІБЕР-АТАКИ ТА ІНТЕРНЕТ-ШАХРАЙСТВО

# СТРУКТУРА УКРАЇНСЬКОЇ КІБЕРПОЛІЦІЇ

## ДЕПАРТАМЕНТ КІБЕРПОЛІЦІЇ

**Відділ кібербезпеки, відділ моніторингу, відділ обробки та аналізу, відділ електронної комерції, відділ платіжних систем, відділ нелегального контенту, національний контактний пункт, управління ІТ та програмування (УІТП)**

1 2 3 4 5 6 7 8

Західне УІТП

Південне УІТП

Східне УІТП

**8 міжрегіональних управлінь, що безпосередньо підпорядковуються центральному апарату**

**3 міжрегіональних управління висококваліфікованих ІТ спеціалістів, які безпосередньо підпорядковуються центральному апарату**

# НАПРЯМКИ РОБОТИ

## ІНФОРМАЦІЙНА БЕЗПЕКА

- розповсюдження шкідливого програмного забезпечення

- несанкціоноване втручання у комп'ютери та їх системи


- атаки DOS, спам, кібершантаж
- крадіжка особистої інформації

- незаконна торгівля міжнародним голосовим трафіком

## НЕЛЕГАЛЬНИЙ КОНТЕНТ ТА ПОРУШЕННЯ ПРАВ ВЛАСНОСТІ


- дитяча порнографія та порнографічна продукція

- розповсюдження та продаж заборонених матеріалів

- піратство медіа-контенту

- піратське програмне забезпечення

- кардшарінг

## ОНЛАЙН ШАХРАЙСТВА ТА ФІНАНСОВІ ЗЛОЧИНИ

- фішинг, кардінг, скімінг, кеш-трепінг

- інтернет-шахрайство

- шахрайство в банківських / платіжних системах

- незаконна торгівля

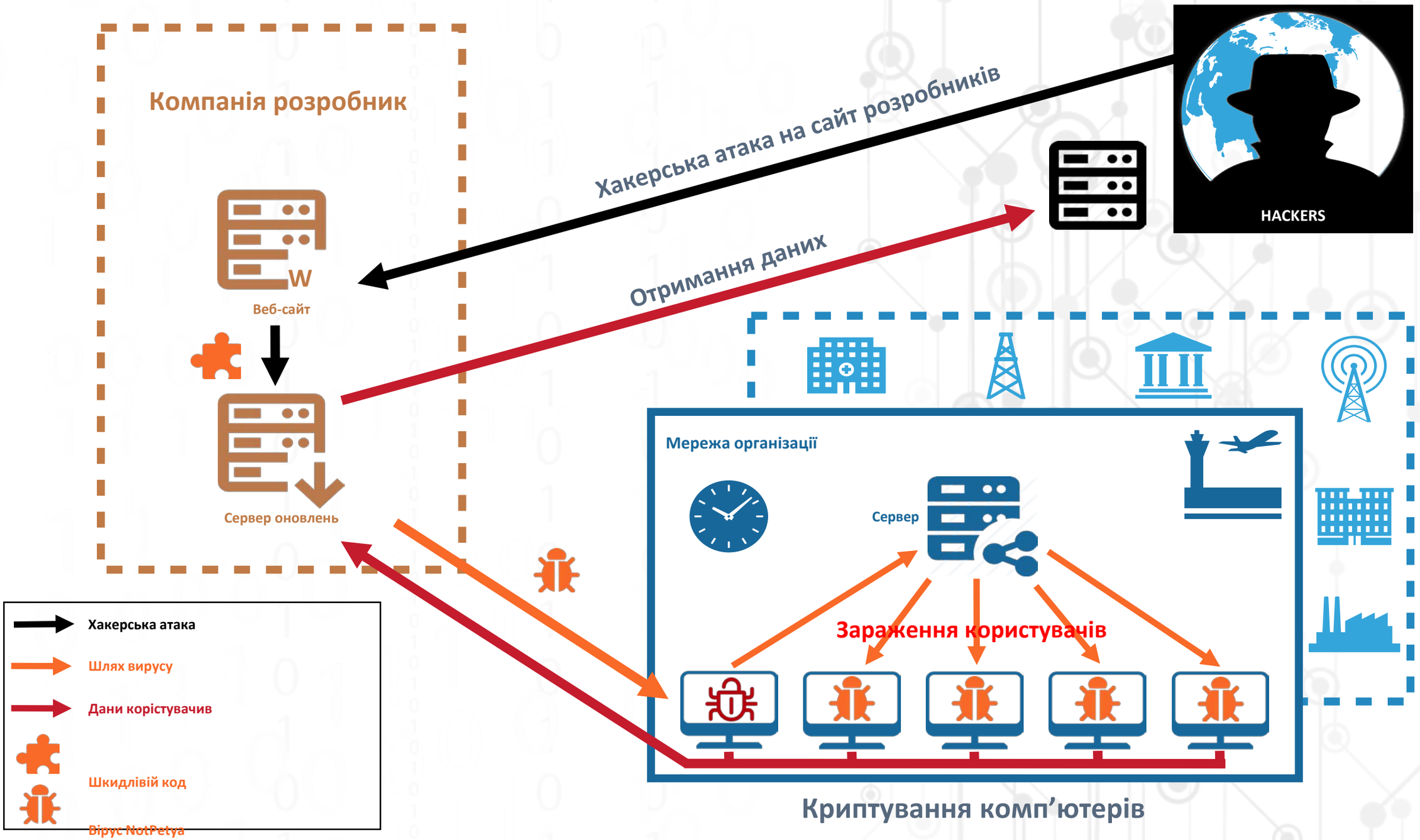
КІБЕРНЕТИЧНІ АТАКИ:
# РОЗПОВСЮДЖЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

програмне забезпечення, спеціально розроблене для перешкоджання роботі комп'ютера, збирання конфіденційної інформації або отримання доступу до комп'ютерних систем (мереж).

Може проявлятися у вигляді виконуваного коду, скриптів, активного контенту, чи іншого програмного забезпечення.

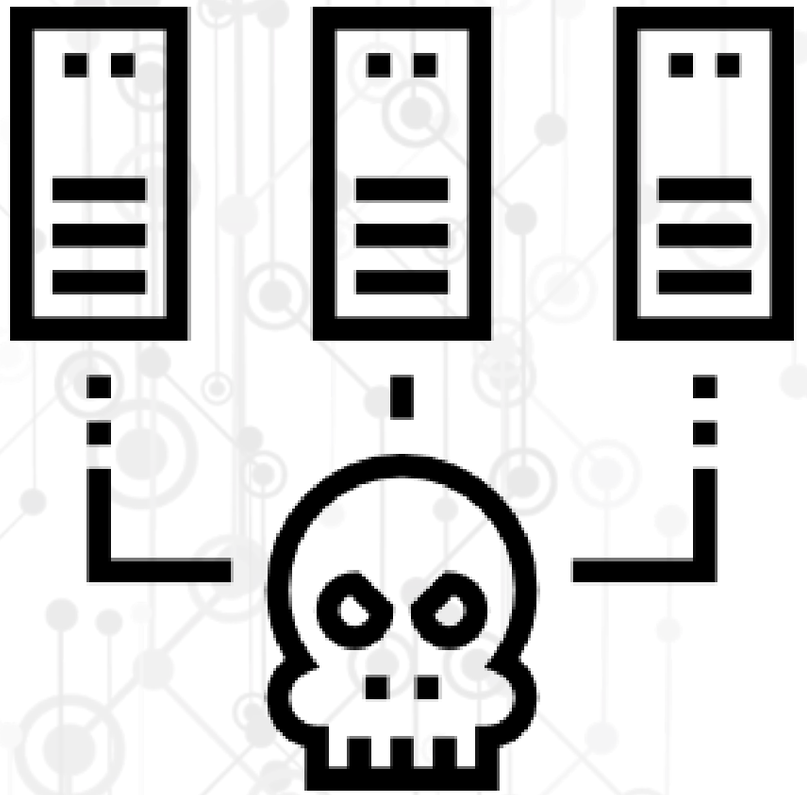
Шкідливий — це загальний термін, який використовується для позначення різних форм ворожого або нелегітимного програмного забезпечення.

# ВІРУСНА АТАКА «NOTPETYA»

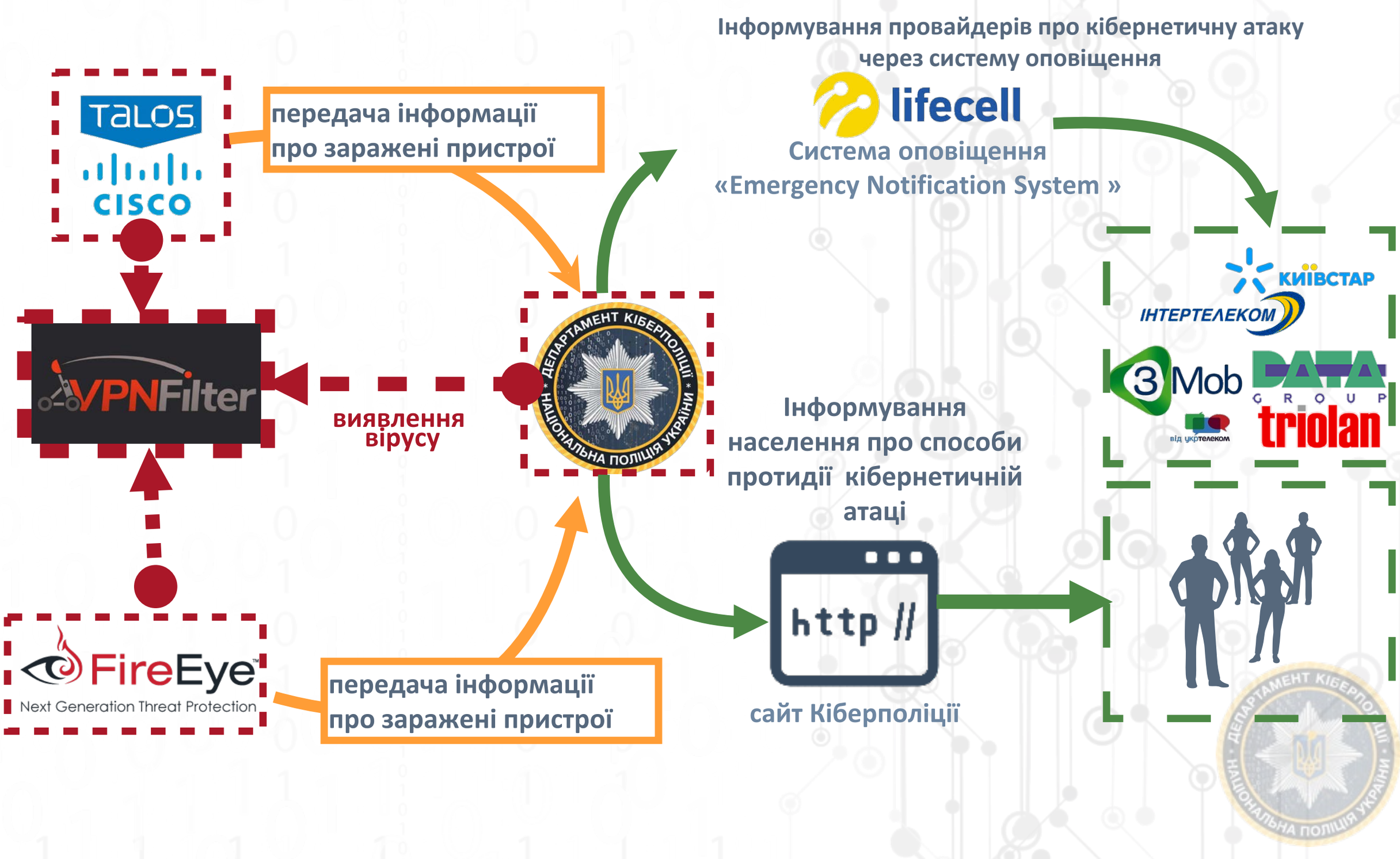


# КІБЕРНЕТИЧНІ АТАКИ:
# **НЕСАНКЦІОНОВАНЕ ВТРУЧАННЯ У КОМП'ЮТЕРИ ТА ЇХ СИСТЕМИ**

проникнення до електронно-обчислюваних машин (ЕОМ), їх систем чи мереж і вчинення дій, які змінюють режим роботи машини, її системи чи комп'ютерної мережі, або ж повністю чи частково припиняють їх роботу, без дозволу (згоди) відповідного власника або уповноважених ним осіб, а так само вплив на роботу ЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машини.



# ВИЯВЛЕННЯ АТАКИ «VPNFILTER»



# КІБЕРНЕТИЧНІ АТАКИ:
# АТАКИ DOS, СПАМ, КІБЕРШАНТАЖ

**атака DOS** - напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.


**спам** - масове розсилання кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів.


**кібершантаж** - зловмисники шантажують жертв з використанням попередньо зібраної інформації, пов’язаної з профілями жертв в Інтернеті, зокрема приватної електронної кореспонденції, облікових записів у соціальних мережах, сімейних стосунків або місць навчання

# РЕКОМЕНДАЦІЇ:

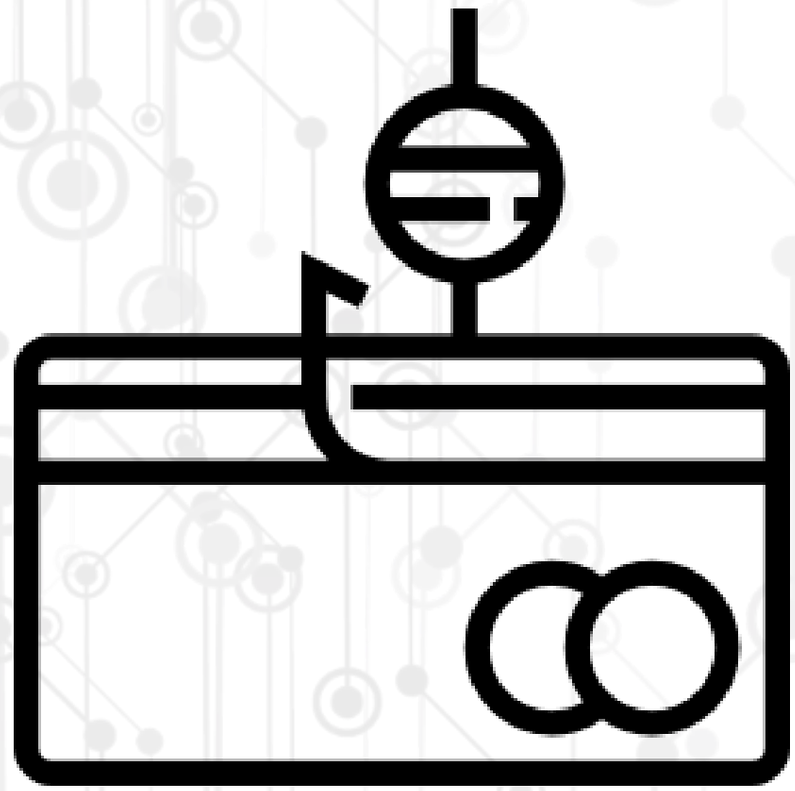
- **Використовувати тільки ліцензійне програмне забезпечення**
- **Використовувати антивірусні програмні засоби**
- **Постійно слідкувати та оновлювати програмні продукти, особливо операційні системи**


- **Не завантажувати, а тим паче не відкривати додатки до листів, які отримані з недовіреної адреси**
- **Дослухатися до рекомендацій спеціалістів з IT-безпеки.**

# ІНТЕРНЕТ-ШАХРАЙСТВО:
# **ФІШИНГ, КАРДІНГ, СКІМІНГ**

фішинг - шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо.

кардінг - рід шахрайства, при якому проводиться операція з використанням банківської картки або її реквізитів, яка не ініційована або не підтверджена її власником.



скімінг - шахрайство шляхом зчитування даних з допомогою спеціального обладнання, яке фіксує дані магнітної стрічки банківської картки і її пін-код.

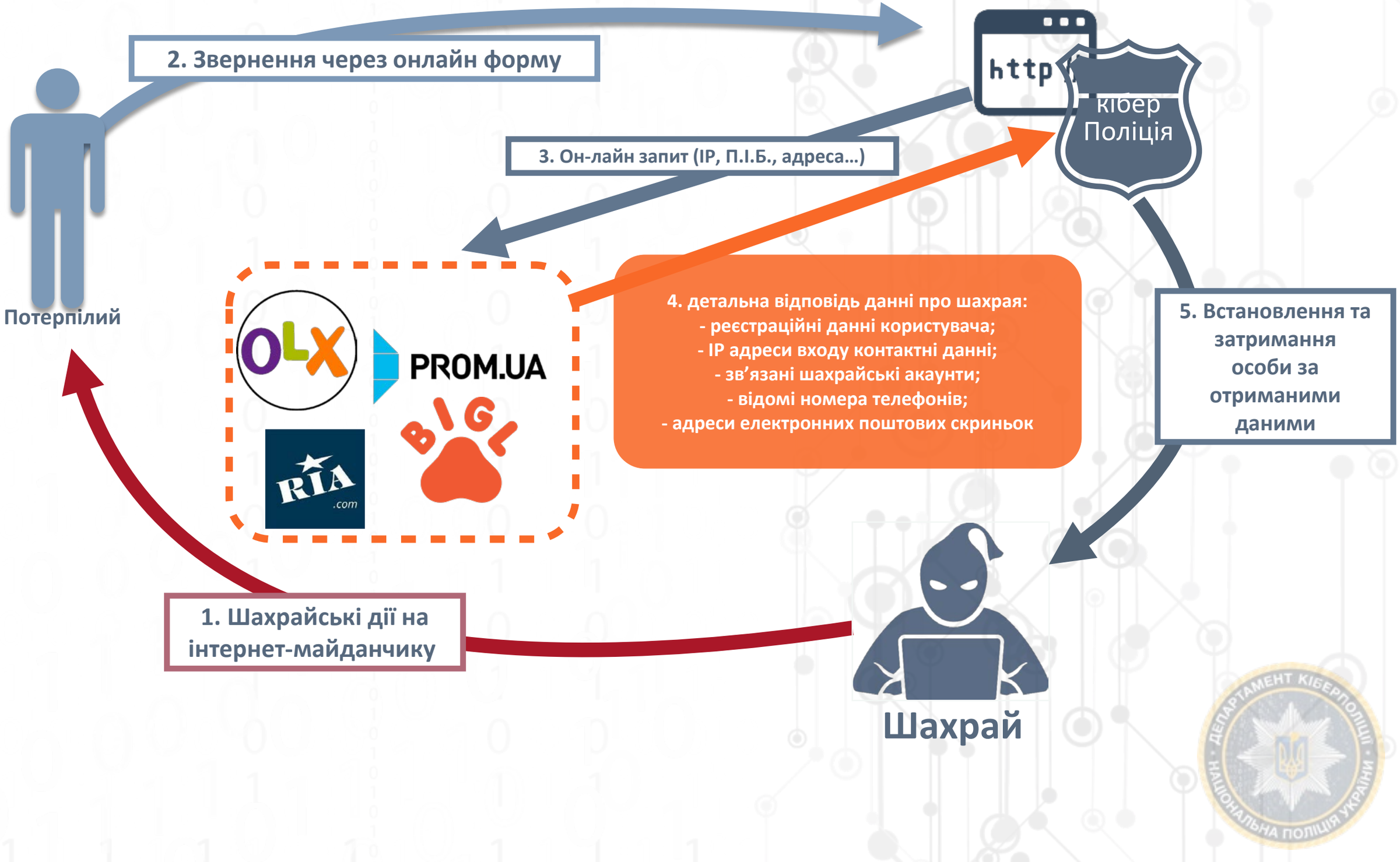
# ІНТЕРНЕТ-ШАХРАЙСТВО:
# **ШАХРАЙСТВО В БАНКІВСЬКИХ / ПЛАТІЖНИХ СИСТЕМАХ**

- доступ до рахунків із застосуванням кліент-банківського програмного забезпечення;

- доступ до рахунків із застосуванням результатів фішингових атак;

- доступ до рахунків із застосуванням результатів скіминг;

# АЛГОРИТМ РОЗСЛІДУВАННЯ



# РЕКОМЕНДАЦІЇ:

- **Не переходити за посиланнями для оплати на неперевірених ресурсах**
- **Використовувати складні паролі (мінімум 8 символів у комбінації великих та малих літер, цифр та символів)**
- **Завжди перевіряти стан банкоматів, з яких знімаються кошти**
- **Уважно відноситися до збереження своєї інформації для авторизації на сервісах**
- **Не проводити фінансові операції із використанням відкритих мереж Wi-Fi**

# ДЯКУЮ ЗА УВАГУ!

- www.cyberpolice.gov.ua
- facebook.com/cyberpoliceua
- twitter.com/cyberpoliceua